



INTERNSHIP PROJECT

Vulnerability Analysis

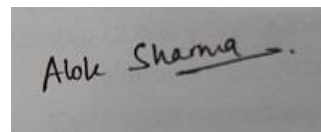
Submitted By
Alok Sharma

Alok Sharma
Alok2520sharma@gmail.com

CERTIFICATION

This is to certify that I Alok Sharma, have completed this project with the best of my ability. All the pentesting processes have been conducted by me and any discrepancy may lead to failure of submission.

Alok Sharma

A photograph of a handwritten signature "Alok Sharma" in black ink on a light-colored surface. The signature is written in a cursive style with a horizontal line underlining the name.

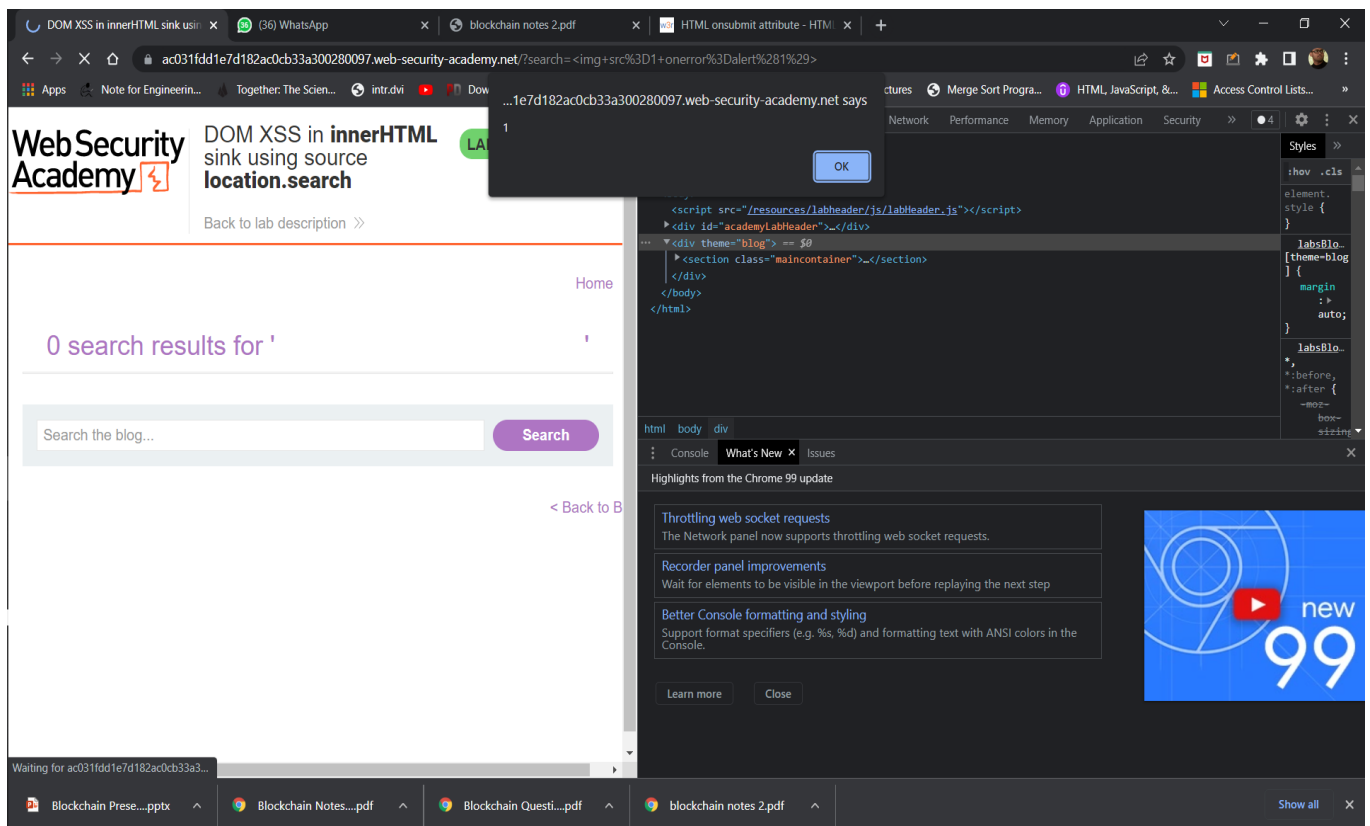
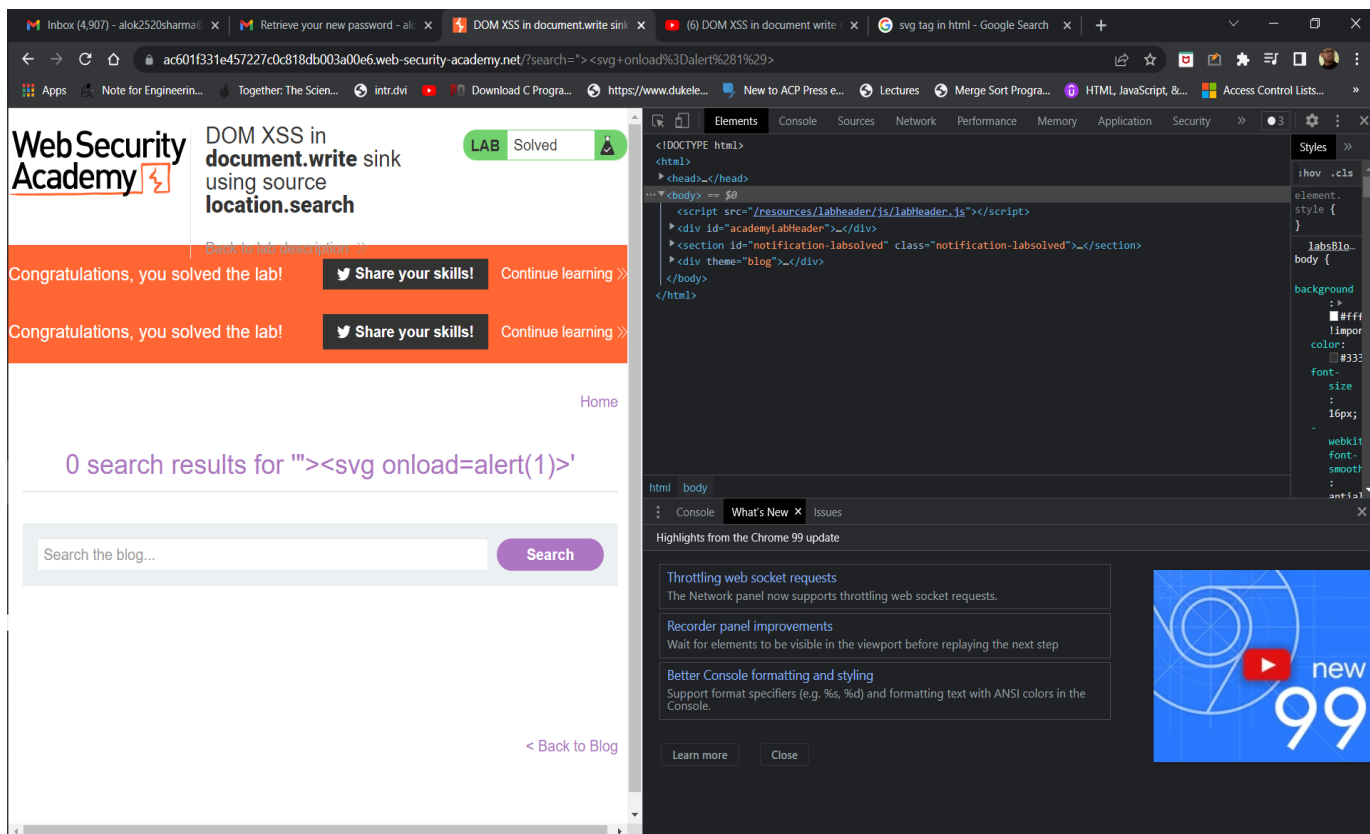
Note : All the tasks have been done by me while on my trek holiday. This has lead to failure of downloading Netsparker and Metasploit.

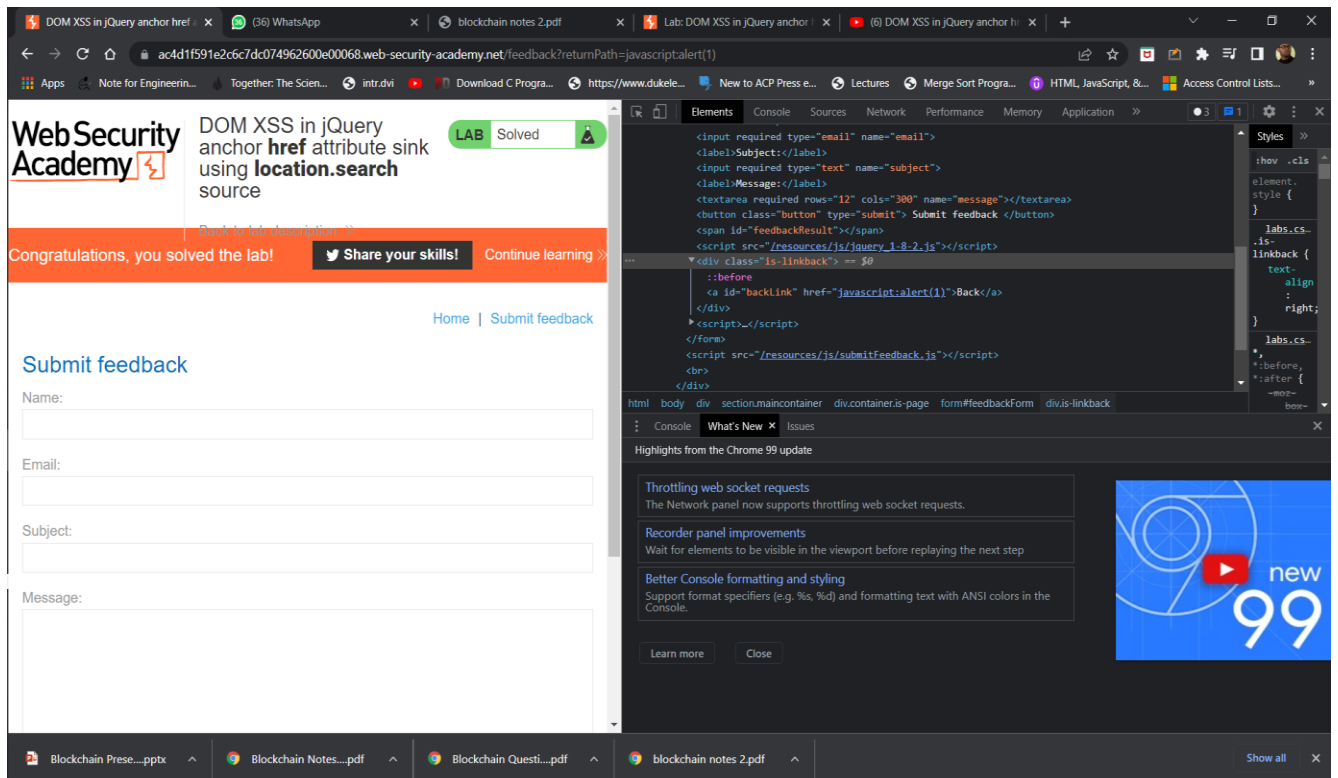
Intentionally left blank

Task 1: XSS Labs

The screenshot shows a web browser window with multiple tabs. The active tab is titled "Stored XSS into HTML context with nothing encoded" and the URL is "acc61f671eabea45c02c0e460091007f.web-security-academy.net/post/comment/confirmation/postId=1". The page header includes the "Web Security Academy" logo and a "LAB Solved" badge. A green banner at the top of the main content area reads "Congratulations, you solved the lab!". Below this, a purple heading says "Thank you for your comment!" followed by the text "Your comment has been submitted." and a "< Back to blog" link. A "Home" link is also visible in the top right of the content area.

The screenshot shows the same web browser window, but now displaying the comment form. The form contains a pre-written comment: "I was having the best date ever. Until he said his favourite blog wasn't yours? I could put up with the previous jail time but not that." Below the comment is a section titled "Leave a comment" with a "Comment:" label. The comment text area contains the payload "<script>alert(1)</script>". Below the text area are input fields for "Name:" (containing "frferf"), "Email:" (containing "feggager@gmail.com"), and "Website:" (containing "https://www.google.com"). A purple "Post Comment" button is at the bottom left, and a "< Back to Blog" link is at the bottom right.





Task 2

Failed to download the Netsparker application.

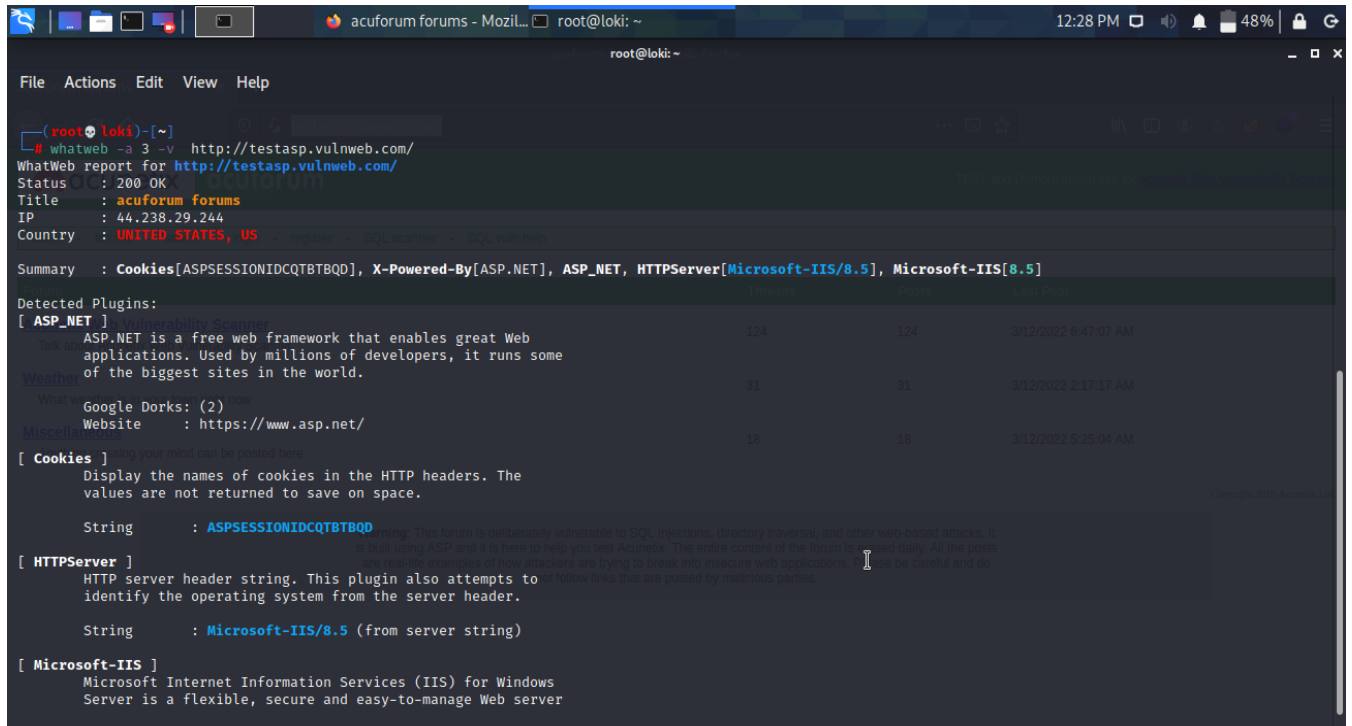
Task 3

Target website : <http://www.testasp.vulnweb.com>

Information gathering

Whatweb command:

Syntax : whatweb -A -v -Pn < IP Address >



```
(root@loki)-[~]
# whatweb -a 3 -v http://testasp.vulnweb.com/
WhatWeb report for http://testasp.vulnweb.com/
Status : 200 OK
Title : acuforum forums
IP : 44.238.29.244
Country : UNITED STATES, US

Summary : Cookies[ASPSESSIONIDCQTBTBQD], X-Powered-By[ASP.NET], ASP.NET, HTTPServer[Microsoft-IIS/8.5], Microsoft-IIS[8.5]

Detected Plugins:
[ ASP.NET ]
ASP.NET is a free web framework that enables great Web applications. Used by millions of developers, it runs some of the biggest sites in the world.

[ Cookies ]
Display the names of cookies in the HTTP headers. The values are not returned to save on space.
String : ASPSESSIONIDCQTBTBQD

[ HTTPServer ]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.
String : Microsoft-IIS/8.5 (from server string)

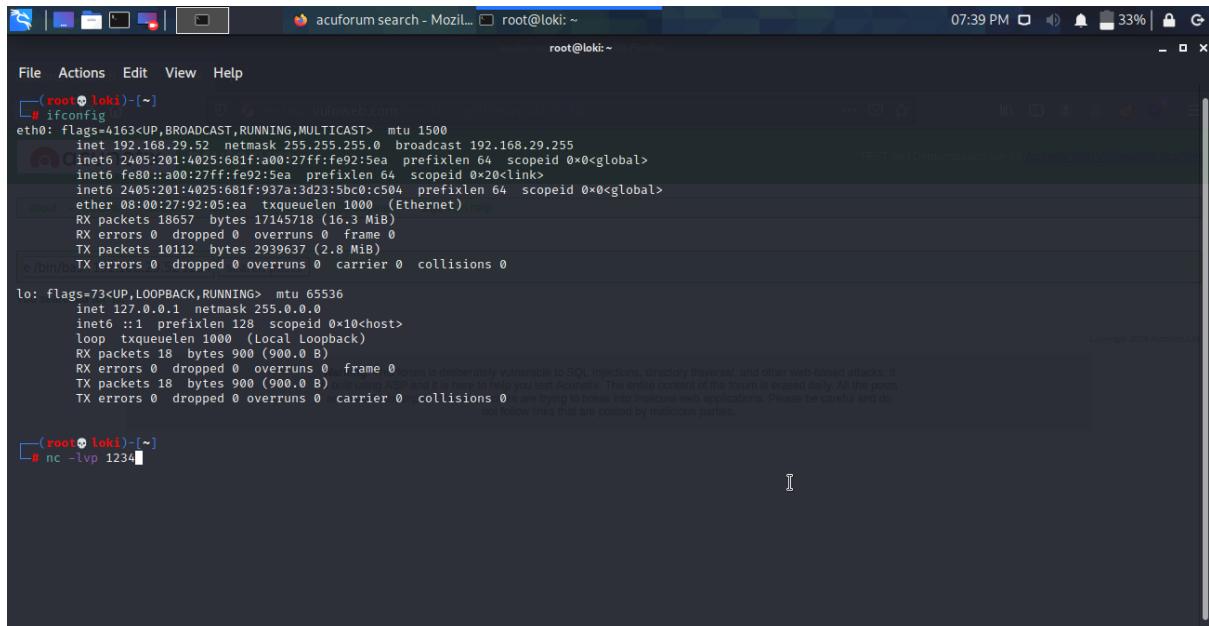
[ Microsoft-IIS ]
Microsoft Internet Information Services (IIS) for Windows
Server is a flexible, secure and easy-to-manage Web server
```

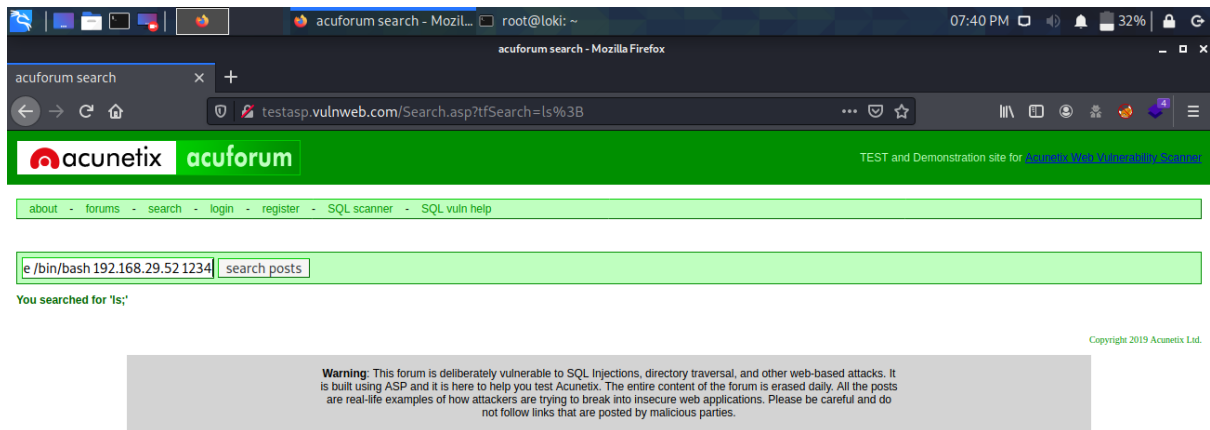
Command Line Injection :



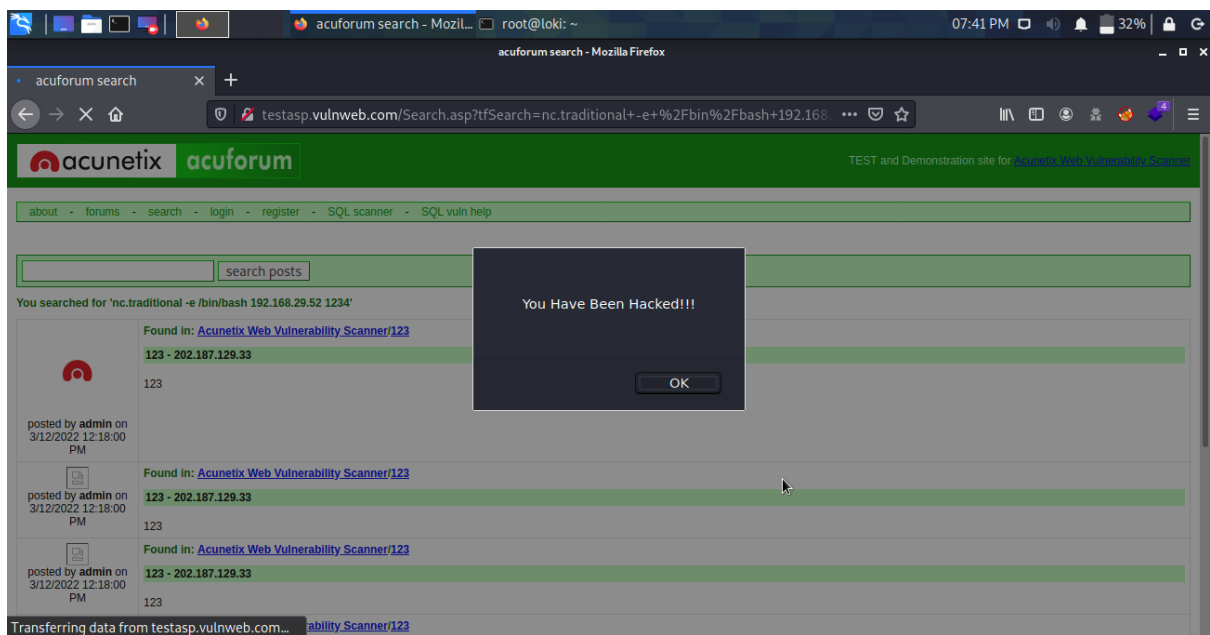
Result : Command injection gives no results.

Blind Line Injection

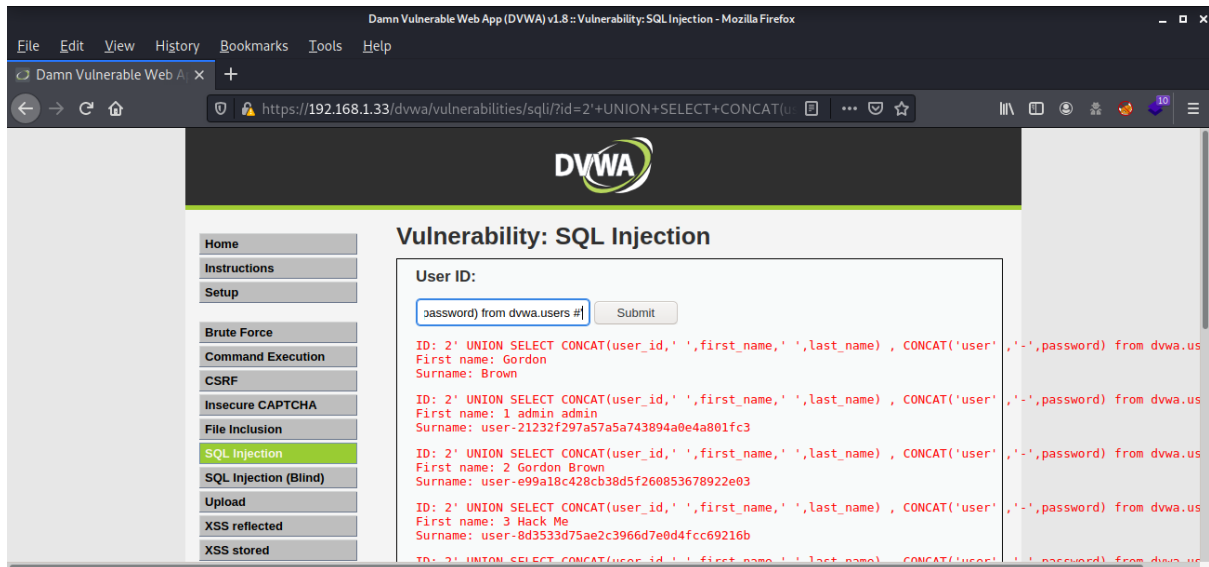




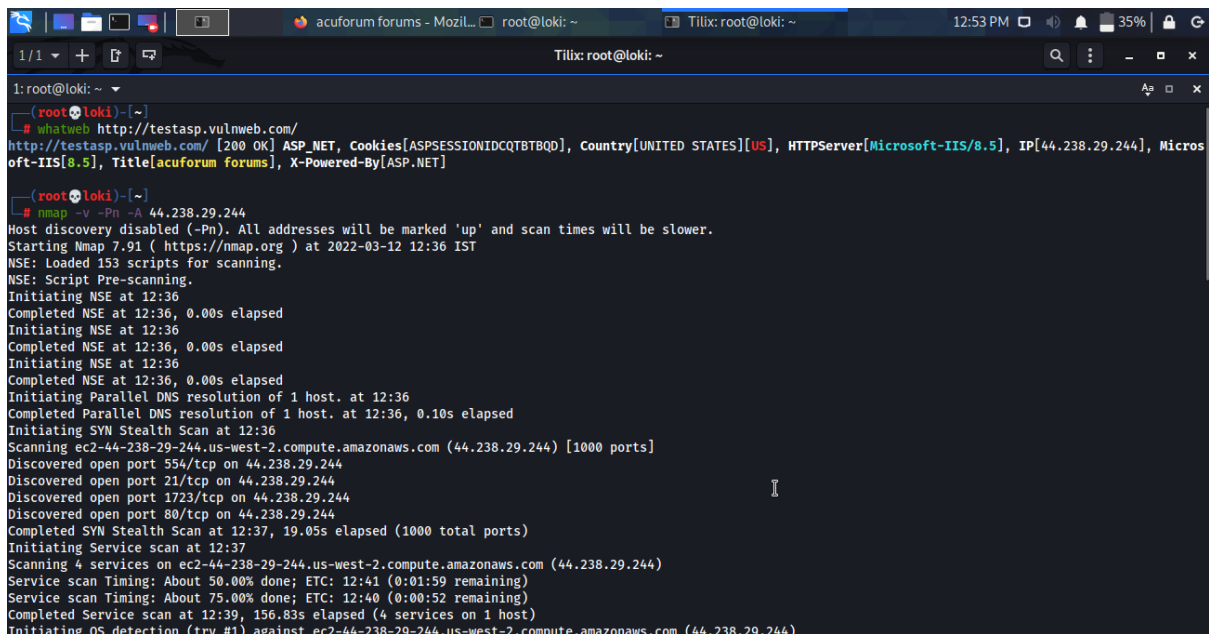
Result :



Checking SQL Injection



Using Nmap



Using Metasploit

