Experiment 09

AIM - Perform and analyze at least 2 injection attacks

Learning Objective: Students should be able to perform and analyze sql injection and html injection attack

Tools: Virtual Machine, Linux

Theory:

An **injection attack** is a form of cyberattack in which information is sent to alter the system's interpretation of commands. An attacker sends harmful information to the interpreter during an injection attack. An injection attack can be done on data from many different places, like environment variables, parameters, online services, and user types, but not just those.

Different types of injection attack are

1. **SQL Injection Attack (SQLi) :**

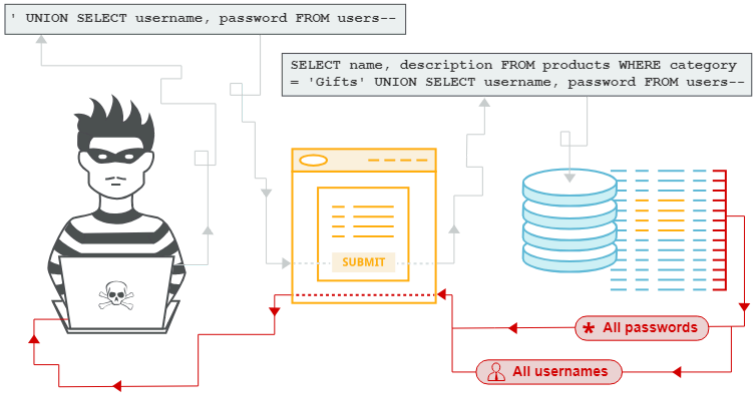
   SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. This can allow an attacker to view data that they are not normally able to retrieve. This might include data that belongs to other users, or any other data that the application can access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

   In some situations, an attacker can escalate a SQL injection attack to compromise the underlying server or other back-end infrastructure. It can also enable them to perform denial-of-service attacks.

   A successful SQL injection attack can result in unauthorized access to sensitive data, such as:

   - Passwords.
   - Credit card details.
   - Personal user information.

   SQL injection attacks have been used in many high-profile data breaches over the years. These have caused reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.

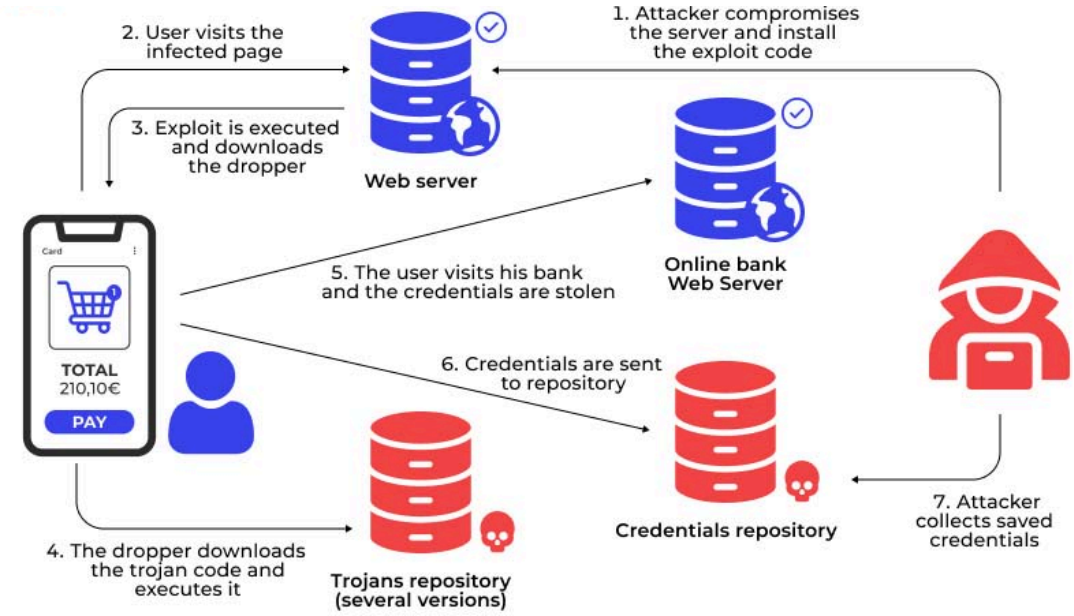


2. **HTML Injection Attack :**

HTML injection is a type of attack where malicious HTML code is inserted into a website. This can lead to a variety of issues, from minor website defacement to serious data breaches. Unlike other web vulnerabilities, HTML injection targets the markup language that forms the backbone of most websites.

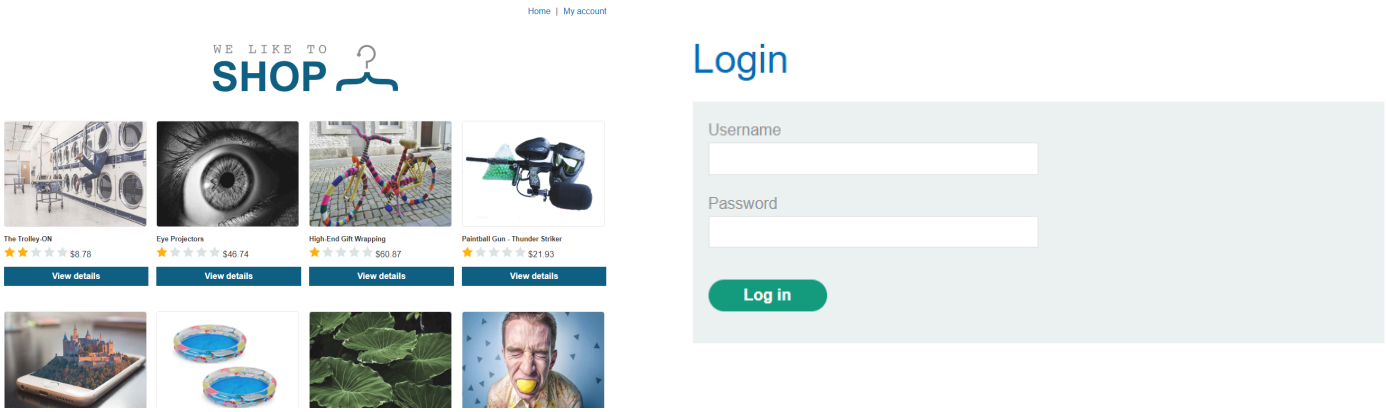
This attack differs from other web vulnerabilities that exploit server or database weaknesses because it focuses on manipulating the structure and content of a webpage.
There are different types of HTML Injection Attack -

- **Stored HTML Injection**
  Stored HTML injection, also known as persistent injection, is a type of attack where the malicious code is permanently stored on the target server. This code is then served to users every time they access a particular page. Once the malicious code is in place, it can affect a large number of users without the attacker having to do anything further.
- **Reflected HTML Injection**
  Unlike stored injections, reflected attacks are not permanently housed on the server. Instead, they trick users into executing malicious code via a URL. This is often achieved through phishing emails or messages that lure users into clicking on a compromised link.
- **DOM-based HTML Injection**
  The attack targets the Document Object Model (DOM) of a webpage, which represents the page's structure. By manipulating the DOM, attackers can introduce malicious scripts that get executed client-side.

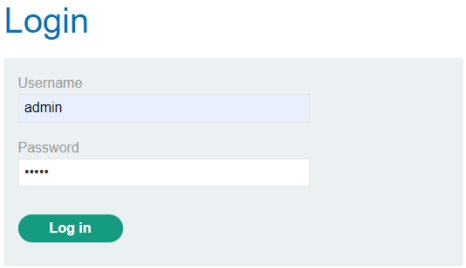


SQL Injection :

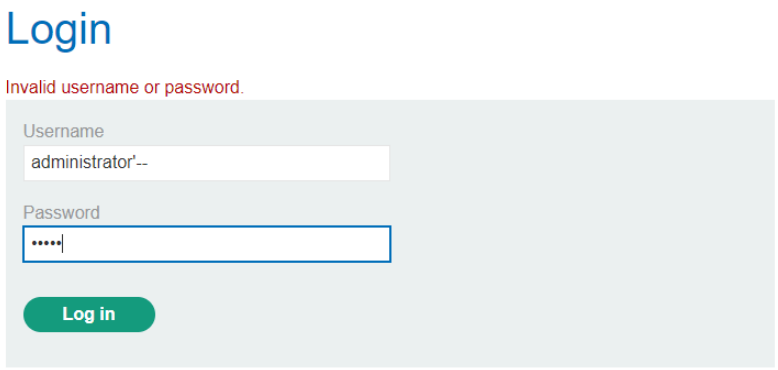
Step 1 : Goto https://portswigger.net/web-security/sql-injection/lab-login-bypass



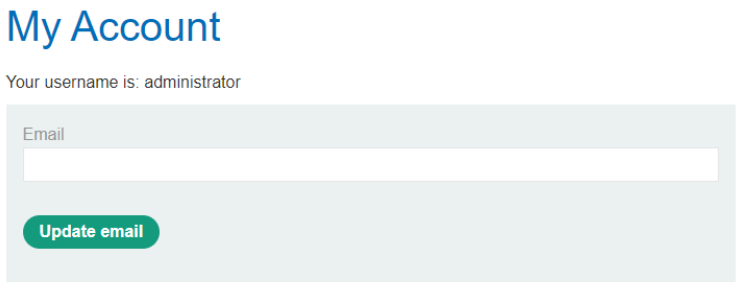
Step 2 : Enter username as **admin** and password as **admin**



Step 3 : It says invalid password, now enter the username as administrator'-- and password as admin

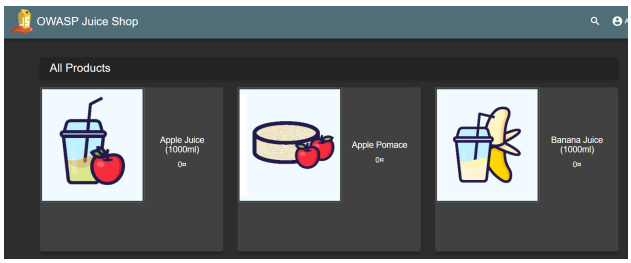


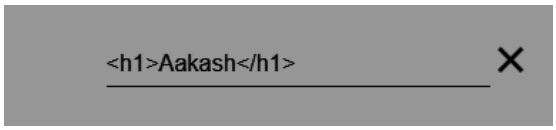
Step 4 : We have successfully login now can update the email address

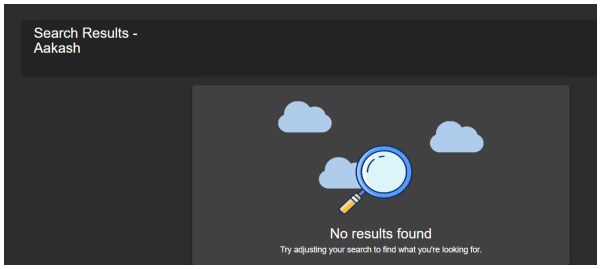


HTML Injection :

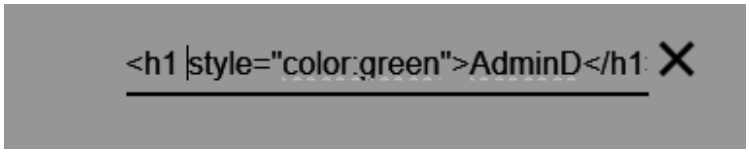
Step 1 : Goto https://juice-shop.herokuapp.com/ and search for **This is HTML Injection by Aakash.**

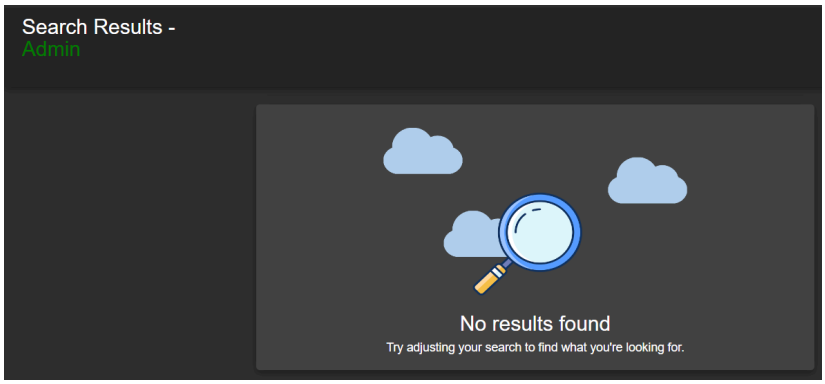






Step 2 : We can modify the input search text as a h1 tag **<h1 style="color: red; font-size:50px"> This is HTML Injection by Aakash</h1>**





Learning Outcomes:
The student should be able to perform various injection attacks
LO1: To understand & implement SQL injection attack
LO2: To understand & implement HTML injection attack

Course Outcomes: Upon completion of the course students will be able to understand & perform various injection attacks

Conclusion:
From this experiment, we were able to understand what an injection attack is and its various types. Furthermore we studied about two injection attacks i.e. SQL injection and HTML injection attack and perform the same.

For Faculty Use:

Correction Parameters	**Formative Assessment [40%]**	**Timely completion of Practical [40%]**	**Attendance / Learning Attitude [20%]**	
Marks Obtained				