



Escàner de vulnerabilitats web

Alumne: Eric Bujeque Escorriola
Caps de projecte: Jordi Duch i Agusti Solanas

ÍNDEX

- Introducció
- Software
- Anàlisi
- Disseny
- Seguretat
- Demostració
- Conclusions

INTRODUCCIÓ

- Context i justificació del Treball

- Hi ha una clara tendència a fer servir la **tecnologia web**.
- Existeixen **aplicacions web** que guarden documents o informació confidencial.



vulnerables a intrusos

- Cal assegurar-nos que cada aplicació web que pengem no siguin vulnerable.
- **Idea:** Fer servir eines gratuïtes que passen diversos tests especialitzats a les webs, i desenvolupar alguns propis ajuntant-los en una única aplicació web, i que a més sigui capaç d'emmagatzemar els resultats per a la seva posterior comparació.

INTRODUCCIÓ

- Objectius:

- Desenvolupar una aplicació que permeti escanejar pàgines i analitzar els resultats.
- Que l'aplicació sigui fàcil d'utilitzar.
- Aconseguir un disseny agradable i intuïtiu.
- Que permeti **guardar els resultats** per la seva posterior comparació.
- *Aprendre a desenvolupar una aplicació web en Python i Django i aprofundir els coneixements en la seguretat web.*

INTRODUCCIÓ

- Enfocament i mètode seguit:

Possibles estratègies:

- Modificar una aplicació existent.
- Desenvolupar una aplicació nova.
- **Desenvolupar una aplicació nova que es recolzi de programes existents.**

¿Com fer la aplicació?:

- Aplicació d'escriptori.
- **Aplicació web.**

INTRODUCCIÓ

- Producte obtingut:

- Un **escàner de vulnerabilitats web** especialitzat en l'entrada de dades dels usuaris.
- Els usuaris registrats poden **escanejar** les web desitjades passant un seguit de tests de vulnerabilitats que poden escollir.
- L'aplicació mostra els resultats dels tests i els guarda en la **base de dades**.
- Alguns dels test de vulnerabilitats que es passen fan servir aplicacions de tercers. Altres estan programats en la pròpia aplicació fent peticions HTTP sobre la pàgina a escanejar.

SOFTWARE

- Software utilitzat i alternatives:

Software utilitzat	Alternativa
Programació: Python + Django	- PHP - Java
Servidor: Propi de Django	- Apache
Base de dades: SQLite	- MySQL
Editors: IntelliJ Idea	- Sublime Text 3
Sistema operatiu: Linux (Fedora)	- Windows

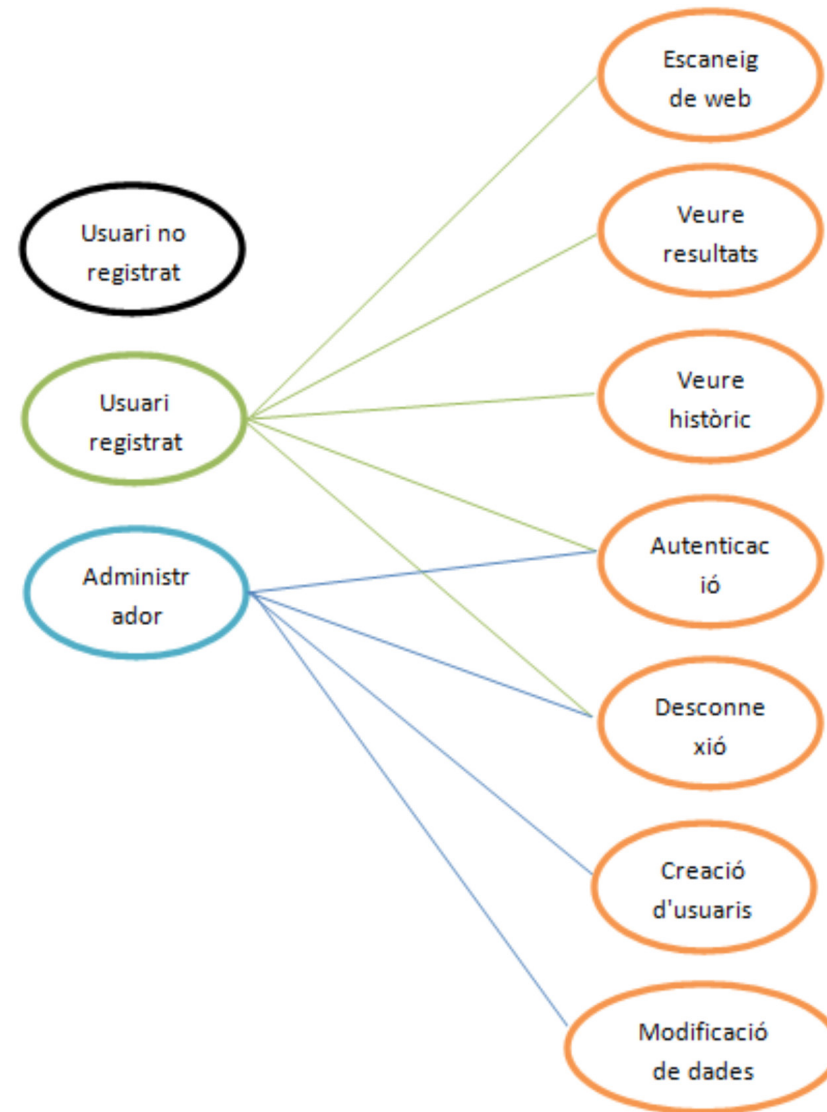
ANÀLISI

Requeriments funcionals:

- Sistema operatiu: **Linux (Fedora).**
- Llenguatge: **Python versió 3.**
- Servidor i Framework: **Django 1.8.2.**
- Base de dades: **SQLite 3.8.10.2.**

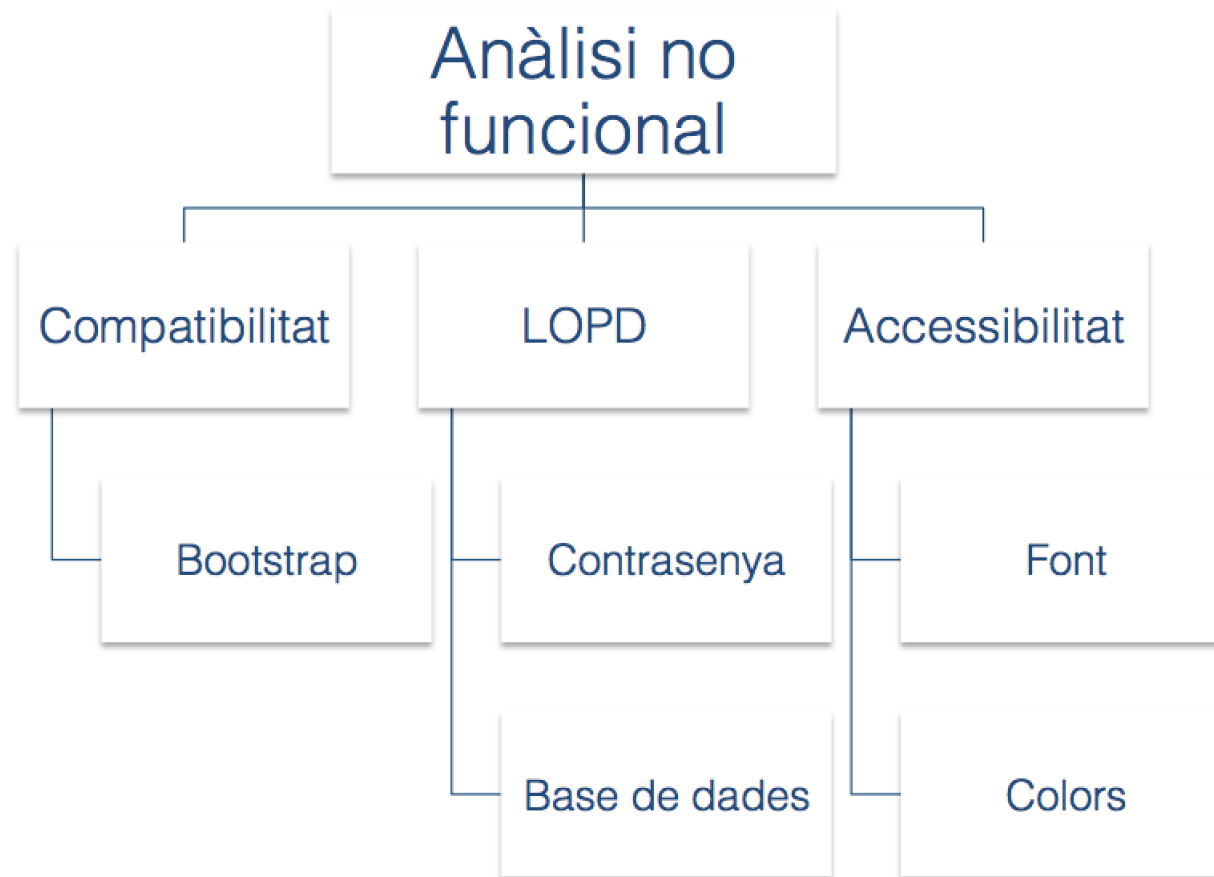
ANÀLISI

Diagrama de casos d'ús :



ANÀLISI


- Anàlisi no funcional:



DISSENY

- Estructura de la web:
 - Simple e intuïtiu

Autenticació



The image shows a screenshot of a web application interface for a web scanner. The header is dark grey with the text "Scanner Web" on the left and "Informació", "Scans", and "Usuari" on the right. The main content area is white and titled "Identificació d'usuari". It contains two input fields: "usuari" and "Password". Below the fields is a checkbox labeled "Recordar". At the bottom is a large blue button labeled "Autenticar".

Pàgina d'escaneig

Scanner Web

Informació

Scans ▾

Usuari ▾

Scanner de vulnerabilitats web

Aquesta aplicació escaneja les webs segons la guia del [OWASP](#) referents a la validació de codi d'entrada en formularis, direccions, crides AJAX... en busca de vulnerabilitats com XSS, Xpath Injection o SQL Injection.

Web i Inputs

www.

Especificar paràmetres

#id

.class

?param

\$post

En cas de no posar un paràmetre en concret, s'exploraran totes les opcions.

Començar a escanear

Tests a aplicar

Seleccionar tot - Anular tota selecció

- Cross Site Scripting (XSS) ?
- HTTP Verb Tampering ?
- HTTP Parameter pollution ?
- SQL Injection ?
- XML Injection ?
- SSI Injection ?
- Code Injection ?

Per escanear una web en busca de vulnerabilitats és obligatori marcar al menys un test.

Pàgina de resultats

Scanner Web Informació Scans ▾ Usuari ▾

Paràmetres del escaneig

Url: http://localhost/vulnerable/index.php?id=1&x=1

#id: id, tal, otraid **.class:** unaclass, dosclasses

?paràmetres: parametro **\$post:** token, search

Resultats

SQL Injection

Parametre	Vulnerabilitat	Descripció	Payload
id (GET)	boolean-based blind	AND boolean-based blind - WHERE or HAVING clause	
id (GET)	error-based	MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause	
id (GET)	AND/OR time-based blind	MySQL >= 5.0.12 AND time-based blind (SELECT)	
id (GET)	UNION query	Generic UNION query (NULL)	<div style="border: 1px solid gray; padding: 5px; width: fit-content; margin-top: 5px;">id=1 UNION ALL SELECT NULL,CONCAT(0x7176787671,0x6e755267645168747752,0x716a717671)- -</div>

Pàgina d'escaneig

Scanner Web Informació Scans ▾ Usuari ▾

Els meus scanejos

- <http://localhost/xml/index.php>
- <http://www.insecurelabs.org/Task/Rule1?query=adfad>
- <http://localhost/vulnerable/index.php?id=1&x=1>
- <http://localhost/vulnerable/index.php>

#ID	URL	TESTS	VULNERABILITATS	DATA
20	http://localhost/vulnerable/index.php	1	0	June 15, 2015, 12:13 a.m.

- <http://pedro.bujeque.com>
- <http://localhost/ssi/index.php?id=1&x=1>
- <http://localhost/code/index.php?p=users.php>
- http://www.bidbcn.com/subastas_online.php?id=133#.VXXXAemsXRY

Administració

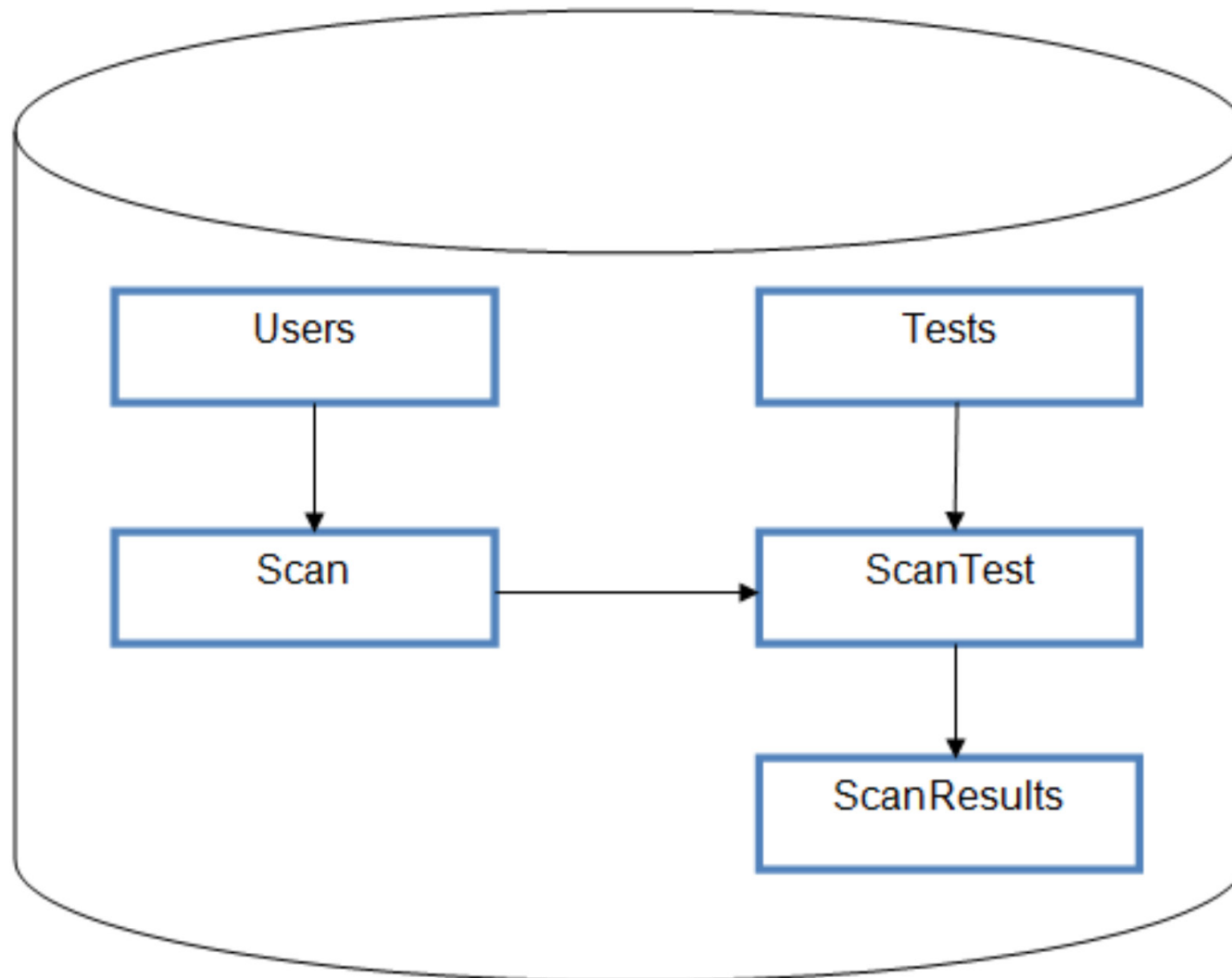
Pantalla d'autenticació de l'administrador

Pantalla de l'administrador

Username	Email address	First name	Last name	Staff status
<input type="checkbox"/> admin	noikzyr3@gmail.com			✓
<input type="checkbox"/> eric	noikzyr3@gmail.com	Eric	Bujeque	✗

Pantalla d'administració d'usuaris

Model de dades



SEGURETAT

Base de dades

- SQLite utilitza un sistema de xifrat “*Caesar cipher*”

Control de sessions

- Per a cada vista que necessiti estar autenticat hi ha posat un “decorator” de Django anomenat **@login_required()**.

Xifratge de contrasenyes

- Django s'encarrega de xifrar les contrasenyes amb el sistema **PBKDF2**.

Protecció CSRF per formularis

- Protecció que se ha de implementar. S'ha d'enviar dintre dels formularis de les plantilles: **{% csrf_token %}**.

DEMOSTRACIÓ



CONCLUSIONS

- Treball molt enriquidor a nivell personal.
- S'han assolit els objectius principals.
- No s'ha seguit la planificació inicial, i s'ha concentrat el treball en les etapes inicials i finals del projecte.
- Les línees futures són aspectes a millorar com:
 - Interacció de l'usuari amb els escanejors.
 - Eficiència dels tests.
 - Millores visuals.
 - Afegir més tests.

