TASK 2

1. FIND 3 BROKEN AUTHENTICATION VULNERABLE WEBSITES DUE TO SOL INJECTION

NOTE:

THE VULNERABLE WEBSITES YOU SUBMIT SHOULDN'T E FROM THE PREVIOUS TASK

2. FIND 2 BROKEN AUTHENTICATION VULNERABLE WEBSITES DUE TO EMAIL VERIFICATION BYPASS VULNERABILITY WHILE REGISTRATION IN A WEBSITE.

CATEGORY:

1. BY MODIFYING THE HTTP RESPONSE

NOTE:

THIS VULNERABILITY SHOULD BE FROM THE WEBSITES WHICH HAVE RESPONSIBLE DISCLOSURE POLICY ONLY.

CATEGORY OF WEBSITE:

1. PRIVATE RESPONSIBLE DISCLOSURE POLICY WEBSITES

2. PUBLIC RESPONSIBLE DISCLOSURE POLICY WEBSITES

HACKERONE, BUGCROWD, INTIGRETY, SYNACK.ETC

3. FIND 1 BROKEN AUTHENTICATION VULNERABLE WEBSITE DUE TO OTP BYPASS VULNERABILITY.

CATEGORY:

1. ACCEPTING NULL OTP

2. BY HTTP RESPONSE MANIPULATION

3. ACCEPTING ANY VALID OTP

Ex:

1. CONSIDER TWO ACCOUNTS ARE CREATED (A1 & A2)

2. TRY TO LOGIN TO BOTH THE ACCOUNTS ON DIFFERENT BROWSERS

3. NOW BOTH ACCOUNTS WILL RECIEVE AN OTP

4. NOW USE A1 ACCOUNT'S OTP IN A2 LOGIN

5. IF YOU ARE ABLE TO LOGIN SUCCEFULLY THEN ITS A OTP BYPASS VULNERABILITY BECAUSE THE SERVER IS ACCEPTING

ANY VALID OTP.

SQL INJECTION:

Summary:

SQL injection is a type of cybersecurity vulnerability that occurs when malicious actors exploit weaknesses in a web application's handling of SQL queries. It allows attackers to insert malicious SQL code into user inputs, which can lead to unauthorized access, data theft, manipulation, or even complete compromise of the underlying database.

The vulnerability arises when a web application fails to properly validate or sanitize user inputs before incorporating them into SQL statements. Attackers take advantage of this oversight by inserting specially crafted inputs that manipulate the SQL query structure and execute unintended commands.

Impact:

Unauthorized access

Data disclosure

Data manipulation

Denial of Service (DoS)

Remedial Actions:

Input validation and sanitization

Parameterized queries or prepared statements

Least privilege principle

Regular patching and updates

Web application firewall (WAF)

Security testing and code review

1.<https://senhas.ipse.ag/login.php>

A screenshot of a login screen

Description automatically generated with medium confidence

Payload used:

‘=’ ‘OR’

A screenshot of a login page

Description automatically generated with low confidence

2.<https://www.smartsupport.pk/php/login.php>

A screenshot of a login box

Description automatically generated with low confidence

Payload used: ‘=’ ‘OR’

A screenshot of a computer

Description automatically generated with medium confidence

3.<https://www.peps.ae/login.php>

A screenshot of a login screen

Description automatically generated with medium confidence

Payload used: ‘=’ ‘OR’

A screenshot of a computer

Description automatically generated with medium confidence

EMAIL VERIFICATION BYPASS VULNERABILITY:

Summary:

Email verification bypass vulnerability refers to a security flaw that allows malicious actors to bypass the email verification process implemented by online platforms. This vulnerability can have significant impacts on user privacy, account security, and the overall integrity of online systems. However, there are remedial actions that can be taken to address this vulnerability and enhance the security of email verification processes.

Impacts:

Unauthorized access

Account takeover

Spam and phishing attacks.

Data breaches

Remedial Actions:

Strengthen email verification.

Enhanced account security measures

Regular security audits

User education

Security monitoring and incident response

1.<https://www.eusc.ae/evaluation/login.php>

A screenshot of a login form

Description automatically generated with low confidence

Burp suite request:

A screenshot of a computer

Description automatically generated

Now we must edit the Email with the approves email and forward the request.

Updated Request:

A screenshot of a computer

Description automatically generated with medium confidence

Now we have entered the website.

This shows that the webpage is vulnerable to the Email bypass vulnerability.

OTP By-pass Vulnerability:

OTP (One-Time Password) By-pass Vulnerability is a security flaw that allows attackers to bypass the intended security measures of OTP systems. OTPs are commonly used as an additional layer of authentication in various domains, including online banking, two-factor authentication, and secure communication.

The vulnerability typically arises when there is a flaw in the implementation or deployment of the OTP system. Attackers can exploit these weaknesses to gain unauthorized access or conduct fraudulent activities. They can intercept or manipulate the OTP during transmission or find ways to bypass the OTP verification process altogether.

Impacts:

Unauthorized Access

Data Breaches

Social Engineering Attacks

Remedial Actions:

Two-Factor Authentication (2FA)

Time-based OTPs

Stronger Account Lockout Policies

Regular Security Audits

User Education