TRABAJO FIN DE MÁSTER:

AUDITORÍA DE adAS

INFORME DE AUDITORÍA

REALIZADO POR:

ALCAY BAILO, VÍCTOR

10 de Enero de 2014

ÍNDICE

INTRODUCCIÓN

Este documento trata de dar una visión general del sistema Single-Sign-On que nos ocupa, AdAS y su funcionamiento junto con la información del entorno del que disponemos para realizar las pruebas. Asimismo se incluye un catálogo de las vulnerabilidades que puede tener un sistema de estas características centrándonos de nuevo en el sistema AdAS. Concretamente en sus aplicaciones Web y los protocolos utilizados. A la par de las posibles vulnerabilidades, se incorporan las pruebas a realizar para cada tipo de vulnerabilidad.

Además se incluirán los resultados de las pruebas realizadas y un análisis de las mismas y de las políticas establecidas.

Con toda esta información estaremos en disposición de realizar el resumen ejecutivo donde se detallarán una visión general de la metodología empleada, unas conclusiones y recomendaciones para finalmente indicar las fortalezas y debilidades detectadas.

Finalmente se detallará la metodología empleada donde se concretarán todas las fases de la auditoría, herramientas y técnicas empleadas, etc.

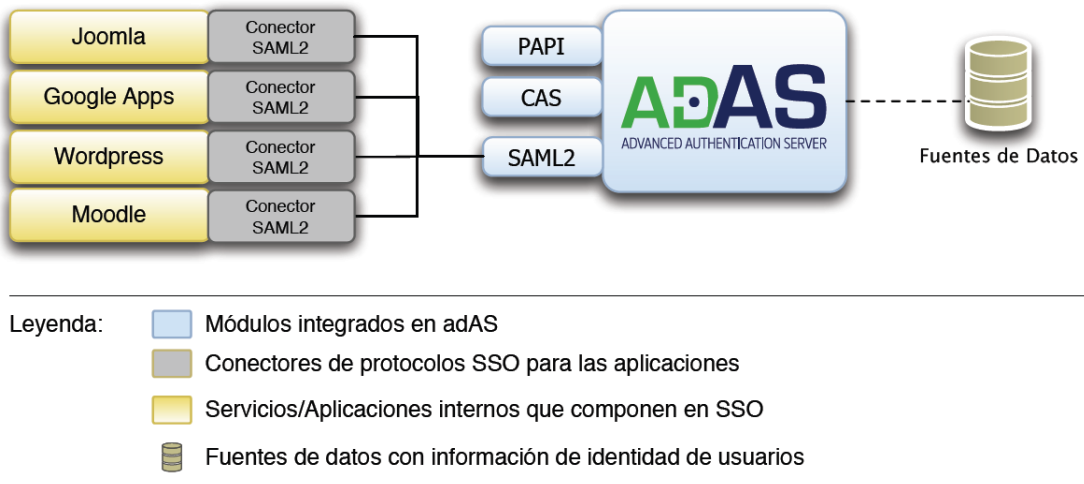
1. INFORMACIÓN PREVIA

1.1. Aplicación a Auditar

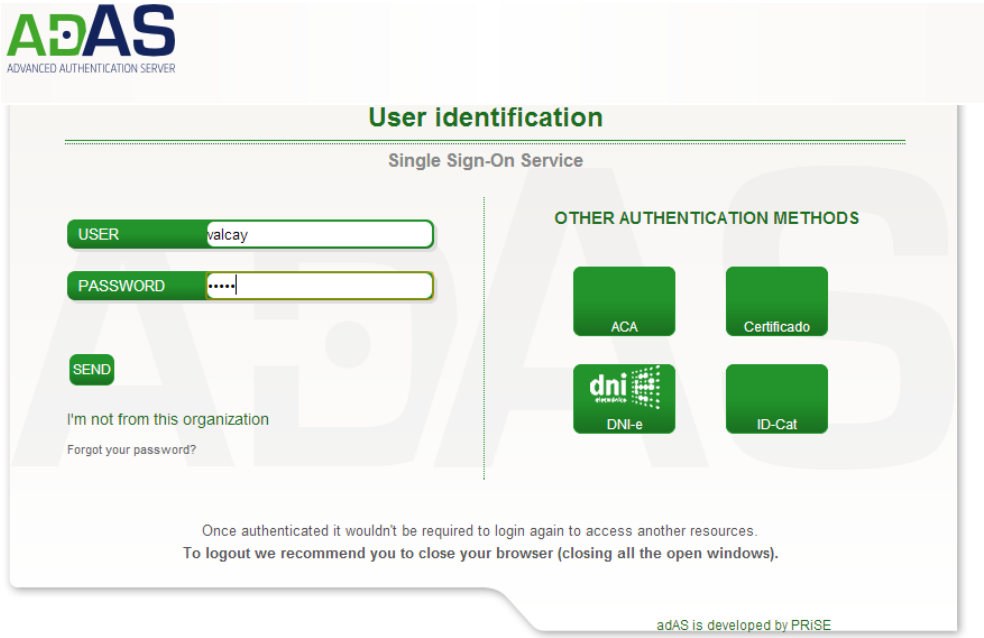
AdAS se trata de un sistema SSO (Single Sign On), es decir, se trata de un procedimiento de autentificación que nos permite acceder a varios sistemas con una única instancia de autenticación. Presentado los credenciales una vez podemos acceder a varios entornos mientras que no cerremos la sesión.

Concretamente a través de este SSO nos podemos validar en 4 entornos diferentes, Google Apps, Joomla, WordPress y Moodle.

AdAS es multiprotocolo, lo que quiere decir que se han utilizado varios protocolos en su arquitectura. Éstos son SAML2, PAPI y CAS, quedando dicha arquitectura de la siguiente manera.



Desde cada uno de los 4 entornos web podemos autenticarnos en el SSO donde nos aparece este formulario donde introduciremos nuestros credenciales o a través de otros métodos como como por ejemplo el DNI Electrónico, Certificado de Red Abogacía o Certificado digital.



1.2. Entorno de Auditoría

Es un entorno basado en 3 capas (datos, modelo, presentación). Es decir, un SGBD modelo de desarrollo en un lenguaje interpretado a ejecutar dentro del servidor web y el propio servidor web.

Las aplicaciones que se ejecutan en estos entornos no orientados a conexión (el protocolo HTTP no mantiene persistencia entre conexiones) deben mantener por sí mismas la persistencia y por lo general resolverán todas las peticiones de manera síncrona bajo la demanda de los clientes.

1.2.1. Sistema Operativo

SS.OO	Linux	3.2.34*55.46.amzn1.x86_64
Distribución	Amazon5Linux5AMI	Release52013.03
Hostname	petasso.prise.es	54.246.89.131
Uname -a	Linux5petasso.prise.es53.2.34*55.46.amzn1.x86_645#15SMP5 Tue5Nov520510:06:155UTC520125x86_645x86_645x86_645GNU/ Linux	

1.2.2. Servicios

SGBD	mysqld5 Ver5 5.5.315for5Linux5on5 x86_645 (MySQL5Community5 Server5(GPL)) Copyright5(c)52000,52013,5Oracle5and/or5its5affiliates.5 All5rights5reserved.
Servidor Web	Server version: Apache/2.2.245(Unix) Server built: Mar 23 2013 00:07:19 Server's Module Magic Number: 20051115:31 Server loaded: APR 1.4.6, APR*Util51.4.1

	Compiled5using: APR 1.4.6, APR*Util 1.4.1 Architecture: 64-bit Server MPM: Prefork threaded:no forked: yes (variable process count) Server compiled with.... -D APACHE_MPM_DIR="server/mpm/prefork" -D APR_HAS_SENDFILE -D APR_HAS_MMAP -D APR_HAVE_IPV65(IPv4*mapped5addresses5enabled) -D APR_USE_SYSVSEM_SERIALIZE -D APR_USE_PTHREAD_SERIALIZE -D SINGLE_LISTEN_UNSERIALIZED_ACCEPT -D APR_HAS_OTHER_CHILD -D AP_HAVE_RELIABLE_PIPED_LOGS -D DYNAMIC_MODULE_LIMIT=128 -D HTTPD_ROOT="/etc/httpd" -D SUEXEC_BIN="/usr/sbin/suexec" -D DEFAULT_PIDLOG="run/httpd.pid" -D DEFAULT_SCOREBOARD="logs/apache_runtime_status" -D DEFAULT_LOCKFILE="logs/accept.lock" -D DEFAULT_ERRORLOG="logs/error_log" -D AP_TYPES_CONFIG_FILE="conf/mime.types" -D SERVER_CONFIG_FILE="conf/httpd.conf"
PHP	PHP5Version55.3.23 Más5información:5http://petasso.prise.es/info.php

1.2.3. VirtualHosts

Los virtualhosts ofrecidos por el servidor web son.
VirtualHost5configuration:
wildcard5NameVirtualHosts5and5_default_5servers:
*:443 idp.petasso.prise.es
*:443 links.petasso.prise.es
*:80 is a NameVirtualHost
default5server5petasso.prise.es
port 80 namevhost petasso.prise.es
alias ec2-54-246-89-131.eu-west-1.compute.amazonaws.com
port 80 namevhost idp.petasso.prise.es
port 80 namevhost links.petasso.prise.es
port 80 namevhost wordpress.petasso.prise.es

1.3. Catálogo de Vulnerabilidades

Una vez descrita la aplicación y el entorno donde se va a realizar la auditoría, vamos a establecer un conjunto de posibles vulnerabilidades que podrían afectar a la aplicación, teniendo en cuenta las tecnologías utilizadas.

1.3.1. Aplicaciones Web

En primer lugar se van a clasificar las vulnerabilidades según el tipo del que se traten y dependiendo de las aplicaciones web afectadas.

1.3.1.1. Ataques de inyección de scripts

Los ataques de inyección de scripts consisten en lograr inyectar en el contexto de un dominio VBScript o simplemente HTML, con la finalidad de engañar al usuario o suplantarle para realizar una acción no deseada por éste.

1.3.1.1.1. Cross Site Scripting (XSS)

Toda petición enviada al servidor va a ser procesada por éste, y, en función de cómo la interprete, será o no factible un ataque mediante XSS. Un entorno web es vulnerable a XSS cuando aquello que nosotros enviamos al se ve posteriormente mostrado en la página de respuesta. Esto es, cuando escribimos un comentario en una página y podemos leer posteriormente nuestro mensaje, modificamos nuestro perfil de usuario y el resto de usuarios puede verlo o realizamos una búsqueda y se nos muestra un mensaje: "No se han encontrado resultados para <texto>", se está incluyendo dentro de la página el mismo texto que nosotros hemos introducido.

Para detectar si cada entorno es vulnerable o no a XSS, se realizarán intentos de ataques aprovechando las vulnerabilidades de las versiones del entorno web o de alguno de sus componentes.

A continuación se detallan una serie de vulnerabilidades para cada uno de los cuatro entornos web.

Joomla

CVE-2013-3267			
Fecha Reporte	17/04/2013	**Fecha Solución**	24/04/2013
Descripción	Vulnerabilidad por filtrado inadecuado del plugin highliter permite a atacantes remotos inyectar scripts web o HTML a través de vectores no especificados.		
Versiones Afectadas	2.5.10 y anteriores dentro de las 2.5.x 3.0.4 y anteriores dentro de las 3.0.x		
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized modification		
Solución	Actualizar a las versiones 2.5.10, *3.1.0 o 3.0.4.		

CVE-2013-3059	
Fecha Reporte	26/02/2013
Descripción	Vulnerabilidad del plugin Voiting permite a atacantes remotos inyectar scripts web o HTML a través de vectores no especificados.
Versiones	2.5.9 y anteriores dentro de las 2.5.x

Afectadas	3.0.2 y anteriores dentro de las 3.0.x
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type: Allows unauthorized modification
Solución	Actualizar a las versiones 2.5.10, *3.1.0 o 3.0.4.

Google Apps

CVE-2013-4204	
Fecha Reporte	05/08/2013
Descripción	Se encontró un fallo en GWTTestCase para aplicaciones que dependen del módulo JUnit
Versiones Afectadas	Anteriores a 2.5.1
Impacto	Prioridad: Media Severidad: Media
Solución	Instalar patch https://code.google.com/p/google-web-toolkit/source/detail?r=11385

CVE-2012-5920			
Fecha Reporte	20/11/2012	**Fecha Solución**	05/08/2013
Descripción	Detectado cuando se usa GWT en JBoss Operations Network y posiblemente en otros productos, permite a atacantes remotos inyectar scripts web o HTML vía vectores no especificados. Existe por un incompleto fix de la vulnerabilidad CVE-2012-4563.		
Versiones Afectadas	GWT 2.4.0 y 2.5.0 JBoss Operations Network 3.1.1		
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized modification		
Solución	Actualizar GWT a la Versión 2.5.1 y JBoss Operations Network a la 3.1.2		

CVE-2012-4563	
Fecha Reporte	20/11/2012
Descripción	Permite a atacantes remotos inyectar scripts web o HTML vía vectores no especificados.
Versiones	GWT 2.4.0 beta

Afectadas	
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized modification
Solución	Actualizar GWT a la Versión 2.5.1

WordPress

CVE-2011-4899	
Fecha Reporte	01/30/2012
Descripción	En la instalación del componente wp-admin/setup-config.php para Wordpress no es obligatorio especificar el servicio MySql apropiado. Lo cual permitiría a atacantes remotos configurar una base de datos arbitraria a través de parámetros de dbhost y enviar inyección de código estático y ataques XSS en solicitudes HTTP o query de MySql.
Versiones Afectadas	WordPress 3.3.1 y anteriores
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar WordPress a version posterior a 3.3.1

CVE-2012-0287	
Fecha Reporte	01/06/2012
Descripción	Vulnerabilidad XSS en wp-comments-post.php in WordPress cuando se utiliza Internet Explorer permite a atacantes remotos inyectar script web arbitrario o HTML a través de una cadena query en una operación POST que no es correctamente manejada por la característica "Duplicate comment detected".
Versiones Afectadas	WordPress 3.3.x anteriores a 3.3.1
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:2.6 (LOW) (AV:N/AC:H/Au:N/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 4.9

	CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: High Authentication: Not required to exploit Impact Type:Allows unauthorized modification
Solución	Actualizar WordPress a las versiones 3.3.1 o posteriores.

CVE-2013-5739	
Fecha Reporte	12/09/2013
Descripción	La configuración por defecto de WordPress no previene subidas de archivos .swf y .exe, lo cual podría facilitar a usuarios autenticados atacar a través de un fichero encubierto. Utilizando la función get_allowed_mime_types en wp-includes/functions.php.
Versiones Afectadas	Anteriores a 3.6.1.
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:3.5 (LOW) (AV:N/AC:M/Au:S/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 6.8 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Required to exploit Impact Type:Allows unauthorized modification
Solución	Instalar version 3.6.1

Moodle

CVE-2013-4942	
Fecha Reporte	29/07/2013
Descripción	Vulnerabilidad en flashuploader.swf en el component Uploader in Yahoo! YUI utilizado en Moodle y otros productos. Permite a atacantes remotos inyectar scripts web o HTML a través de un string encubierto en una URL.
Versiones Afectadas	YUI de la 3.5.0 a la 3.9.1 Moodle de la 2.1.10 a la 2.2.x antes de la 2.2.11, 2.3.x a la 2.3.8 antes de la 2.4.x y de la 2.4.5 a la 2.5.x antes de la 2.5.1.
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized modification

Solución	Actualizar a las versiones 2.2.11, 2.3.8, 2.4.5 o 2.5.1

CVE-2013-4939	
Fecha Reporte	29/07/2013
Descripción	Vulnerabilidad en io.swf del componente IO YUI permite a atacantes remotos inyectar scripts web o HTML.
Versiones Afectadas	YUI de 3.0.0 a 3.9.1 Moodle 2.1.10, 2.2.x hasta la 2.2.11, 2.3.x hasta la 2.3.8, 2.4.x hasta la 2.4.5, 2.5.x hasta la 2.5.1.
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized modification
Solución	Actualizar la librería YUI a la versión 3.9.1 o superior y/o actualizar Moodle a las versiones 2.2.11, 2.3.8, 2.4.5 o 2.5.1

CVE-2013-4341	
Fecha Reporte	16/09/2013
Descripción	Múltiples vulnerabilidades XSS en algunas versiones de Moodle permitirían a atacantes remotos inyectar scripts web o HTML.
Versiones Afectadas	2.2.11, 2.3.x hasta la 2.3.9, 2.4.x hasta la 2.4.6, 2.5.x hasta la 2.5.2.
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized modification
Solución	Actualizar a las versiones 2.2.11, 2.3.9, 2.4.6 o 2.5.2

1.3.1.1.2. Cross Site Request Forgery (CSRF)

El CSRF es una técnica con la cual vamos a lograr que el usuario realice acciones no deseadas en dominios remotos. Se basa en la idea de aprovechar la persistencia de sesiones entre las pestañas de un navegador.

Del mismo modo que para XSS, para realizar las pruebas de intrusión se intentarán realizar ataques CSRF sobre los entornos web, aprovechando las vulnerabilidades que podría tener dependiendo de su versión y la de sus componentes.

Éstas son algunas de las vulnerabilidades CSRF que podrían tener los entornos web de nuestro sistema SSO.

Joomla

CVE-2009-1280	
Fecha Reporte	04/09/2009
Descripción	Múltiples vulnerabilidades CSRF en algunas versiones de Joomla permitirían a atacantes remotos inyectar scripts web o HTML a través de vectores desconocidos.
Versiones Afectadas	1.5.x hasta la 1.5.9
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar a la versión 1.5.9

CVE-2007-6642	
Fecha Reporte	04/01/2008
Descripción	Múltiples vulnerabilidades CSRF en algunas versiones de Joomla permitirían a atacantes añadir un Super Admin , subir una extensión php con código malicioso y modificar la configuración como administradores a través de vectores no especificados.
Versiones Afectadas	Versiones anteriores a la 1.5 RC4
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar a la versión 1.5.9

Wordpress

CVE-2012-1936	
Fecha Reporte	05/03/2012
Descripción	La función wp_create_nonce en wp-includes/pluggable.php de WordPress asocial una cuenta de usuario con una sesión de usuario, lo cual permitiría facilitar a atacantes remotos realizar ataques CSRF en acciones específicas y objetos realizando "sniffing en la red".
Versiones Afectadas	WordPress 3.3.1 y anteriores
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar WordPress a una versión posterior a la 3.3.1

CVE-2013-3491	
Fecha Reporte	16/07/2013
Descripción	Múltiples vulnerabilidades CSRF en el plugin Sharebar 1.2.5 para Wordpress permitiría a atacantes remotos saltarse la autentificación de administradores para solicitudes de añadir o modificar botones, o insertar secuencias XSS.
Versiones Afectadas	Plugin Sharebar 1.2.5
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar Plugin Sharebar

CVE-2013-3479	
Fecha Reporte	09/05/2013
Descripción	Vulnerabilidad en el plugin ShareThis para Wordpress permitiría a atacantes remotos saltarse la autentificación de administradores y modificar la configuración de este plugin.

Versiones Afectadas	ShareThis 7.0.6
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar Plugin ShareThis

Moodle

CVE-2012-6103	
Fecha Reporte	08/01/2013
Descripción	Múltiples vulnerabilidades CSRF en user/messafeselect.php en el sistema de mensajes de Moodle permite a atacantes remotos saltarse la autentificación de usuarios arbitrarios para peticiones que envían mensajes.
Versiones Afectadas	2.2.x hasta la 2.2.7, anteriores a la 2.3.4 y 2.4.x hasta la 2.4.1
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Instalar versiones 2.2.7, 2.3.4 o 2.4.1

CVE-2011-4298	
Fecha Reporte	07/11/2012
Descripción	Múltiples vulnerabilidades CSRF en componentes mod/wiki de Moodle permite a atacantes remotos saltarse la autentificación de usuarios arbitrarios para solicitudes que modifican los datos de la wiki.
Versiones Afectadas	2.0.x gasta la 2.0.5 y 2.1.x hasta la 2.1.2
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 8.6

	CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar a las versiones 2.0.5 o 2.1.2

CVE-2011-4281	
Fecha Reporte	16/07/2012
Descripción	Múltiples vulnerabilidades CSRF que permiten a atacantes remotos saltarse la autentificación de usuarios arbitrarios y poder finalizar una actividad a través de una petición.
Versiones Afectadas	2.0.x hasta la 2.0.2
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar a la versión 2.0.2

1.3.1.1.3. Clickjacking

Las técnicas de clickjacking se basan en engañar a los usuarios para que hagan clic sobre elementos de un sitio web donde ellos nunca lo harían voluntariamente. Esto se consigue superponiendo dos páginas. Una, la principal, con la página donde queremos que realmente los usuarios hagan clic en zonas. Otra, la que sirve de señuelo, superpuesta sobre la anterior y con contenidos que sirvan de aliciente para que el usuario realice los clics en las zonas deseadas.

Esta técnica se basa en el uso de iframes superpuestos. Los iframes son elementos HTML que permiten la inclusión de un recurso externo dentro de nuestra página. Aunque contienen una serie de limitaciones a la hora de acceder a ellos mediante Javascript, son de posible uso para engañar al usuario.

La prueba en este caso sería comprobar si los entornos web de nuestro SSO previenen de renderezación o no, para evitar el uso de iframes superpuestos que podrían engañar al usuario y ejecutar elementos indeseados.

Éstas son algunas de las vulnerabilidades que podrían afectar a nuestro entorno SSO.

Joomla

CVE-2011-2892	
Fecha Reporte	27/07/2011
Descripción	Algunas versiones de Joomla son vulnerables a ataques clickjacking ya que no previenen la renderización de una página dentro de una ventana en un documento HTML "third-party". Esto podría realizarse a través de una página encubierta.
Versiones Afectadas	1.6.x hasta la 1.6.2
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized modification
Solución	Actualizar a la versión 1.6.2 o superior

Wordpress

CVE-2011-3127	
Fecha Reporte	08/10/2011
Descripción	Algunas versiones de WordPress no previenen la renderización para páginas de login o administración dentro de una ventana en un documento HTML "third party", lo cual facilita que atacantes remotos enviar ataques clickjacking a través de sitios web encubiertos.
Versiones Afectadas	3.1.x hasta la 3.1.3 y 3.2 anterior a la Beta 2
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:5.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:N) Impact Subscore: 4.9 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification
Solución	Actualizar a las versiones 3.1.3 o posteriores a la Beta 2 de la 3.2.

1.3.1.2. Ataques de inyección de código

Consiste en realizar un ataque a aplicaciones web siendo su objetivo aprovechar las conexiones a bases de datos desde las aplicaciones web que carecen de protocolos de seguridad y así poder ejecutar comandos directamente en la base de datos.

1.3.1.2.1. SQL inyection

A través de la inyección SQL un atacante remoto podría realizar descubrimiento de información, elevación de privilegios, denegación de servicio y suplantación de usuarios.

La prueba en este tipo de vulnerabilidad sería testear si es posible ejecutar comandos SQL en cada entorno y de este modo aprovechar la posible vulnerabilidad.

A continuación algunas vulnerabilidades encontradas.

WordPress

CVE-2013-5917	
Fecha Reporte	23/08/2013
Descripción	Vulnerabilidad en wp-comments-post.php en el plugin NOSpam PTI para WordPress permite a atacantes remotos ejecutar comandos SQL arbitrarios a través de comment_post_ID.
Versiones Afectadas	NOSpam PTI 2.1
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar NOSpam PTI

CVE-2013-5673	
Fecha Reporte	09/10/2013
Descripción	Vulnerabilidad de testimonial.php en plugin IndiaNIC Testimonial permite a atacantes remotos ejecutar comandos SQL arbitrarios a través del parámetro custom_query en una acción testimonial_add en wp-admin/admin-ajax.php
Versiones Afectadas	IndiaNIC Testimonial 2.2
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar IndiaNIC Testiomonial

CVE-2013-3532	
Fecha Reporte	05/10/2013
Descripción	Vulnerabilidad en settings.php en el plugin Web Dorado Spider Video Player, permite a atacante remotos ejecutar comandos SQL arbitrarios a través del parámetro “theme”
Versiones Afectadas	Web Dorado Spider Video Player 2.1
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar Web Dorado Spider Video Player 2.1

Moodle

CVE-2012-2363	
Fecha Reporte	21/07/2013
Descripción	Vulnerabilidad en calendar/event.php en la implementación del calendario en Moodle permite a atacantes remotos ejecutar comandos SQL a través de un evento de calendario encubierto.
Versiones Afectadas	1.9.x hasta la 1.9.18
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:6.5 (MEDIUM) (AV:N/AC:L/Au:S/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 8.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar a la versión 1.9.18

CVE-2010-1615	
Fecha Reporte	29/04/2013
Descripción	Múltiples vulnerabilidades SQL en moodle permite a atacantes ejecutar comandos SQL a través de vectores relacionados con la función the add_to_log en el módulo mod/wiki/view.php en el módulo wiki o validación de datos en algunos elementos de ventana relacionado con lib/form/selectgroups.php
Versiones Afectadas	1.8.x hasta la 1.8.12 y 1.9.x hasta la 1.9.8

Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar a las versiones 1.8.12 o 1.9.8

CVE-2013-4313	
Fecha Reporte	
Descripción	Algunas versions de Moodle no previenen el uso de caracteres '\0' en cadenas query, lo que permitiría ataques remotos a través de SQL injection contra Microsoft SQL Server a través de cadenas encapsuladas.
Versiones Afectadas	Moodle 2.2.11, 2.3.x anteriores a la 2.3.9, 2.4.x anteriores a la 2.4.6 y 2.5.x anteriores a la 2.5.2.
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar Moodle a las versiones 2.2.11, 2.3.9,2.4.6 o 2.5.2.

1.3.1.2.2. LDAP inyection

Se puede realizar ataques de elevación de privilegios, de salto de protecciones de acceso y de acceso a datos en árboles LDAP mediante el uso de inyecciones de código LDAP. Estas inyecciones de código pueden ser en inyecciones And LDAP Injection, OR LDAP Injection y Blind LDAP Injection.

Ante esta vulnerabilidad deberemos probar si se puede realizar inyecciones de código LDAP ya sean AND, OR o BLIND.

Se ha encontrado una vulnerabilidad LDAP en Moodle.

Moodle

CVE-2012-3394	
Fecha Reporte	24/07/2012
Descripción	auth/ldap/ntlmsso_attempt.php redirecciona a usuarios de una URL de login https LDAP, lo cual permite a atacantes remotos obtener información sensitiva haciendo "snifing" en la red.
Versiones	2.0.x hasta la 2.0.10, 2.1 hasta la 2.1.7, 2.2.x hasta la 2.2.4, y 2.3.x hasta la

Afectadas	2.3.1.
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:P/I:N/A:N) Impact Subscore: 2.9 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information
Solución	Actualizar a las versiones 2.0.10, 2.1.7, 2.2.4 o 2.3.1

1.3.1.3. Ataques de inyección de ficheros

1.3.1.3.1. Remote File Inclusion

Esta vulnerabilidad cosiste en ejecutar código remoto dentro de la aplicación vulnerable. Se basa en la idea de que, al igual que es posible cargar un fichero local para su inclusión dentro de la página, podríamos cargar uno remoto que contuviese código malicioso. Esto es posible en lenguajes interpretados, donde podemos incluir un fichero con código y añadirlo a la ejecución.

Ante esta posible situación comprobaremos si podemos realizar la inclusión dinámica de ficheros mediante lenguaje interpretado de tal modo que podría ejecutarse dicho fichero en el servidor.

Éstas son algunas de las vulnerabilidades que podrían afectar a nuestro entorno.

Wordpress

CVE-2012-1205	
Fecha Reporte	24/02/2012
Descripción	Vulnerabilidad en relocate-upload.php de Relocate Upload plugin, permite a atacantes remotos ejecutar código PHP arbitrario a través de una URL en parámetro abspath.
Versiones Afectadas	Relocate Upload 0.20
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar Relocate Upload 0.20

CVE-2012-0934	
Fecha Reporte	02/01/2012
Descripción	Vulnerabilidad en ajax/savetag.php en el plugin Theme Tuner para

	WordPress anterior a 0.8 permite a atacantes remotos ejecutar código PHP arbitrario a través de una URL en el parámetro tt-abspath.
Versiones Afectadas	Theme Tuner 0.8
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar Theme Tuner

CVE-2011-4342	
Fecha Reporte	08/10/2012
Descripción	Vulnerabilidad en wp_xml_export.php del plugin BackWPup permite a atacantes remotos ejecutar código arbitrario PHP a través de una URL en el parámetro wpabs.
Versiones Afectadas	BackWPup anteriores a BackWPup.
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar plugin BackWPup

Moodle

CVE-2007-1429	
Fecha Reporte	13/03/2007
Descripción	Múltiples vulnerabilidades permiten a un usuario remoto ejecutar código PHP arbitrario a través de una URL en el parámetro “cmd” en admin/utfdbmigrate.php o filter.php.
Versiones Afectadas	1.7.1
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 10.0 CVSS Version 2 Metrics:

	Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Provides unauthorized access, Allows partial confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service
Solución	Actualizar Moodle

1.3.1.3.2. Local File Inclusion

Esta vulnerabilidad afecta tanto a lenguajes compilados como interpretados. Se basa en la posibilidad de incluir dentro de la página un fichero local del usuario con el que se ejecuta el servidor de aplicaciones web que tenga permisos de lectura. Esta vulnerabilidad puede ocurrir en cualquier lugar de un sitio web pero suele ser más común en dos sitios bien diferenciados:

- Páginas de plantillas: Carga un fichero desde otro y le da formato.
- Páginas de descargas: Recibe un parámetro con el nombre del fichero a descargar y lo envía al cliente.

La comprobación en este caso sería simplemente intentar incluir ficheros de un directorio superior usando los caracteres ../ en sistemas Linux o ..\ en sistemas Windows más el nombre de un fichero del que conozcamos su existencia. Esto se haría modificando la URL incluyendo el directorio antes mencionado.

A continuación se detallan vulnerabilidades de este tipo halladas para nuestro entorno.

WordPress

CVE-2009-4672	
Fecha Reporte	05/03/2010
Descripción	Vulnerabilidad de directorio transversal en main.php en el plugin WP-Lytebox para WordPress permite a atacantes remotos incluir código arbitrario en ficheros locales a través de ".." escalando directorios en el parámetro pg.
Versiones Afectadas	WP-Lytebox 1.3
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar WP-Lytebox

CVE-2007-2483	
Fecha Reporte	03/05/2007
Descripción	Vulnerabilidad de directorio transversal en js/wptable-button.php en wp-Table. Cuando register_globals está habilitado, permite a atacantes remotos incluir y ejecutar ficheros locales arbitrarios en el parámetro wpPATH.
Versiones Afectadas	en wp-Table 1.43 y anteriores
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Medium Authentication: Not required to exploit Impact Type:Provides unauthorized access, Allows partial confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service
Solución	Actualizar wp-Table

CVE-2007-2482	
Fecha Reporte	03/05/2007
Descripción	Vulnerabilidad de directorio transversal en wordtube-button.php en wordTube cuando register_globals está habilitado, permite a atacantes remotos incluir y ejecutar ficheros locales a través de ".." escalando directorios en el parámetro wpPATH.
Versiones Afectadas	wordTube 1.43 y anteriores
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar wordTube a la versión posterior a la 1.43

1.3.1.4. Webtrojans

Una de las funcionalidades de un entorno web es la posibilidad de subir ficheros, si no los comprobamos cuando nos son enviados podríamos estar copiando en nuestro servidor un fichero malintencionado conocido como *webtrojan*. Un webtrojan es una shell remota que podemos subir a un servidor aprovechando un fallo de seguridad.

Existen multitud de shells remotas en distintos lenguajes a disposición de cualquiera. Estas shells suelen ser detectadas por los antivirus para evitar que pasen desapercibidas a administradores despistados, pero pueden estar "camufladas" dentro de otros ficheros.

La prueba a realizar para este tipo de vulnerabilidad sería intentar ejecutar una Shell remota en el servidor camuflando el código tras la cabecera de una imagen por ejemplo.

Se ha encontrado una vulnerabilidad en WordPress que permitiría poder realizar un ataque de este tipo.

WordPress

CVE-2013-1949	
Fecha Reporte	25/04/2013
Descripción	El plugin Social Media Widget contiene una modificación externa que permite a atacantes remotos forzar la subida de ficheros arbitrarios.
Versiones Afectadas	Social Media Widget 4.0
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized modification
Solución	Actualizar Social Media Widget

1.3.1.5. Ataques de cookies/sesión

Como su propio nombre indica este tipo de ataques se realizan mediante las cookies que genera nuestra aplicación web o los datos que quedan guardados de la sesión de un usuario cuando se autentica. A continuación 2 posibles ataques de los que podríamos ser víctimas en nuestro entorno.

1.3.1.5.1. Session Fixation

Este ataque consiste en obtener o modificar el id o la cookie de sesión de tal modo que un atacante remoto podría acceder a nuestra aplicación web con un usuario válido teniendo acceso a información privada pudiendo realizar acciones maliciosas.

Moodle

CVE-2010-1613	
Fecha Reporte	29/04/2010
Descripción	No tiene habilitado regenerar el id de sesión durante la autentificación por defecto lo cual podría propiciar que atacantes remotos realizar un ataque de tipo “sesión fixation”.
Versiones Afectadas	Moodle 1.8.x y 1.9.x hasta la 1.9.8
Impacto	CVSS Severity (version 2.0):

	CVSS v2 Base Score:6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service
Solución	Actualizar Moodle a la 1.9.8 o posterior

Wordpress

CVE-2012-5868	
Fecha Reporte	27/12/2012
Descripción	No invalida la cookie de sesión "wordpress_sec" una vez el administrador realiza una acción de deslogeo. Lo cual hace más fácil a atacantes remotos descubrir los identificadores de sesión por ataque de fuerza bruta o modificarlos por ataque de repetición.
Versiones Afectadas	Wordpress 3.4.2
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:2.6 (LOW) (AV:N/AC:H/Au:N/C:P/I:N/A:N) Impact Subscore: 2.9 Exploitability Subscore: 4.9 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: High Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information
Solución	Instalar versión superior a la 3.4.2

1.3.1.5.2. Password Autocomplete in Browser

Este tipo de ataque se aprovecha de vulnerabilidades que pueda tener nuestra aplicación web para obtener la contraseña de inicio de sesión de un usuario válido.

Moodle

CVE-2012-0800	
Fecha Reporte	17/07/2012
Descripción	La funcionalidad form-autocompletion hace más fácil a atacantes que estén próximos físicamente descubrir contraseñas leyendo los contenidos del campo "non-password".
Versiones Afectadas	Moodle 2.0.x hasta la 2.0.7, 2.1.x hasta la 2.1.4 y 2.2.x hasta la 2.2.1.
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:2.1 (LOW) (AV:L/AC:L/Au:N/C:P/I:N/A:N) Impact Subscore: 2.9 Exploitability Subscore: 3.9

	CVSS Version 2 Metrics: Access Vector: Locally exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information
Solución	Actualizar Moodle a las versiones 2.0.7, 2.1.4 o 2.2.1

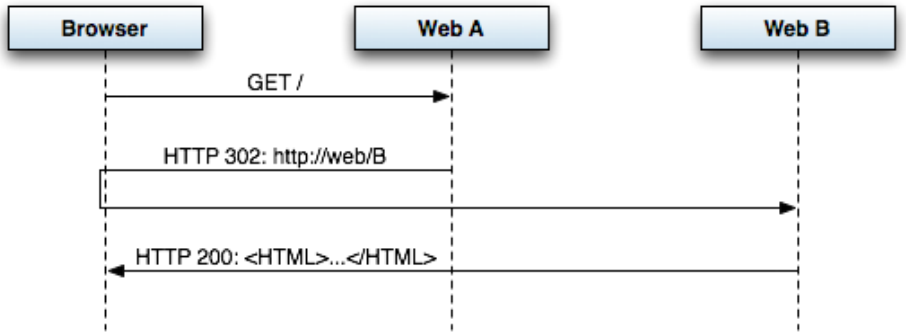
1.3.2. Protocolos AdAS

1.3.2.1. PAPI

PAPI(Point of Access for Providers of Information) es una tecnología que te permite desplegar una infraestructura de autenticación y autorización y un sistema de Single Sign-On fácilmente.

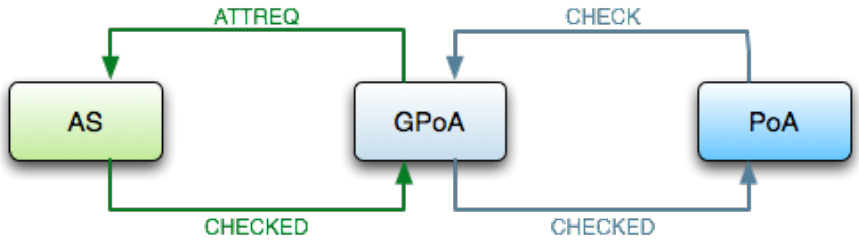
Se trata de un sistema que facilita el acceso, a través de Internet, a recursos de información que están restringidos a usuarios autorizados. Sus mecanismos de autenticación empleados para identificar a los usuarios se han diseñado para ser lo más flexibles posible, permitiendo que cada organización emplee un esquema de autenticación propio, manteniendo así los datos dentro de su propio ámbito, a la vez que los proveedores de información disponen de datos suficientes para realizar estadísticas.

Los mecanismos de control de acceso son transparentes para el usuario y compatibles con los navegadores comúnmente empleados en cualquier sistema operativo. Dado que PAPI emplea procedimientos HTTP estándar, su uso para proveer servicios de identidad digital y control de acceso no requiere de ningún hardware o software específico, garantizando a los usuarios un acceso ubicuo a cualquier recurso de información al que tengan derecho.



Los mensajes del protocolo de PAPI se transmiten utilizando métodos GET o POST sobre HTTP mientras que, por otro lado, las respuestas serán redirecciones 302 de HTTP, incluyendo además cookies en el caso de que el usuario deba almacenar algún tipo de información útil para el protocolo.

En el siguiente diagrama podemos ver el conjunto de mensajes que definen el protocolo de PAPI:



No se hallaron vulnerabilidades documentadas para este protocolo.

1.3.2.2. SAML2

Security assertion markup language (SAML) es un estándar de OASIS basado en XML para el intercambio de información de autenticación y autorización entre dominios de seguridad.

La especificación SAML 2 está divida en los componentes que se muestran en la siguiente figura.

Se ha encontrado una vulnerabilidad de SAML para google.

CVE-2008-3891	
Fecha Reporte	09/03/2008
Descripción	El estándar SAML para google apps permite que un proveedor de servicio se haga pasar por usuarios utilizando el registro de acceso almacenado en la base de datos, de tal modo que podría acceder a la parte privada de google apps que haya accedido el usuario con anterioridad.
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:7.5 (HIGH) (AV:N/AC:L/Au:N/C:P/I:P/A:P) Impact Subscore: 6.4 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low **NOTA: Access Complexity puntuada como Low por información insuficiente
Prueba	En este caso la prueba consistiría en acceder a google apps con nuestros credenciales, posteriormente accedemos a la BD con otro usuario que sea administrador de la misma, accedemos al registro de entrada de dicho

	usuario e intentamos acceder de manera fraudulenta a su zona privada.

1.3.2.3. CAS

El protocolo CAS(Central Administration Service) consistente en un sistema de autenticación creado en la universidad de Yale para proveer de una autenticación de confianza.

CAS provee a un sistema SSO de:

- Un protocolo abierto y bien documentado
- Un componente open-source de Java server
- Una Librería de clientes para Java, .Net, PHP, Perl, Apache, uPortal, y otros.
- Integración con uPortal, Sakai, BlueSocket, TikiWiki, Mule, Liferay, Moodle y otros.
- Comunidad de documentación y soporte de implementación.
- Una extensa comunidad de innovadores.

Estas son las vulnerabilidades que afectan a este protocolo.

CVE-2012-2357	
Fecha Reporte	07/21/2012
Descripción	Característica de la funcionalidad del servicio de multiautentificación en la funcionalidad CAS de auth/cas/cas_form.html en Moodle no utiliza HTTPS, lo cual permite a atacantes remotos obtener credenciales haciendo "sniffing" en la red.
Versiones Afectadas	Moodle 2.1.x gasta la 2.1.6 y 2.2.x hasta la 2.2.3.
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:P/I:N/A:N) Impact Subscore: 2.9 Exploitability Subscore: 10.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Not required to exploit Impact Type:Allows unauthorized disclosure of information
Solución	Actualizar Moodle a las versiones 2.1.6 o 2.2.3
Prueba	Comprobar la versión de Moodle y si auth/cas/cas_form.html utiliza HTTPS.

CVE-2010-3690	
Fecha Reporte	10/07/2010
Descripción	Múltiples vulnerabilidades XSS en phpCAS, cuando el modo proxy está habilitado, permite a atacantes remotos inyectar scripts vía web o HTML a través del parámetro Proxy Granting Ticket IOU a la función callback en client.php, en vectores involucrados en funciones que hacen llamadas "getCallbackURL", o vectores involucrados en funciones que hacen llamadas "getURL".

Versiones Afectadas	phpCAS en versiones anteriores a la 1.1.3
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium Authentication: Not required to exploit Impact Type:Allows unauthorized modification
Solución	Actualizar phpCAS a 1.1.3 o posterior.
Prueba	Intentar inyectar scripts vía web o HTML a través del parámetro Proxy Granting Ticket IOU a la función callback

CVE-2010-2795	
Fecha Reporte	08/05/2010
Descripción	phpCAS permite a usuarios remotos autenticados secuestrar sesiones a través de cadenas query que contengan un valor de ticket encapsulado.
Versiones Afectadas	phpCAS en versiones anteriores a la 1.1.3
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:4.0 (MEDIUM) (AV:N/AC:L/Au:S/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 8.0 CVSS Version 2 Metrics: Access Vector: Network exploitable Access Complexity: Low Authentication: Required to exploit Impact Type:Allows unauthorized modification
Solución	Actualizar phpCAS a la versión 1.1.3 o posterior.
Prueba	Una vez autenticado intentar utilizar cadenas query para secuestrar la sesión.

CVE-2010-1618	
Fecha Reporte	04/29/2010
Descripción	Vulnerabilidad XSS en la librería de phpCAS utilizada en Moodle permite a atacantes remotos inyectar código script o HTML arbitrario en una URL encapsulada, lo cual no es manejado correctamente en un mensaje de error.
Versiones Afectadas	Versiones anteriores a la 1.1.0 de phpCAS Moodle 1.8.x hasta la 1.8.12 y 1.9.x hasta la 1.9.8
Impacto	CVSS Severity (version 2.0): CVSS v2 Base Score:4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:P/A:N) Impact Subscore: 2.9 Exploitability Subscore: 8.6 CVSS Version 2 Metrics: Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism Access Complexity: Medium

	Authentication: Not required to exploit Impact Type:Allows unauthorized modification References to Advisories, Solutions, an
Solución	Actualizar phpCAP a 1.1.0 o posterior y moodle a las versiones 1.8.12 o 1.9.8.
Prueba	Intentar inyectar script o HTML arbitrario en una URL encapsulada.

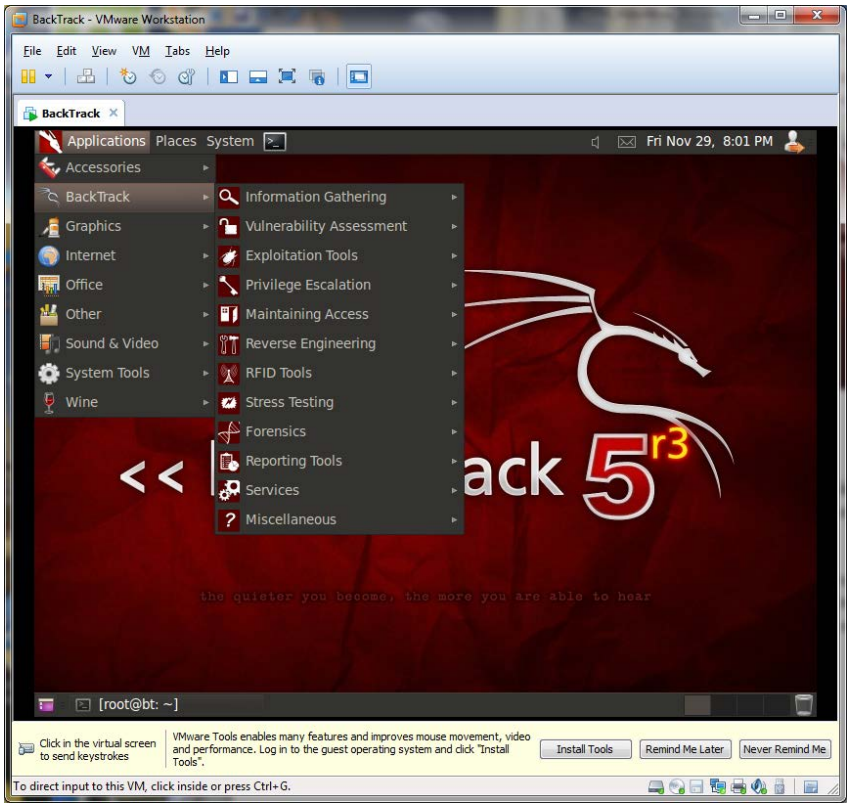
1.4. Entorno de Pruebas

El entorno de pruebas desde el cual se van a realizar las pruebas de auditoría se trata de Linux BackTrack 5 R3.

Se ha seleccionado esta opción por dos razones. En primer lugar por tener un entorno aislado y en segundo lugar esta distribución nos proporciona todas las herramientas necesarias para poder realizar las pruebas necesarias para esta auditoría.

Para ello se ha preparado una máquina virtual en VMWare con esta distribución y así poder realizar las pruebas pertinentes.

A continuación el entorno mencionado.



2. PRUEBAS DE AUDITORÍA

2.1. Pruebas Hosts

En primer lugar se han realizado pruebas sobre los hosts donde se encuentra alojado el entorno AdAS. Para ello se han utilizado las herramientas nmap y nessus.

2.1.1. Escaneo de puertos con nmap

Nmap es una herramienta muy útil que nos permite realizar un escaneo de los puertos TCP/UDP del host que nosotros deseemos, pudiendo elegir entre los diferentes parámetros la forma de realizar el escaneo así como los puertos que queremos analizar. Para este caso se ha utilizado el siguiente comando.

```
Nmap –sS –p0-65535 54.246.89.131
```

Y estos los resultados obtenidos

```
Starting Nmap 6.01 ( http://nmap.org ) at 2013-11-19 00:45 CET
Nmap scan report for ec2-54-246-89-131.eu-west-1.compute.amazonaws.com (54.246.89.131)
Host is up (0.00014s latency).
Not shown: 65532 filtered ports
PORT    STATE  SERVICE
0/tcp   closed unknown
22/tcp  open   ssh
80/tcp  open   http
443/tcp open   https

Nmap done: 1 IP address (1 host up) scanned in 1398.87 seconds.
```

Se han detectado abiertos los puertos 0 utilizado por un servicio desconocido, el Puerto 22 utilizado por el servicio ssh, el puerto 80 utilizado por el servicio http y el 443 por el servicio https.

2.1.2. Escaneo con nessus

Con la herramienta nessus se realiza también un escaneo de puertos así como un análisis de las posibles vulnerabilidades. Dicho análisis se ha realizado sobre todos los virtual hosts del entorno obteniendo los siguientes resultados.

Estos son os plugins utilizados para realizar el análisis

Plugin Id	#	Plugin Name	Severity
19506	8	Nessus Scan Information	Low Severity problem(s) found
12053	8	Host Fully Qualified Domain Name (FQDN) Resolution	Low Severity problem(s) found
10287	8	Traceroute Information	Low Severity problem(s) found
45590	7	Common Platform Enumeration (CPE)	Low Severity problem(s) found
46215	6	Inconsistent Hostname and IP Address	Low Severity problem(s) found
22964	6	Service Detection	Low Severity problem(s) found
70658	4	SSH Server CBC Mode Ciphers Enabled	Low Severity problem(s) found
70657	4	SSH Algorithms and Languages Supported	Low Severity problem(s) found
24260	4	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found

10107	4	HTTP Server Type and Version	Low Severity problem(s) found
39520	3	Backported Security Patch Detection (SSH)	Low Severity problem(s) found
10919	3	Open Port Re-check	Low Severity problem(s) found
10267	3	SSH Server Type and Version Information	Low Severity problem(s) found
48243	2	PHP Version	Low Severity problem(s) found
11002	2	DNS Server Detection	Low Severity problem(s) found
10881	1	SSH Protocol Versions Supported	Low Severity problem(s) found

En la fase de análisis se dará una información mucho más detallada de los plugins.

A continuación los datos acumulados de las vulnerabilidades detectadas en cada host.

wordpress.petasso.prise.es

Scan Time

Start time:	Wed Nov 20 22:40:09 2013
End time:	Wed Nov 20 23:02:28 2013

Number of vulnerabilities

High	0
Medium	0
Low	16

Remote Host Information

DNS name:	wordpress.petasso.prise.es
IP address:	54.246.89.131

petasso.prise.es

Scan Time

Start time:	Wed Nov 20 22:40:09 2013
End time:	Wed Nov 20 23:03:16 2013

Number of vulnerabilities

High	0
Medium	0
Low	12

Remote Host Information

DNS name:	petasso.prise.es
IP address:	54.246.89.131

moodle.petasso.prise.es

Scan Time

Start time:	Wed Nov 20 22:40:09 2013
End time:	Wed Nov 20 23:11:24 2013

Number of vulnerabilities	
High	0
Medium	0
Low	21

Remote Host Information	
DNS name:	moodle.petasso.prise.es
IP address:	54.246.89.131

links.petasso.prise.es

Scan Time	
Start time:	Wed Nov 20 22:40:09 2013
End time:	Wed Nov 20 22:58:12 2013

Number of vulnerabilities	
High	0
Medium	0
Low	7

Remote Host Information	
DNS name:	links.petasso.prise.es
IP address:	54.246.89.131

idp.petasso.prise.es

Scan Time	
Start time:	Wed Nov 20 22:40:09 2013
End time:	Wed Nov 20 22:59:45 2013

Number of vulnerabilities	
High	0
Medium	0
Low	17

Remote Host Information	
DNS name:	idp.petasso.prise.es
IP address:	54.246.89.131

Como podemos observar se han detectado varias vulnerabilidades calificadas con riesgo bajo que vamos a ver más detalladamente a continuación.

petasso.prise.es

Port ▲	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	tcp	general	3	0	0	3	0
0	udp	general	1	0	0	1	0
22	tcp	ssh	7	0	0	6	1
80	tcp	http?	3	0	0	2	1
443	tcp	https?	1	0	0	0	1

Puerto 0/tcp

Plugin ID	Name	Port	Severity
12053	Host Fully Qualified Domain Name (FQDN) Resolution	general/tcp	Low
45590	Common Platform Enumeration (CPE)	general/tcp	Low
19506	Nessus Scan Information	general/tcp	Low

Puerto 0/udp

Plugin ID	Name	Port	Severity
10287	Traceroute Information	general/udp	Low

Puerto 22/tcp

Plugin ID	Name	Port	Severity
22964	Service Detection	ssh (22/tcp)	Low
10267	SSH Server Type and Version Information	ssh (22/tcp)	Low
70657	SSH Algorithms and Languages Supported	ssh (22/tcp)	Low
70658	SSH Server CBC Mode Ciphers Enabled	ssh (22/tcp)	Low
10881	SSH Protocol Versions Supported	ssh (22/tcp)	Low
39520	Backported Security Patch Detection (SSH)	ssh (22/tcp)	Low

Puerto 80/tcp

Plugin ID	Name	Port	Severity
10107	HTTP Server Type and Version	http? (80/tcp)	Low
24260	HyperText Transfer Protocol (HTTP) Information	http? (80/tcp)	Low

idp.petasso.prise.es

Port ▲	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	tcp	general	9	0	0	9	0
0	udp	general	2	0	0	2	0
22	tcp	ssh	6	0	0	4	2
80	tcp	http?	4	0	0	2	2
443	tcp	https?	1	0	0	0	1

Puerto 0/TCP

Plugin ID	Name	Port	Severity
12053	Host Fully Qualified Domain Name (FQDN) Resolution	general/tcp	Low
46215	Inconsistent Hostname and IP Address	general/tcp	Low
46215	Inconsistent Hostname and IP Address	general/tcp	Low
12053	Host Fully Qualified Domain Name (FQDN) Resolution	general/tcp	Low
10919	Open Port Re-check	general/tcp	Low
19506	Nessus Scan Information	general/tcp	Low
45590	Common Platform Enumeration (CPE)	general/tcp	Low
10919	Open Port Re-check	general/tcp	Low
19506	Nessus Scan Information	general/tcp	Low

Puerto 0/UDP

Plugin ID	Name	Port	Severity
10287	Traceroute Information	general/udp	Low
10287	Traceroute Information	general/udp	Low

Puerto 22/tcp

Plugin	Name	Port	Severity
22964	Service Detection	ssh (22/tcp)	Low
22964	Service Detection	ssh (22/tcp)	Low
70657	SSH Algorithms and Languages Supported	ssh (22/tcp)	Low
70658	SSH Server CBC Mode Ciphers Enabled	ssh (22/tcp)	Low

Puerto 80/tcp

Plugin	Name	Port	Severity
10107	HTTP Server Type and Version	http? (80/tcp)	Low
24260	HyperText Transfer Protocol (HTTP) Information	http? (80/tcp)	Low

links.petasso.prise.es

Port ▲	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	tcp	general	4	0	0	4	0
0	udp	general	1	0	0	1	0
80	tcp	www	3	0	0	2	1
443	tcp	https?	1	0	0	0	1

Puerto0/tcp

Plugin	Name	Port	Severity
46215	Inconsistent Hostname and IP Address	general/tcp	Low
12053	Host Fully Qualified Domain Name (FQDN) Resolution	general/tcp	Low
45590	Common Platform Enumeration (CPE)	general/tcp	Low
19506	Nessus Scan Information	general/tcp	Low

Puerto 0/udp

Plugin	Name	Port	Severity
10287	Traceroute Information	general/udp	Low

Puerto80/tcp

Plugin	Name	Port	Severity
22964	Service Detection	www (80/tcp)	Low
24260	HyperText Transfer Protocol (HTTP) Information	www (80/tcp)	Low

moodle.petasso.prise.es

Port ▲	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	tcp	general	8	0	0	8	0
0	udp	general	2	0	0	2	0
22	tcp	ssh	13	0	0	10	3
53	udp	dns	1	0	0	1	0
80	tcp	http?	2	0	0	0	2
443	tcp	https?	3	0	0	0	3

Puerto 0/tcp

Plugin	Name	Port	Severity
12053	Host Fully Qualified Domain Name (FQDN) Resolution	general/tcp	Low
46215	Inconsistent Hostname and IP Address	general/tcp	Low
45590	Common Platform Enumeration (CPE)	general/tcp	Low
19506	Nessus Scan Information	general/tcp	Low
12053	Host Fully Qualified Domain Name (FQDN) Resolution	general/tcp	Low
45590	Common Platform Enumeration (CPE)	general/tcp	Low
10919	Open Port Re-check	general/tcp	Low
19506	Nessus Scan Information	general/tcp	Low

Puerto 0/udp

Plugin	Name	Port	Severity
10287	Traceroute Information	general/udp	Low
10287	Traceroute Information	general/udp	Low

Puerto 22/tcp

Plugin	Name	Port	Severity
22964	Service Detection	ssh (22/tcp)	Low
10267	SSH Server Type and Version Information	ssh (22/tcp)	Low
70657	SSH Algorithms and Languages Supported	ssh (22/tcp)	Low
70658	SSH Server CBC Mode Ciphers Enabled	ssh (22/tcp)	Low
39520	Backported Security Patch Detection (SSH)	ssh (22/tcp)	Low
22964	Service Detection	ssh (22/tcp)	Low
10267	SSH Server Type and Version Information	ssh (22/tcp)	Low
70657	SSH Algorithms and Languages Supported	ssh (22/tcp)	Low
70658	SSH Server CBC Mode Ciphers Enabled	ssh (22/tcp)	Low
39520	Backported Security Patch Detection (SSH)	ssh (22/tcp)	Low

Puerto 53/udp

Plugin	Name	Port	Severity
11002	DNS Server Detection	dns (53/udp)	Low

worpress.petasso.prise.es

Port ▲	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	tcp	general	8	0	0	8	0
0	udp	general	2	0	0	2	0
53	udp	dns	1	0	0	1	0
80	tcp	http?	7	0	0	5	2
443	tcp	https?	2	0	0	0	2

Puerto 0/tcp

Plugin ID	Name	Port	Severity
46215	Inconsistent Hostname and IP Address	general/tcp	Low
12053	Host Fully Qualified Domain Name (FQDN) Resolution	general/tcp	Low
12053	Host Fully Qualified Domain Name (FQDN) Resolution	general/tcp	Low
46215	Inconsistent Hostname and IP Address	general/tcp	Low
45590	Common Platform Enumeration (CPE)	general/tcp	Low
19506	Nessus Scan Information	general/tcp	Low
45590	Common Platform Enumeration (CPE)	general/tcp	Low
19506	Nessus Scan Information	general/tcp	Low

Puerto 0/udp

Plugin ID	Name	Port	Severity
10287	Traceroute Information	general/udp	Low
10287	Traceroute Information	general/udp	Low

Puerto 53/udp

Plugin ID	Name	Port	Severity
11002	DNS Server Detection	dns (53/udp)	Low

Puerto 80/tcp

Plugin ID	Name	Port	Severity
10107	HTTP Server Type and Version	http? (80/tcp)	Low
48243	PHP Version	http? (80/tcp)	Low
24260	HyperText Transfer Protocol (HTTP) Information	http? (80/tcp)	Low
10107	HTTP Server Type and Version	http? (80/tcp)	Low
48243	PHP Version	http? (80/tcp)	Low

2.2. Pruebas de las Aplicaciones Web

2.2.1. Pruebas "XSS"

El entorno backtrack nos proporciona una herramienta llamada XSSer que precisamente se encarga de escanear si un entorno web es vulnerable a este tipo de ataques, se han escaneado todas las urls y estas son las que han dado un resultado positivo.

Comando	XSSer –u https://idp.petasso.prise.es/adas/SAML2/SSOService.php?SAMLRequest=pVJdb9swDPwrht5tx3bcNUISIGswLEC3BnW6h70MjMQsAmRJE%2Bl9%2FPspdgd0HZCXPQki747HA5cEvQ1yM%2FDZPeK3AYmzn711JMfGSgzRSQ9kSDrokSQr2W0%2B3Mu6mMkQPXvlrXhBuc4AIoxsvBPZbrsSX%2BDYHqu2ns9UpecL1agaT4ubebNoT4vbCgCbpm5vb3StRPYJIyXmSiShRCcacOeIwXEqzaomr6q8bg%2FVG9k2smk%2Bi2ybtjEOeGSdmQPJsjQ6FAE5OfFFiIawQCpBA5UXl3XZdQ8dxu9GYRHOQWSbP5bvvKOhx%2FjcfXq8n0STZu%2B9tvivLJk%2BWLzEkiB6sKNkOf5peuscFI1VjScYLOeUZu6fg31rnDbu6%2FVMjxOI5PvDYZ%2FvH7qDWC8v2nLMKK7%2Fy2Sf4BoYXnlcli8nLKcr%2Bpi87bZ7b436lb3zsQe%2Bbv1SMTo%2FjVDJERwZdJxCt9b%2FuIsIjCvBcUBRrqeRf9%2Fq%2Bjc%3D --no-head
Resultado	[*] Final Results: ========== - Injections: 1 - Failed: 0 - Sucessfull: 1 - Accur: 100 % ========== [*] List of possible XSS injections: ==========

	[I] Target: https://idp.petasso.prise.es/adas/SAML2/SSOService.php?SAMLRequest=pVJdb9swDPwrht5tx3bcNUISIGswLEC3BnW6h70MjMQsAmRJE%2Bl9%2FPspdgd0HZCXPQki747HA5cEvQ1yM%2FDZPeK3AYmzn711JMfGSgzRSQ9kSDrokSQr2W0%2B3Mu6mMkQPXvlrXhBuc4AIoxsvBPZbrsSX%2BDYHqu2ns9UpecL1agaT4ubebNoT4vbCgCbpm5vb3StRPYJIyXmSiShRCcacOeIwXEqzaomr6q8bg%2FVG9k2smk%2Bi2ybtjEOeGSdmQPJsjQ6FAE5OfFFiIawQCpBA5UXl3XZdQ8dxu9GYRHOQWSbP5bvvKOhx%2FjcfXq8n0STZu%2B9tvivLJk%2BWLzEkiB6sKNkOf5peuscFI1VjScYLOeUZu6fg31rnDbu6%2FVMjxOI5PvDYZ%2FvH7qDWC8v2nLMKK7%2Fy2Sf4BoYXnlcli8nLKcr%2Bpi87bZ7b436lb3zsQe%2Bbv1SMTo%2FjVDJERwZdJxCt9b%2FuIsIjCvBcUBRrqeRf9%2Fq%2Bjc%3D [+] Injection: https://idp.petasso.prise.es/adas/SAML2/SSOService.php?SAMLRequest=pVJdb9swDPwrht5tx3bcNUISIGswLEC3BnW6h70MjMQsAmRJE%2Bl9%2FPspdgd0HZCXPQki747HA5cEvQ1yM%2FDZPeK3AYmzn711JMfGSgzRSQ9kSDrokSQr2W0%2B3Mu6mMkQPXvlrXhBuc4AIoxsvBPZbrsSX%2BDYHqu2ns9UpecL1agaT4ubebNoT4vbCgCbpm5vb3StRPYJIyXmSiShRCcacOeIwXEqzaomr6q8bg%2FVG9k2smk%2Bi2ybtjEOeGSdmQPJsjQ6FAE5OfFFiIawQCpBA5UXl3XZdQ8dxu9GYRHOQWSbP5bvvKOhx%2FjcfXq8n0STZu%2B9tvivLJk%2BWLzEkiB6sKNkOf5peuscFI1VjScYLOeUZu6fg31rnDbu6%2FVMjxOI5PvDYZ%2FvH7qDWC8v2nLMKK7%2Fy2Sf4BoYXnlcli8nLKcr%2Bpi87bZ7b436lb3zsQe%2Bbv1SMTo%2FjVDJERwZdJxCt9b%2FuIsIjCvBcUBRrqeRf9%2Fq%2Bjc%3D/">82b80285f9819ec5a60e9f1481789915 [-] Method: xss [-] Browsers: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]

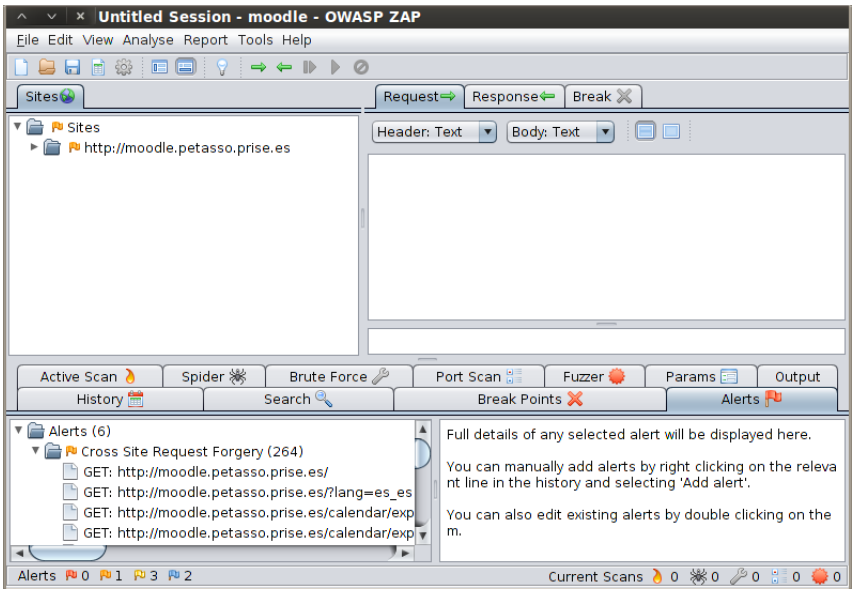
Comando	XSSer –u http://wordpress.petasso.prise.es/?p=1 --no-head
Resultado	[*] Final Results: ========== - Injections: 1 - Failed: 0 - Sucessfull: 1 - Accur: 100 % ========== [*] List of possible XSS injections: ========== [I] Target: http://wordpress.petasso.prise.es/?p=1 [+] Injection: http://wordpress.petasso.prise.es/?p=1/">f44f23b5362cdbc957a5b9482cf0a5a5 [-] Method: xss [-] Browsers: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]

Comando	XSSer –u http://wordpress.petasso.prise.es/?p=1#comments --o-head
Resultado	[*] Final Results: ========== - Injections: 1 - Failed: 0 - Sucessfull: 1 - Accur: 100 % ========== [*] List of possible XSS injections: ========== [I] Target: http://wordpress.petasso.prise.es/?p=1#comments [+] Injection: http://wordpress.petasso.prise.es/?p=1#comments/">642060308c125a67efb129b3abb8fb22 [-] Method: xss [-] Browsers: [IE7.0|IE6.0|NS8.1-IE] [NS8.1-G|FF2.0] [O9.02]

2.2.2. Pruebas "CSRF"

Para realizar este test se ha utilizado la herramienta OWASP ZAP con los siguientes resultados

Moodle



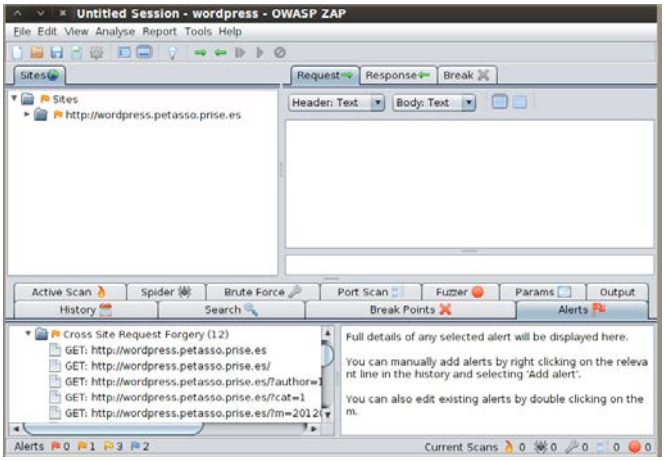
Estas son las urls afectadas

http://moodle.petasso.prise.es/
http://moodle.petasso.prise.es/login/index.php **
http://moodle.petasso.prise.es/course/category.php?id=2
http://moodle.petasso.prise.es/my/
http://moodle.petasso.prise.es/calendar/view.php **
http://moodle.petasso.prise.es/index.php? **
http://moodle.petasso.prise.es/?lang=es_es

http://moodle.petasso.prise.es/login/forgot_password.php
http://moodle.petasso.prise.es/theme/switchdevice.php **
http://moodle.petasso.prise.es/login/index.php?lang=es_es
http://moodle.petasso.prise.es/calendar/set.php **
http://moodle.petasso.prise.es/calendar/export.php **
http://moodle.petasso.prise.es/index.php **
http://moodle.petasso.prise.es/theme/switchdevice.php **

** Urls que derivan de esta

Wordpress



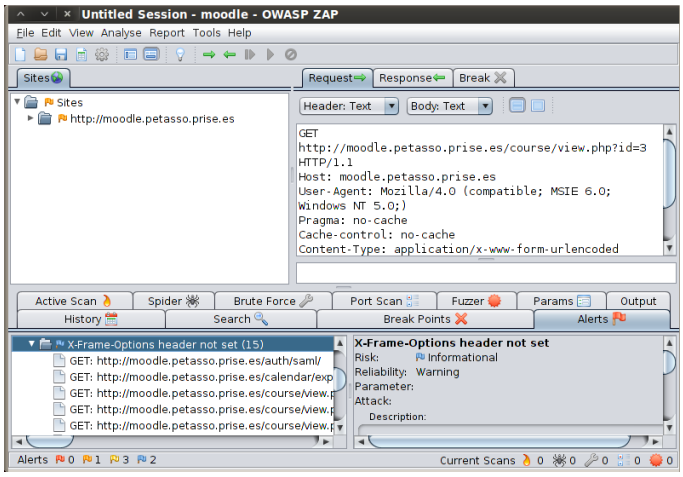
Estas son las urls afectadas

http://wordpress.petasso.prise.es/
http://wordpress.petasso.prise.es/wp-admin/
http://wordpress.petasso.prise.es/?page_id=2
http://wordpress.petasso.prise.es/?p=1
http://wordpress.petasso.prise.es/?author=1
http://wordpress.petasso.prise.es/?cat=1
http://wordpress.petasso.prise.es/?m=201203
http://wordpress.petasso.prise.es/?s=1&submit=Search
http://wordpress.petasso.prise.es
http://wordpress.petasso.prise.es/?s=1&
http://wordpress.petasso.prise.es/wp-includes/js/jquery/jquery.form.dev.js
http://wordpress.petasso.prise.es/simplesaml/admin/metadata-converter.php

2.2.3. Pruebas "Clickjacking"

La herramienta OWASP ZAP nos proporciona también información de las vulnerabilidades clickjacking encontradas, a continuación las evidencias.

Moodle

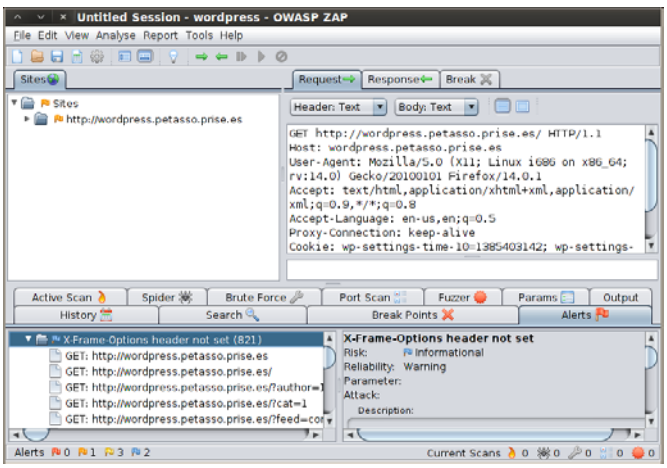


Estas son las urls afectadas

http://wordpress.petasso.prise.es/
http://wordpress.petasso.prise.es/wp-content/ **
http://wordpress.petasso.prise.es/simplesaml/ **
http://wordpress.petasso.prise.es/wp-includes **
http://wordpress.petasso.prise.es/wp-admin/ **
http://wordpress.petasso.prise.es/?page_id=2
http://wordpress.petasso.prise.es/?p=1
http://wordpress.petasso.prise.es/?author=1
http://wordpress.petasso.prise.es/?cat=1
http://wordpress.petasso.prise.es/?m=201203
http://wordpress.petasso.prise.es/?feed=rss2
http://wordpress.petasso.prise.es/?feed=comments-rss2
http://wordpress.petasso.prise.es/?s=1&submit=Search
http://wordpress.petasso.prise.es/xmlrpc.php
http://wordpress.petasso.prise.es/xmlrpc.php?rsd
http://wordpress.petasso.prise.es/a

** Urls que derivan de esta

Wordpress



Estas son las urls afectadas

http://moodle.petasso.prise.es/auth/saml/
http://moodle.petasso.prise.es/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
http://moodle.petasso.prise.es/course/view.php?id=3
http://moodle.petasso.prise.es/user/view.php?id=5&course=1
http://moodle.petasso.prise.es/course/view.php?id=2
http://moodle.petasso.prise.es/theme/yui_combo.php?3.4.1/build/cssreset/reset-min.css&3.4.1/build/cssfonts/fonts-min.css&3.4.1/build/cssgrids/grids-min.css&3.4.1/build/cssbase/base-min.css
http://moodle.petasso.prise.es/lib/yui/3.4.1/build/yui/yui-min.js
http://moodle.petasso.prise.es/theme/yui_combo.php?2.9.0/build/assets/skins/sam/skin.css
http://moodle.petasso.prise.es/login/index.php
http://moodle.petasso.prise.es/theme/styles.php?theme=standard&rev=281&type=plugins
http://moodle.petasso.prise.es/theme/styles.php?theme=standard&rev=281&type=theme
http://moodle.petasso.prise.es/theme/styles.php?theme=standard&rev=281&type=parents
http://moodle.petasso.prise.es/user/profile.php?id=5
http://moodle.petasso.prise.es/course/view.php?id=1
http://moodle.petasso.prise.es/calendar/export_execute.php?preset_what=all&preset_what=courses&preset_time=weeknow&preset_time=monthnow&preset_time=monthnext&preset_time=recentupcoming&cal_d=&cal_m=&cal_y=&userid=0&authtoken=bf4045ab0d6bbb418ff84bbb4dd54cb7c1168004&generateurl=Obtener+URL+del+calendario

2.2.4. Pruebas “SQL Inyection”

Para testear posibles vulnerabilidades de inyección SQL se ha utilizado la herramienta sqlmap, se ha realizado la comprobación con varias urls con resultado negativo. A continuación 1 ejemplo del comando utilizado y la salida para cada entorno.

Moodle

```
python sqlmap.py -u http://wordpress.petasso.prise.es/wp-admin/  --dbms=mysql

    sqlmap/1.0-dev-25eca9d - automatic SQL injection and database takeover tool

    http://sqlmap.org

[!] legal disclaimer: usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Authors assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 00:02:22

[00:02:22] [WARNING] you've provided target url without any GET parameters (e.g. www.site.com/article.php?id=1) and without providing any POST parameters through --data option

do you want to try URI injections in the target url itself? [Y/n/q] Y

[00:02:24] [INFO] testing connection to the target url

sqlmap got a 302 redirect to 'http://wordpress.petasso.prise.es/wp-login.php'. Do you want to follow? [Y/n] Y

[00:02:29] [INFO] testing if the url is stable, wait a few seconds

[00:02:31] [WARNING] URI parameter '#1*' appears to be not dynamic

[00:02:31] [WARNING] reflective value(s) found and filtering out

[00:02:31] [WARNING] heuristic test shows that URI parameter '#1*' might not be injectable

[00:02:31] [INFO] testing for SQL injection on URI parameter '#1*'
```

```
[00:02:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:02:33] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[00:02:34] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[00:02:34] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
[00:02:35] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[00:02:44] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[00:02:53] [WARNING] URI parameter '#1*' is not injectable
[00:02:53] [CRITICAL] all parameters appear to be not injectable. Try to increase --level/--risk values to perform more tests. Also, you can try to rerun by providing either a valid --string or a valid --regexp, refer to the user's manual for details
[00:02:53] [WARNING] HTTP error codes detected during testing:
400 (Bad Request) - 27 times, 404 (Not Found) - 109 times
```

Wordpress

```
python sqlmap.py -u http://wordpress.petasso.prise.es/wp-admin/index.php?id=1 --dbs

sqlmap got a 302 redirect to 'http://wordpress.petasso.prise.es/wp-login.php'. Do you want to follow? [Y/n] y

[23:21:33] [INFO] testing if the url is stable, wait a few seconds
[23:21:35] [WARNING] GET parameter 'id' appears to be not dynamic
[23:21:37] [WARNING] reflective value(s) found and filtering out
[23:21:37] [WARNING] heuristic test shows that GET parameter 'id' might not be injectable
[23:21:37] [INFO] testing for SQL injection on GET parameter 'id'
[23:21:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:21:55] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[23:22:01] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:22:08] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'
[23:22:14] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:22:20] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[23:22:26] [INFO] testing 'PostgreSQL > 8.1 stacked queries'
[23:22:31] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[23:22:36] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
[23:22:44] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:22:49] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[23:22:59] [INFO] GET parameter 'id' is 'Microsoft SQL Server/Sybase time-based blind' injectable
[23:22:59] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[23:22:59] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other injection technique found
[23:23:57] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[23:24:23] [INFO] checking if the injection point on GET parameter 'id' is a false positive
[23:24:24] [WARNING] false positive or unexploitable injection point detected
[23:24:24] [WARNING] GET parameter 'id' is not injectable
[23:24:24] [CRITICAL] all parameters appear to be not injectable. Try to increase --level/--risk values to perform more tests. Also, you can try to rerun by providing either a valid --string or a valid --regexp, refer to the user's manual for details
```

2.2.5. Pruebas “File Intrusion”

Para realizar las pruebas de si existía alguna vulnerabilidad que permitiera incluir algún fichero de manera remota en el servidor, se ha utilizado la herramienta filemap. Se han escaneado todas las urls susceptibles de incluir un fichero, es decir, aquellas donde aparezca la estructura:

- "?id="
- "?p="
- "?page="

En todos los casos ha dado resultado negativo, a continuación un ejemplo de cada entorno.

Moodle

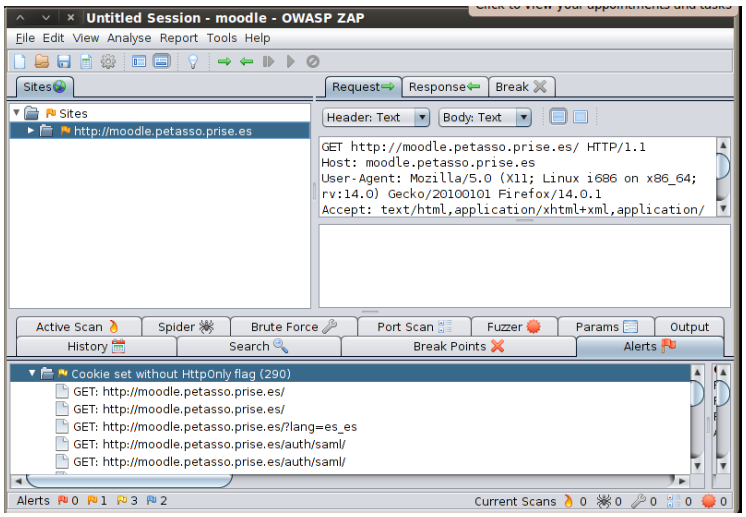
Comando	Python fimap.py –u http://moodle.petasso.prise.es/enrol/index.php?id=3
Resultado	SingleScan is testing URL: 'http://moodle.petasso.prise.es/enrol/index.php?id=3' [OUT] Parsing URL 'http://moodle.petasso.prise.es/enrol/index.php?id=3'... [INFO] Fiddling around with URL... Target URL isn't affected by any file inclusion bug :(fimap v.08.1 by Iman Karim - Automatic LFI/RFI scanner and exploiter [INFO] 0 plugins loaded.

Wordpress

Comando	Python fimap.py –u http://wordpress.petasso.prise.es/?p=1
Resultado	[INFO] 0 plugins loaded. SingleScan is testing URL: 'http://wordpress.petasso.prise.es/?p=1' [OUT] Parsing URL 'http://wordpress.petasso.prise.es/?p=1'... [INFO] Fiddling around with URL... Target URL isn't affected by any file inclusion bug :(fimap v.08.1 by Iman Karim - Automatic LFI/RFI scanner and exploiter [INFO] 0 plugins loaded.

2.2.6. Pruebas Session Fixation

Moodle

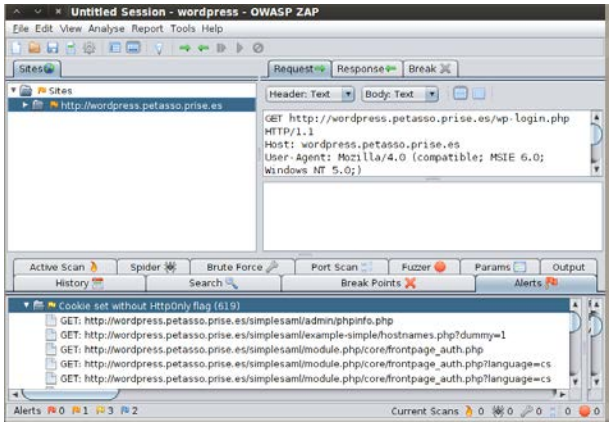


Estas son las URLs afectadas

http://moodle.petasso.prise.es/
http://moodle.petasso.prise.es/auth/saml/
http://moodle.petasso.prise.es/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
http://moodle.petasso.prise.es/login/index.php
http://moodle.petasso.prise.es/course/view.php?id=3
http://moodle.petasso.prise.es/user/view.php?id=5&course=1
http://moodle.petasso.prise.es/index.php?cal_m=10&cal_y=2013
http://moodle.petasso.prise.es/index.php?cal_m=12&cal_y=2013
http://moodle.petasso.prise.es/index.php?cal_m=9&cal_y=2013
http://moodle.petasso.prise.es/index.php?cal_m=11&cal_y=2013
http://moodle.petasso.prise.es/?lang=es_es
http://moodle.petasso.prise.es/login/forgot_password.php
http://moodle.petasso.prise.es/index.php?cal_m=1&cal_y=2014
http://moodle.petasso.prise.es/theme **
http://moodle.petasso.prise.es/calendar **

** Urls que derivan de esta

Wordpress

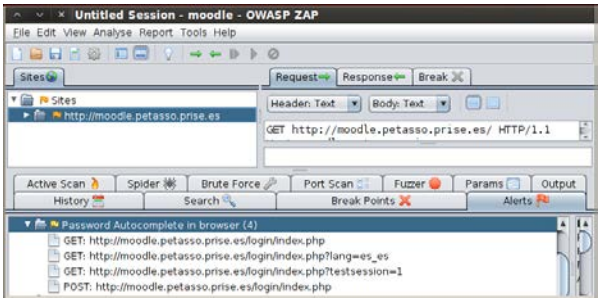


Estas son las URLs afectadas

http://wordpress.petasso.prise.es/wp-login.php
http://wordpress.petasso.prise.es/simplesaml/module.php/saml/sp/saml2-acs.php/default-sp
http://wordpress.petasso.prise.es/wp-login.php?redirect_to=http%3A%2F%2Fwordpress.petasso.prise.es%2Fwp-admin%2F&reauth=1
http://wordpress.petasso.prise.es/wp-login.php?redirect_to=http%3A%2F%2Fwordpress.petasso.prise.es%2Fwp-admin%2Foptions-writing.php&reauth=1
http://wordpress.petasso.prise.es/wp-login.php?action=logout&
http://wordpress.petasso.prise.es/wp-login.php?action=logout&_wpnonce=4277f7a7f4
http://wordpress.petasso.prise.es/simplesaml/module.php **

** Urls que derivan de esta

2.2.7. Pruebas "Password Autocomplete in Browser"

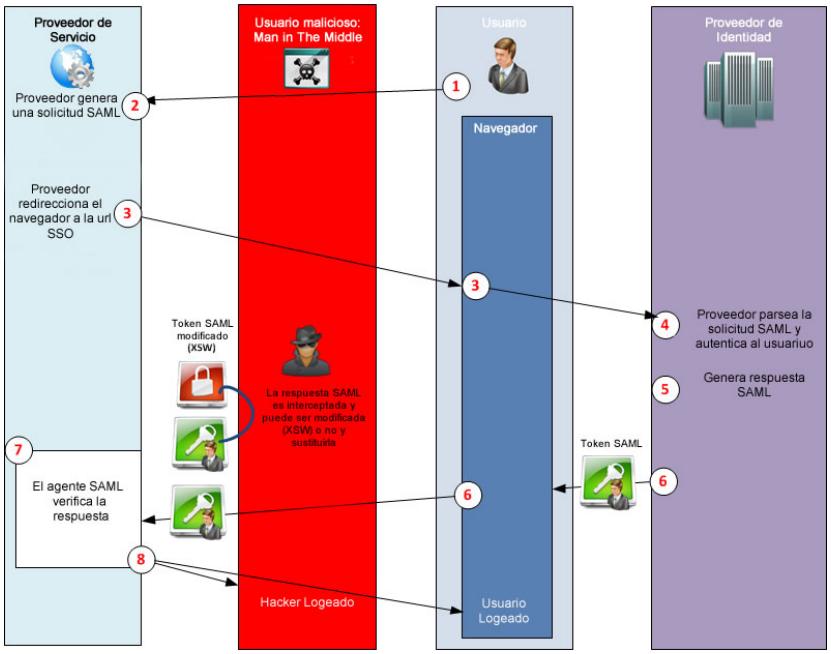


Estas son las URLs afectadas

http://moodle.petasso.prise.es/login/index.php
http://moodle.petasso.prise.es/login/index.php?lang=es_es
http://moodle.petasso.prise.es/login/index.php?testsession=1

2.3. Pruebas SAML

Si utilizamos un protocolo SAML que no esté adecuadamente securizado podemos ser susceptibles de recibir un ataque man-in-the-middle. Esto es que un usuario malicioso que fuera capaz de "escuchar" el tráfico que generamos podría utilizar el token generado por nuestro proveedor de identidad y validarse, a continuación un esquema de cómo funcionaría el ataque.

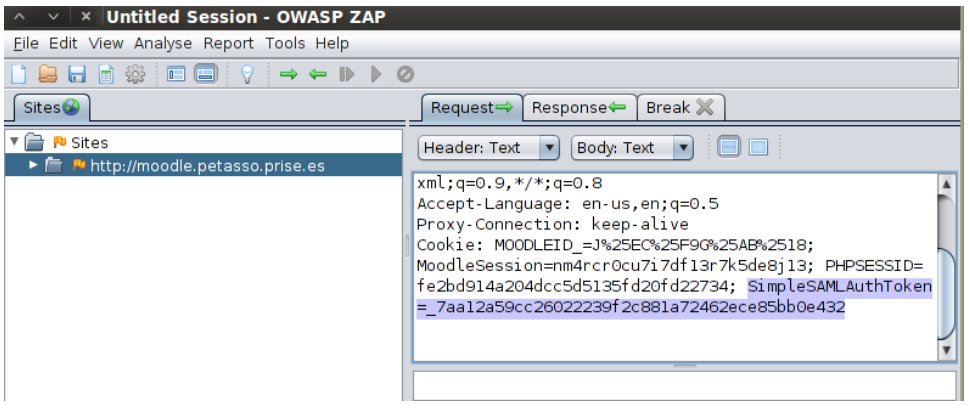


1. El usuario trata de autenticarse en el proveedor de servicio.
2. Éste genera una solicitud SAML al proveedor de identidad, que es donde se encuentran almacenados los usuarios dados de alta.
3. El proveedor redirecciona al navegador al proveedor de identidad.
4. Éste recibe la solicitud y hace la comprobación.
5. Genera la respuesta SAML.

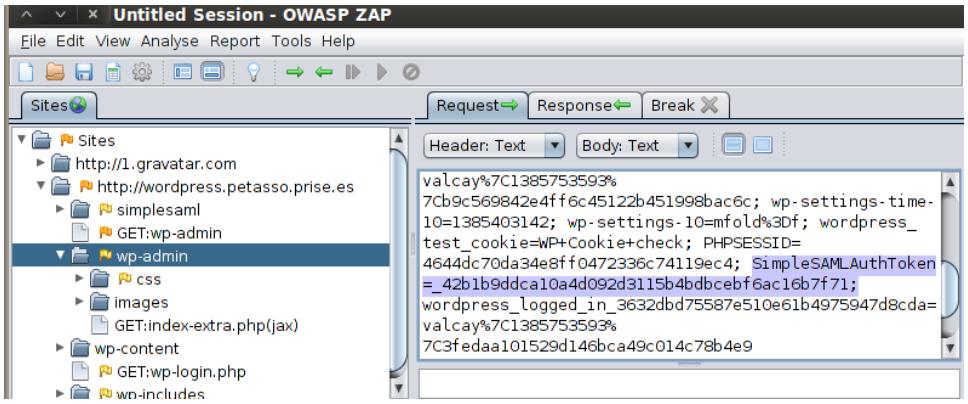
6. Envía token que sirve para comprobar que el usuario es el correcto. Es aquí donde el usuario malicioso a través de un ataque man-in-the-middle podría modificar la respuesta SAML.
7. El agente SAML verifica la respuesta ya modificada.
8. Y finalmente el usuario malintencionado se logearia.

Observando el tráfico de red con la herramienta Owasp Zap antes mencionada se ha detectado que, aunque esté encriptado, podemos acceder al token SAML. Lo cual podría suponer un riesgo ante el posible ataque antes mencionado. A continuación las evidencias de lo que se acaba de citar

Moodle



Wordpress



3. ANÁLISIS

Una vez obtenidos los resultados de las pruebas realizadas pasamos a realizar el análisis de los mismos, previamente se realizará también una revisión de las políticas.

3.1. Revisión de Políticas

En este punto se va a tratar de realizar una revisión de las políticas de seguridad de nuestro entorno respondiendo a las 5 preguntas citadas en la planificación de esta auditoría. What, Who, Why, Where, How. De la correcta definición de las mismas dependerán los tres pilares de la seguridad de la información, disponibilidad, integridad, confidencialidad.

3.1.1. Política vulnerabilidades de los Hosts

Ésta política hace referencia a la seguridad que tienen los hosts del entorno, desde la buena configuración de los puertos y la utilización de los elementos software y hardware necesarios hasta las actualizaciones del software y el propio sistema operativo. El responsable de emitir dicha política es el proveedor del servicio, en este caso la empresa Prise y los afectados son los usuarios de dicho servicio. Es relevante ya que para el correcto funcionamiento del servicio debemos mantener nuestro host a pleno rendimiento y minimizar las posibles amenazas. Afecta al host propiamente dicho y el activo de la información se protege con una buena configuración de puertos, software, hardware y manteniendo actualizados sistema operativo y aplicaciones.

3.1.2. Política vulnerabilidades de las Aplicaciones Web

En este caso nos referimos a las posibles vulnerabilidades de las aplicaciones web que son "XSS", "CSRF", "Clickjacking", "Sql Injection" y "File Intrusion". El responsable de emitir la política nuevamente es el proveedor de servicio y los afectados los usuarios del servicio. Esta política es relevante ya que de la seguridad de nuestra aplicaciones web depende que los datos de nuestros usuarios estén expuestos o no. Afecta al servicio y el activo de información en este caso es la información de los propios usuarios.

3.1.3. Política vulnerabilidades SAML

Finalmente ésta política hace referencia al protocolo utilizado en este sistema SSO, una buena configuración del mismo es fundamental para que la información de los usuarios no sea accesible por otros que puedan tener fines maliciosos. El responsable de emitir la política nuevamente vuelve a ser el proveedor del servicio y los afectados los usuarios del servicio. Afectará a la información de los usuarios principalmente, ésta será también el activo.

3.2. Revisión de la información de las pruebas

En este apartado se va a realizar un análisis de los resultados obtenidos en las pruebas realizadas sobre el entorno auditado.

3.2.1. Revisión pruebas Hosts

La herramienta nessus nos proporciona una información detallada de las vulnerabilidades relacionadas con cada puerto que se ha detectado abierto en los hosts analizados. En primer lugar se va a dar una descripción de los plugins, con su impacto.

Nessus Scan Information

Simplemente hace referencia a la información del escaneo como la versión del plugin, el tipo de escaneo, el puerto…

Host Fully Qualified Domain Name (FQDN) Resolution

Es posible resolver el nombre del host, no hay riesgo por lo que no es necesario aplicar una solución.

Traceroute Information

Es pssible obtener información de traceroute, no comporta riesgo y no es necesario aplicar ninguna solución.

Common Platform Enumeration (CPE)

Es posible enumerar los nombres de algún hardware y software del equipo remoto, no comporta riesgo y no es necesaria ninguna solución.

Inconsistent Hostname and IP Address

El nombre del host remoto no es consistente con la información DNS, el nombre de la máquina no resuelve o resuelve a una IP diferente. No hay riesgo pero se podría solucionar reparando el DNS inverso o el fichero de host.

Service Detection

Es posible detectar el servicio remoto, no hay riesgo ni es necesaria ninguna solución.

SSH Server CBC Mode Ciphers Enabled

El servidor ssh está configurado para utilizar Cipher Block Chaining, esto permitiría a un atacante recuperar el mensaje en texto plano de un mensaje cifrado. El riesgo es bajo y la solución pasaría pos desactivar el modo CBC y activar los modos CTR o GCM de encriptación.

SSH Algorithms and Languages Supported

Detecta qué algoritmos y lenguajes son soportados por el servicio remoto para encriptar las comunicaciones.

HyperText Transfer Protocol (HTTP) Information

Es possible extraer alguna información de la configuración HTTP remota. NO hay riesgo ni es necesaria ninguna solución.

HTTP Server Type and Version

Simplemente checkea si hay un servidor web corriendo en la máquina, no supone ningún riesgo ni es necesaria ninguna solución.

Backported Security Patch Detection (SSH)

Comprueba si se detecta algún parche de seguridad se ha aplicado a versiones anteriores de SSH y no se ha cambiado el número de la versión. Es meramente informativo, no hay riesgo alguno.

Open Port Re-check

Uno de los puertos que previamente estaban abiertos no lo están actualmente o no responden. Esto puede deberse a diferentes razones pero no comporta ningún riesgo y en todo caso habría que hacer modificaciones en la herramienta de escaneo nessus no en el host.

SSH Server Type and Version Information

Comprueba si es posible obtener información acerca del servidor SSH remoto enviando un petición de autentificación vacía. No supone ningún riesgo ni es necesaria ninguna corrección.

PHP Version

Se intenta obtener el número de versión de la instalación PHP remota. No supone un riesgo ni es necesaria una solución.

DNS Server Detection

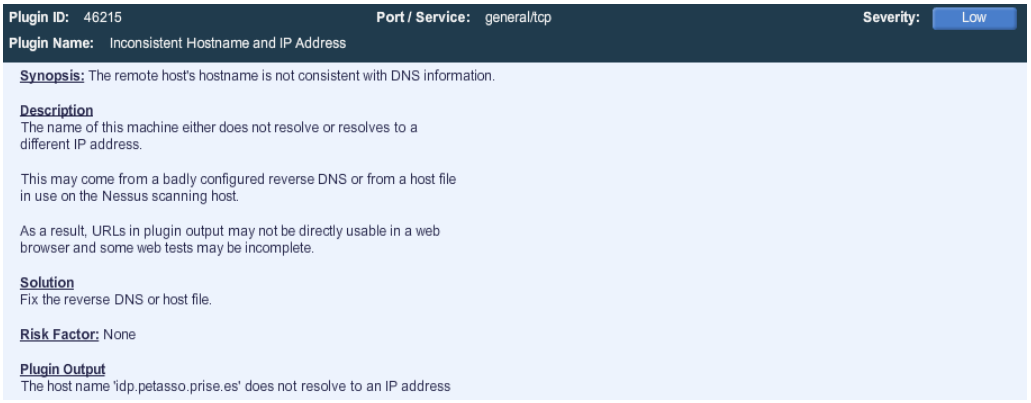
Detecta si hay un servidor DNS (Domain Name System) corriendo en el host. Este servicio realiza un mapeo entre nombres de host y direcciones ip. No hay ningún factor de riesgo pero sería recomendable deshabilitar el servicio en caso de que no sea necesario.

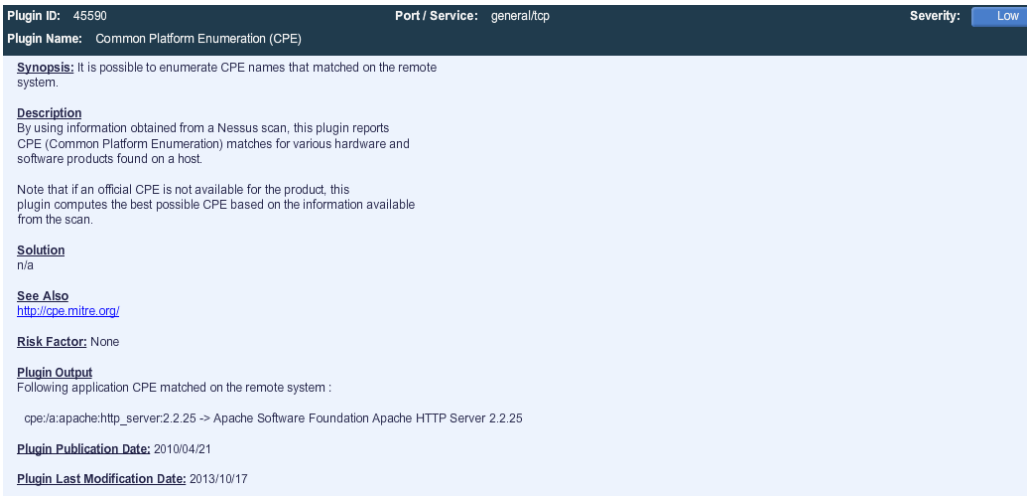
SSH Protocol Versions Supported

Se comprueba las versiones soportadas por el protocolo ssh para el demonio ssh remoto. Es informativo, sin riesgo.

Ahora vamos a asociar dichos plugins a los puertos donde se han encontrado hallazgos.

Puerto 0/tcp





Puerto 0/udp

Puerto 22/tcp

Plugin ID: 70657 **Port / Service:** ssh (22/tcp) **Severity:** Low

Plugin Name: SSH Algorithms and Languages Supported

Synopsis: An SSH server is listening on this port.

Description
This script detects which algorithms and languages are supported by the remote service for encrypting communications.

Solution
n/a

Risk Factor: None

Plugin Output
Nessus negotiated the following encryption algorithm with the server : aes128-cbc

The server supports the following options for kex_algorithms :

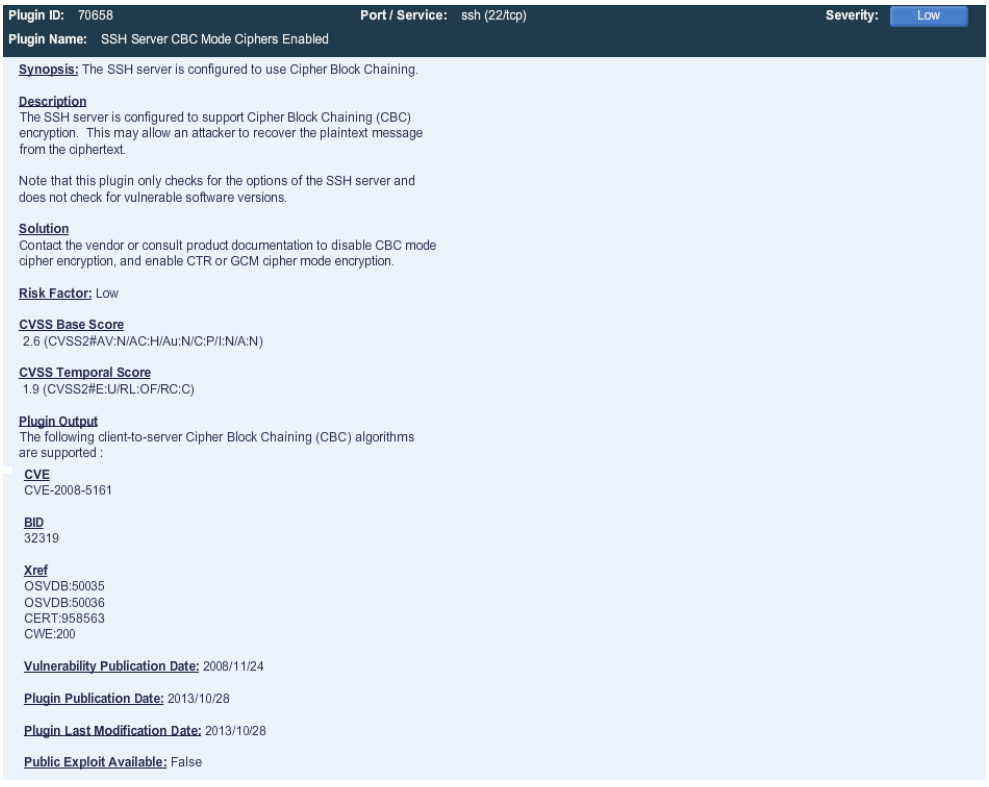
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1

The server supports the following options for server_host_key_algorithms :

ssh-dss
ssh-rsa

Plugin Publication Date: 2013/10/28

Plugin Last Modification Date: 2013/10/28



Plugin ID: 70658 **Port / Service:** ssh (22/tcp) **Severity:** Low

Plugin Name: SSH Server CBC Mode Ciphers Enabled

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description
The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution
Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor: Low

CVSS Base Score
2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score
1.9 (CVSS2#E:U/RL:OF/RC:C)

Plugin Output
The following client-to-server Cipher Block Chaining (CBC) algorithms are supported :

CVE
CVE-2008-5161

BID
32319

Xref
OSVDB:50035
OSVDB:50036
CERT:958563
CWE:200

Vulnerability Publication Date: 2008/11/24

Plugin Publication Date: 2013/10/28

Plugin Last Modification Date: 2013/10/28

Public Exploit Available: False

Plugin ID: 39520 **Port / Service:** ssh (22/tcp) **Severity:** Low

Plugin Name: Backported Security Patch Detection (SSH)

Synopsis: Security patches are backported.

Description
Security patches may have been 'backported' to the remote SSH server without changing its version number.

Banner-based checks have been disabled to avoid false positives.

Note that this test is informational only and does not denote any security problem.

Solution
n/a

See Also
http://www.nessus.org/u?d636c8c7

Risk Factor: None

Plugin Output
Give Nessus credentials to perform local checks.

Plugin Publication Date: 2009/06/25

Plugin Last Modification Date: 2013/04/03

Plugin ID: 70658 **Port / Service:** ssh (22/tcp) **Severity:** Low

Plugin Name: SSH Server CBC Mode Ciphers Enabled

Synopsis: The SSH server is configured to use Cipher Block Chaining.

Description
The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Solution
Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Risk Factor: Low

CVSS Base Score
2.6 (CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N)

CVSS Temporal Score
1.9 (CVSS2#E:U/RL:OF/RC:C)

Plugin Output
The following client-to-server Cipher Block Chaining (CBC) algorithms are supported :

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

CVE
CVE-2008-5161

BID
32319

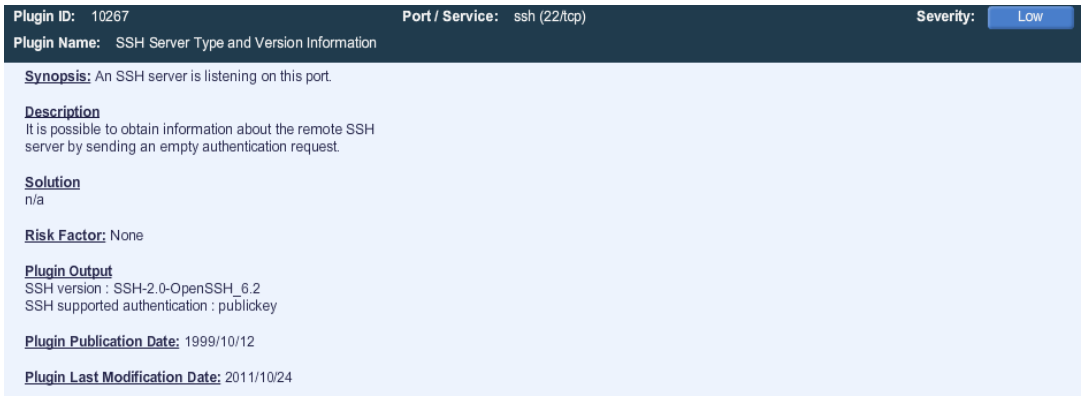
Xref
OSVDB:50035
OSVDB:50036
CERT:958563
CWE:200

Vulnerability Publication Date: 2008/11/24

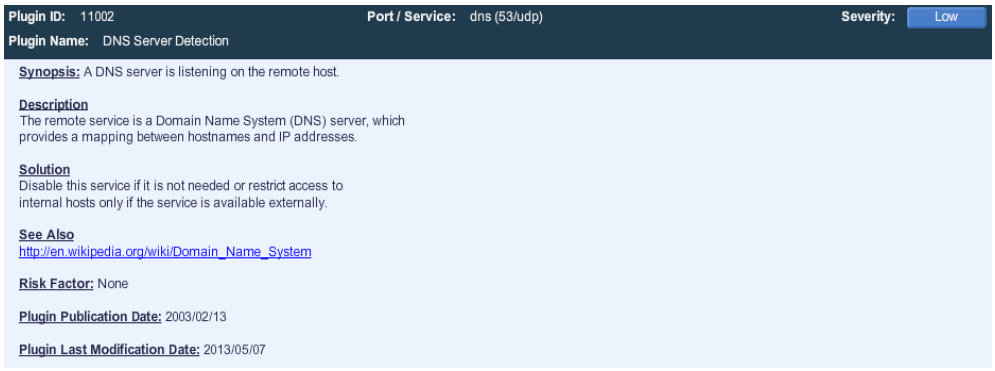
Plugin Publication Date: 2013/10/28

Plugin Last Modification Date: 2013/10/28

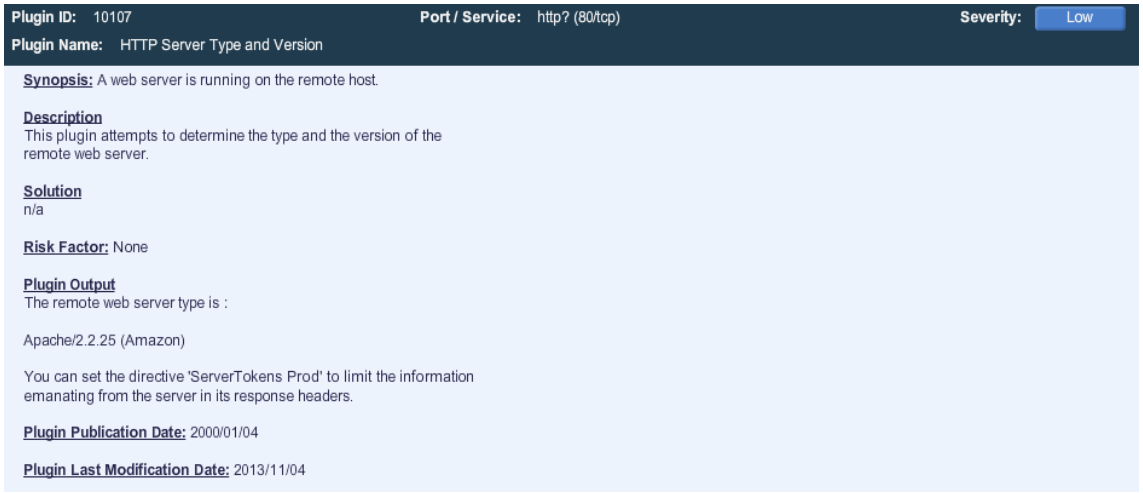
Public Exploit Available: False

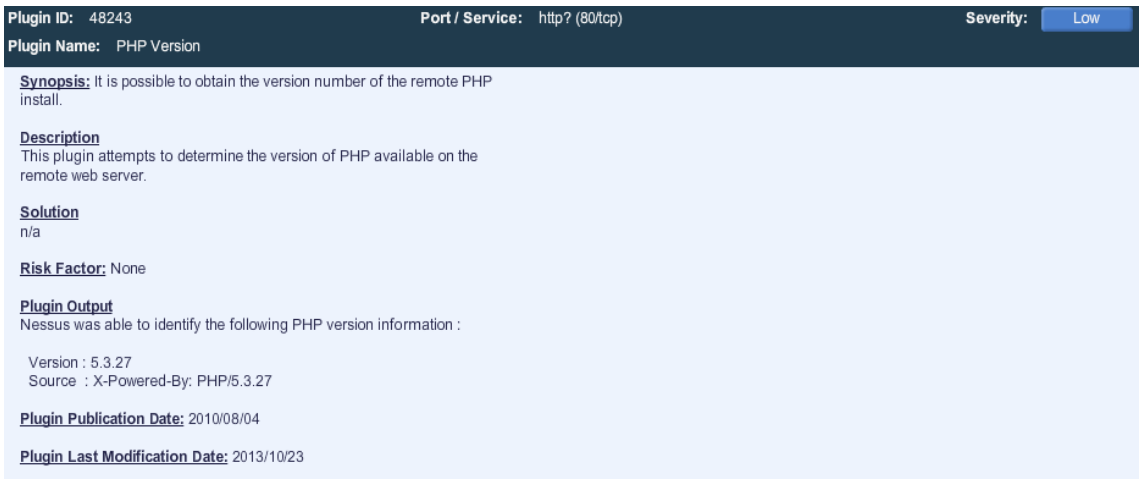


Puerto 53/udp



Puerto 80/tcp





3.2.2. Revisión pruebas "XSS"

Debido a un error en la programación del entorno web se ha detectado ésta vulnerabilidad en tres enlaces, esto implica la posibilidad de ejecutar código JavaScript malicioso en nuestro entorno, lo cual podría resultar potencialmente peligroso. A continuación el análisis del riesgo, solución e impacto.

Riesgo Alto

Solución Realizar un filtrado de los datos que se pueden introducir en el navegador para que no sea posible inyectar código JavaScript.

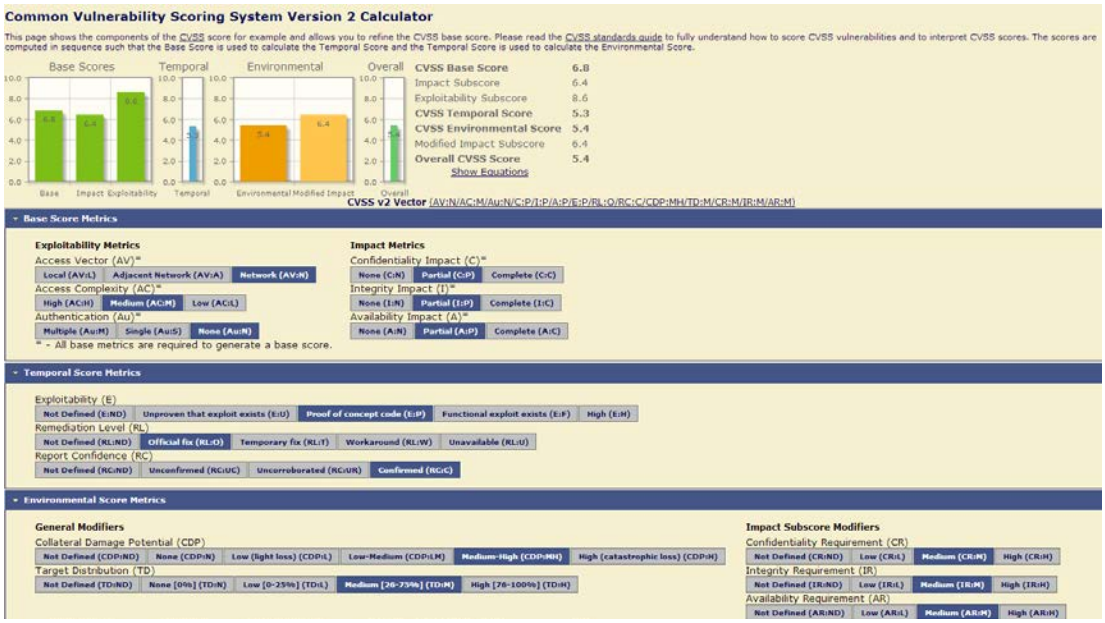
Impacto Puntuación Base: 6.8 → Acceso de red, Complejidad media de acceso y no es necesaria autenticación. Confidencialidad, integridad y disponibilidad parcialmente afectadas.

Puntuación Temporal: 5.3 → Hay prueba del aprovechamiento de la vulnerabilidad, hay solución oficial, y las evidencias están confirmadas.

Puntuación de Entorno: 5.4 → Daños colaterales medio-alto, distribución del objetivo medio, confidencialidad, integridad y disponibilidad medio.

Puntuación General: 5.4 → Es una puntuación no excesivamente elevada por lo que no supone un impacto alto, pero si lo suficiente como para tener esta vulnerabilidad muy en cuenta.

A continuación una captura de lo que se acaba de describir.



3.2.3. Revisión pruebas "CSRF"

Si en XSS explota la confianza que tiene el usuario en el sitio web, CSRF explota la confianza que tiene el sitio web en el usuario. En este caso un usuario logeado podría ejecutar comandos maliciosos.

Riesgo Medio

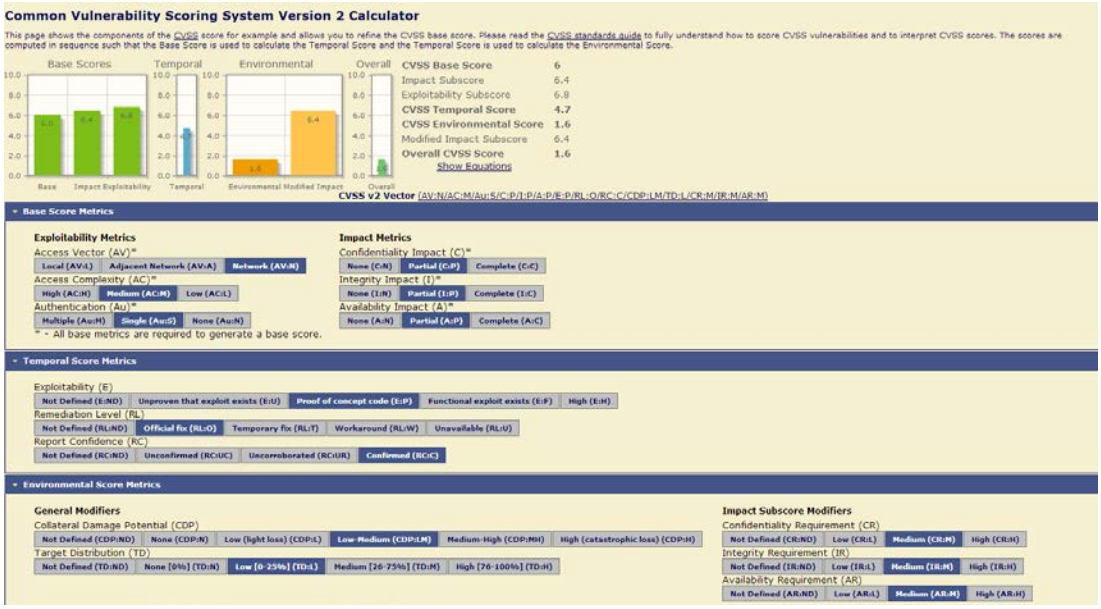
Solución Asociar un identificador único para que podamos verificarlo en cada acción.

Impacto Puntuación Base: 6 → Acceso de red, complejidad de acceso media y requiere autenticación simple. Confidencialidad, integridad y disponibilidad parcialmente afectadas.

Puntuación Temporal: 4.7 → Hay prueba del aprovechamiento de la vulnerabilidad, hay solución oficial, y las evidencias están confirmadas.

Puntuación de Entorno: 1.6 → Daños colaterales medio-alto, distribución del objetivo bajo, confidencialidad, integridad y disponibilidad medio.

Puntuación General: 1.6 → El hecho de que la distribución del objetivo sea baja ha hecho que la puntuación general baje hasta 1.6 con lo cual nos encontramos ante una vulnerabilidad con un impacto bajo.



3.2.4. Revisión pruebas "Clickjacking"

Se ha detectado que las opciones X-Frame de la cabecera de una serie de páginas del entorno no está configurada, lo cual podría provocar que se utilizará la técnica de Clickjacking. Lo que permitiría colocar ventanas ocultas en lugares de la página donde aparentemente hay un botón o un menú, pero en lugar de ejecutar la acción deseada se ejecutaría la de la ventana oculta.

Riesgo Bajo

Solución Configurar las opciones X-Frame para evitar ese suceso.

Impacto Puntuación Base: 4.9 → Acceso de red, complejidad de acceso media y requiere autenticación simple. Integridad y disponibilidad parcialmente afectadas. La confidencialidad en este caso no está afectada.

Puntuación Temporal: 3.8 → Hay prueba del aprovechamiento de la vulnerabilidad, hay solución oficial, y las evidencias están confirmadas.

Puntuación de Entorno: 0.8 → Daños colaterales bajo, distribución del objetivo bajo, confidencialidad, integridad y disponibilidad bajo.

Puntuación General: 0.8 → De nuevo la puntuación de entorno ha hecho bajar la puntuación general a 0.8 por lo que el impacto es bajo.

Aquí la captura.

3.2.5. Revisión pruebas "Sql Injection"

El resultado de este test ha sido negativo con lo cual no hay riesgo alguno.

3.2.6. Revisión pruebas "File Intrusión"

Al igual que la anterior vulnerabilidad ésta no presenta ningún riesgo al no haberse encontrado ninguna.

3.2.7. Revisión "Session Fixation"

Se han detectado que en ambos entornos existe esta vulnerabilidad para una serie de urls ya que la cookie de sesión ha sido enviada sin el HttpOnlyFlag, lo cual puede propiciar que dicha cookie sea accedida mediante JavaScript de tal modo que es posible acceder a ella o modificarla al antojo de un atacante.

Riesgo Medio

Solución Habilitar HttpOnlyFlag.

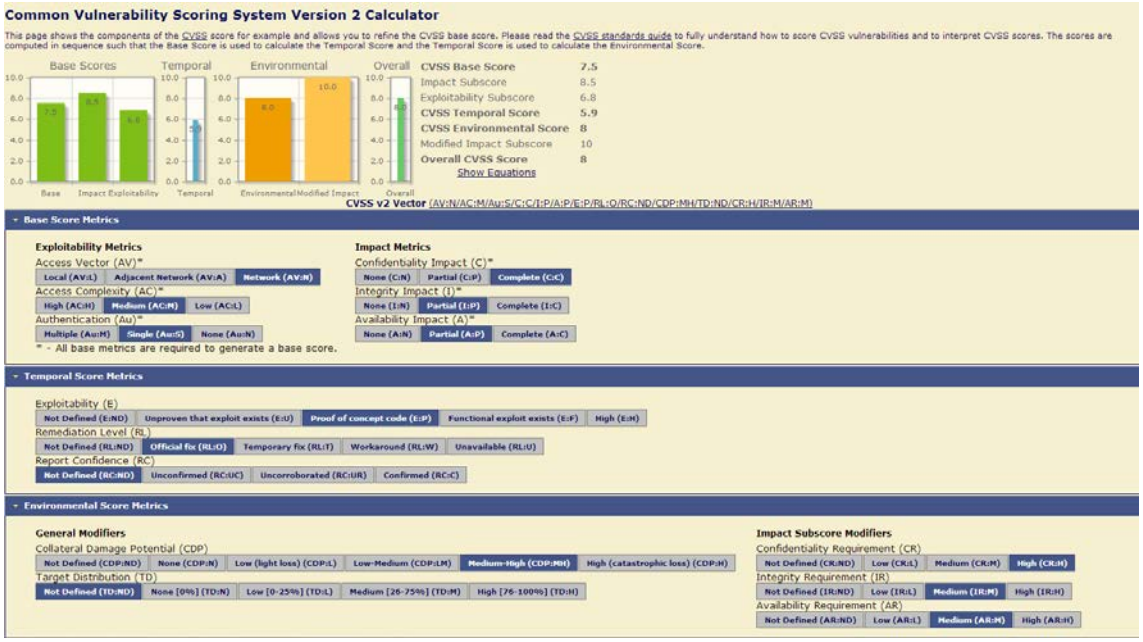
Impacto Puntuación Base: 7.5 → Acceso de red, complejidad de acceso media y requiere autenticación simple. Integridad y disponibilidad parcialmente afectadas (depende del nivel de privilegio del usuario). La confidencialidad afectada completamente.

Puntuación Temporal: 5.9 → Hay prueba del aprovechamiento de la vulnerabilidad y hay solución oficial.

Puntuación de Entorno: 8 → Daños colaterales medio, confidencialidad alto, integridad y disponibilidad medio.

Puntuación General: 8 → El alto impacto que puede tener sobre el entorno ha hecho que suba la media de la puntuación general por lo que estamos ante una vulnerabilidad con un impacto elevado.

Aquí la captura.



3.2.8. Revisión "Password Autocomplete in Browser"

El atributo autocompletar no está deshabilitado en el input de formulario html que contiene el password de login, Éste podría ser restaurado en el navegador y utilizado para autenticarse.

Riesgo Bajo

Solución Deshabilitar Autocompletado.

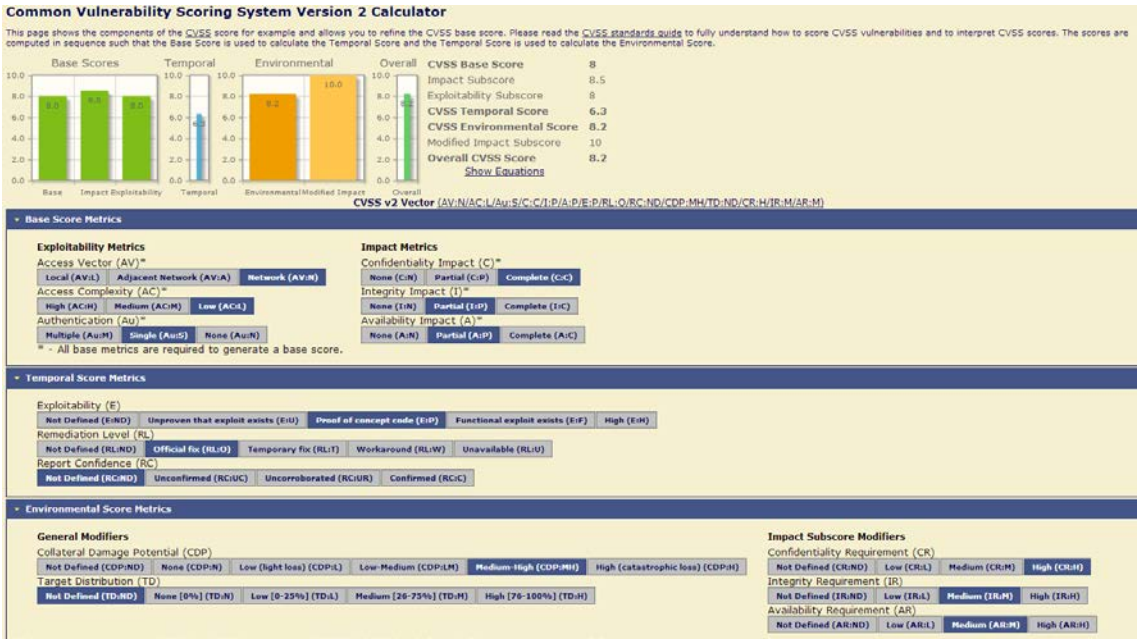
Impacto Puntuación Base: 8 → Acceso de red, complejidad de acceso baja y requiere autenticación simple. Integridad y disponibilidad parcialmente afectadas (depende del nivel de privilegio del usuario). La confidencialidad afectada completamente.

Puntuación Temporal: 6.3 → Hay prueba del aprovechamiento de la vulnerabilidad y hay solución oficial.

Puntuación de Entorno: 8.2 → Daños colaterales medio, confidencialidad alto, integridad y disponibilidad medio.

Puntuación General: 8.2 → A pesar de que el riesgo de esta vulnerabilidad es bajo el impacto es alto por la facilidad de acceso y los altos daños colaterales.

A continuación la captura de dicho impacto.



3.2.9. Revisión pruebas SAML

Se ha demostrado que debido a que el token de SAML está accesible en caso de que podamos acceder al tráfico de red el sistema es susceptible de sufrir un ataque man-in-the-middle. A continuación se detallan riesgo, soluciones e impacto de este hallazgo.

Riesgo Alto

Soluciones La librería SAML debe validar los mensajes de respuesta contra los esquemas SAML aplicados.

La librería SAML debe respetar el orden y la posición de los elementos firmados y ejecutados en el árbol de mensajes. Si no, esto podría forzar a los módulos de procesamiento a tener vistas de datos inconsistentes.

La librería SAML debe tener firmas de validación.

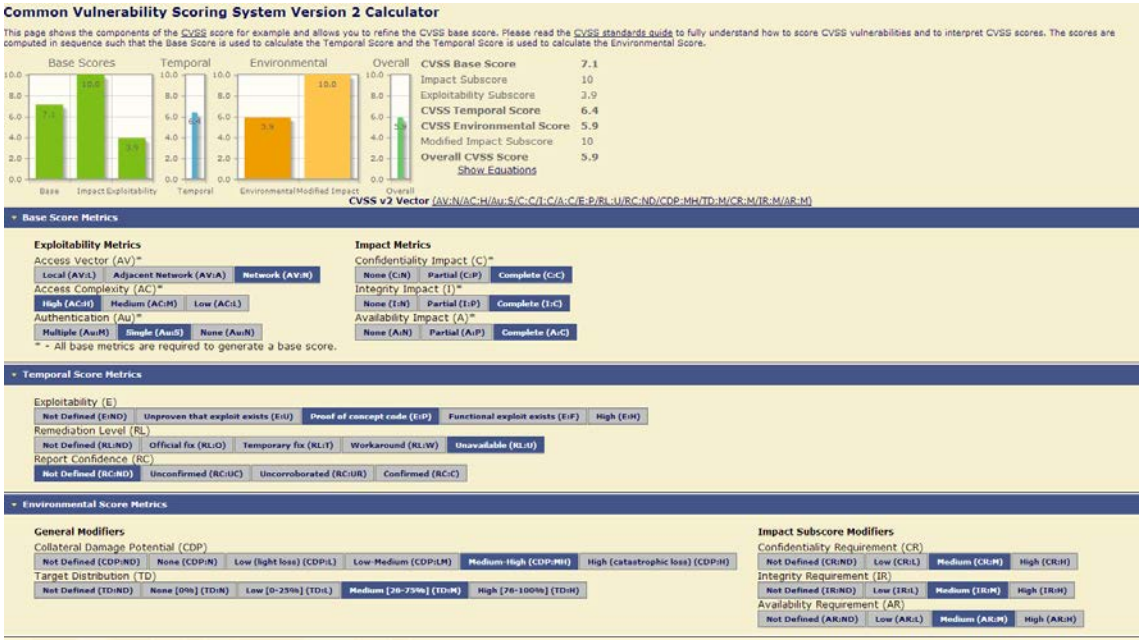
La librería SAML tiene que comprobar que la firma fue creada con una clave de confianza

Impacto Puntuación Base: 7.1 → Acceso de red, complejidad de acceso alta y requiere autenticación simple. Integridad, disponibilidad y confidencialidad completamente afectadas.

Puntuación Temporal: 6.4 → Hay prueba del aprovechamiento de la vulnerabilidad, solución oficial no disponible y evidencias no definidas.

Puntuación de Entorno: 5.9 → Daños colaterales medio-alto, distribución del objetivo medio, confidencialidad, integridad y disponibilidad medio.

Puntuación General: 5.9 → El impacto en este caso tiene una puntuación a tener muy en cuenta siendo de grado medio.



4. RESUMEN EJECUTIVO

En este apartado vamos se va a dar una visión general de la metodología empleada, las principales conclusiones que se hayan obtenido y las recomendaciones más relevantes que se puedan hacer. Asimismo contendrá tanto las fortalezas como las debilidades o fallos detectados.

4.1. Visión general de la metodología empleada

En primer lugar se ha estudiado el entorno que íbamos a auditar para posteriormente poder establecer un catálogo de posibles vulnerabilidades que podrían afectarnos y finalmente decidir qué herramientas utilizar para realizar las pruebas e auditoría y el análisis.

Con toda esta información obtenida podemos obtener una serie de conclusiones y recomendaciones.

4.2. Conclusiones y Recomendaciones

Las vulnerabilidades detectadas en relación a los puertos abiertos en los hosts no revisten una gran importancia porque ni el riesgo ni el impacto que ello supondría son elevados, aunque sí conviene tener presente la situación en la que se encuentran los hosts.

En cuanto a las vulnerabilidades relacionadas con las aplicaciones web debemos prestar especialmente atención a las vulnerabilidades CSRF y XSS encontradas por si moderado o elevado riesgo y tomar las medidas indicadas en el apartado de análisis. La vulnerabilidad Session Fixation supone una de las vulnerabilidades encontradas más críticas ya que tiene un riesgo medio y un impacto elevado para ello es fundamental habilitar HttpOnlyFlag como ya se indicó en el apartado de análisis. En cuanto a la vulnerabilidad “Password Autocomplete in Browser”, a pesar de que el riesgo es bajo ya que sería necesaria una presencia física de la persona que pudiera aprovechar la vulnerabilidad, el impacto es elevado y es importante que tomemos la medida de deshabilitar el autocompletado como también se ha indicado.

Finalmente debemos hacer especial hincapié en lo relacionado a la accesibilidad del token del protocolo SAML y estudiar la posibilidad de utilizar una encriptación lo más segura posible o estudiar la posibilidad de utilizar alguna tecnología en combinación con SAML como puede ser la OTP (One Time Password) que reforzara la inquebrantabilidad de nuestro sistema.

Asimismo se recomienda tener siempre actualizados a la última versión los CMS así como sus plugins y componentes. De este modo tendremos resueltas todas las vulnerabilidades conocidas.

4.3. Fortalezas y Debilidades

Las principales fortalezas de nuestro sistema son

- El buen grado de seguridad detectado en las bases de datos al no haber encontrado ninguna vulnerabilidad.
- La buena configuración de los puertos de los hosts dejando únicamente los imprescindibles abiertos imposibilitando el aprovechamiento de alguna vulnerabilidad con más riesgo de las encontradas.

En contrapartida estas son las debilidades detectadas:

- Se han detectado una mala configuración y/o programación en las aplicaciones web lo cual da a lugar el tener las vulnerabilidades mencionadas en este informe.

- Un nivel bajo de securización del token de SAML lo cual puede propiciar un ataque man-in-the-middle, como ya se ha explicado con anterioridad.

5. METODOLOGÍA EMPLEADA

La metodología empleada se ha basado en realizar análisis con diferentes herramientas del entorno que nos ocupa así como de los diferentes hosts y del protocolo SAML, estas son las herramientas empleadas que nos proporciona la distribución Backtrack.

- nmap: Es una herramienta que nos permite realizar un rastreo de puertos del host que nosotros pasemos como parámetro, así mismo podeos indicarle el tipo de rastreo que queremos que realice así como el rango de puertos que deseamos escanear.

- nessus: Al igual que nmap, nessus realiza un escaneo de puertos pero mucho más exhaustivo, ya que utiliza una serie de plugins para evaluar las posibles vulnerabilidades que podrían afectar a los puertos que encuentre abiertos.

- owasp zap (Zed Attack Proxy): Se trata de una herramienta de testeo de vulnerabilidades de aplicaciones web. Una vez configurado correctamente el proxy, podemos realizar un análisis en profundidad de las aplicaciones web que nosotros deseemos, facilitándonos una información extensa y útil.

- sqlmap: Finalmente esta herramienta realiza un escaneo en busca de vulnerabilidades relacionadas con las bases de datos.

Una vez realizadas dichas pruebas se ha realizado la fase de análisis indicando, riesgo, posibles soluciones e impacto. Para calcular el impacto se ha utilizado la calculadora que nos proporciona el nist (National Institute of Standards and Technology)

- NVD CVSS v2 Calculator: Nos permite realizar una evaluación del impacto que tendría el aprovechamiento de una vulnerabilidad teniendo en cuenta.
    - Puntuación Base
        - Tipo de acceso
        - Complejidad de Acceso
        - Tipo de Autenticación
        - Métrica de disponibilidad, confidencialidad e integridad.
    - Puntuación Temporal
        - Tipo de exploit
        - Nivel de remedio de los daños ocasionados
        - Confirmación del reporte
    - Puntuación de Entorno
        - Daños colaterales
        - Distribución del objetivo
        - Impacto de confidencialidad, disponibilidad e integridad.

6. LICENCIA CREATIVE COMMONS

Reconocimiento — Debe reconocer adecuadamente la autoría, proporcionar un enlace a la licencia http://creativecommons.org/licenses/by-nc-sa/4.0/legalcode indicar si se han realizado cambios. Puede hacerlo de cualquier manera razonable, pero no de una manera que sugiera que tiene el apoyo del licenciador o lo recibe por el uso que hace.

NoComercial — No puede utilizar el material para una finalidad comercial.

CompartirIgual — Si remezcla, transforma o crea a partir del material, deberá difundir sus contribuciones bajo la misma licencia que el original.

No additional restrictions — No puede aplicar términos legales o medidas tecnológicas que legalmente restrinja realizar aquello que la licencia permite.

Creative Commons Corporation ("Creative Commons") is not a law firm and does not provide legal services or legal advice. Distribution of Creative Commons public licenses does not create a lawyer-client or other relationship. Creative Commons makes its licenses and related information available on an "as-is" basis. Creative Commons gives no warranties regarding its licenses, any material licensed under their terms and conditions, or any related information. Creative Commons disclaims all liability for damages resulting from their use to the fullest extent possible.

Using Creative Commons Public Licenses

Creative Commons public licenses provide a standard set of terms and conditions that creators and other rights holders may use to share original works of authorship and other material subject to copyright and certain other rights specified in the public license below. The following considerations are for informational purposes only, are not exhaustive, and do not form part of our licenses.

Considerations for licensors: Our public licenses are intended for use by those authorized to give the public permission to use material in ways otherwise restricted by copyright and certain other rights. Our licenses are irrevocable. Licensors should read and understand the terms and conditions of the license they choose before applying it. Licensors should also secure all rights necessary before applying our licenses so that the public can reuse the material as expected. Licensors should clearly mark any material not subject to the license. This includes other CC-licensed material, or material used under an exception or limitation to copyright. More considerations for licensors.

Considerations for the public: By using one of our public licenses, a licensor grants the public permission to use the licensed material under specified terms and conditions. If the licensor's permission is not necessary for any reason–for example, because of any applicable exception or limitation to copyright–then that use is not regulated by the license. Our licenses grant only permissions under copyright and certain other rights that a licensor has authority to grant. Use of the licensed material may still be restricted for other reasons, including because others have copyright or other rights in the material. A licensor may make special requests, such as asking that all changes be marked or described. Although not required by our licenses, you are encouraged to respect those requests where reasonable. More considerations for the public.

Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License

By exercising the Licensed Rights (defined below), You accept and agree to be bound by the terms and conditions of this Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License ("Public License"). To the extent this Public License may be interpreted as a contract, You are granted the Licensed Rights in consideration of Your acceptance of these terms and conditions, and the Licensor grants You such rights in consideration of benefits the Licensor receives from making the Licensed Material available under these terms and conditions.

Section 1 – Definitions.

a. **Adapted Material** means material subject to Copyright and Similar Rights that is derived from or based upon the Licensed Material and in which the Licensed Material is translated, altered, arranged, transformed, or otherwise modified in a manner requiring permission under the Copyright and Similar Rights held by the Licensor. For purposes of this Public License, where the Licensed Material is a musical work, performance, or sound recording, Adapted Material is always produced where the Licensed Material is synched in timed relation with a moving image.

b. **Adapter's License** means the license You apply to Your Copyright and Similar Rights in Your contributions to Adapted Material in accordance with the terms and conditions of this Public License.

c. **BY-NC-SA Compatible License** means a license listed at creativecommons.org/compatiblelicenses, approved by Creative Commons as essentially the equivalent of this Public License.

d. **Copyright and Similar Rights** means copyright and/or similar rights closely related to copyright including, without limitation, performance, broadcast, sound recording, and Sui Generis Database Rights, without regard to how the rights are labeled or categorized. For purposes of this Public License, the rights specified in Section 2(b)(1)-(2) are not Copyright and Similar Rights.

e. **Effective Technological Measures** means those measures that, in the absence of proper authority, may not be circumvented under laws fulfilling obligations under Article 11 of the WIPO Copyright Treaty adopted on December 20, 1996, and/or similar international agreements.

f. **Exceptions and Limitations** means fair use, fair dealing, and/or any other exception or limitation to Copyright and Similar Rights that applies to Your use of the Licensed Material.

g. **License Elements** means the license attributes listed in the name of a Creative Commons Public License. The License Elements of this Public License are Attribution, NonCommercial, and ShareAlike.

h. **Licensed Material** means the artistic or literary work, database, or other material to which the Licensor applied this Public License.

i. **Licensed Rights** means the rights granted to You subject to the terms and conditions of this Public License, which are limited to all Copyright and Similar Rights that apply to Your use of the Licensed Material and that the Licensor has authority to license.

j. **Licensor** means the individual(s) or entity(ies) granting rights under this Public License.

k. **NonCommercial** means not primarily intended for or directed towards commercial advantage or monetary compensation. For purposes of this Public License, the exchange of the Licensed Material for other material subject to Copyright and Similar Rights by digital file-sharing or similar means is NonCommercial provided there is no payment of monetary compensation in connection with the exchange.

l. **Share** means to provide material to the public by any means or process that requires permission under the Licensed Rights, such as reproduction, public display, public performance, distribution, dissemination, communication, or importation, and to make material available to the public including in ways that members of the public may access the material from a place and at a time individually chosen by them.

m. **Sui Generis Database Rights** means rights other than copyright resulting from Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, as amended and/or succeeded, as well as other essentially equivalent rights anywhere in the world.

n. **You** means the individual or entity exercising the Licensed Rights under this Public License. **Your** has a corresponding meaning.

Section 2 – Scope.

a. **License grant**.

1. Subject to the terms and conditions of this Public License, the Licensor hereby grants You a worldwide, royalty-free, non-sublicensable, non-exclusive, irrevocable license to exercise the Licensed Rights in the Licensed Material to:

A. reproduce and Share the Licensed Material, in whole or in part, for NonCommercial purposes only; and

B. produce, reproduce, and Share Adapted Material for NonCommercial purposes only.

2. Exceptions and Limitations. For the avoidance of doubt, where Exceptions and Limitations apply to Your use, this Public License does not apply, and You do not need to comply with its terms and conditions.

3. Term. The term of this Public License is specified in Section 6(a).

4. Media and formats; technical modifications allowed. The Licensor authorizes You to exercise the Licensed Rights in all media and formats whether now known or hereafter created, and to make technical modifications necessary to do so. The Licensor waives and/or agrees not to assert any right or authority to forbid You from making technical modifications necessary to exercise the Licensed Rights, including technical modifications necessary to circumvent Effective Technological Measures. For purposes of this Public License, simply making modifications authorized by this Section 2(a)(4) never produces Adapted Material.

5. Downstream recipients.

A. Offer from the Licensor – Licensed Material. Every recipient of the Licensed Material automatically receives an offer from the Licensor to exercise the Licensed Rights under the terms and conditions of this Public License.

B. Additional offer from the Licensor – Adapted Material. Every recipient of Adapted Material from You automatically receives an offer from the Licensor to exercise the Licensed Rights in the Adapted Material under the conditions of the Adapter's License You apply.

C. No downstream restrictions. You may not offer or impose any additional or different terms or conditions on, or apply any Effective Technological Measures to, the Licensed Material if doing so restricts exercise of the Licensed Rights by any recipient of the Licensed Material.

6. No endorsement. Nothing in this Public License constitutes or may be construed as permission to assert or imply that You are, or that Your use of the Licensed Material is, connected with, or sponsored, endorsed, or granted official status by, the Licensor or others designated to receive attribution as provided in Section 3(a)(1)(A)(i).

b. **Other rights**.

1. Moral rights, such as the right of integrity, are not licensed under this Public License, nor are publicity, privacy, and/or other similar personality rights; however, to the extent possible, the Licensor waives and/or agrees not to assert any such rights held by the Licensor to the limited extent necessary to allow You to exercise the Licensed Rights, but not otherwise.
2. Patent and trademark rights are not licensed under this Public License.
3. To the extent possible, the Licensor waives any right to collect royalties from You for the exercise of the Licensed Rights, whether directly or through a collecting society under any voluntary or waivable statutory or compulsory licensing scheme. In all other cases the Licensor expressly reserves any right to collect such royalties, including when the Licensed Material is used other than for NonCommercial purposes.

Section 3 – License Conditions.

Your exercise of the Licensed Rights is expressly made subject to the following conditions.

a. **Attribution**.

1. If You Share the Licensed Material (including in modified form), You must:
   A. retain the following if it is supplied by the Licensor with the Licensed Material:
      i. identification of the creator(s) of the Licensed Material and any others designated to receive attribution, in any reasonable manner requested by the Licensor (including by pseudonym if designated);
      ii. a copyright notice;
      iii. a notice that refers to this Public License;
      iv. a notice that refers to the disclaimer of warranties;
      v. a URI or hyperlink to the Licensed Material to the extent reasonably practicable;
   B. indicate if You modified the Licensed Material and retain an indication of any previous modifications; and
   C. indicate the Licensed Material is licensed under this Public License, and include the text of, or the URI or hyperlink to, this Public License.
2. You may satisfy the conditions in Section 3(a)(1) in any reasonable manner based on the medium, means, and context in which You Share the Licensed Material. For example, it may be reasonable to satisfy the conditions by providing a URI or hyperlink to a resource that includes the required information.

3. If requested by the Licensor, You must remove any of the information required by Section 3(a)(1)(A) to the extent reasonably practicable.

b. **ShareAlike**.

In addition to the conditions in Section 3(a), if You Share Adapted Material You produce, the following conditions also apply.

1. The Adapter's License You apply must be a Creative Commons license with the same License Elements, this version or later, or a BY-NC-SA Compatible License.
2. You must include the text of, or the URI or hyperlink to, the Adapter's License You apply. You may satisfy this condition in any reasonable manner based on the medium, means, and context in which You Share Adapted Material.
3. You may not offer or impose any additional or different terms or conditions on, or apply any Effective Technological Measures to, Adapted Material that restrict exercise of the rights granted under the Adapter's License You apply.

Section 4 – Sui Generis Database Rights.

Where the Licensed Rights include Sui Generis Database Rights that apply to Your use of the Licensed Material:

a. for the avoidance of doubt, Section 2(a)(1) grants You the right to extract, reuse, reproduce, and Share all or a substantial portion of the contents of the database for NonCommercial purposes only;
b. if You include all or a substantial portion of the database contents in a database in which You have Sui Generis Database Rights, then the database in which You have Sui Generis Database Rights (but not its individual contents) is Adapted Material, including for purposes of Section 3(b); and
c. You must comply with the conditions in Section 3(a) if You Share all or a substantial portion of the contents of the database.

For the avoidance of doubt, this Section 4 supplements and does not replace Your obligations under this Public License where the Licensed Rights include other Copyright and Similar Rights.

Section 5 – Disclaimer of Warranties and Limitation of Liability.

a. Unless otherwise separately undertaken by the Licensor, to the extent possible, the Licensor offers the Licensed Material as-is and as-available, and makes no representations or warranties of any kind concerning the Licensed Material, whether express, implied, statutory, or other. This includes, without limitation, warranties of title, merchantability, fitness for a particular purpose, non-infringement, absence of latent or other defects, accuracy, or the presence or absence of errors, whether or not known or discoverable. Where disclaimers of warranties are not allowed in full or in part, this disclaimer may not apply to You.

b. To the extent possible, in no event will the Licensor be liable to You on any legal theory (including, without limitation, negligence) or otherwise for any direct, special, indirect, incidental, consequential, punitive, exemplary, or other losses, costs, expenses, or damages arising out of this Public License or use of the Licensed Material, even if the Licensor has been advised of the possibility of

such losses, costs, expenses, or damages. Where a limitation of liability is not allowed in full or in part, this limitation may not apply to You.

c. The disclaimer of warranties and limitation of liability provided above shall be interpreted in a manner that, to the extent possible, most closely approximates an absolute disclaimer and waiver of all liability.

Section 6 – Term and Termination.

a. This Public License applies for the term of the Copyright and Similar Rights licensed here. However, if You fail to comply with this Public License, then Your rights under this Public License terminate automatically.

b. Where Your right to use the Licensed Material has terminated under Section 6(a), it reinstates:
   1. automatically as of the date the violation is cured, provided it is cured within 30 days of Your discovery of the violation; or
   2. upon express reinstatement by the Licensor.

   For the avoidance of doubt, this Section 6(b) does not affect any right the Licensor may have to seek remedies for Your violations of this Public License.

c. For the avoidance of doubt, the Licensor may also offer the Licensed Material under separate terms or conditions or stop distributing the Licensed Material at any time; however, doing so will not terminate this Public License.

d. Sections 1, 5, 6, 7, and 8 survive termination of this Public License.

Section 7 – Other Terms and Conditions.

a. The Licensor shall not be bound by any additional or different terms or conditions communicated by You unless expressly agreed.

b. Any arrangements, understandings, or agreements regarding the Licensed Material not stated herein are separate from and independent of the terms and conditions of this Public License.

Section 8 – Interpretation.

a. For the avoidance of doubt, this Public License does not, and shall not be interpreted to, reduce, limit, restrict, or impose conditions on any use of the Licensed Material that could lawfully be made without permission under this Public License.

b. To the extent possible, if any provision of this Public License is deemed unenforceable, it shall be automatically reformed to the minimum extent necessary to make it enforceable. If the provision cannot be reformed, it shall be severed from this Public License without affecting the enforceability of the remaining terms and conditions.

c. No term or condition of this Public License will be waived and no failure to comply consented to unless expressly agreed to by the Licensor.

d. Nothing in this Public License constitutes or may be interpreted as a limitation upon, or waiver of, any privileges and immunities that apply to the Licensor or You, including from the legal processes of any jurisdiction or authority.

7. FUENTES

http://www.joomlaspanish.org
https://bugzilla.redhat.com/
http://cve.mitre.org/
http://web.nvd.nist.gov
http://www.jasig.org/cas
http://www.papisoftware.net
http://www.backtrack-linux.org/
http://nvd.nist.gov/cvss.cfm?calculator&version=2
https://www.elca.ch/secutalk/?p=650
https://www.owasp.org
Módulo 4. Identidad Digital
Módulo 4. Vulnerabilidades de Seguridad