

**REALIZE & REACT SECURITY**

**SECURITY ASSESSMENTS FINDINGS REPORT FOR ForEver25**

**BUSINESS CONFIDENTIAL**

**Date: January 24th, 2022**

**Project: Basic Pentesting**

Table of Contents

[Confidentiality Statement 3](#_Toc98312094)

[Disclaimer 3](#_Toc98312095)

[Contact Information 3](#_Toc98312096)

[Assessment Overview 4](#_Toc98312097)

[Assessment Components 4](#_Toc98312098)

[Internal Penetration Test 4](#_Toc98312099)

[Finding Severity Ratings 6](#_Toc98312100)

[Scope 7](#_Toc98312101)

[Scope Exclusions 7](#_Toc98312102)

[Client Allowances 7](#_Toc98312103)

[Executive Summary 8](#_Toc98312104)

[Attack Summary 8](#_Toc98312105)

[SQL Injection 9](#_Toc98312106)

[Broken Authentication 11](#_Toc98312107)

[Data exposure 15](#_Toc98312108)

[Broken Access Control 17](#_Toc98312109)

[Cross Site Scripting (XSS) 22](#_Toc98312110)

[Security Weaknesses and Findings 25](#_Toc98312111)

[Missing Multi-Factor Authentication 25](#_Toc98312112)

[Weak Password Policy 25](#_Toc98312113)

[Unrestricted Logon Attempts 25](#_Toc98312114)

[Weak or No Encryption 25](#_Toc98312115)

[Lack of Input validation and filtering in code 25](#_Toc98312116)

[Lack of access control lists 26](#_Toc98312117)

[Severity ratings 26](#_Toc98312118)

# Confidentiality Statement

This document is the exclusive property of ForEver25 and REALIZE & REACT Security (REALIZE & REACTS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both FOREVER25 and REALIZE & REACTS.

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

# 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. REALIZE & REACTS prioritized the assessment to identify the weakest security controls an attacker would exploit. REALIZE & REACTS 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 |
| **Demo Company** | | |
| Jonathan Helmus | Instructor | Office: (555) 555-5555  Email: Jonathan.helmus@metrostate.edu |
| **REALIZE & REACT Security** | | |
| Edajei Alvine | Lead Penetration Tester | Office: (555) 555-5555  Email: vu8547fr@go.minnstate.edu |

# Assessment Overview

From February 14th to March 14th 2022, Realize & React engaged ForEver25 to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal penetration test. All testing performed is based on requirements stated in tryhackme room, OWASP Juice Shop.

Phases of penetration testing activities include the following:

* Planning – Customer goals are gathered, and rules of engagement obtained.
* Discovery – Perform 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.

Diagram

Description automatically generated

# Assessment Components

## Internal Penetration Test

An internal penetration test is meant to identify what could be accomplished by an attacker who has internal access to your network. A Realize & React Engineer performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

# Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

| Severity | CVSS V3 Score Range | 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. |

# Scope

|  |  |
| --- | --- |
| Assessment | Details |
| Internal Penetration Test | 10.10.105.249  10.10.15.199  10.10.238.32  10.10.155.189 |

* Full scope information provided in “**ForEver25.. Full Findings.xslx”**

## Scope Exclusions

Per client request, REALIZE & REACT Security did not perform any Denial-of-Service attacks during testing.

## Client Allowances

FOREVER25 did not provide any allowances to assist the testing.

# Executive Summary

REALIZE & REACT evaluated FOREVER25’s internal security posture through an internal network penetration test from February 14th to March 14th. By leveraging a series of attacks, REALIZE & REACTS found critical level vulnerabilities that allowed full internal access to the FOREVER25 user accounts and webpage. It is highly recommended that FOREVER25 addresses these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

## Attack Summary

The following describes how REALIZE & REACT Security gained internal network access, step by step:

Admin email found

By going to the Juice shop webpage and hovering over one of the products, the admin email was found which was then used for other exploits during penetration

Graphical user interface, application

Description automatically generated

## SQL Injection

Logging into admin account:

Using the admin email and without a proper password, the traffic from the log in attempt was intercepted and changed to an SQL statement (‘ OR 1=1- -), before it was forwarded and then access was gained into the admin account .

Graphical user interface, website

Description automatically generated

Logging into Bender’s account:

Similarly, the bender’s account was logged into without use of a proper password as the information was intercepted using burp suite and an sql injection command was added to email ([bender@juice-sh.op’-](mailto:bender@juice-sh.op’-) -) and sent to the server and login was granted.

The screenshot shows a successful login into bender’s account.

A screenshot of a computer

Description automatically generated with medium confidence

Remediation:

Use industry standard passwords and input validation in the fields should be enforced as well.

## Broken Authentication

Since the admin password wasn’t known before the injection attack, I was able to perform a brute force attack using a list of words to find the admin password which was then used to login into the account as the admin with all admin privileges.

Graphical user interface, text, application, email

Description automatically generated

The screenshot below shows the bruteforce processing of different being tried and then the password was found which showed at status 200.

Graphical user interface

Description automatically generated

The password found via brute forcing, shown by status 200 was then used to log into the admin account. The 2nd flag below indicated a successful login.

Graphical user interface, text, website

Description automatically generated

Resetting Jim’s password:

Resetting Jim’s password was easy using his email. The forgotten email showed a security question. The information was found on the internet as Jim’s family is shown with a search associated to him. The information was used to answer his security question, password changed, and access gained into his account with the new password assigned.

Graphical user interface, application, website

Description automatically generated

Remediation

Use of industry standard passwords is highly encouraged together with input validation in text field fields. An end-to-end encryption standard between the client and servers should as well be implemented to prevent

## Data exposure

Using the admin credentials, I was able to login and access some confidential documents .

Graphical user interface, text, application, website

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Backup file was also downloaded

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, chat or text message

Description automatically generated

Remediation

Permissions should be used on documents as well as encryption with keys

## Broken Access Control

Admin page accessed

Text

Description automatically generated

Viewing another’s shopping basket

Traffic was intercepted and I was able to view and change the number of items in another person’s shopping basket.

Graphical user interface, application, website

Description automatically generated

Graphical user interface, website

Description automatically generated

Five-star reviews were deleted through the admin section of the admin account .

Graphical user interface, text

Description automatically generated

## Cross Site Scripting (XSS)

Graphical user interface, text, application, email

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Graphical user interface, text, application, chat or text message

Description automatically generated

**Remediation**:

Strict input validation and filtering should be used

# Security Weaknesses and Findings

## Missing Multi-Factor Authentication

REALIZE & REACTS leveraged multiple attacks against FOREVER25 login forms using valid credentials harvested through open-source intelligence. Successful logins included admin, employee and customer accounts through Web page Access and internal access . The use of multi-factor authentication would have prevented full access and required REALIZE & REACTS to utilize additional attack methods to gain internal network access.

## Weak Password Policy

REALIZE & REACTS successfully performed password guessing attacks against FOREVER25 login forms, providing internal network access. A predictable password format was attempted and successful.

## Unrestricted Logon Attempts

During the assessment, REALIZE & REACTS performed multiple brute-force attacks against login forms found on the internal network. For all logins, unlimited attempts were allowed, which permitted an eventual successful login on the Web page

## Weak or No Encryption

REALIZE & REACT successfully intercepted traffic from the juice shop web page and found all passwords in plaintext meaning no encryption over the network was used

## Lack of Input validation and filtering in code

Due to lack of input validation, REALIZE & REACT successfully put in harmful sql code to send to the server which allowed access to the accounts. Also lack of input validation allowed for a single letter password to be accepted in the password field leading to a successful interception

## Lack of access control lists

This led to the successful breaking of access control, making it possible to change items in another customer’s cart.

Default setting in software were not changed .

## Severity ratings

| Risks | Severity | CVSS V3 Score Range | Definition |
| --- | --- | --- | --- |
| * SQl Injection * Insufficient logging and monitoring * Weak passwords | 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. |
| * XXS * Broken Acess control * Broken authentication | 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. |
| * Data exposure | 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. |