Generic Company

Logo Here

Generic Company

Web Application (WebApp) Findings Report

Prepared by: Nutt Security (NS)

Jake Nutt - GWAPT

Confidential

This document is the exclusive property of Generic Company and NS. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Generic Company and NS.

NS may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Last Modified Date: February 14, 2022

Project: WebApp

# Contents

[Contents 2](#_Toc96414806)

[Document Control 2](#_Toc96414807)

[Disclaimer 2](#_Toc96414808)

[Contact Information 3](#_Toc96414809)

[Revision History 3](#_Toc96414810)

[Executive Summary 3](#_Toc96414811)

[Assessment Summary 3](#_Toc96414812)

[Assessment Components 4](#_Toc96414813)

[Technical Summary 4](#_Toc96414814)

[Scope 4](#_Toc96414815)

[Scope Exclusions 4](#_Toc96414816)

[Finding Severity Ratings 4](#_Toc96414817)

[Client Allowances 5](#_Toc96414818)

[Summary of Findings 5](#_Toc96414819)

[Graphical Representation of Vulnerabilities 5](#_Toc96414820)

[Security Strengths 6](#_Toc96414821)

[Security Weaknesses 6](#_Toc96414822)

[WebApp - Web Application Detailed Findings 6](#_Toc96414823)

[Finding 1 – Stored Cross Site Scripting (XSS) – High 6](#_Toc96414824)

[Finding 2 – Vulnerable Software Detected – Medium 7](#_Toc96414825)

[Finding 3 – Weak Password Policy – Low 8](#_Toc96414826)

[Finding 4 – Security Answers Not Masked – Informational 9](#_Toc96414827)

# Document Control

## Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. NS prioritized the assessment to identify the weakest security controls an attacker would exploit. NS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

## Contact Information

|  |  |  |
| --- | --- | --- |
| Name | Title | Contact Information |
| Generic Company | | |
| John Doe | CTO | Office: (123) 456-7890 x1000 Email: [John.Doe@GenericCompany.com](mailto:John.Doe@GenericCompany.com) |
| Rob Alt | IT Manager | Office: (123) 456-7890 x1001 Email: [Rob.Alt@GenericCompany.com](mailto:Rob.Alt@GenericCompany.com) |
| Nutt Security | | |
| Jake Nutt | Lead Penetration Tester | Office: (123) 456-7890 x100  Email: [Jake.Nutt@NuttSecurity.com](mailto:Jake.Nutt@NuttSecurity.com) |

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **Date** | **Author** | **Comments** |
| 1.0 | 2/14/2022 | Jake Nutt | Initial Findings Report |
|  |  |  |  |
|  |  |  |  |

# Executive Summary

NS evaluated Generic Company WebApp web application through an external web application penetration test. Testing occurred from February 7th, 2022, to February 11th, 2022. By leveraging a series of attacks, NS found several high-level vulnerabilities that allowed accessing content from other users, changing other user’s permissions for role escalation, XSS vulnerabilities, and finding outdated software. It is highly recommended that Generic Company addresses these vulnerabilities as soon as possible as these vulnerabilities can be easily manipulated and lead to severe risks.

## Assessment Summary

From February 7th, 2022, to February 11th, 2022, NS evaluated Generic Company’ WebApp web application compared to current industry best practices that included a web application penetration test. All testing is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment[[1]](#footnote-1), and OWASP Testing Guide (v4)[[2]](#footnote-2).

Phases of penetration testing activities include the following:

* Planning – NS gathered goals, and established rules of engagement.
* Discovery – NS performed scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
* Attack – confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
* Reporting – document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

## Assessment Components

Web Application Penetration Test

A web application penetration test emulates the role of an attacker attempting to gain access to a web application. A NS engineer attempts to bypass login pages along other methods to gain access. In this test NS was given four different user accounts with different permission levels and roles. The engineer also performed scanning and enumeration to identify potential vulnerabilities in hopes of exploitation and role escalation.

# Technical Summary

## Scope

|  |  |
| --- | --- |
| Assessment | Details |
| Web Application Penetration Test | webapp.genericcompany.com |

## Scope Exclusions

Per client request, NS did not perform any Denial of Service attacks during testing.

## Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score[[3]](#footnote-3) range that are used throughout the document to assess vulnerability and risk impact.

|  |  |  |
| --- | --- | --- |
| **Severity** | **CVSS V3 Score** | **Definition** |
| Critical | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| High | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| Medium | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| Low | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| Informational | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

## Client Allowances

Generic Company did provide login credentials for the following user roles:

* SuperAdmin (Super Admin)
* ClientAdmin (High Level Admin)
* ClientUser (Normal Client User)
* VendorUser(Normal Vendor User)

# Summary of Findings

NS tested the Generic Company WebApp Web Application and during testing NS found WebApp overall risk to be high.

Text

Description automatically generated

## Graphical Representation of Vulnerabilities

The following table is an abstract of findings which summarizes the overall risks identified during penetration testing.

A total of 4 unique risks were identified during the testing.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Critical | High | Medium | Low | Informational |
| Open | 0 | 1 | 1 | 1 | 1 |
| Closed | 0 | 0 | 0 | 0 | 0 |

## Security Strengths

Good strengths of the application are user accounts can only be created by a previously validated admin user account. There also seems to be no SQL injection vulnerabilities present to bypass login pages or to access information stored within the backend database.

## Security Weaknesses

The basic permissions between user role levels have no validation checks on whether certain content should or shouldn’t be available. There are many other issues around input and upload validation checks, along with proper formatting and content restrictions. The overall application should be checked for external JavaScript libraries as most of them haven’t been updated in over ten years.

# WebApp - Web Application Detailed Findings

## Finding 1 – Stored Cross Site Scripting (XSS) – High

### Risk – High

### Description

The support ticket description and comments suffer from XSS vulnerabilities as show by the code snippet below. The contents should be checked for JavaScript tags before the entry is saved.

<script>alert('Hello');</script>

### Location

<https://webapp.genericcompany.com/Support/SupportTickets>

### References

<https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/07-Input_Validation_Testing/02-Testing_for_Stored_Cross_Site_Scripting>

### Proof of concept

Screenshots here

## Finding 2 – Vulnerable Software Detected – Medium

### Risk – Medium

### Description

Outdated and vulnerable version of jQuery Migrate version 1.41 should be removed and/or updated to the latest version. Vulnerable version can lead to Cross-Site Scripting (XSS) vulnerabilities which is shown in Finding 1.

### Location

<https://webapp.genericcompany.com/Scripts/Jquery/jquery-migrate-1.4.1.js>

### References

<https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/>

<https://releases.jquery.com/>

### Proof of concept

Screenshots here

## Finding 3 – Weak Password Policy – Low

### Risk – Low

### Description

Users can set very weak passwords and are not required to meet special characters requirements other than the password being a minimum of 8 characters.

### Location

<https://webapp.genericcompany.com/Account/ChangePassword>

### References

<https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy>  
<https://linfordco.com/blog/nist-password-policy-guidelines/>

### Proof of concept

Screenshots here

## Finding 4 – Security Answers Not Masked – Informational

### Risk – Informational

### Description

When logging into the WebApp application and successfully entering a valid username and password a security question is prompted. The answer given should be masked when entered just like the password.

### Location

<https://webapp.genericcompany.com/Authentication/ValidateSecurityQuestion>

### References

<https://owasp.org/Top10/A01_2021-Broken_Access_Control/>

### Proof of concept

Screenshots here

1. <https://csrc.nist.gov/publications/detail/sp/800-115/final> [↑](#footnote-ref-1)
2. <https://owasp.org/www-project-web-security-testing-guide/stable/> [↑](#footnote-ref-2)
3. <https://www.first.org/cvss/v3.1/specification-document> [↑](#footnote-ref-3)