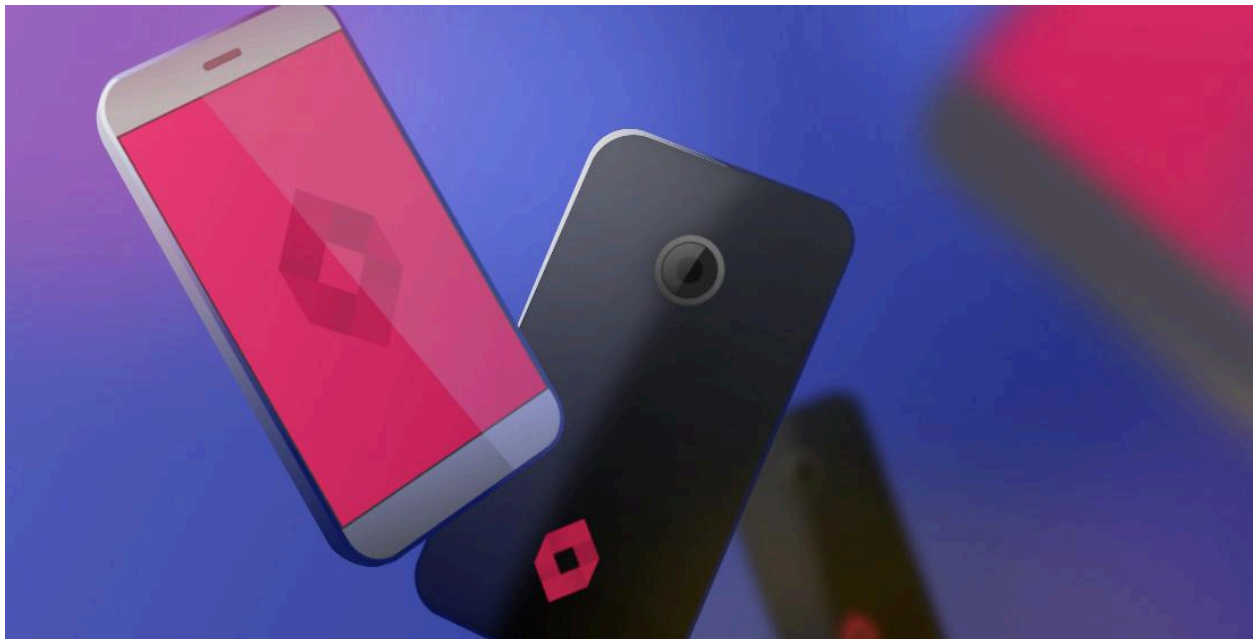


ASSIGNMENT

# VULNERABILITY ANALYSIS

FEBRUARY 23, 2025

---



---

## TASKS TO BE PERFORMED

1. Scan the Web Application: Perform a comprehensive scan of the target web application using Nikto.
2. Analyze Nikto Scan Results: Analyze the Nikto scan results to identify potential vulnerabilities, misconfigurations, or security issues in the web application.
3. Provide Recommendations: Based on the findings from the Nikto scan, provide recommendations on how to address the identified vulnerabilities and security concerns in the web application

[TOOL :- NIKTO](#)

## SOLUTIONS :-

by **MUHAMMED SAFAYATH T**

**INTELLIPAAT STUDENT**

**KERALA**

**CEH**





NIKTO:-

<http://www.goodshopping.com>

---

## Nikto Scan Analysis Report

### 1. Overview

The Nikto web server scanner identified multiple vulnerabilities and potential security misconfigurations on the target system. These issues include **Cross-Site Scripting (XSS)**, **outdated web applications**, **sensitive information disclosure**, and **possible remote code execution vulnerabilities**.

### 2. Key Findings

#### A. Cross-Site Scripting (XSS) Vulnerabilities



---

Several web pages are vulnerable to **reflected XSS**, allowing an attacker to inject malicious scripts into URL parameters. This can lead to **session hijacking, credential theft, and phishing attacks**.

- Affected applications: **Sambar Server, Bonsai, Oracle 9iAS, VP-ASP Shopping Cart, Tomcat Demo Files, Lyris ListManager**
- CVEs: **CVE-2003-0153, CVE-2003-0154, CVE-2005-3685, CVE-2005-4838**

## **B. Outdated and Misconfigured Applications**

Several default scripts and demo pages are accessible, exposing the server to known exploits. These include:

- **Oracle Reports Servlet:** May allow arbitrary report execution.
- **Tomcat Demo Files:** XSS vulnerabilities in test pages.
- **SharePoint & FrontPage Files:** May expose user and administrative data.

## **C. Information Disclosure Issues**


The scan detected files and endpoints that could leak sensitive information:

- **Citrix Server Advanced Tab:** Could reveal internal server details.
- **Oracle Applications Help Page:** Potential exposure of database connection details.

## **D. Potential Remote Code Execution (RCE) & DoS Risks**

- **BEA WebLogic Vulnerability (CVE-2019-2725):** May allow remote takeover of the server.
- **MyWebServer 1.0.2 Buffer Overflow (CVE-2002-1452):** May crash the server if exploited.
- **HP Instant TopTools DoS (CVE-2003-0169):** Could cause denial of service.

## **3. Recommendations**

- **Patch & Update Software:** Upgrade outdated applications and apply security patches.
  - **Sanitize User Input:** Implement proper input validation to prevent XSS.
- 

- 
- **Restrict Access:** Remove unnecessary default scripts and misconfigured pages.
  - **Enhance Server Security:** Use Web Application Firewalls (WAF) to mitigate attacks.