بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيْمِ

SECURITY PRO

PROJECT # 3

DVWA(DAMN VULNERABLE WEB APPLICATION)

SECURITY PRO

INTRODUCTION

Name: Arslan Ali

Qualification: BS Software Engineering

Cohort: IEC Cybersecurity Cohort -5

Instructor: Shahzaib Ali Khan

Project: Project 3 Web penetration Test

Web: DVWA

SECURITY PRO


```
o access official Ubuntu documentation, please visit:
ttp://help.ubuntu.com/
o mail.
sfadmin@metasploitable:~$ ifconfig
th0       Link encap:Ethernet  HWaddr 08:00:27:4b:b5:27
          inet addr:192.168.0.101  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4b:b527/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5805 (5.6 KB)  TX bytes:7419 (7.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

o         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:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

sfadmin@metasploitable:~$
```

DAMN VULNERABLE WEB APPLICATION (DVWA)

Username: admin
Password: password

In this project, I installed the Virtual box on my laptop and then install the mirror of metasploitable 2. The default username and password of the metasploitable 2 is "msfadmin" and find ip address of this machine and open it in Firefox

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

SECURITY PRO

01

XSS Attack(Reflected)

Cross-Site Scripting (XSS) attacks with Javascript

02

XSS Attack(Stored)

Cross-Site Scripting (XSS) attacks with Javascript

03

HTML Injection Stored

Type of Cross-Site Scripting (XSS) attacks with HTML language

04

HTML Injection Reflected

Type of Cross-Site Scripting (XSS) attacks with HTML language

05

SQL Injection

Attack on the database by using SQL language

06

Blind SQL Injection

Attack on the database by using SQL language

SECURITY PRO

07

Command Line Injection

involves executing arbitrary commands on a host operating system (OS)

08

CSRF Attack

Cross-Site Request Forgery (CSRF)

09

Malicious file upload Attack

Placing files onto a server or computer in such a way that they contain some form of backdoor code

10

File inclusion Attack

Trick the application into exposing or running files on the server

11

SQL Login Injection

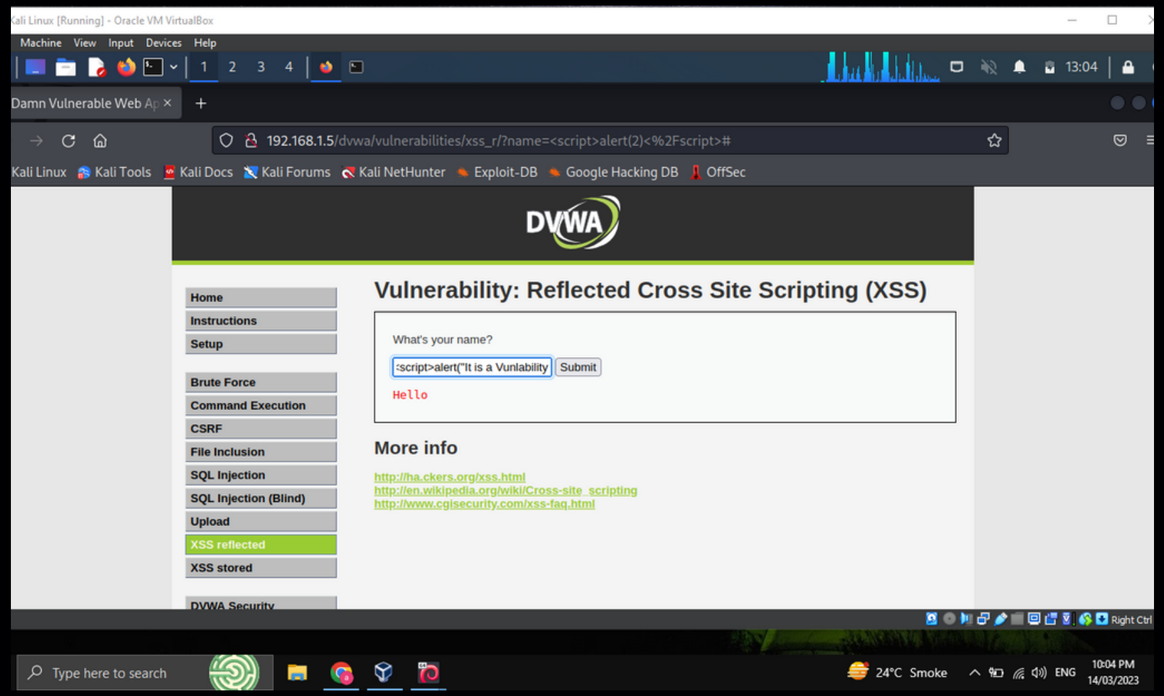
Bypass login page with using SQL language trick

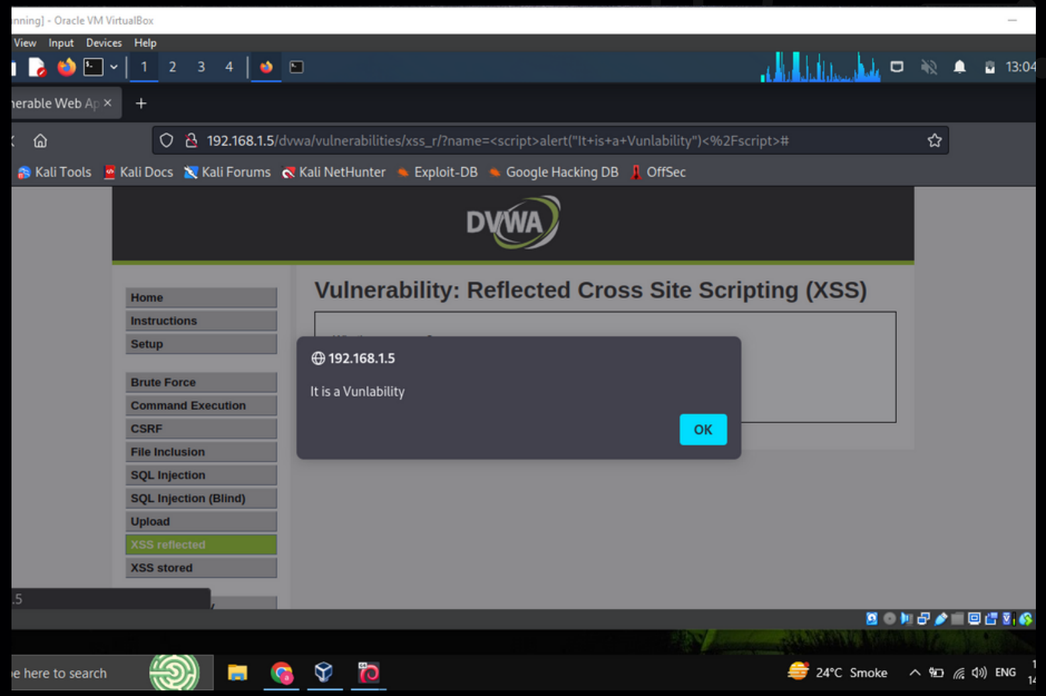
12

Brute force Attack

'guessing' usernames and passwords to gain unauthorized access to a system

XSS ATTACK(REFLECTED)





Code:

<script>alert("Hello i am error")</script>

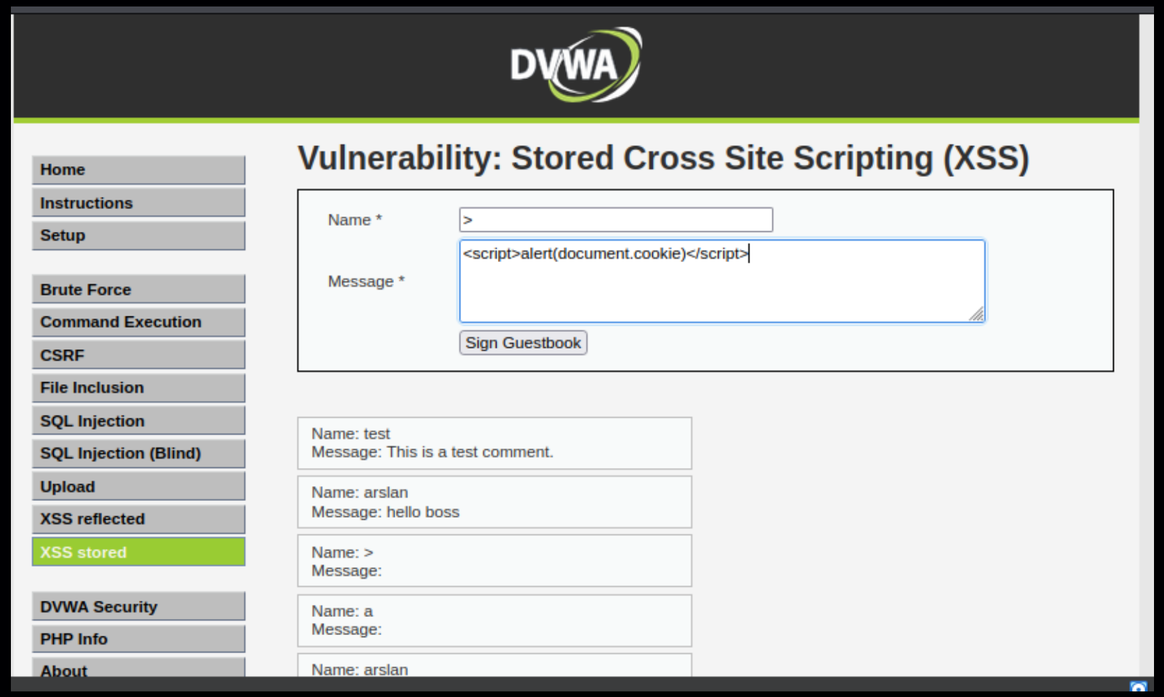
Severity:

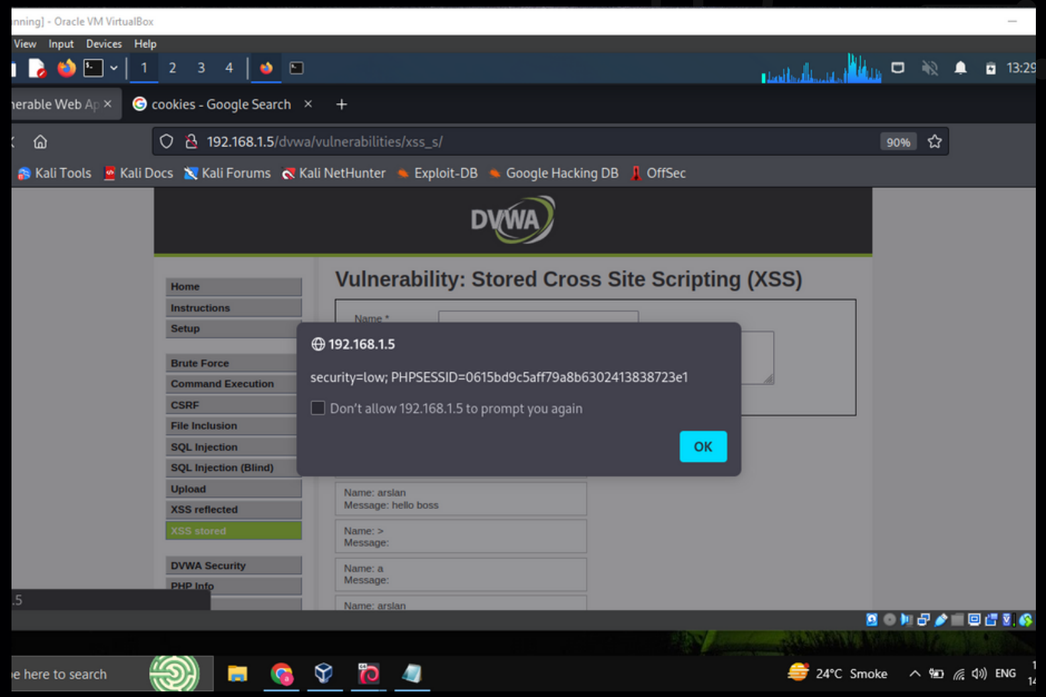
High

Risk:

- Steal sensitive information
- Steal cookies
- Modify the appearance of a website

XSS ATTACK(STORED)





Code:

<script>alert(document. cookie);</script>

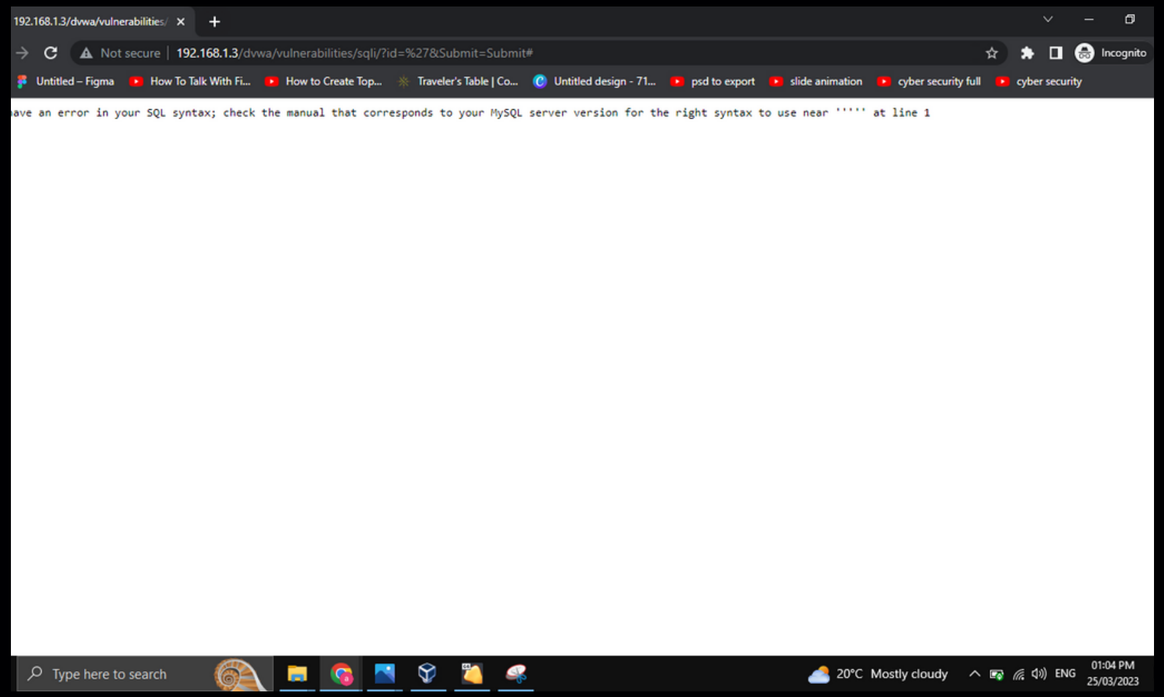
Severity:

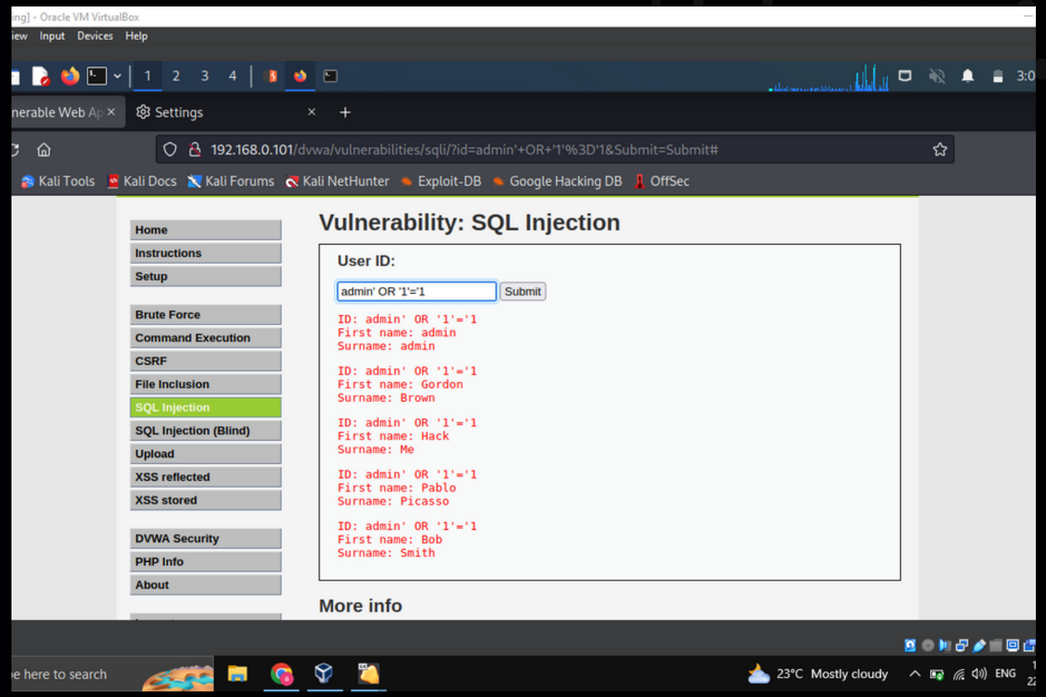
High

Risk:

- Session hijacking
- Malware distribution
- Steal cookies
- Website defacement

SQL INJECTION





Code:

admin' OR '1'='1

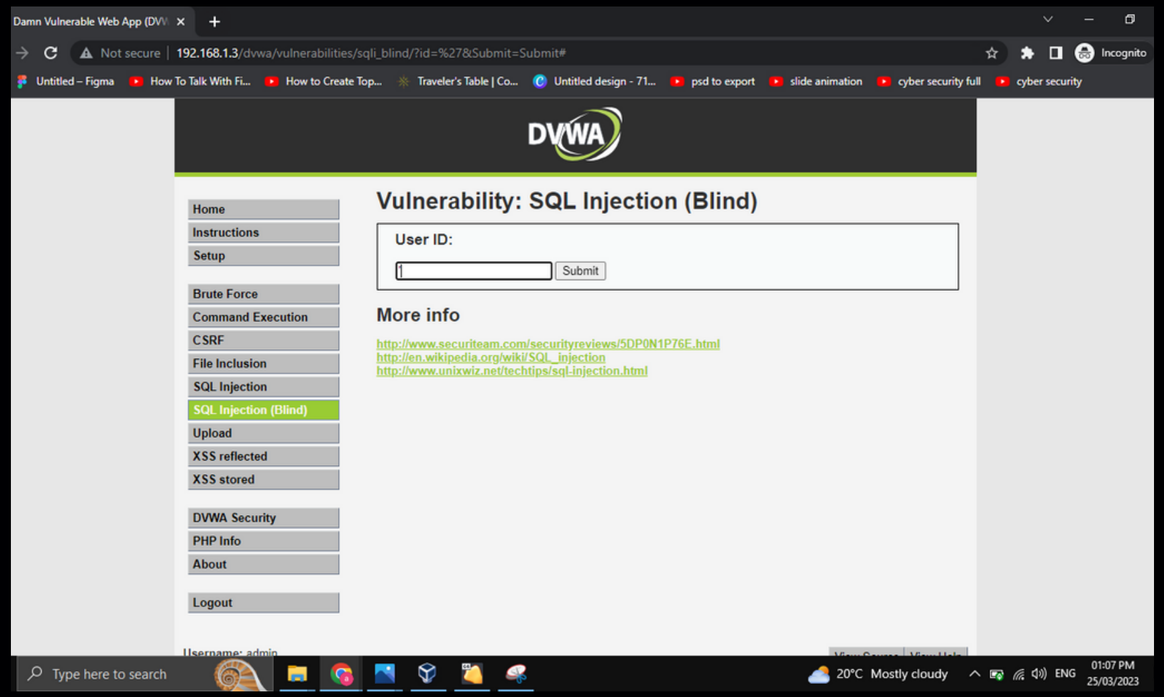
Severity:

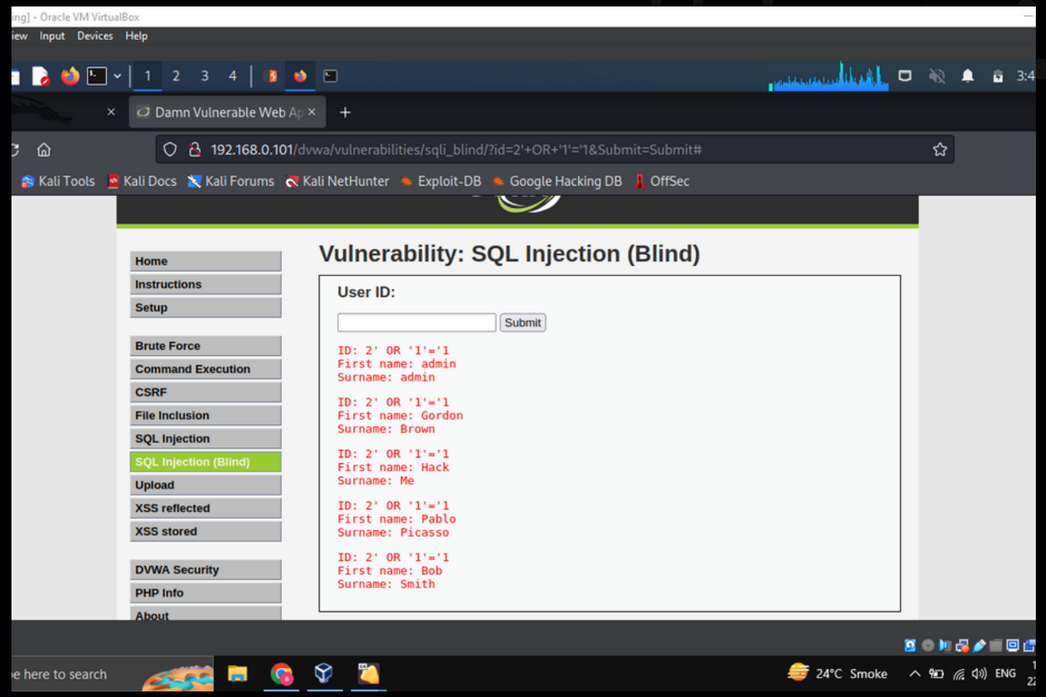
Critical

Risk:

- Unauthorized data access
- Data manipulation or deletion
- Server compromise

BLIND SQL INJECTION





Code:

admin' OR '1'='1

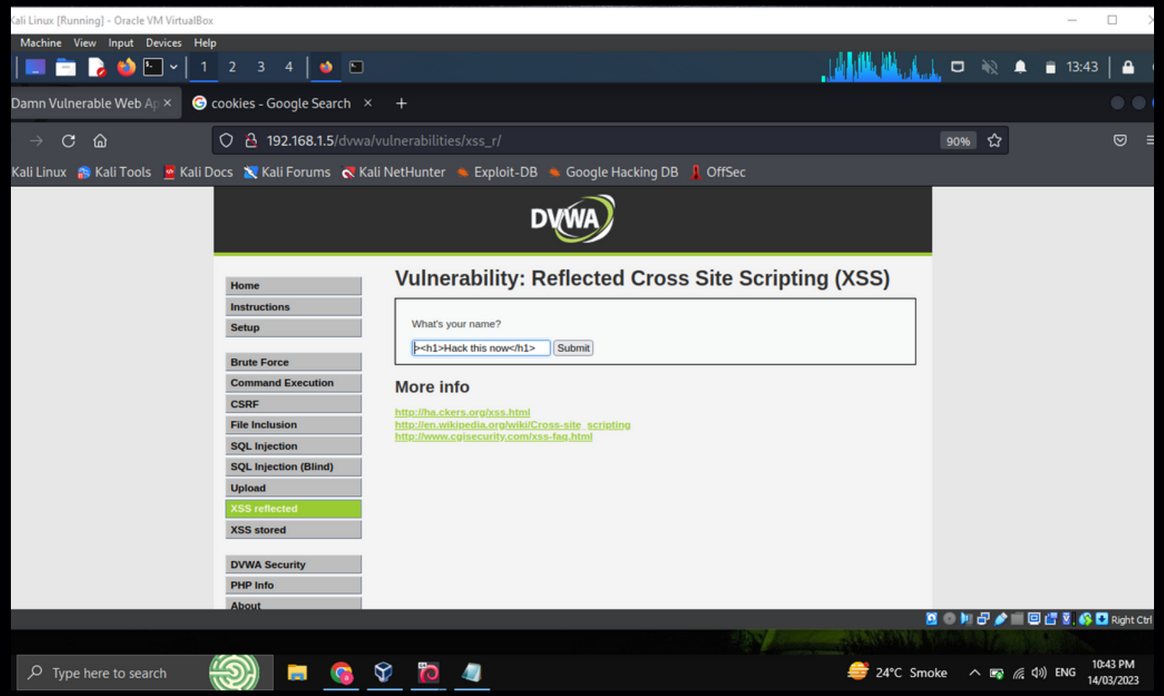
Severity:

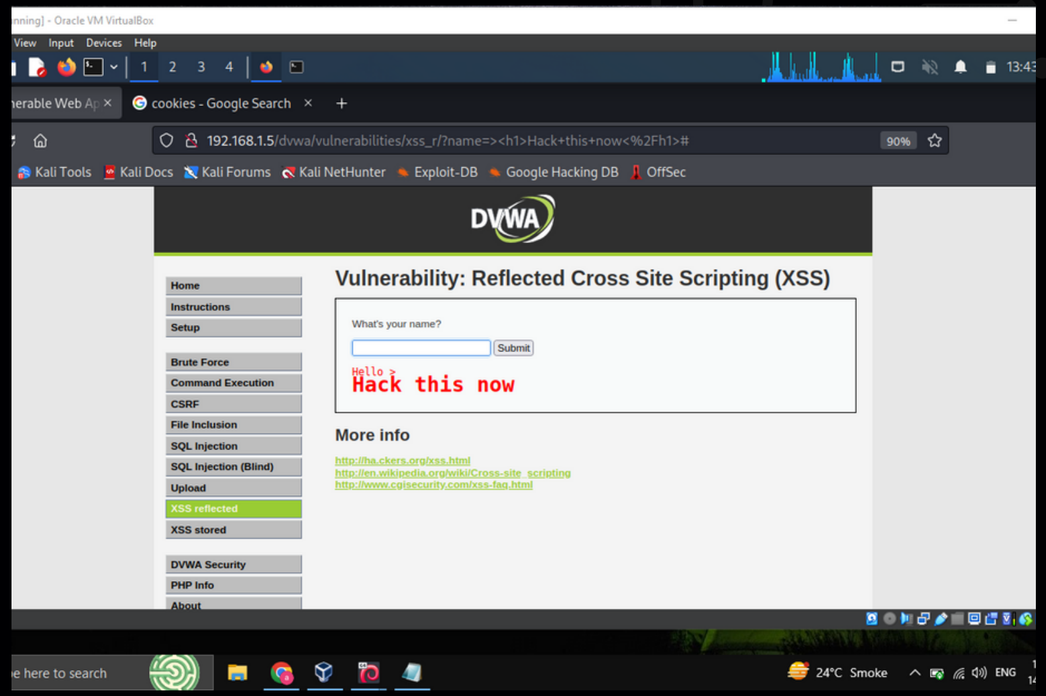
Critical

Risk:

- Unauthorized data access
- Data manipulation or deletion
- Server compromise

HTML INJECTION (REF)





Code:

><h1>Hack this now</h1>

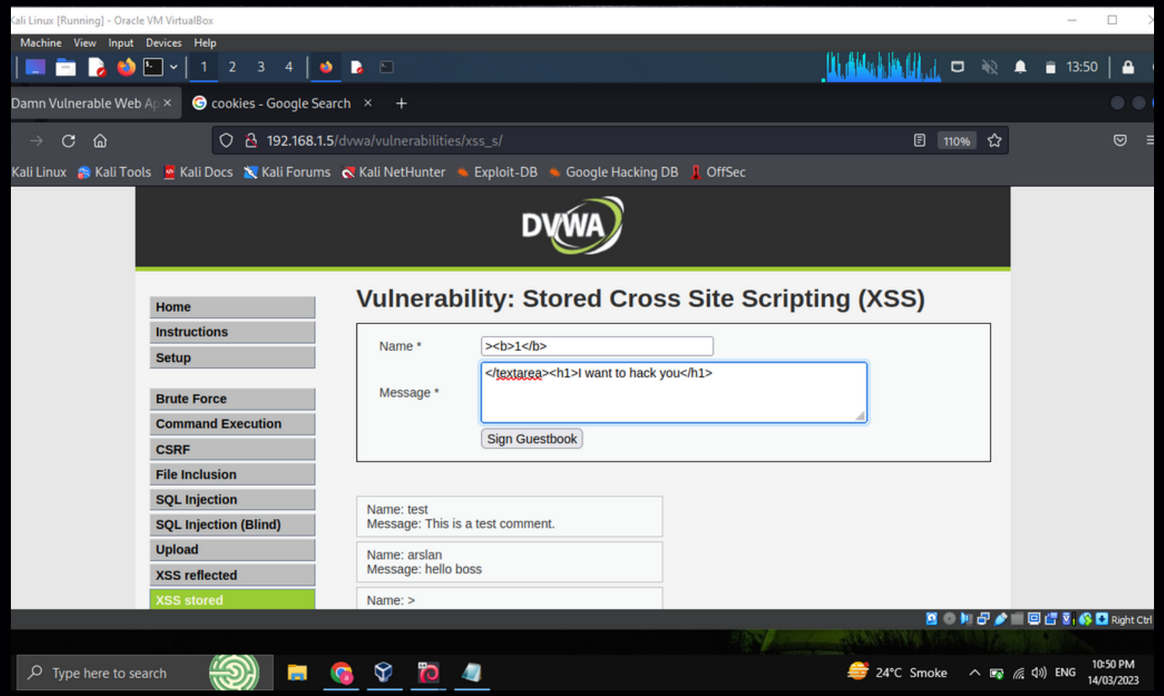
Severity:

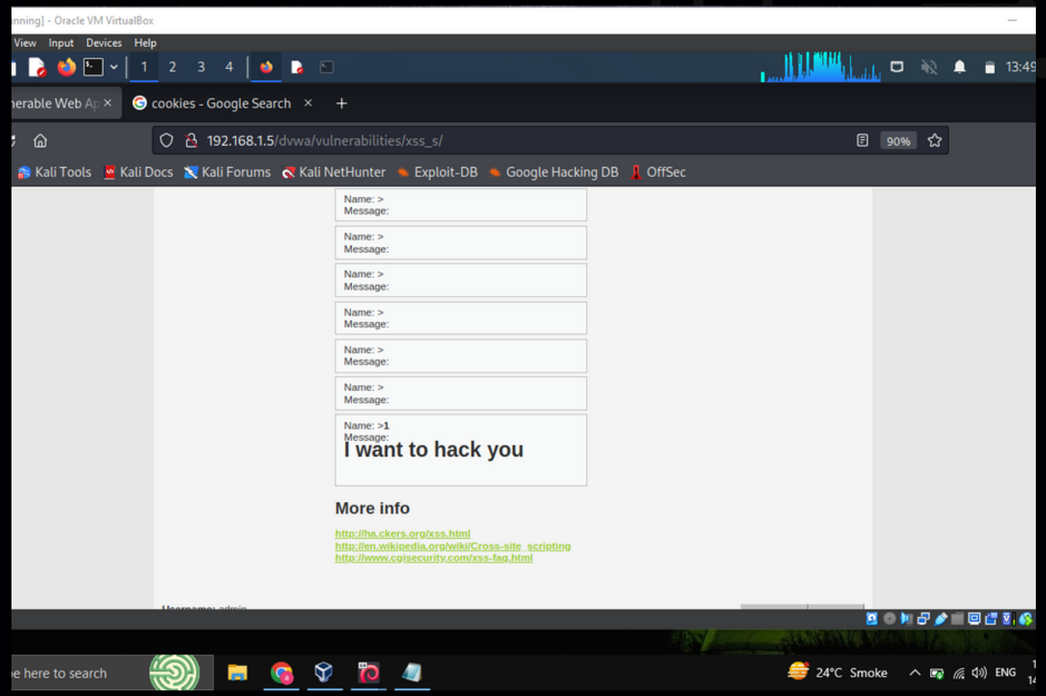
High

Risk:

- Steal sensitive information
- Steal cookies
- Modify the appearance of a website

HTML INJECTION (STORED)





Code:

/textarea><h1>I want to hack You</h1>

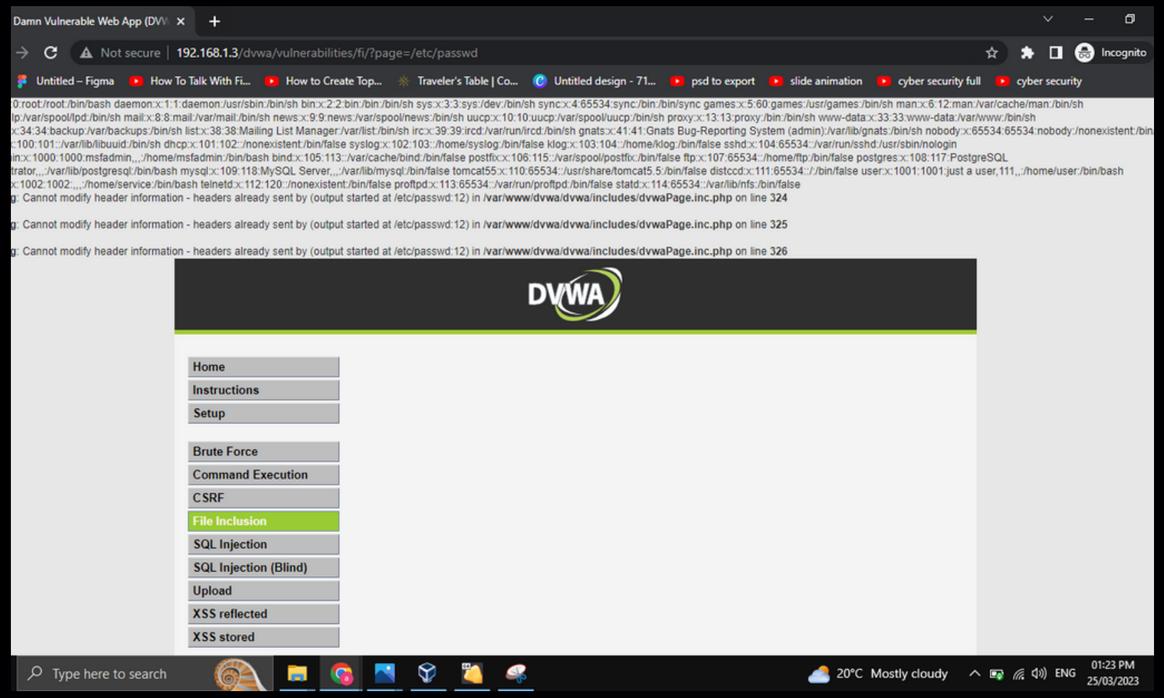
Severity:

High

Risk:

- Session hijacking
- Malware distribution
- Steal cookies
- Website defacement

FILE INCLUSION ATTACK



Code:

http://192.168.1.3/dvwa/vulnerabilities/fi/?page=/etc/passwd

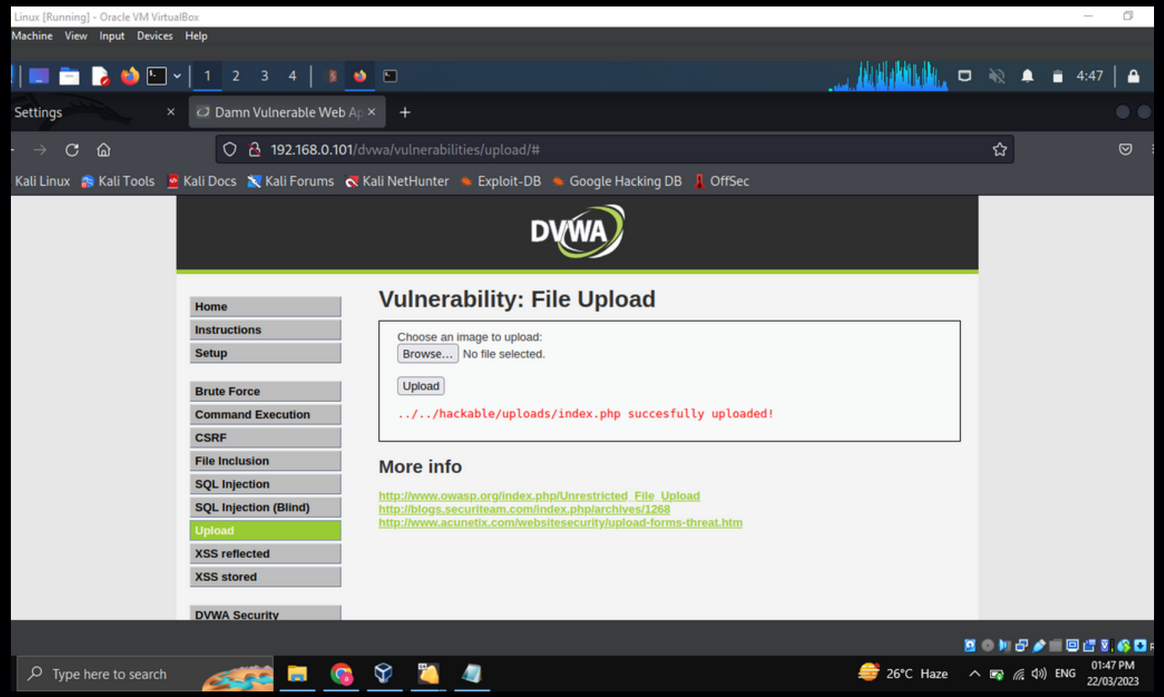
Severity:

Critical

Risk:

- Unauthorized access
- Information theft
- Malware distribution

MALICIOUS FILE UPLOAD



Code:

upload a malicious file like php or python file instead a jpg or png file.

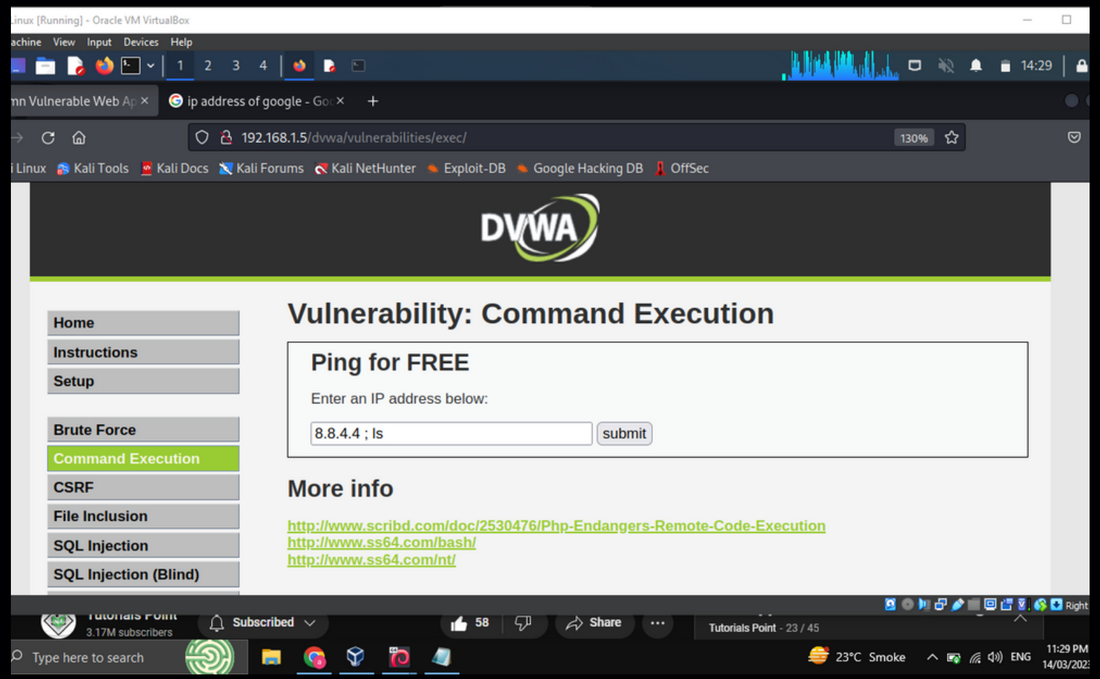
Severity:

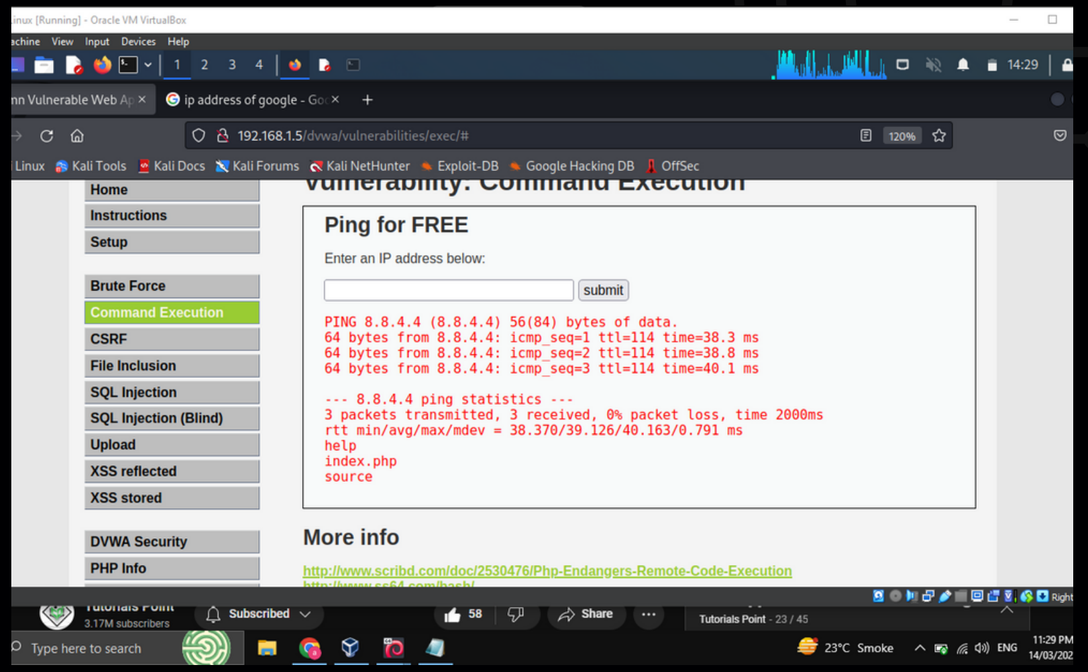
Critical

Risk:

- Server compromise
- Information theft
- Malware distribution

COMMAND LINE INJECTION





Code:

ping 8.8.4.4 and also ls

"8.8.4.4 ; ls"

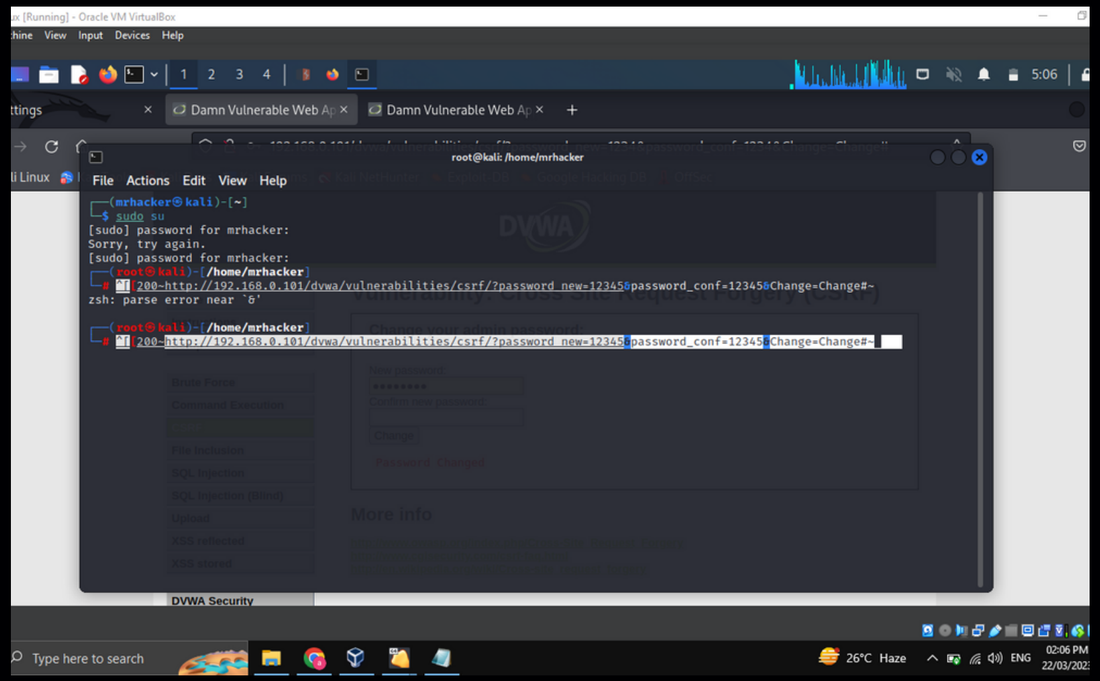
Severity:

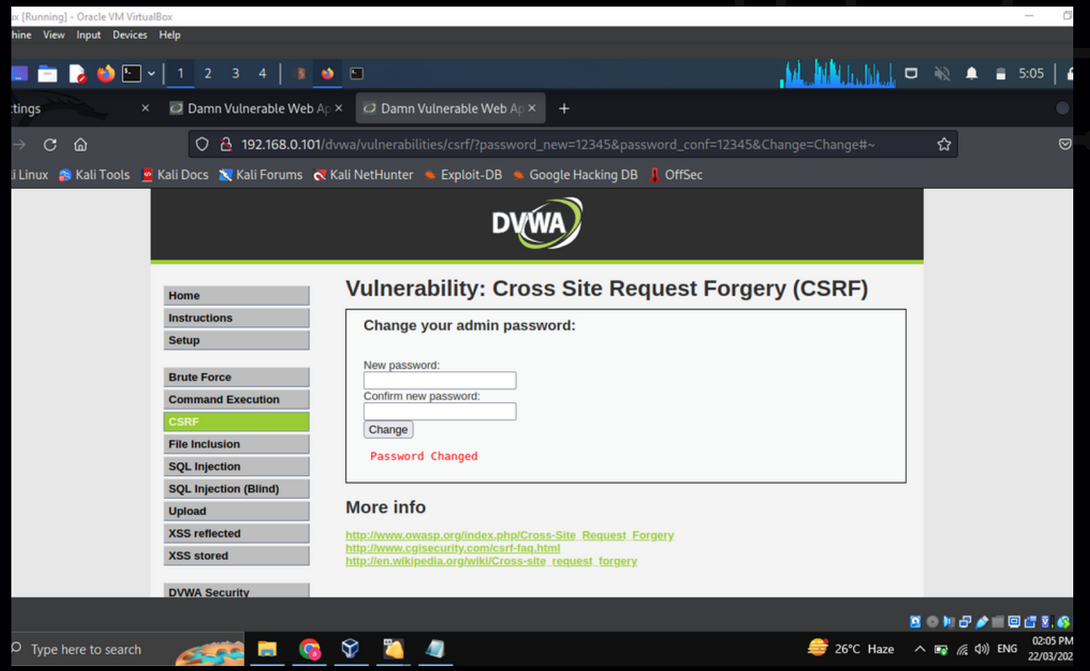
Criticala

Risk:

- Server compromise
- Information theft
- Malware distribution

CSRF ATTACK





Code:

http://192.168.0.101/dvwa/vulnerabilities/csrf/?password_current=password&password_new=1234&password_conf=1234&Change=Change#

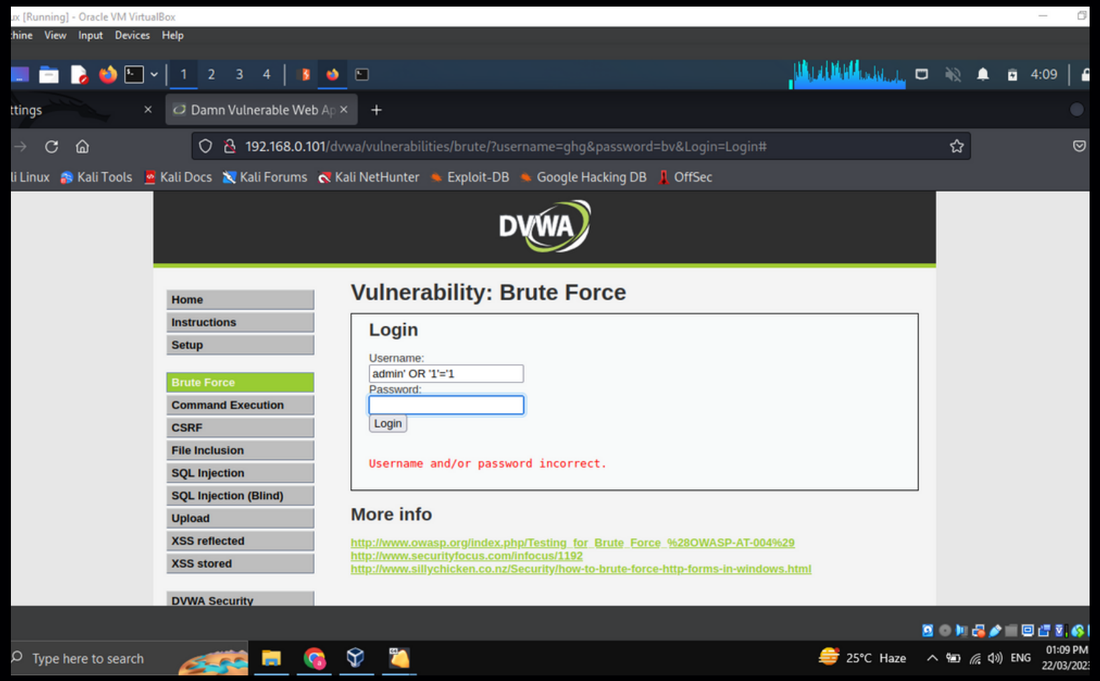
Risk:

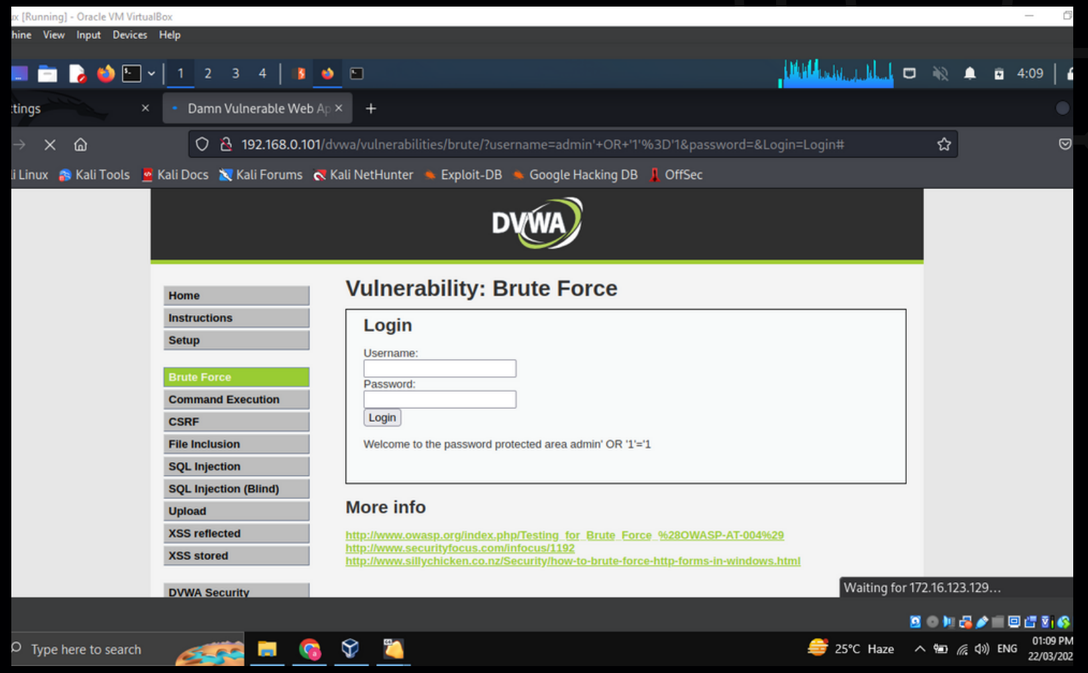
- Unauthorized actions
- Information theft
- Reputation damage

Severity:

Low

SQL LOGIN INJECTION





Code:

admin' OR '1'='1

Severity:

Critical

Risk:

- Unauthorized actions
- Information theft
- Reputation damage

DVWA

THANK YOU

SECURITY PRO