Test Webseite

Penetration Test Report #1

September 28, 2023

Document Properties

Client	Die Organisation
Title	Penetration Test Report #1
Targets	Test Website
Version	1.0
Pentester	

Version Control

Version	Date	Author	Description
0.1	October 04, 2020	Max Mustermann	First draft
1.0	October 04, 2020	Max Mustermann	Release

Table of Contents

1 Executive Summary

1.1 Introduction

1.2 Scope

1.3 Objectives

1.4 Summary of Findings

Title	Severity
Cross-Site Scripting	**High**
SQLi	**High**
CSP not implemented	**Informational**
Huh	**Undetermined**

2 Methodology

2.1 Planning

2.2 Risk Classification

2.3 CWE

The Common Weakness Enumeration (CWE) data, including titles, descriptions, and related content referenced in this report, are owned by The MITRE Corporation (MITRE). For detailed terms of use and further information, please refer to MITRE's CWE Terms of Use which can be found at https://cwe.mitre.org/about/termsofuse.html.

3 Findings

3.1 Cross-Site Scripting

Severity: **High**

Target: Test Website

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Description

The “Test Website” allows unfiltered user input to be rendered on its search results page, leading to a persistent Cross-Site Scripting (XSS) vulnerability. Specifically, when a user submits a search query, the input is echoed back on the page without proper sanitization. An attacker can craft a malicious link containing a script payload, and once clicked by an unsuspecting user, it can lead to session hijacking, defacement, or potentially more severe actions.

To demonstrate:

1. Visit https://example.org/search
2. In the search bar, input `<script>alert('XSS')</script>` and submit.
3. The alert box pops up, indicating the vulnerability.

This poses a risk as it can be exploited to run any arbitrary JavaScript code in the context of the victim’s browser session.

Remediation

- Always validate and sanitize user input. Ensure that any user-provided data is treated as untrusted and is sanitized properly before rendering it on the page.
- Use Content Security Policy (CSP) headers to reduce the risk of XSS attacks. This can limit the sources and types of content that can be executed in the web page context.
- Ensure that all user input is properly encoded when being output to the page. This will prevent special characters from being interpreted as code.
- Adopt web application firewalls (WAFs) or other security mechanisms that can detect and block malicious input.

Regularly review and update web applications to patch any vulnerabilities and to stay ahead of potential security threats.

3.2 SQLi

Severity: **High**

Target: Test Website

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Description

Remediation

3.3 CSP not implemented

Severity: **Informational**

Target: Test Website

CWE-1021: Improper Restriction of Rendered UI Layers or Frames

The web application does not restrict or incorrectly restricts frame objects or UI layers that belong to another application or domain, which can lead to user confusion about which interface the user is interacting with.

Description

Remediation

3.4 Huh

Severity: **Undetermined**

Target: Test Website

Description

Remediation