

# REPORT S3/L1

Obiettivo: Sfruttamento di una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shell in PHP.

## SVOLGIMENTO

Dopo aver verificato la connessione tra le due macchine virtuali, Kali Linux e Metasploitable, ho proceduto ad accedere alla DVWA tramite il browser di Kali.



**Welcome to Damn Vulnerable Web Application!**

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

### General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

### WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

Ho realizzato un file shell.php e l'ho caricato nella sezione upload.

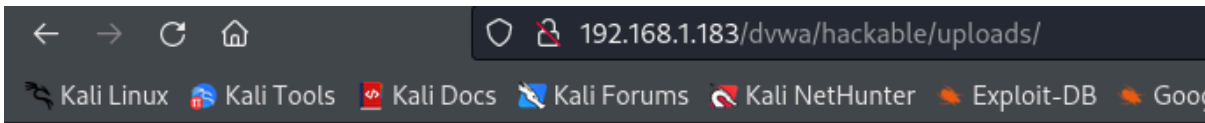
## Vulnerability: File Upload

Choose an image to upload:

No file selected.

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

Successivamente, ho ottenuto l'accesso alla shell caricata attraverso il browser.



# Index of /dvwa/hackable/uploads

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<hr/>			
<a href="#">Parent Directory</a>		-	
<a href="#">dvwa_email.png</a>	16-Mar-2010 01:56	667	
<a href="#">shell.php</a>	13-Jan-2025 09:54	0	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.1.183 Port 80

Infine ho utilizzato BurpSuite come proxy per intercettare le richieste HTTP/HTTPS effettuate durante il processo di upload e di esecuzione della shell.

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Intercept

HTTP history

WebSockets history

Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME
1	http://192.168.1.183	POST	/dvwa/vulnerabilities/upload/	✓				
2	http://192.168.1.183	GET	/dvwa/					
3	http://192.168.1.183	GET	/dvwa/					
4	http://192.168.1.183	GET	/dvwa/					
5	http://192.168.1.183	GET	/dvwa/					
6	http://192.168.1.183	GET	/dvwa/					
7	http://192.168.1.183	GET	/dvwa/					
8	http://192.168.1.183	GET	/dvwa/					
9	http://192.168.1.183	GET	/dvwa/					
10	http://192.168.1.183	GET	/dvwa/					
11	http://192.168.1.183	GET	/dvwa					
12	http://192.168.1.183	GET	/dvwa/vulnerabilities/upload/					
14	http://192.168.1.183	GET	/dvwa/					

Request

Pretty

Raw

Hex

1

POST /dvwa/vulnerabilities/upload/ HTTP/1.1

2

Host: 192.168.1.183

3

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate, br

7

Content-Type: multipart/form-data; boundary=-----41539665371021696986868437009

8

Content-Length: 469

9

Origin: http://192.168.1.183

10

Connection: keep-alive

11

Referer: http://192.168.1.183/dvwa/vulnerabilities/upload/

12

Cookie: security=low; PHPSESSID=648f26ee336506ae16152ed8b397a148

13

Upgrade-Insecure-Requests: 1

14

15

-----41539665371021696986868437009

16

Content-Disposition: form-data; name="MAX\_FILE\_SIZE"

17

18

100000

19

-----41539665371021696986868437009

20

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

21

Content-Type: application/octet-stream

22

23

24

-----41539665371021696986868437009

25

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

26

27

Upload

28

-----41539665371021696986868437009--

29