Name – Devasy Patel

Roll Number – 20BCE057

Subject – Ethical Hacking and Vulnerability Assessment Practical – 1

Aim: Practical 1 involves compiling a report on your learnings about -

- Overview of Information Security
- The browser security-related information
- Overview of the Contents of a Digital Certificate
- Implementing a fake authentication to carry out phishing attack: 1. Identify a website to carry out fake authentication i.e. recreating the

Cyber Security has become today's need based on the tremendous growth in the volume of data and people's growing awareness regarding the privacy of their data!

There are various types of security like:

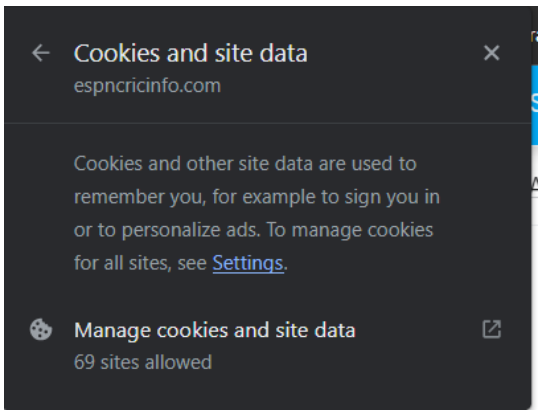
1) Information Security
2) Network Security
3) Application Security
4) Web Security
5) Secure Wi-Fi communication using methods like Cryptography and Hashing

In the 1st practical, we explored the basics of browser security. It deals with the security of the websites on internet. With the growth in the number of

websites, it is of prime importance to ensure that the users have safe browsing!

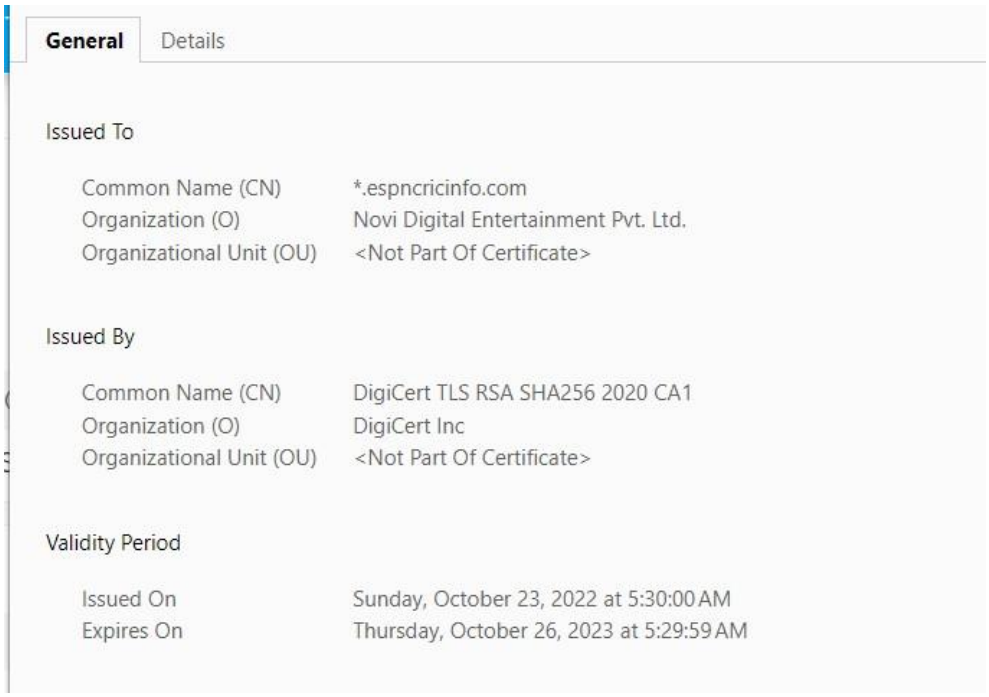
A website is not only the page that appears. It contains 2 major backend parts, that are:

1) Cookies – they are used to remember the user and track the user's browsing pattern (called user profiling) for better and personalized recommendations and advertisements.



2) Digital Certificates

A digital certificate can be used to confirm the legitimacy and identification of websites and organizations. A Certificate Authority (CA), a dependable third party, issues it and digitally signs it. This is particularly useful in preventing Man in the Middle (MitM) attacks!



Few attacks on websites include:

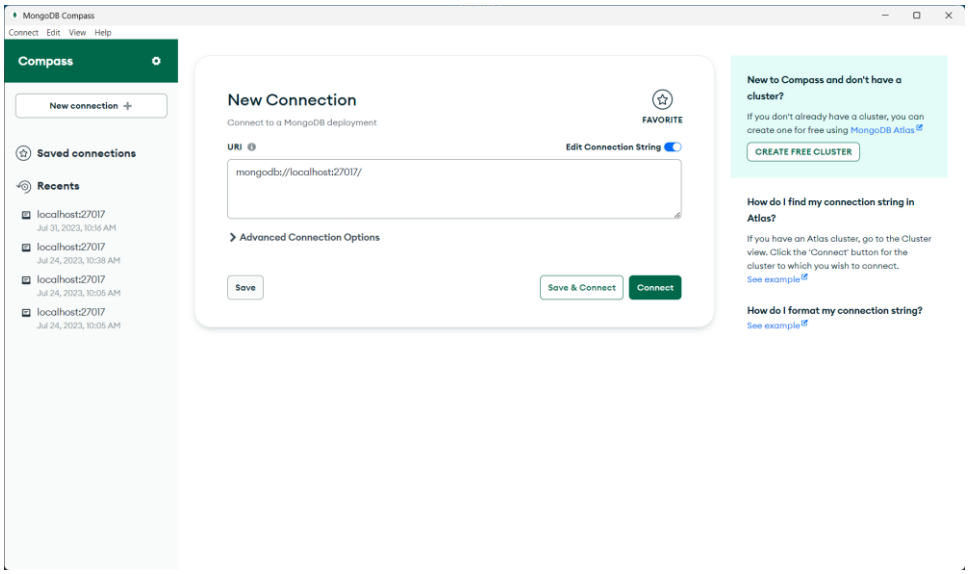
1) Cross-Site Scripting (XSS): Injecting malicious scripts into web pages using JavaScript, thereby stealing sensitive information like username and password of the users.
2) SQL Injection (SQLi): Manipulating SQL Queries to get unauthorized and unrestricted entry in the database.
3) Phishing: Deceptive techniques to trick users into providing sensitive information, such as passwords or credit card details.

In this practical, we demonstrated a Phishing attack.

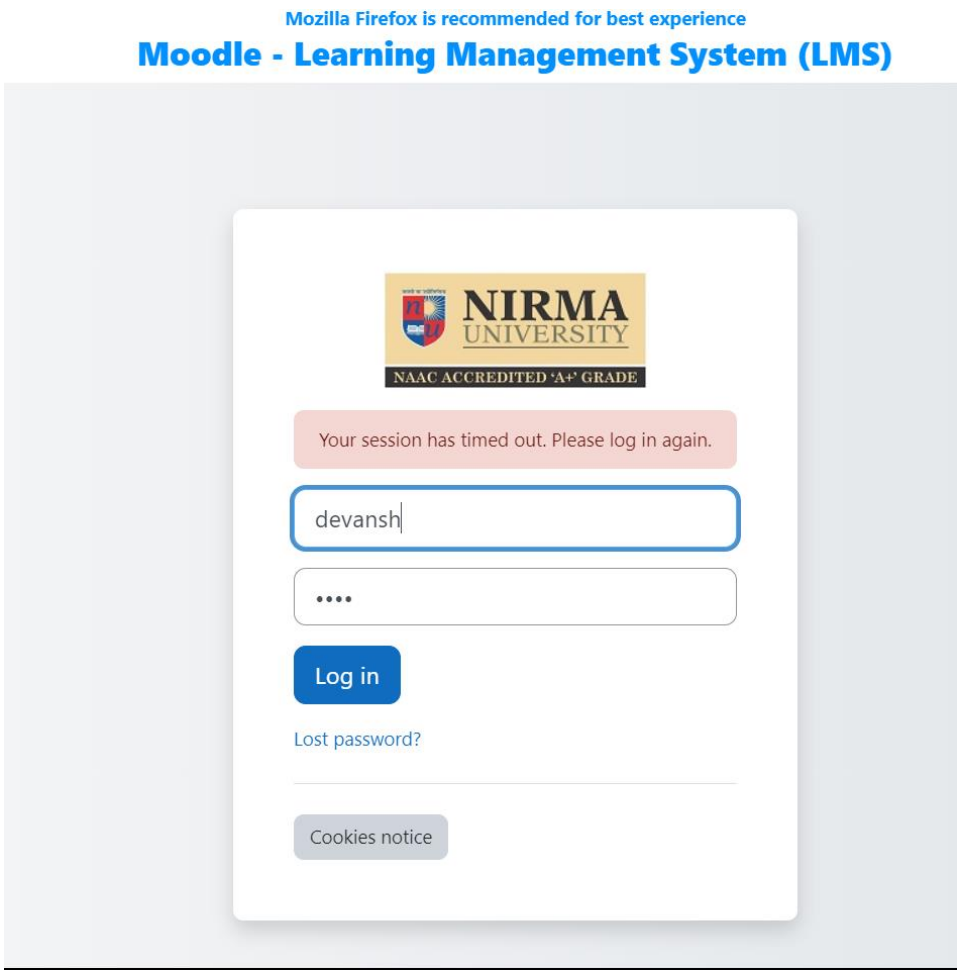
Steps:

1) Cloning an actual website
2) Connecting it to database
3) Capturing the user's credentials entered
4) Redirecting the user to the actual login page

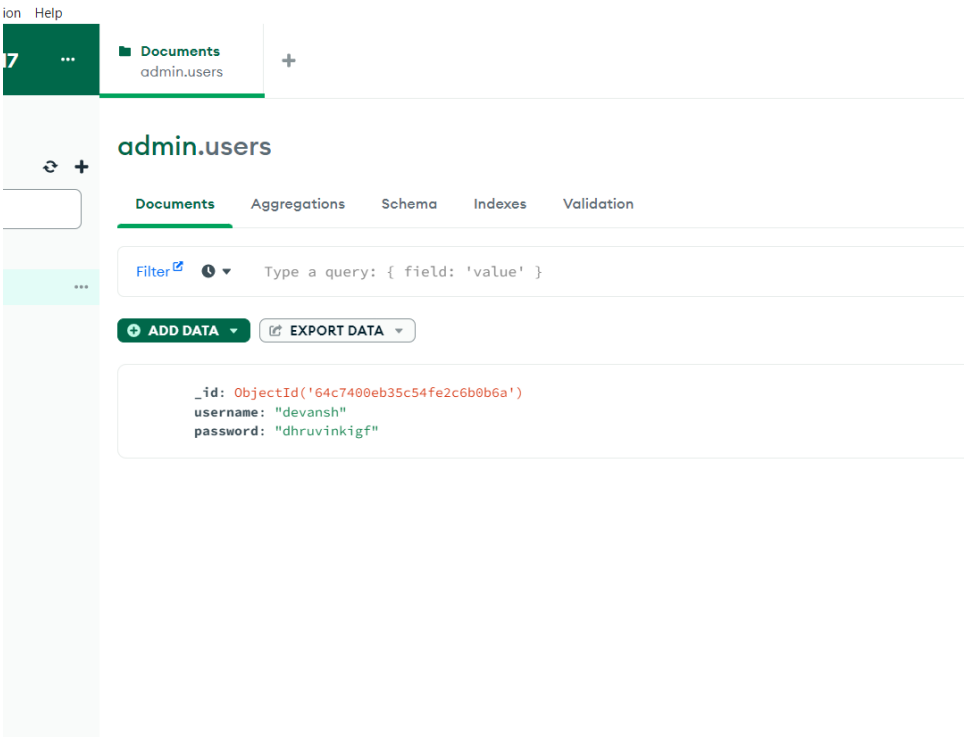
Screenshots:



Starting Mongo DB server to and connect with its database



Entering my username and password



Displaying the entered Credentials