



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Batch: _____ **C2** _____ **Roll**
No.: _____ **16010121110** _____
Experiment No. 4

Title: SQL injection using burp suite

Objective: To hack websites using the burp suite software

Expected Outcome of Experiment:

CO	Outcome
CO3	Identify and analyze web attacks

Books/ Journals/ Websites referred:

<https://portswigger.net/web-security/all-labs>

<https://www.pluralsight.com/paths/web-security-testing-with-burp-suite#:~:text=Burp%20Suite%20is%20an%20integrated,finding%20and%20exploiting%20security%20vulnerabilities.>

Abstract:-

Burp Suite is an integrated platform and graphical tool for performing security testing of web applications, it supports the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

vulnerabilities. It is a comprehensive platform for web application security testing. It is developed by PortSwigger Security. Burp Suite is widely used by cybersecurity professionals, including penetration testers, security researchers, and web developers, to identify security vulnerabilities in web applications.

Related Theory: -

Burp Suite is a popular and powerful toolkit designed for web security testing, also known as penetration testing or pen testing. It offers a comprehensive set of tools to help security professionals identify and exploit vulnerabilities in web applications before malicious actors can.

Ethical Usage:

- **Penetration Testing with Permission:** Ethical pen testing involves testing the security of a web application with the explicit consent and cooperation of the owner. This allows security professionals to identify and report vulnerabilities before they can be exploited in real-world attacks.
- **Learning and Research:** Burp Suite can be a valuable tool for learning about web security vulnerabilities and how to mitigate them. However, it's crucial to use it responsibly and avoid any actions that could be considered illegal or harmful.

Key Features:






- **Intercept and Modify Traffic:** Burp Suite allows you to intercept and modify HTTP traffic between your browser and a web server. This can be used to test for vulnerabilities such as SQL injection and cross-site scripting (XSS).
- **Scan for Vulnerabilities:** Burp Suite includes an automated scanner that can identify common web vulnerabilities. However, it's important to note that manual testing is still essential for comprehensive security testing.
- **Security Analysis Tools:** Burp Suite provides various tools for analyzing web security, such as a decoder, encoder, and repeater. These can be helpful for understanding and exploiting vulnerabilities.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering







Implementation Details:

Solved almost all SQL injection LABS from portswigger website. These labs contain dummy websites. In order to solve the labs, we have to figure out how to inject malicious code into the website as per the topic.

 LAB	APPRENTICE SQL injection vulnerability in WHERE clause allowing retrieval of hidden data →	✓ Solved
 LAB	APPRENTICE SQL injection vulnerability allowing login bypass →	✓ Solved
 LAB	PRACTITIONER SQL injection attack, querying the database type and version on Oracle →	✓ Solved
 LAB	PRACTITIONER SQL injection attack, querying the database type and version on MySQL and Microsoft →	✓ Solved
 LAB	PRACTITIONER SQL injection attack, listing the database contents on non-Oracle databases →	✓ Solved










Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

 LAB	PRACTITIONER SQL injection attack, querying the database type and version on MySQL and Microsoft →	✓ Solved
 LAB	PRACTITIONER SQL injection attack, listing the database contents on non-Oracle databases →	✓ Solved
 LAB	PRACTITIONER SQL injection attack, listing the database contents on Oracle →	✓ Solved
 LAB	PRACTITIONER SQL injection UNION attack, determining the number of columns returned by the query →	✓ Solved
 LAB	PRACTITIONER SQL injection UNION attack, finding a column containing text →	✓ Solved
 LAB	PRACTITIONER SQL injection UNION attack, retrieving data from other tables →	✓ Solved



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

 LAB	PRACTITIONER SQL injection UNION attack, retrieving multiple values in a single column →	✓ Solved
 LAB	PRACTITIONER Blind SQL injection with conditional responses →	✓ Solved
 LAB	PRACTITIONER Blind SQL injection with conditional errors →	✓ Solved
 LAB	PRACTITIONER Visible error-based SQL injection →	✓ Solved
 LAB	PRACTITIONER Blind SQL injection with time delays →	✓ Solved
 LAB	PRACTITIONER Blind SQL injection with time delays and information retrieval →	Not solved
 LAB	PRACTITIONER Blind SQL injection with out-of-band interaction →	Not solved



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Sample Screenshots

Web Security Academy

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home

WE LIKE TO SHOP

Food & Drink' or 1=1 --

Refine your search:

All Clothing, shoes and accessories Corporate gifts Food & Drink Tech gifts

Request

1 GET /filter?category=Food&20126%20Drink%20or%201%3d1%20-- HTTP/2

2 Host: 0a34004004a86d618048d5e200e0044.web-security-academy.net

3 Cookie: session=q59shpr16Py70Pue2EDJ2p1B1p2qut

4 Sec-Ch-Ua: "Chromium";v="121", "Not A Brand";v="99"

5 Sec-Ch-Ua-Mobile: ?0

6 Sec-Ch-Ua-Platform: "Windows"

7 Upgrade-Insecure-Requests: 1

8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36

9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

10 Sec-Fetch-Site: same-origin

11 Sec-Fetch-Mode: navigate

12 Sec-Fetch-User: ?1

13 Sec-Fetch-Dest: document

14 Referer: https://0a34004004a86d618048d5e200e0044.web-security-academy.net/filter?category=Clothing&20+shoes&and+accessories

15 Accept-Encoding: gzip, deflate, br

16 Accept-Language: en-US,en;q=0.9

17 Priority: u=0, i

18

19

Response

Web Security Academy

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

LAB Not solved

Back to lab home

Back to lab description

WE LIKE TO SHOP

Food & Drink' or 1=1 --

Refine your search:

Inspector

Selection 47 (0x2f)

Selected text

category=Food&20126%20Drink%20or%201%3d1%20--

Decoded from: URL encoding

category=Food & Drink' or 1=1 --

Cancel Apply changes

Request attributes 2

Request query parameters 1

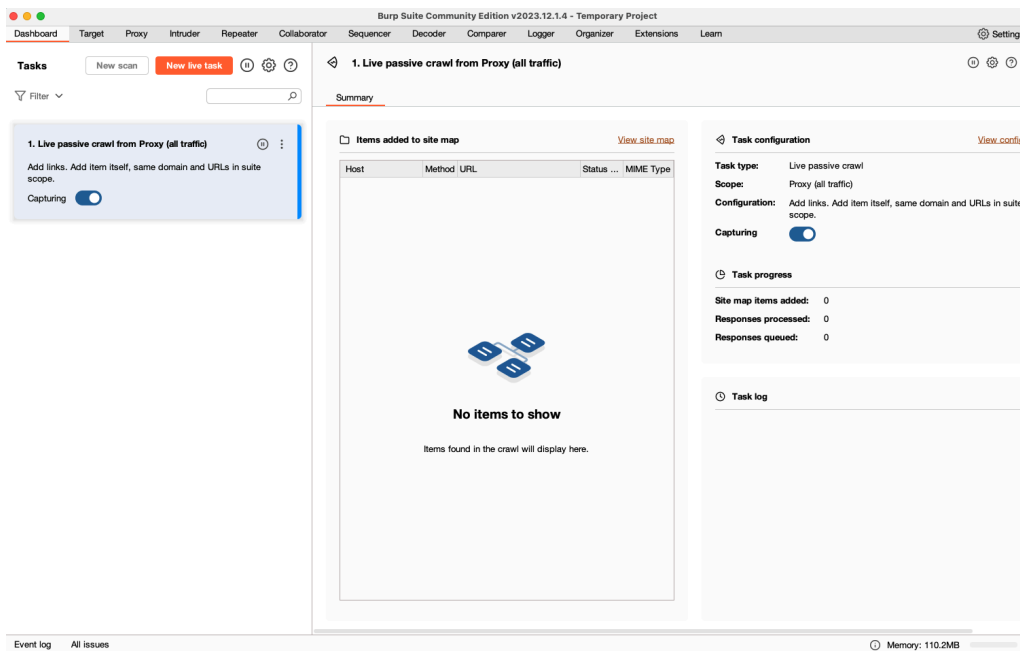
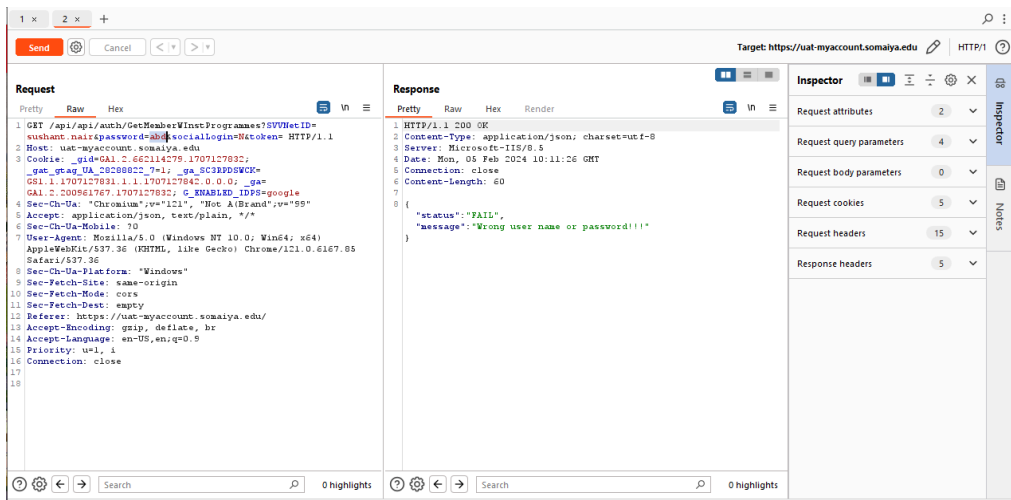
Request body parameters 0

Request cookies 1

Request headers 19



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering



SQL queries used

```
SELECT * FROM products WHERE category = 'Gifts' AND  
released = 1
```

Bypassed by

```
SELECT * FROM products WHERE category = 'Gifts'--'  
AND released = 1
```



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

Conclusion:- Thus we have performed experiments on burp suite by hacking several dummy websites. We have understood various forms of SQL injection like session hijacking, cookie SQL injection, normal SQL injection, retrieval of hidden data, password authentication bypass, etc.

Post-Lab Questions:

4. 1 Major Types of Web Application Attacks:

Web application attacks are malicious activities aimed at exploiting vulnerabilities in web applications. Some major types include:

1. SQL Injection (SQLi): Attackers inject malicious SQL code into input fields to manipulate the application's database. This can lead to data leakage, data manipulation, and even unauthorized access to the system.
2. Cross-Site Scripting (XSS): Attackers inject malicious scripts into web pages viewed by other users. These scripts can steal session cookies, redirect users to malicious sites, or deface the website.
3. Cross-Site Request Forgery (CSRF): Attackers trick authenticated users into executing unwanted actions on a web application where they are currently authenticated. This can lead to unauthorized transactions or changes in the user's account.
4. Directory Traversal: Attackers manipulate file paths in URLs to access files and directories they're not supposed to access. This can result in unauthorized data disclosure or even execution of arbitrary code.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

5. Injection Flaws: Apart from SQL injection, injection flaws can also include Command Injection, XML Injection, and LDAP Injection, where attackers inject malicious commands or code into input fields to execute unauthorized commands or queries.

6. Broken Authentication: This includes weaknesses in authentication mechanisms, such as weak passwords, session fixation, or improper session management, leading to unauthorized access to user accounts.

7. Security Misconfiguration: This involves improper configuration of security settings, such as default passwords, unnecessary services, or overly permissive access controls, which can expose vulnerabilities to attackers.

4.2 Mitigating SQL Injection Attacks:

To mitigate SQL injection attacks, you can implement several best practices:

1. Use Parameterized Queries: Instead of concatenating user input directly into SQL queries, use parameterized queries or prepared statements provided by your programming language's database access library. These methods separate SQL code from user input, preventing injection attacks.

2. Input Validation: Validate and sanitize user input to ensure that it matches the expected format and doesn't contain any malicious characters or SQL code. This can be done using regular expressions or libraries specifically designed for input validation.

3. Least Privilege Principle: Restrict database permissions for application accounts to the minimum required for normal operation. Avoid using privileged accounts for routine tasks, as this can limit the impact of a successful SQL injection attack.



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

4. Web Application Firewalls (WAF): Deploy a WAF to monitor and filter HTTP traffic for suspicious or malicious patterns, including SQL injection attempts. WAFs can help block attacks in real-time before they reach the application server.

5. Regular Security Audits: Conduct regular security audits and penetration testing of your web applications to identify and remediate vulnerabilities, including potential SQL injection vulnerabilities.

4.3 Man-in-the-Middle (MitM) Attack:

A Man-in-the-Middle (MitM) attack occurs when a malicious actor intercepts and possibly alters communication between two parties without their knowledge. Here's how it typically works:

1. Interception: The attacker positions themselves between the communication flow, often by exploiting vulnerabilities in the network infrastructure or by being physically present on the network path.

2. Interception of Data: The attacker intercepts the data being exchanged between the two parties. This could include login credentials, sensitive information, or any data transmitted over the network.

3. Modification (optional): In some cases, the attacker may modify the intercepted data before passing it along to the intended recipient. For example, they might alter the contents of a message or inject malicious code into a web page.

4. Passing Data Along: After intercepting and potentially modifying the data, the attacker forwards it to the intended recipient, who may be unaware that the communication has been compromised.

MitM attacks can occur in various contexts, including insecure Wi-Fi networks, compromised routers or switches, and even malicious software installed on a user's



Somaiya Vidyavihar University
K. J. Somaiya College of Engineering
Department of Computer Engineering

device. To mitigate MitM attacks, encryption protocols like SSL/TLS can be used to secure communication channels, and strong authentication mechanisms can be employed to verify the identity of communicating parties. Additionally, users should be cautious when connecting to untrusted networks and ensure that they are using secure communication protocols whenever possible.