(Fake Company Logo)

Fake Company

WebApp Findings Report

Prepared by: Nutt Security

Confidential

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

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

Date: January 1, 2022

Project: WebApp

Table of Contents

[Document Control 3](#_Toc93047172)

[Disclaimer 3](#_Toc93047173)

[Contact Information 3](#_Toc93047174)

[Revision History 3](#_Toc93047175)

[Executive Summary 4](#_Toc93047176)

[Assessment Summary 4](#_Toc93047177)

[Assessment Components 4](#_Toc93047178)

[Technical Summary 5](#_Toc93047179)

[Scope 5](#_Toc93047180)

[Scope Exclusions 5](#_Toc93047181)

[Finding Severity Ratings 5](#_Toc93047182)

[Client Allowances 5](#_Toc93047183)

[Summary of Findings 6](#_Toc93047184)

[Graphical Representation of Vulnerabilities 6](#_Toc93047185)

[Security Strengths 6](#_Toc93047186)

[Security Weaknesses 6](#_Toc93047187)

[Web Application Detailed Findings 7](#_Toc93047188)

# 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. Nutt Security prioritized the assessment to identify the weakest security controls an attacker would exploit. Nutt Security 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 |
| Fake Company | | |
| Jim Bob | VP, Production Services | Office: (123) 456-7890 x111 Email: [Jim.Bob@FakeCompany.com](mailto:Jim.Bob@FakeCompany.com) |
| Ricky Bobby | Infrastructure Manager | Office: (123) 456-7890 x112 Email: [Ricky.Bobby@FakeCompany.com](mailto:Ricky.Bobby@FakeCompany.com) |
| Nutt Security | | |
| Jake Nutt | Lead Penetration Tester | Office: (913) 825-0000  Email: [Jake.Nutt@NuttSecurity.com](mailto:Jake.Nutt@NuttSecurity.com) |

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **Date** | **Author** | **Comments** |
| 1.0 |  | Jake Nutt | Initial Findings Report |
|  |  |  |  |
|  |  |  |  |

# Executive Summary

Nutt Security evaluated Fake Company’ WebApp web application through an external web application penetration test. Testing occurred from May 20th, 2022 to May 29th, 2022. By leveraging a series of attacks, Nutt Security found critical level vulnerabilities that allowed full internal network access to the Fake Company’ headquarter office. It is highly recommended that Fake Company address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

## Assessment Summary

From May 20th, 2019 to May 29th, 2019, Nutt Security evaluated Fake Company’ WebApp web application compared to current industry best practices that included an 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), OWASP Testing Guide (v4)[[2]](#footnote-2), and customized testing frameworks.

Phases of penetration testing activities include the following:

* Planning – Nutt Security gathered goals, and established rules of engagement.
* Discovery – Nutt Security 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

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A Nutt Security engineer attempts to gather sensitive information through open-source intelligence (“OSINT”), including employee information, historical breached passwords, and to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

# Technical Summary

## Scope

|  |  |
| --- | --- |
| Assessment | Details |
| Web Application Penetration Test | WebApppentest.Fake Company.net |

* Full scope information provided in “Fake Company-WebApp Full Scope.xslx”

## Scope Exclusions

Per client request, Nutt Security 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. |
| Moderate | 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

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

* Admin (Super Admin)
* ClientAdmin (High Level Admin)
* ClientUser ()
* VendorAdmin()
* VendorUser()

# Summary of Findings

Nutt Security tested the Fake Company Web Application and during testing Nutt Security found WebApp to be …………………………………………………………………………………………………………………………..

## Graphical Representation of Vulnerabilities

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

A total of 0 unique risks were identified during the testing.

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

## Security Strengths

Just a couple of sentences talking about good or strong points of the web app

## Security Weaknesses

Just a couple of sentences talking about the weak areas of the web app

# Web Application Detailed Findings

## Finding 1 – Insecure Direct Object Reference (IDOR) – Critical

### Risk – Critical

### Description

Talking about idor stuff here

### Location

List url here

### References

Links to miter and owasp here

### Proof of concept

List screenshots on how the exploit was accomplished

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)