HACKTHEBOX

Bug Bounty Program

CBBH Exam Report

Report of Findings

HTB Certified Bug Bounty Hunter (CBBH) Exam Report

Candidate Name: TODO Candidate Name

TODO Customer Ltd.

Version: TODO 1.0

Table of Contents

1 Statement of Confidentiality 3

2 Engagement Contacts 4

3 Executive Summary 5

3.1 Approach 5

3.2 Scope 5

3.3 Assessment Overview and Recommendations 6

4 Web Application Assessment Summary 7

4.1 Summary of Findings 7

5 Technical Findings Details 8

TODO FINDING TITLE 8

A Appendix 9

A.1 Flags Discovered 9

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

TODO Customer Contacts		
Contact	**Title**	**Contact Email**

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

3 Executive Summary

TODO Customer Ltd. (“TODO Customer” herein) invited TODO Candidate Name to a private bug bounty program to perform a targeted Web Application Penetration Test of TODO Customer’s externally facing web applications to identify high-risk security weaknesses, determine the impact to TODO Customer, document all findings in a clear and repeatable manner, and provide remediation recommendations. The following types of findings were in-scope for this private bug bounty program:

- Sensitive or personally identifiable information disclosure
- Cross-Site Scripting (XSS)
- Server-side or remote code execution (RCE)
- Arbitrary file upload
- Authentication or authorization flaws, such as insecure direct object references (IDOR), and authentication bypasses
- All forms of injection vulnerabilities
- Directory traversal
- Local file read
- Significant security misconfigurations and business logic flaws
- Exposed credentials that could be leveraged to gain further access

The following types of activities were considered out-of-scope for this bug bounty program:

- Scanning and assessing any other IP in the Entry Point's network
- Physical attacks against TODO Customer properties
- Unverified scanner output
- Man-in-the-Middle attacks
- Any vulnerabilities identified through DDoS or spam attacks
- Self-XSS
- Login/logout CSRF
- Issues with SSL certificates, open ports, TLS versions, or missing HTTP response headers
- Vulnerabilities in third party libraries unless they can be leveraged to significantly impact the target
- Any theoretical attacks or attacks that require significant user interaction or low risk

TODO Candidate Name performed testing under a “Black Box” approach from , to without credentials or any advance knowledge of TODO Customer’s web applications with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely. 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.

3.1 Approach

3.2 Scope

The scope of this assessment was as follows TODO *.tricolor.local and any and all open web server ports discovered on the target IP address provided at the start of the assessment.

In Scope Assets

Host/URL/IP Address	Description
TODO www.triclor.local	Main Tricolor website/unauthenticated
TODO exam IP address	PR website/unauthenticated
TODO exam IP address	Jobs Portal/unauthenticated
TODO exam IP address	HR website/unauthenticated
TODO exam IP address	Tricolor online store/unauthenticated

3.3 Assessment Overview and Recommendations

During the course of testing against TODO Candidate Name identified ...

TODO SUMMARY OF FINDINGS AND RECOMMENDATIONS HERE

4 Web Application Assessment Summary

TODO Candidate Name began all testing activities from the perspective of an unauthenticated user on the internet. TODO Customer provided the tester with a single URL and IP address but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

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

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

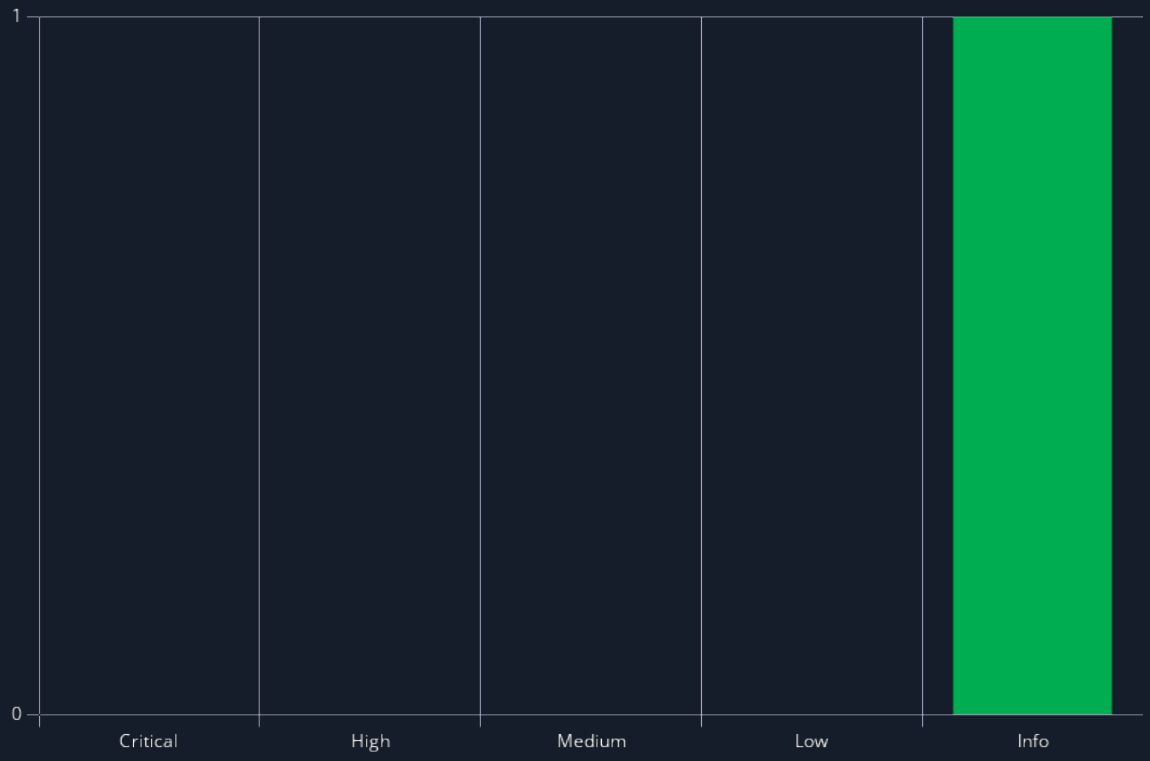

Figure 1 - Distribution of identified vulnerabilities

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

#	Severity Level	Finding Name	Page
1	0.0 (Info)	TODO FINDING TITLE	8

5 Technical Findings Details

1. TODO FINDING TITLE - Info

CWE	TODO CWE
CVSS 3.1	N/A
Root Cause	TODO DESCRIPTION
Impact	TODO IMPACT
Remediation	TODO REMEDIATION
References	-

Finding Evidence

```
ADD COMMAND OUTPUT AS APPROPRIATE
```

TODO ADD SCREENSHOTS AS APPROPRIATE

A Appendix

A.1 Flags Discovered

Flag #	Application	Flag Value	Flag Location	Method Used
1.	TODO HOSTNAME	TODO HTB RANDOM VALUE	TODO Web root	TODO Command Injection (example)
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

End of Report

This report was rendered
by SysReptor with
♥