Pen testing report

Purpose: the main purpose is to test the website and its vulnerabilities and to learn which is critical and effects the whole website and to learn in alive environment that vulnerable and accessible to all who wants to learn .

Findings : we have drown to the conclusion of many vulnerabilities that exits within the website which some of thema are critical and some are normal such as the cross site scripting (xss) and SQL injection and open network that can be intercepted and CSRF which allows the hackers to operate and perform an unauthorized actions on behalf of the trusted users.

Recommendations : 1)implement proper input validation and output to protect against xss attacks.

2)use prepared statements to prevent SQL injection.

3) apply CSRF tokens to protect against unauthorized requests.

4) regular check of the website security.

Scoop and methodology:

(1)Scope: websites(juice shop)

APIs: (juice shop Api)

(2)Approach : Black-box :- the test was preformed without any knowledge about the website.

\*\*Tools: // Burb suite: it’s a tool that analyze the network and can intercept the connection between the two factors.

// manual testing : we test some of the vulnerabilities .

// foxy proxy : an extension that connect the website with the burb suite application.

Vulnerability findings: 1) SQL injection :- we identify the SQL injection points where the user inputs isn’t well tracked;

It got a high level impact where attackers could bypass authentication .

\*Evidence : we injected a simple (OR 1=1) payload into the login form.

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

\*\*Remediation: use prepared statements to prevent SQL injection.

2)XSS:- we found several places where malicious scripts could be injected which allows the attackers to effect on the user session;

It got a high impact on the system where attackers could steal session cookies or redirect the user to a desired website or even make a popup ads that interfere with user session.

\*Evidence : A screen shot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

3)CSRF:- Some forms lacked CSRF tokens, which makes it possible for an attacker to forge requests on behalf of authenticated users.

\*Evidence : we made a request to change an account setting by tricking an authenticated user. A screenshot of a computer

AI-generated content may be incorrect.

\*\*Remediation: implement a two factor authentication technique , implement CSRF tokens in all state-changing forms.

Exploitation and attack simulation:

-Tools and techniques used for Exploitation:

Burp suite: used to intercept network traffic .

Manual Exploitation: we manually tested for more vulnerabilities such as SQL injection.

-outcome and impact : (SQL injection): we were able to access the website throw an admin user name without the need for the password.

(XSS):we were able to make a script that can read and provide the session cookie and redirect the user to a different website and also to make a popups ads that interfere with the user session and to make an audio show up or a video.

(CSRF): we were able to change the user settings and access the admin password.

Conclusion:

Overall, the security posture of the applications tested was found to be lacking in several key areas. The presence of critical vulnerabilities like XSS, SQL Injection, and missing CSRF protections exposes the system to serious risks, such as data theft and unauthorized actions.

Remediation :

Immediately address the critical vulnerabilities by implementing the recommended fixes.

Conduct a thorough code review to ensure secure coding practices are being followed.

Schedule regular security audits to catch potential vulnerabilities early and improve the overall security posture..

DRIVE LINK : https://drive.google.com/drive/folders/1yD2AOWP9LRw0nnMVc1En3gsBLAFVqX1C?usp=sharing