UOC www.uoc.edu
UAB Universitat Autònoma de Barcelona
Universitat Rovira i Virgili
UIB Universitat de les Illes Balears

ANÀLISI D'ERRORS EN SERVIDORS WEB

Estudiant: Genís Domínguez
Directors: Jordi Duch i Agustí Solanas

Resum

- Introducció – OWASP, anàlisi d'errors i exemples
  - Demostració – Cerca a Google
- Classificació dels errors
- Estudi dels errors en servidors web
- Estudi del error 404 en diferents servidors
- Aplicació ErrorMint i HttpErrors
  - Demostració Aplicació
- Publicació i Conclusions

Resum

- Introducció – Owasp, errors i exemples
  - Demostració – Cerca a Google
- Classificació dels errors
- Estudi dels errors en servidors web
- Estudi del error 404 en diferents servidors
- Aplicació ErrorMint i HttpErrors
  - Demostració Aplicació
- Publicació i Conclusions

OWASP

- **O**pen **W**eb **A**pplication **S**ecurity **P**roject
- Projecte- OWASP Top 10

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

OWASP

- Projecte – Testing Guide

- v3 publicada l'any 2008
- v4 en desenvolupament

- Secció 4.9. Error Handling
  - 4.9.1 Analysis of Error Codes

Anàlisi dels codis d'error

- Situacions fora del comportament habitual de l'aplicació web

- Informació que podem obtenir dels errors web
  - Versions de software i components utilitzats
  - Informació de l'estructura de la base de dades
  - Estructura de carpetes
  - Informació d'usuaris i contrasenyes

Importància dels errors web

- Atac a una aplicació web
- MITRE i NVD – CVE DB
  - Base de dades de vulnerabilitats
- Offensive Security – Exploit DB
  - Base de dades d'exploits
- Identificar la versió del servidor

Com obtenir infromació dels errors

- Provocar els errors per obtenir la informació desitjada
  - Objectiu específic
- Utilitzar cercadors per trobar pàgines que continguin errors
  - Sense un objectiu específic
- Errors casuals
  - Aquells que es produeixen en moments determinats per factors externs.

Exemple – Banc Sabadell

Error provocat mitjançant una petició a una pàgina no existent

JBossWeb 2.0.0 és una versió d'agost del 2011 amb 3 vulnerabilitats CVE conegudes

Exemple – Imaginarium

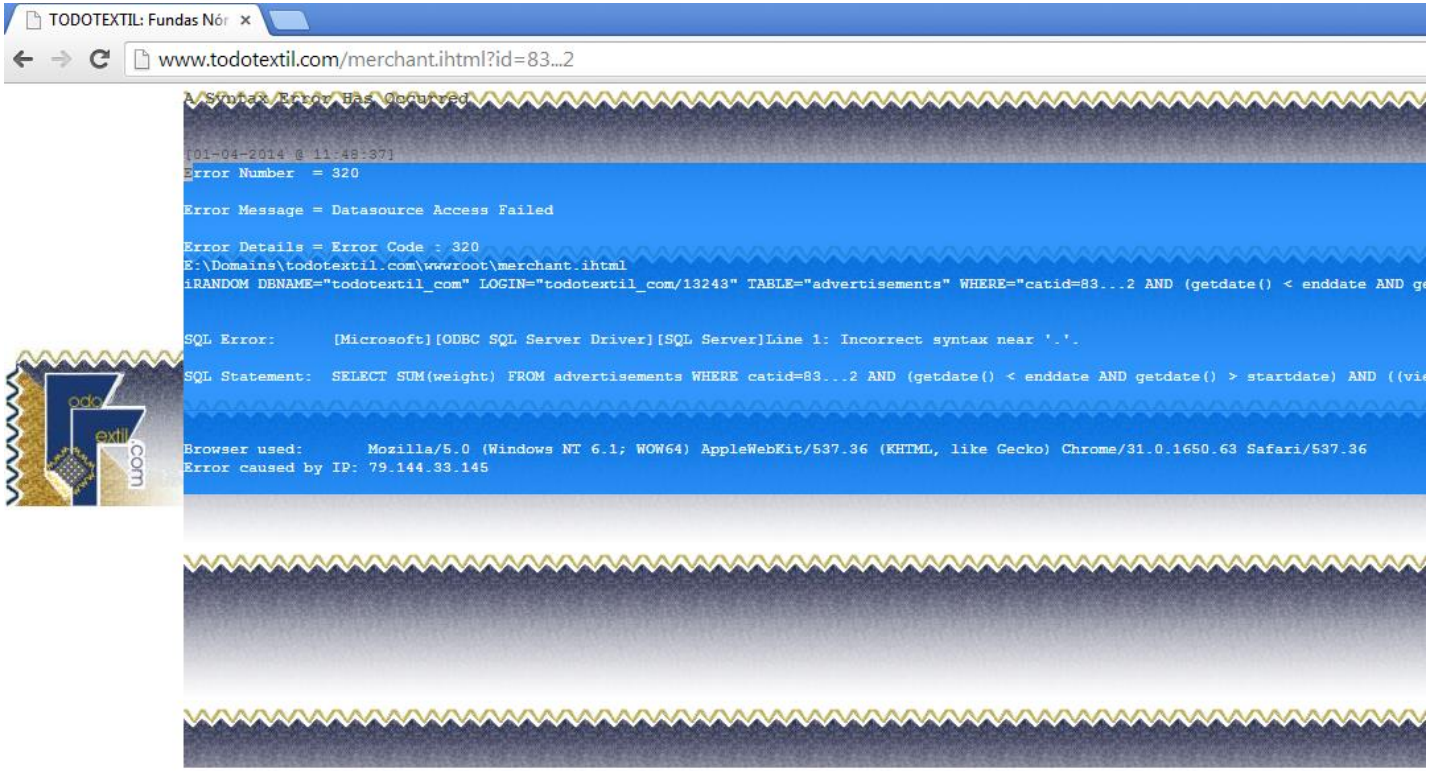
Error provocat mitjançant una petició a una pàgina no existent

Tomcat 5.5.26 es va publicar el febrer del 2008

Exemple – Loteria De Catalunya

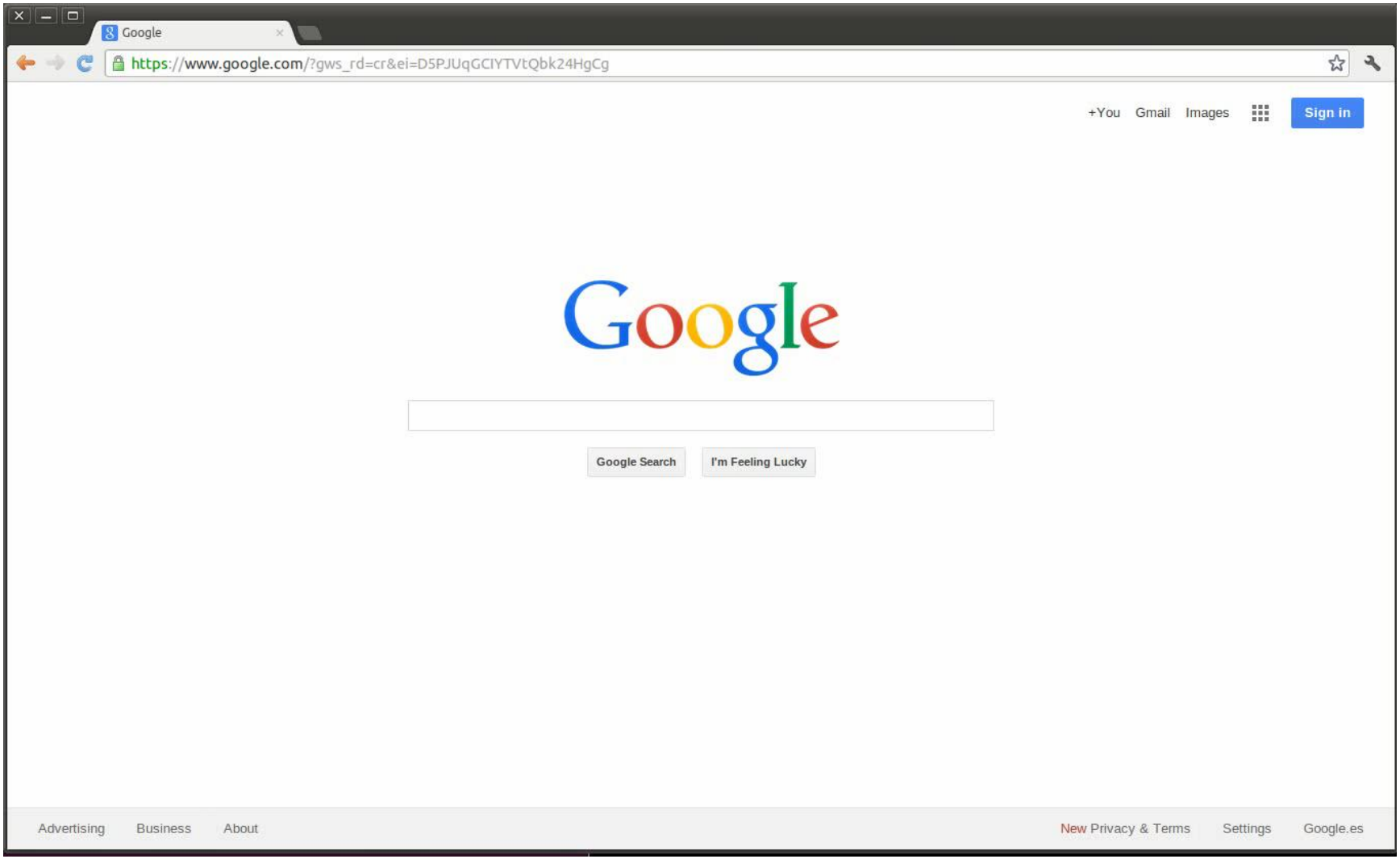
No és possible provocar aquest error. Problemes en el servidor.
Apache 1.3.12 és una versió del 25 de febrer del any 2000.

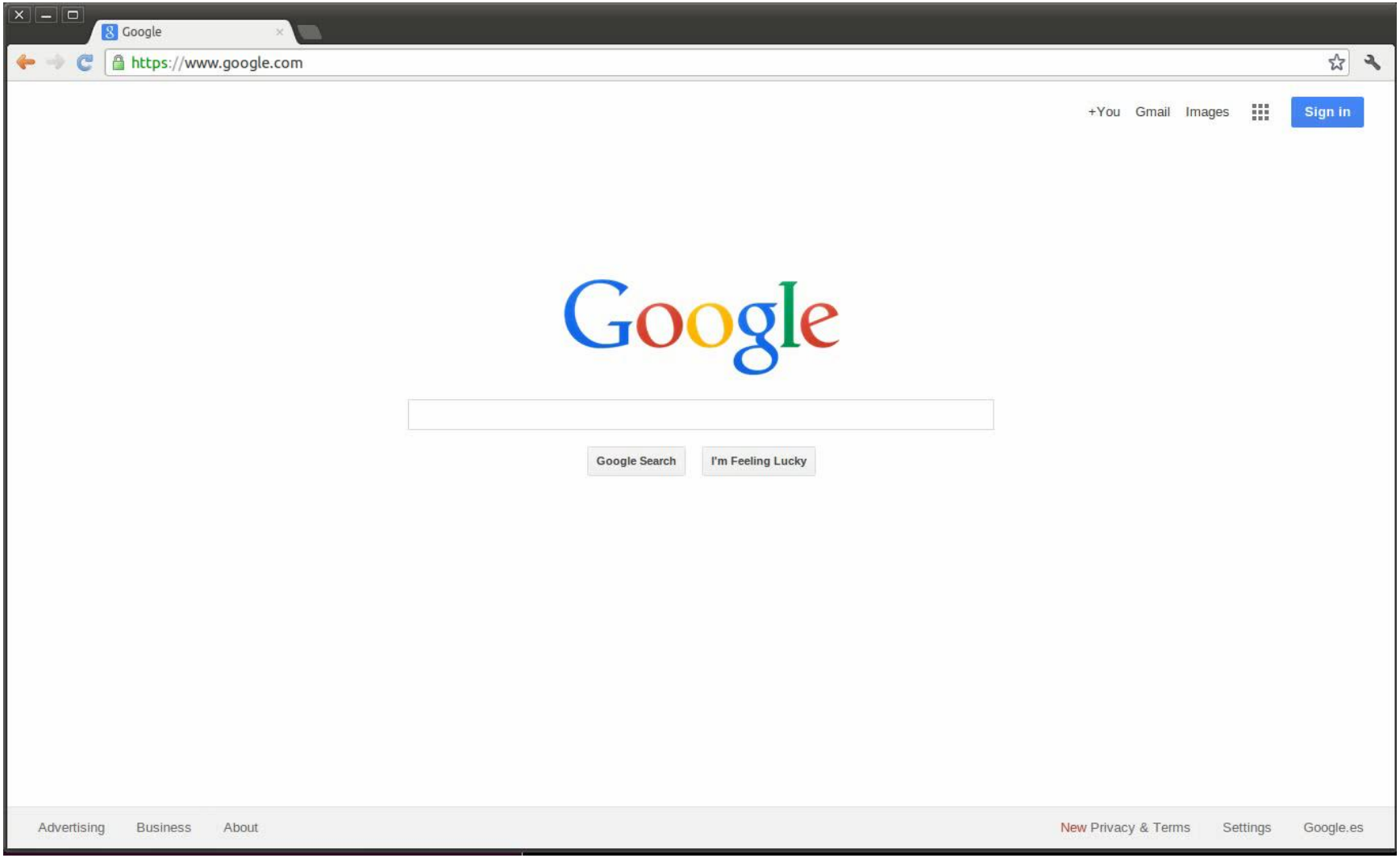
Exemple – Todotextil.com

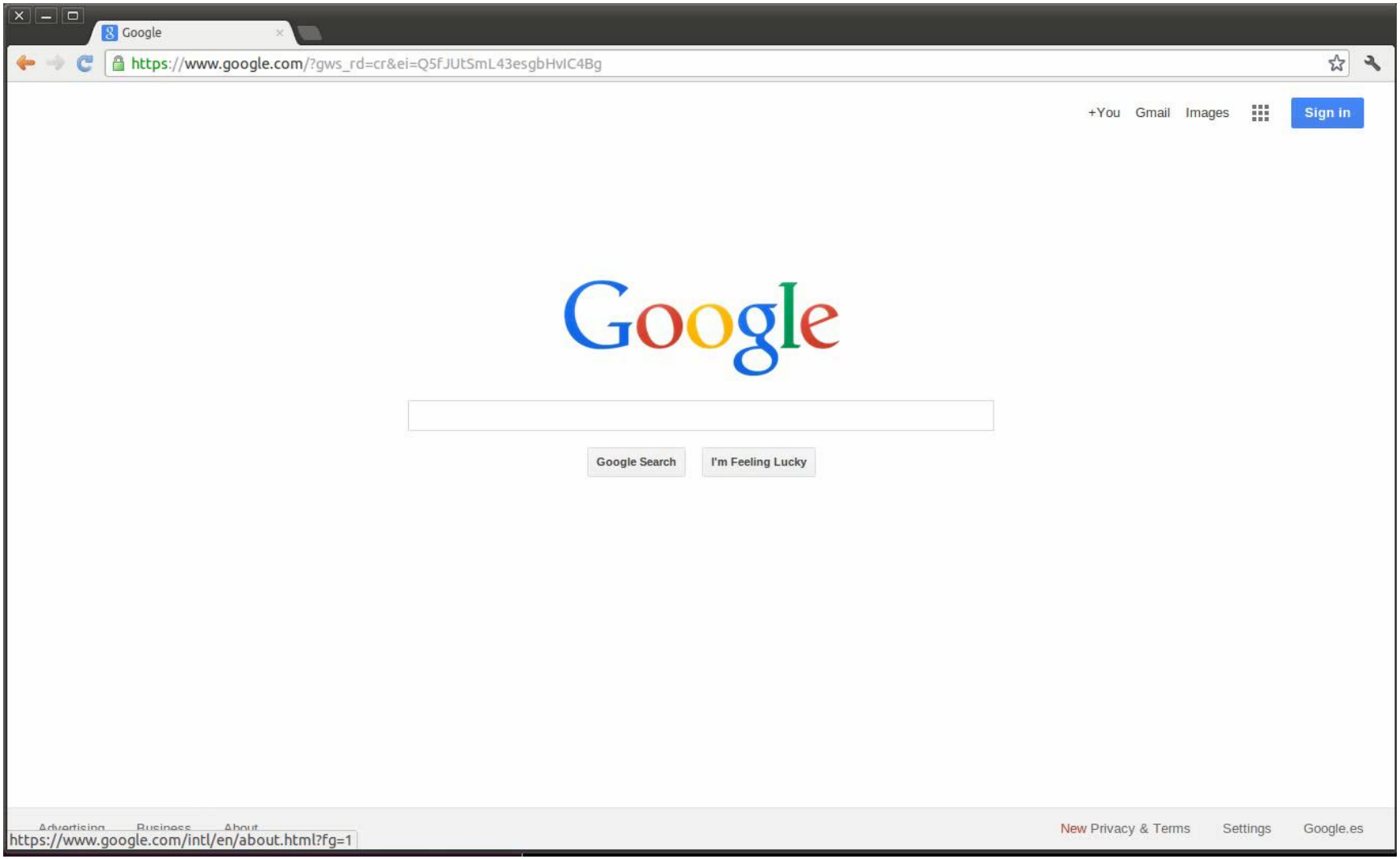


Error trobat a través de Google mitjançant la cerca "A syntax error has occurred" filetype:ihtml. Conté nom d'usuari i contrasenya de la base de dades, taules, rutes,...

Demostració – Cerques Google


Google
https://www.google.com/?gws_rd=cr&ei=D5PJUqGCIYTVtQbk24HgCg
+You
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Advertising
Business
About
New Privacy & Terms
Settings
Google.es


Google
https://www.google.com
+You
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Advertising
Business
About
New Privacy & Terms
Settings
Google.es


Google
https://www.google.com/?gws_rd=cr&ei=Q5fJUtSmL43esgbHvIC4Bg
+You
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Advertising
Business
About
New Privacy & Terms
Settings
Google.es
https://www.google.com/intl/en/about.html?fg=1

Resum

- Introducció – Owasp, errors i exemples
  - Demostració – Cerca a Google
- Classificació dels errors
- Estudi dels errors en servidors web
- Estudi del error 404 en diferents servidors
- Aplicació ErrorMint i HttpErrors
  - Demostració Aplicació
- Publicació i Conclusions

Classificació dels errors

- Errors en servidors web

- Errors en aplicacions

- Errors en bases de dades

Errors en servidors web

- Basats en els codis d'error del protocol HTTP
  - 400 – Error en el client
  - 500 – Error en el servidor

- Informació proporcionada:
  - tecnologies i versions utilitzades
  - sistema operatiu
  - components instal·lats en el servidor

Errors en aplicacions

- Gran varietat de tecnologies i sistemes
  - HTML, CSS, JavaScript, XML, ASP, PHP, JSP, CGI, C, C++, Python, Perl, Python, VisualBasic, .Net, Java
  - PhpBB, vBulletin, SugarCRM, Drupal, Wordpress, OpenERP, Joomla, PrestaShop, Magento, Indexhibit
- Aplicacions programades sota demanda i aplicacions basades en paquets
- Informació proporcionada:
  - tecnologies utilitzades
  - rutes del servidor
  - noms d'arxius

Errors en bases de dades

- Interès addicional degut a les injeccions SQL

- Informació proporcionada:
  - tecnologies utilitzades
  - servidors de bases de dades
  - noms de bases de dades, taules i camps
  - Informació de login: usuaris i contrasenyes

Resum

- Introducció – Owasp, errors i exemples
  - Demostració – Cerca a Google
- Classificació dels errors
- Estudi dels errors en servidors web
- Estudi del error 404 en diferents servidors
- Aplicació ErrorMint i HttpErrors
  - Demostració Aplicació
- Publicació i Conclusions

Codis d'error HTTP

- **400 Bad Request**
- 401 Unauthorized
- 402 Payment Required
- **403 Forbidden**
- **404 Not Found**
- **405 Method Not Allowed**
- 406 Not Acceptable
- 407 Proxy Authentication Required
- **408 Request Time-out**
- 409 Conflict
- 410 Gone
- 411 Length Required
- 412 Precondition Failed
- 413 Request Entity Too Large
- 414 Request-URI Too Large
- 415 Unsupported Media Type
- 416 Requested range not satisfiable
- 417 Expectation Failed

- 500 Internal Server Error
- **501 Method Not Implemented**
- 502 Bad Gateway
- 503 Service Unavailable
- 504 Gateway Time-out
- 505 HTTP Version not supported

400 – Errors de client

500 – Errors en servidor

Peticions mitjançant Telnet

GET /index.html HTTP/1.1
host: 192.168.195.145

```
genis@MATRIX:~$ telnet 192.168.195.145 80
Trying 192.168.195.145...
Connected to 192.168.195.145.
Escape character is '^]'.
GET /index.html HTTP/1.1
host: 192.168.195.145

HTTP/1.1 200 OK
Date: Fri, 06 Dec 2013 20:12:50 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Sat, 30 Nov 2013 13:23:00 GMT
ETag: "a1fec-b1-4ec64d884e138"
Accept-Ranges: bytes
Content-Length: 177
Vary: Accept-Encoding
Content-Type: text/html
X-Pad: avoid browser bug

<html><body><h1>It works!</h1>
<p>This is the default web page for this server.</p>
<p>The web server software is running but no content has been added, yet.</p>
</body></html>
Connection closed by foreign host.
genis@MATRIX:~$
```

Error 400 Bad Request

GET /index.html HTTP/1.1

```
genis@MATRIX:~$ telnet 192.168.195.145 80
Trying 192.168.195.145...
Connected to 192.168.195.145.
Escape character is '^]'.
GET /index.html HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Fri, 06 Dec 2013 23:57:53 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 301
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 127.0.1.1 Port 80</address>
</body></html>
Connection closed by foreign host.
genis@MATRIX:~$
```

Error 403 Forbidden

GET /testforbidden/index.html HTTP/1.1
host: 192.168.195.145

```
genis@MATRIX:~$ telnet 192.168.195.145 80
Trying 192.168.195.145...
Connected to 192.168.195.145.
Escape character is '^]'.
GET /testforbidden/index.html HTTP/1.1
host:192.168.195.145

HTTP/1.1 403 Forbidden
Date: Sun, 08 Dec 2013 09:43:23 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 307
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access /testforbidden/index.html
on this server.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 192.168.195.145 Port 80</address>
</body></html>
Connection closed by foreign host.
```

Error 405 Method not allowed

DELETE /index.html HTTP/1.1
host: 192.168.195.145

```
genis@MATRIX:~$ telnet 192.168.195.145 80
Trying 192.168.195.145...
Connected to 192.168.195.145.
Escape character is '^]'.
DELETE /index.html HTTP/1.1
host: 192.168.195.145

HTTP/1.1 405 Method Not Allowed
Date: Sat, 07 Dec 2013 00:48:57 GMT
Server: Apache/2.2.22 (Ubuntu)
Allow: GET,HEAD,POST,OPTIONS
Vary: Accept-Encoding
Content-Length: 315
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>405 Method Not Allowed</title>
</head><body>
<h1>Method Not Allowed</h1>
<p>The requested method DELETE is not allowed for the URL /index.html.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 192.168.195.145 Port 80</address>
</body></html>
Connection closed by foreign host.
genis@MATRIX:~$
```

Error 408 Request Time-Out

GET/index.html HTTP/1.1

```
genis@MATRIX:~$ telnet 192.168.195.145 80
Trying 192.168.195.145...
Connected to 192.168.195.145.
Escape character is '^]'.
GET /index.html HTTP/1.1
HTTP/1.1 408 Request Time-out
Date: Sat, 07 Dec 2013 00:58:33 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 298
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>408 Request Time-out</title>
</head><body>
<h1>Request Time-out</h1>
<p>Server timeout waiting for the HTTP request from the client.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 127.0.1.1 Port 80</address>
</body></html>
Connection closed by foreign host.
```

Error 501 Method Not Implemented

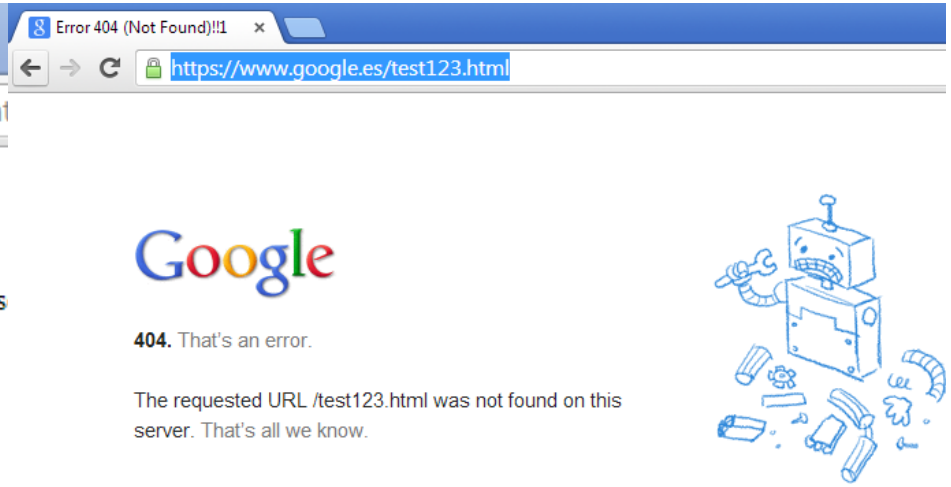
RENAME/index.html HTTP/1.1
host: 192.168.195.145

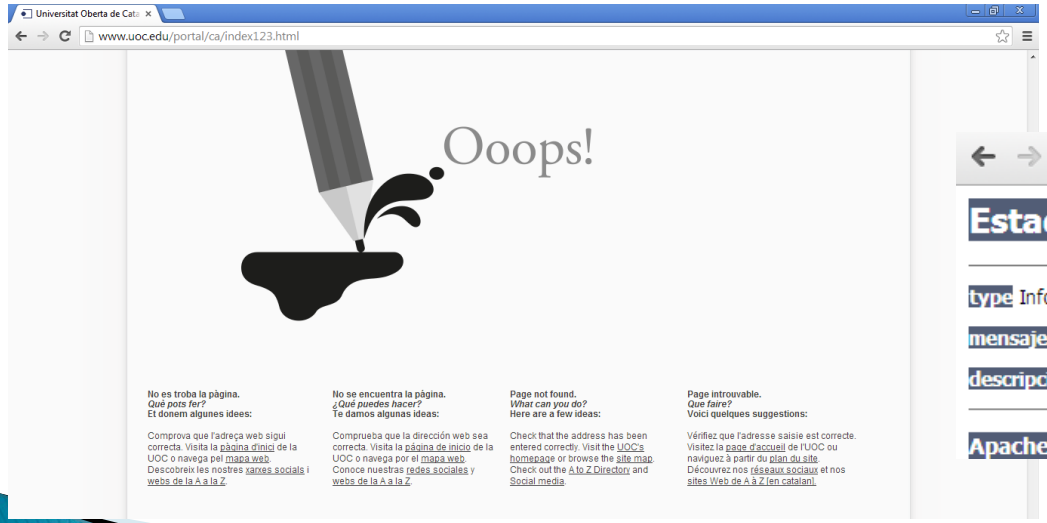
```
genis@MATRIX:~$ telnet 192.168.195.145 80
Trying 192.168.195.145...
Connected to 192.168.195.145.
Escape character is '^]'.
GET /index.html HTTP/1.1
HTTP/1.1 408 Request Time-out
Date: Sat, 07 Dec 2013 00:58:33 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 298
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>408 Request Time-out</title>
</head><body>
<h1>Request Time-out</h1>
<p>Server timeout waiting for the HTTP request from the client.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 127.0.1.1 Port 80</address>
</body></html>
Connection closed by foreign host.
```

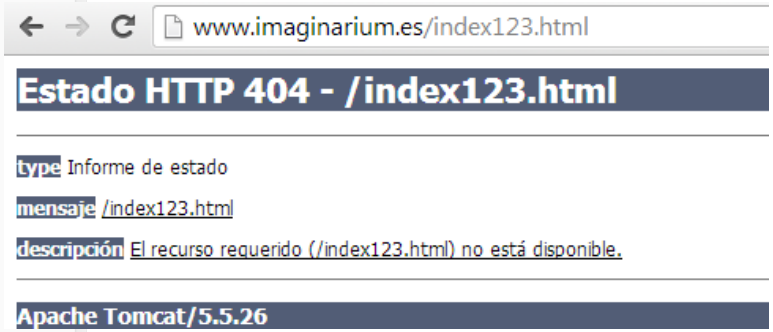
Resum

- Introducció – Owasp, errors i exemples
  - Demostració – Cerca a Google
- Classificació dels errors
- Estudi dels errors en servidors web
- Estudi del error 404 en diferents servidors
- Aplicació ErrorMint i HttpErrors
  - Demostració Aplicació
- Publicació i Conclusions

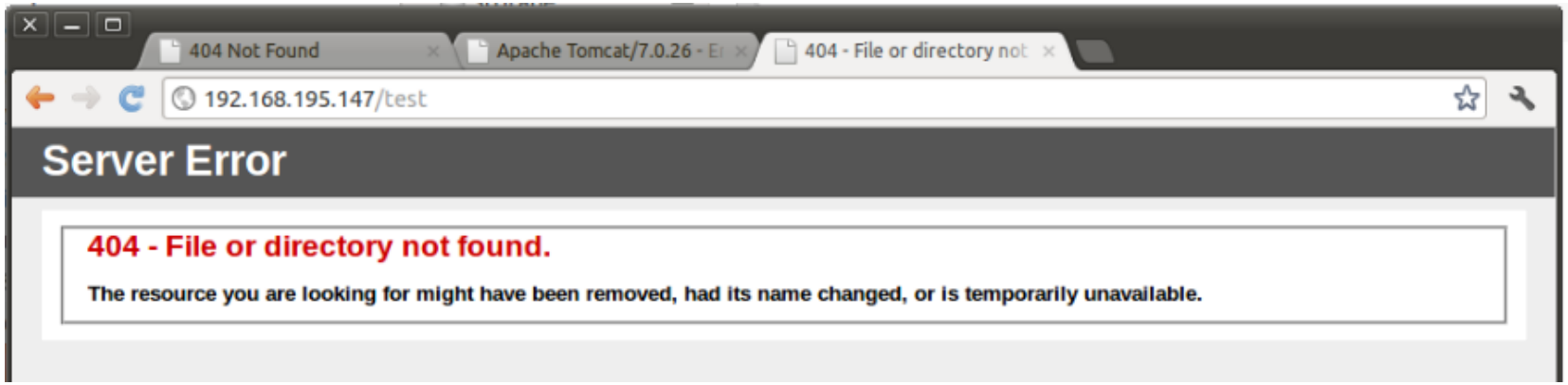
Error 404 Not Found







Error 404 a IIS



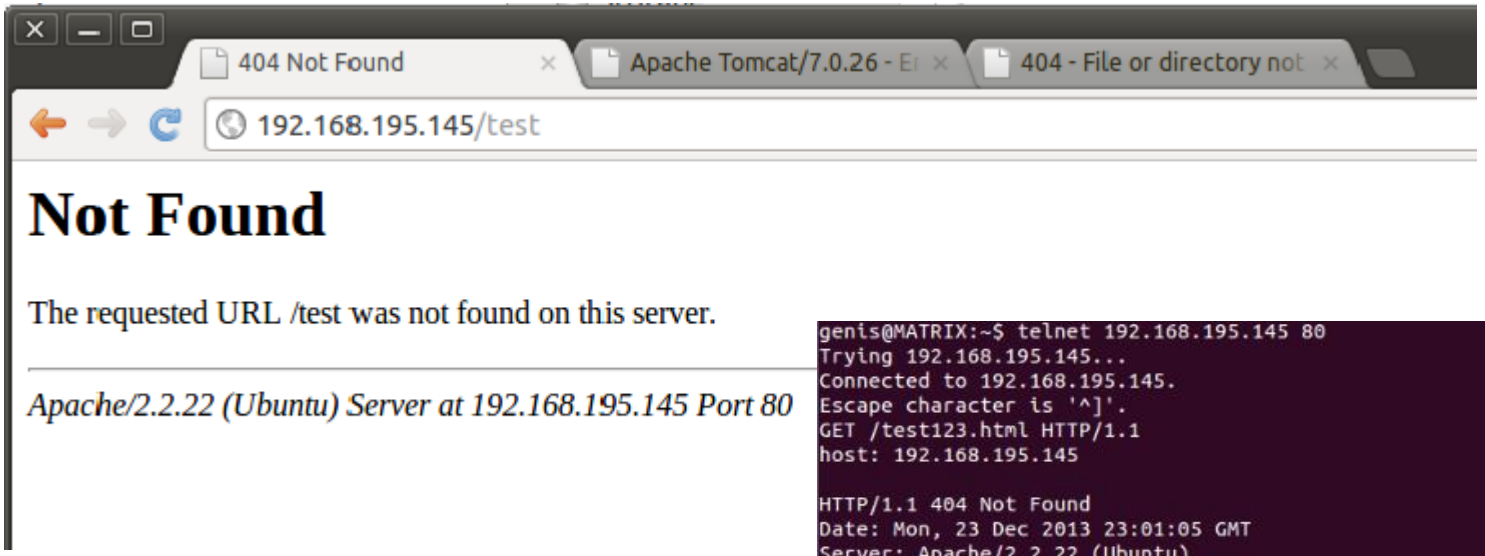

```
genis@MATRIX:~$ telnet 192.168.195.147 80
Trying 192.168.195.147...
Connected to 192.168.195.147.
Escape character is '^]'.
GET /test123.html HTTP/1.1
host: 192.168.195.147

HTTP/1.1 404 Not Found
Content-Type: text/html
Server: Microsoft-IIS/8.5
Date: Wed, 18 Dec 2013 20:41:52 GMT
Content-Length: 1245
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/x
html1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>404 - File or directory not found.</title>
<style type="text/css">
<!--
body{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;b
ackground:#EEEEEE;}
fieldset{padding:0 15px 10px 15px;}
h1{font-size:2.4em;margin:0;color:#FFF;}
h2{font-size:1.7em;margin:0;color:#CC0000;}
h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;}
#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS
", Verdana, sans-serif;color:#FFF;
background-color:#555555;}
#content{margin:0 0 0 2%;position:relative;}
.content-container{background:#FFF;width:96%;margin-top:8px;padding:10px;positio
n:relative;}
-->
</style>
</head>
<body>
<div id="header"><h1>Server Error</h1></div>
<div id="content">
 <div class="content-container"><fieldset>
  <h2>404 - File or directory not found.</h2>
  <h3>The resource you are looking for might have been removed, had its name cha
nged, or is temporarily unavailable.</h3>
 </fieldset></div>
</div>
</body>
</html>
```

Error 404 a IIS

- Configuració dels errors HTTP a través del panell d'administració del site
- No és possible modificar el camp Server de la capçalera HTTP
- Versions anteriors d'IIS es comporten de la mateixa manera

Error 404 a Apache

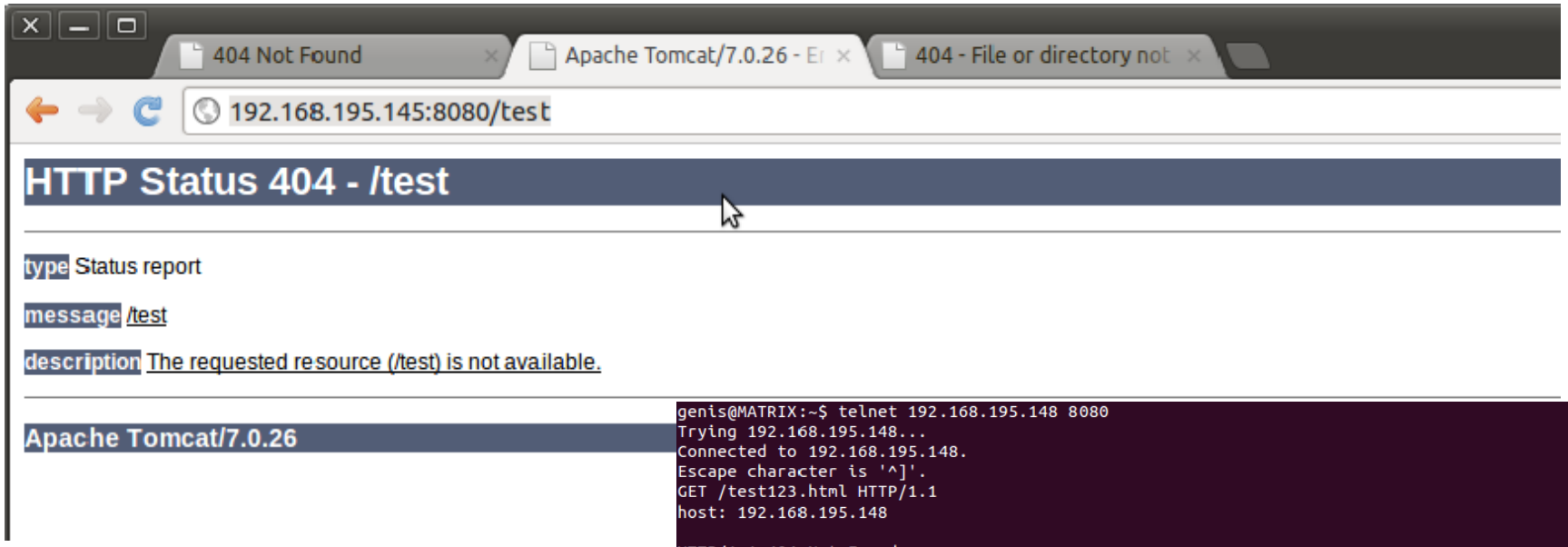



```
genis@MATRIX:~$ telnet 192.168.195.145 80
Trying 192.168.195.145...
Connected to 192.168.195.145.
Escape character is '^]'.
GET /test123.html HTTP/1.1
host: 192.168.195.145

HTTP/1.1 404 Not Found
Date: Mon, 23 Dec 2013 23:01:05 GMT
Server: Apache/2.2.22 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 291
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /test123.html was not found on this server.</p>
<hr>
<address>Apache/2.2.22 (Ubuntu) Server at 192.168.195.145 Port 80</address>
</body></html>
```

Error 404 a Apache

- Configuració dels errors HTTP mitjançant
  - Directiva ErrorDocument global
  - Directiva ErrorDocument per virtual host (htaccess)
  - Directives ServerSignature i ServerTokens
- Configuració del camp server de la capçalera HTTP mitjançant mod_security i la directiva SecServerSignature

Error 404 a Tomcat




```
genis@MATRIX:~$ telnet 192.168.195.148 8080
Trying 192.168.195.148...
Connected to 192.168.195.148.
Escape character is '^]'.
GET /test123.html HTTP/1.1
host: 192.168.195.148

HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 991
Date: Wed, 25 Dec 2013 18:51:19 GMT

<html><head><title>Apache Tomcat/7.0.26 - Error report</title><style><!--H1 {font-family:Tah
oma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:T
ahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family
:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-fa
mily:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Aria
l,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-serif;b
ackground:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {col
or : #525D76;}--></style> </head><body><h1>HTTP Status 404 - /test123.html</h1><HR size="1"
noshade="noshade"><p><b>type</b> Status report</p><p><b>message</b> <u>/test123.html</u></p>
<p><b>description</b> <u>The requested resource (/test123.html) is not available.</u></p><HR
 size="1" noshade="noshade"><h3>Apache Tomcat/7.0.26</h3></body></html>
```

Error 404 a Tomcat

- Configuració dels errors HTTP Tomcat mitjançant l'etiqueta <error-page> de web.xml
- Configuració de la capçalera HTTP mitjançant l'etiqueta <connector /> de server.xml
- Les versions anteriors de Tomcat es comporten exactament igual

Diferències entre servidors

	IIS	Apache	Tomcat
Per defecte oculta la versió del servidor en els errors HTTP	Sí	No	No
Permet configurar les respostes HTTP	Sí	Sí	Sí
Per defecte oculta la versió del servidor en les capçaleres HTTP	No	No	Sí
Permet configurar la capçalera HTTP Server	No	Sí	Sí

Resum

- Introducció – Owasp, errors i exemples
  - Demostració – Cerca a Google
- Classificació dels errors
- Estudi dels errors en servidors web
- Estudi del error 404 en diferents servidors
- Aplicació ErrorMint i HttpError
  - Demostració Aplicació
- Publicació i Conclusions

ErrorMint

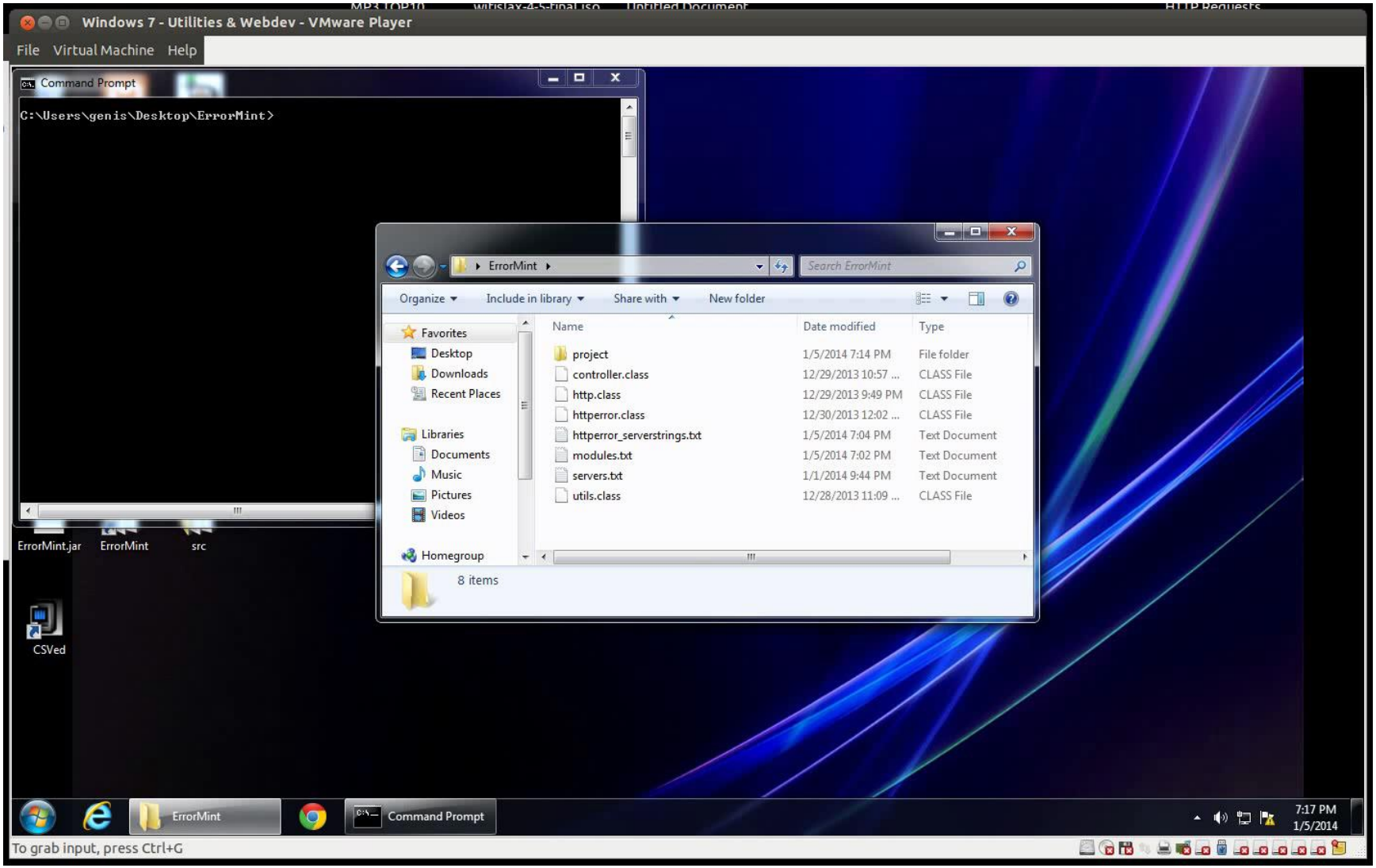
- Aplicació Base
  - Gestió de projectes
  - Definició d'objectius
  - Gestió de mòduls
  - Eines per desenvolupar nous mòduls

  Permet afegir mòduls sense modificar el codi principal

ErrorMint – HttpError

- Bateria de proves
  - Petició vàlida – Codi 200
  - Not Found – Error 404
  - Method Not Valid / Not Allowed – Errors 405 i 501
  - Bad Request – Error 400
  - Time-Out – Error 408
  - Bad Host
  - Bad Version – Error 505
- Informe CSV amb els resultats obtinguts

Demostració – ErrorMint


Windows 7 - Utilities & Webdev - VMware Player
File Virtual Machine Help
Command Prompt
C:\Users\genis\Desktop\ErrorMint>
ErrorMint
Search ErrorMint
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Name
Date modified
Type
project 1/5/2014 7:14 PM File folder
controller.class 12/29/2013 10:57 ... CLASS File
http.class 12/29/2013 9:49 PM CLASS File
httperror.class 12/30/2013 12:02 ... CLASS File
httperror_serverstrings.txt 1/5/2014 7:04 PM Text Document
modules.txt 1/5/2014 7:02 PM Text Document
servers.txt 1/1/2014 9:44 PM Text Document
utils.class 12/28/2013 11:09 ... CLASS File
8 items
ErrorMint.jar
ErrorMint
src
CSVed
ErrorMint
Command Prompt
7:17 PM
1/5/2014
To grab input, press Ctrl+G

Resum

- Introducció – Owasp, errors i exemples
  - Demostració – Cerca a Google
- Classificació dels errors
- Estudi dels errors en servidors web
- Estudi del error 404 en diferents servidors
- Aplicació ErrorMint i HttpErrors
  - Demostració Aplicació
- Publicació i Conclusions

Publicació OWASP i SourceForge

- ErrorMint publicat a SourceForge
  - http://sourceforge.net/projects/errormint/

- Secció Analysis of Error Codes de la OWASP Testing Guide editada amb la investigació realitzada en aquest treball

Conclusions

- Gran quantitat d'errors per analitzar
- Configuració important i senzilla de realitzar
- Treballs futurs

Gràcies

Preguntes i contacte – genisd@gmail.com