CYBER SECURITY

Top 17 Security Test Checklist For Web Application

Wasif Zaman 14 Mar 2024 4 173 1 Share

1. **Data protection from external threats:**

An external threat refers to the risk of somebody from the outside of a company who attempts to exploit system vulnerabilities through the use of malicious software, hacking, sabotage or social engineering.
Uncontrolled system access restrictions: Unwanted access.

2. **Data breach:**

A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.

3. **Payment:**

Payment authentication. Intruders can play without paying.

4. **Swatting and doxing:**

Where attackers target a specific user and get all your information.

gather information about a person or organization and send it to another entity in a way that harms the user—for example, by violating their privacy or endangering their device's security.

6. **Data breaches:**
A data breach is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

7. **Cross-site scripting:** Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.

8. **DDoS attacks:**
In computing, a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network.

9. **Phishing emails:**
Phishing is an attempt to steal personal information or break into online accounts using deceptive emails, messages, ads, or sites that look similar to sites you already use. For example, a phishing email might look like it's from your bank and request private information about your bank account.

10. **SMTP Header Injection:**
SMTP header injection vulnerabilities arise when user input is placed into email headers without adequate sanitization, allowing an attacker to inject additional headers with arbitrary values.

transmit it to memory, a database, or a file. Its main purpose is to save the state of an object in order to be able to recreate it when needed. The reverse process is called deserialization.

12. Cross-Site Scripting(DOM-Based):
DOM Based XSS (or as it is called in some texts, “type-0 XSS”) is an XSS attack wherein the attack payload is executed as a result of modifying the DOM “environment” in the victim's browser used by the original client side script, so that the client side code runs in an “unexpected” manner.

13. External Service Interaction(HTTP):
External service interaction arises when it is possible to induce an application to interact with an arbitrary external service, such as a web or mail server.

14. Web Cache Poisoning:
Web cache poisoning is an advanced technique whereby an attacker exploits the behavior of a web server and cache so that a harmful HTTP response is served to other users.

15. Server-Side Template Injection:
Server-side template injection is when an attacker is able to use native template syntax to inject a malicious payload into a template, which is then executed server-side.

16. SQL Injection:
A SQL injection is a technique that attackers use to gain unauthorized access to a web application database by adding a string of malicious code to a database query. A SQL injection (SQLi) manipulates SQL code to provide access to protected resources, such as sensitive data, or execute malicious SQL statements.

17. OS Command Injection:
OS command injection (also known as shell injection) is a web security vulnerability that allows an attacker to execute arbitrary operating system (OS) commands on the server that is running an application, and typically fully compromise the application and all its data.

cyber security | security testing checklist | penetration testing

Share your thoughts Or Start discussion

Comments (1)

Sorted by Newest

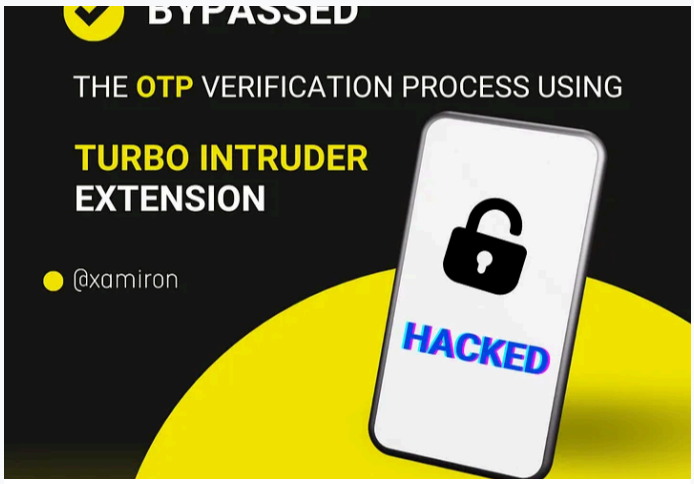
Md. Rezwan-Ul-Haque • 1y ago • Likes 0 • (Edited)

Thanks For sharing, Wasif Zaman.

REPLY

REPLY

Related Blogs



CYBER SECURITY 1 0 234

Bypassed the OTP verification process using “Turbo Intruder” Extension.

Today, in this article, we will explore methods and techniques that have been us

Sabuj Modak Samiron
22 Dec 2024

CYBER SECURITY 0 0 268

Ultimate Guide to Security Testing for Web Applications: Protect Your Site from...

Security Testing has become a critical component of web application development

Nishi Khan
25 Nov 2024

Popular Tags

sqa testing qa software testing qabrains testing tool automationtesting softwaretesting mobiletesting selenium

View All

Popular Post

Can a Software Tester Become a Game Tester? Here’s What You Need t...

As the gaming industry continues to grow, fueled by innovations in virtual reali

Essential Bugs to Check for in Game Testing: A Guide for Beginners

Game testing is crucial to ensure a smooth, engaging, and bug-free experience fo

JMeter: Short technique for Generating an HTML load test report using...

Pre-requisites:Install Java:Java Version: "1.8.0_291" or higher (minimum require

View All

Popular Discussion

01 Top Software Testing Interview Questions and Expert Tips from QA Leaders

02 AI tools for QA engineer

03 What is SQL?

04 Appium, WebDriver

05 What are the most effective strategies you've found for balancing speed and...

View All

Follow Us

For Support

support@qabrains.com