HACKTHEBOX

Penetration Test

CWEE Exam Report

Report of Findings

HTB Certified Web Exploitation Expert (CWEE) Exam Report

Candidate Name: TODO Candidate Name

February 23, 2024

Version: TODO 1.0

Table of Contents

1 Statement of Confidentiality 3

2 Engagement Contacts 4

3 Executive Summary 5

3.1 Approach 5

4 Scope 6

5 Web Application Security Assessment Summary 7

5.1 Summary of Findings 7

5.2 Assessment Overview and Recommendations 7

6 Technical Findings Details 8

Stored Cross-Site Scripting (XSS) 8

A Appendix 9

A.1 Finding Severities 9

A.2 Flags Discovered 10

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

Contacts		
Contact	**Title**	**Contact Email**
Yelon Husk	Chief Executive Officer	yelon@royalflush.htb
Zeyad AlMadani	Chief Technical Officer	zeyad@securedata.htb

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
TODO Candidate Name	TODO Candidate Title	TODO Candidate Email

3 Executive Summary

Royal Flush Ltd. (“RoyalFlush” herein), Secure Data Ltd. (“SecureData” herein), and Vita Medix Ltd. (“VitaMedix” herein) have invited TODO Candidate Name to perform a targeted Web Application Penetration Test of their web applications to identify high-risk security weaknesses, assess their impact, document all findings in a clear, professional, and repeatable manner, and provide remediation recommendations.

All web-related findings were considered in-scope, as long as they can be proven harmful to the client with a Medium-High impact. The following types of activities were considered out-of-scope for this test:

- Physical attacks against the clients' properties
- Unverified scanner output
- Any vulnerabilities identified through DDoS or spam attacks
- Vulnerabilities in third-party libraries unless they can be leveraged to impact the target significantly
- Any theoretical attacks or attacks that require significant user interaction or are considered low-risk

3.1 Approach

TODO Candidate Name performed testing under a mixture of "blackbox" and a "whitebox" approach from February 18, 2024 to February 23, 2024, as follows:

- `RoyalFlush` A whitebox penetration test was carried against their targets, with access to their web applications' source code on http://git.royalflush.htb/.
- `SecureData` A blackbox penetration test was performed, with no further details or access to their web applications.
- `VitaMedix` A mixture of blackbox and whitebox was carried against all web applications under their sub-domains.

Testing was performed remotely from a non-evasive standpoint, with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential.

TODO Candidate Name sought to demonstrate the full impact of every vulnerability, up to and including internal network access. Furthermore, TODO Candidate Name has also documented the sources of vulnerabilities that were identified through source code analysis, and provided recommended patches to fix them.

4 Scope

The scope of this assessment was as follows:

URL	Description
www.royalflush.htb	Main RoyalFlush website
git.royalflush.htb	RoyalFlush Git Repositories
forum.royalflush.htb	RoyalFlush Forums
vault.royalflush.htb	RoyalFlush Secure Vault
*.securedata.htb	SecureData web app(s)
*.vitamedix.htb	VitaMedix web app(s)

5 Web Application Security Assessment Summary

5.1 Summary of Findings

During the course of testing, TODO Candidate Name uncovered a total of **1** findings that pose a material risk to client's web applications and systems. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **1 Medium** vulnerabilities were identified:

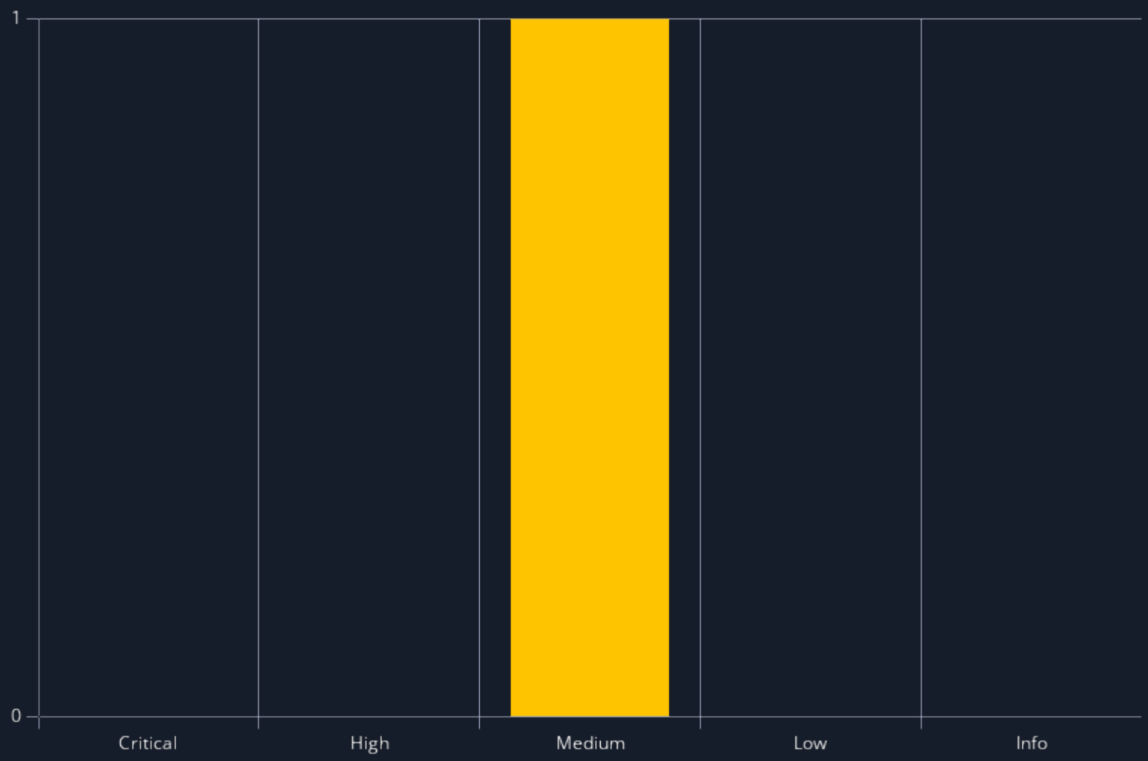

Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during the course of testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	5.3 (Medium)	Stored Cross-Site Scripting (XSS)	8

5.2 Assessment Overview and Recommendations

TODO: 1 page summary of all identified vulnerabilities, as well as their respective recommended remediations.

6 Technical Findings Details

1. Stored Cross-Site Scripting (XSS) - Medium

CWE	CWE-79
CVSS 4.0	5.3 / CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N
Description & Cause	TODO DESCRIPTION & CAUSE
Security Impact	TODO SECURITY IMPACT
Affected Component(s)	TODO AFFECTED COMPONENT
External References	TODO EXTERNAL REFERENCES

Detailed Walkthrough

TODO DETAILED WALKTHROUGH

Patching and Remediation

TODO PATCHING AND REMEDIATION

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of 's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Flags Discovered

TODO: fill in any identified flags.

Flag #	Application	Flag Value	Method Used
1.	**RoyalFlush - Auth**	**HASH**	**Command Injection**
2.	**RoyalFlush - RCE**		
3.	**SecureData - Auth**		
4.	**SecureData - RCE**		
5.	**VitaMedix - Auth**		
6.	**VitaMedix - RCE**		

End of Report

This report was rendered by SysReptor with ♥