

Penetration and Security Assessment Report

OuiCroissant

Performed by:

XPLOIT Cybersecurity

Nov. 16, 2024

Version 1.0

Table of Contents

[Statement of Confidentiality 4](#_heading=h.gjdgxs)

[Document Properties 4](#_heading=h.30j0zll)

[Version Control 4](#_heading=h.1fob9te)

[Engagement Contacts 4](#_heading=h.3znysh7)

[Executive Summary 4](#_heading=h.2et92p0)

[Approach 4](#_heading=h.tyjcwt)

[Scope 4](#_heading=h.3dy6vkm)

[Assessment Overview and Recommendations 5](#_heading=h.1t3h5sf)

[Network Penetration Test Assessment Summary 5](#_heading=h.4d34og8)

[Summary of Findings 5](#_heading=h.2s8eyo1)

[Risk Evaluation 5](#_heading=h.17dp8vu)

[Recommendation 5](#_heading=h.3rdcrjn)

[Detail Findings 5](#_heading=h.26in1rg)

[Vulnerabilities 5](#_heading=h.lnxbz9)

[Impact 5](#_heading=h.35nkun2)

[Likelihood 5](#_heading=h.1ksv4uv)

[References 5](#_heading=h.44sinio)

[Appendices 5](#_heading=h.2jxsxqh)

[Glossary 5](#_heading=h.z337ya)

[References 5](#_heading=h.3j2qqm3)

# 

# 1. Statement of Confidentiality

This document is the exclusive property of **OuiCroissant** and **Xploit Cyber Security**. This document contains confidential and proprietary information, distribution of any part or in whole, and or duplication of this document, in any form or medium, requires consent of both OuiCroissant and Xploit Cyber Security.

**2. Privacy Information**

We collect various types of information acquired by our personnel to provide our products and services. This may include such information as:

**Contact and Identifying Information:** We may collect contact and identifying information, such as names, addresses, email addresses, phone numbers, place of business, or other information as it relates to the services involved.

**Automatically Collected Information:** We and third-party online advertising and analytics companies may use cookies, web beacons, or similar technologies to automatically collect information about your online activity, browser and device, as well as to collect information when you interact with our Services or other product offerings.

**How We Use Information**

We use information provided by individuals who use our Services to fulfill the purpose for which the user provided the information and for other purposes as permitted by law, such as:

**Services** that you request, such as by completing security assessments, penetration testing, online training, or providing a quote or estimate for one of our products

**Communicating** with you, for example to respond to inquiries

**Providing** you with information, including communications and interest-based advertisements, on the Website and other websites you visit and marketing communications

**Informing** you of job opportunities and evaluating your suitability for a job

**Developing** operating, delivering, maintaining, improving, enhancing, and protecting the Website and other Services we provide

**Monitoring**, analysis, and research, including of trends, and usage, and advertising-related services

**Enhancing** the safety and security of the Services and preventing fraud or protecting our or our customers’ rights or property

**Enforcing** applicable terms and conditions and other applicable policies

**Other** purposes specifically disclosed at the time the information is requested

We may remove identifiable information collected by removing identifiers, such as your name, or by aggregating information about multiple users. We may work with third parties to aggregate such information on our behalf. Aggregate information collected on the Services does not personally identify you, and we may use aggregated information for the purposes described above and share aggregate information with third parties for lawful purposes.

We also may combine information collected through the Services with other information about you.

We may disclose your information to:

1. Comply with applicable laws
2. Respond to governmental inquiries or requests
3. Comply with valid legal processes
4. Protect the rights, privacy, safety, users of Services, customers, and the public
5. Permit us to pursue available remedies or limit the damages that we may sustain
6. Enforce our Terms of Service

# 

# 3. Document Properties

# Version Control

| Revision No | Editor Name | Revision Date | Reason for Revision | Revision Description |
| --- | --- | --- | --- | --- |
| 1 | Name | 1 | Updating table | Added Column |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# 

# 4. Engagement Contacts

**Executive Contact:**

Office Number:

Email:

**Team Lead Contact:**

Office Number:

Email:

## 

## 

## 

## 

## 

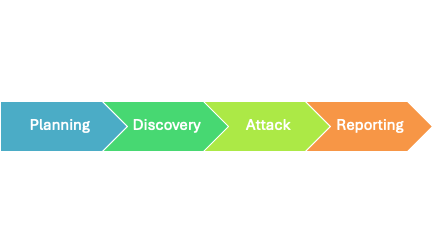
## 

## 

## 5. Assessment Overview and Recommendations

From <month> xth, 20XX to <month> yth, 20XX XPLOIT attempted to evaluate the security posture of the infrastructure of OuiCroissant and compared it to the current industry best practices by performing an web application penetration test Phases of penetration testing activities including 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 discoveries upon new access.
* **Reporting** – Document all found vulnerabilities, exploits, failed attempts, and company strengths and weaknesses.



# 

# 6. Assessment Components

## 6.1 Web Application Penetration Test

A web application penetration test emulates the role of an attacker from outside the network. An engineer will scan the assets that face the internet to identify potential vulnerabilities.

# 

# 7. Findings Severity Ratings

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

**Finding Severity Ratings**

| Severity | CVSS V3.0 Score Range | Definitions |
| --- | --- | --- |
| Critical | 9.0-10.0 | **Exploitation:** Exploitation is straightforward which results in system-level compromise. **Plan of action:** Patch immediately or remove system from environment. |
| High | 7.0-8.9 | **Exploitation:** Exploitation is more difficult and its very probable that it would cause elevated privileges. Potential loss of data or downtime. **Plan of action:** Patch as soon as possible or remove the system from the environment. |
| Medium | 4.0-6.9 | **Exploitation:** Vulnerabilities exist but are not exploitable. It's very likely extra steps are required to make the vulnerability exploitable. **Plan of action:** Patch after high-priority issues have been remediated. |
| Low | 0.1-3.9 | **Exploitation: V**ulnerabilities are non-exploitable. Mitigation will very likely reduce the attack surface. **Plan of action:** Patch during the next maintenance window. |
| None | 0 | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# 8.Risk Factors

Risk is measured by two factors: Likelihood & impact.

## 8.1 Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, the attacker's skill level, and the client environment.

## 8.2 Impact

Impact measures the potential vulnerability’s effect on operations, including confidentiality, integrity and availability of client systems and/or data, reputational harm, and financial loss.

# 9. Scope

| Assessment | Details |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Details

## 9.1 Scope Exclusions

Xploit Cyber Security did not perform any of the following attacks during testing:

Denial of Service (DoS)

Phishing/Social Engineering

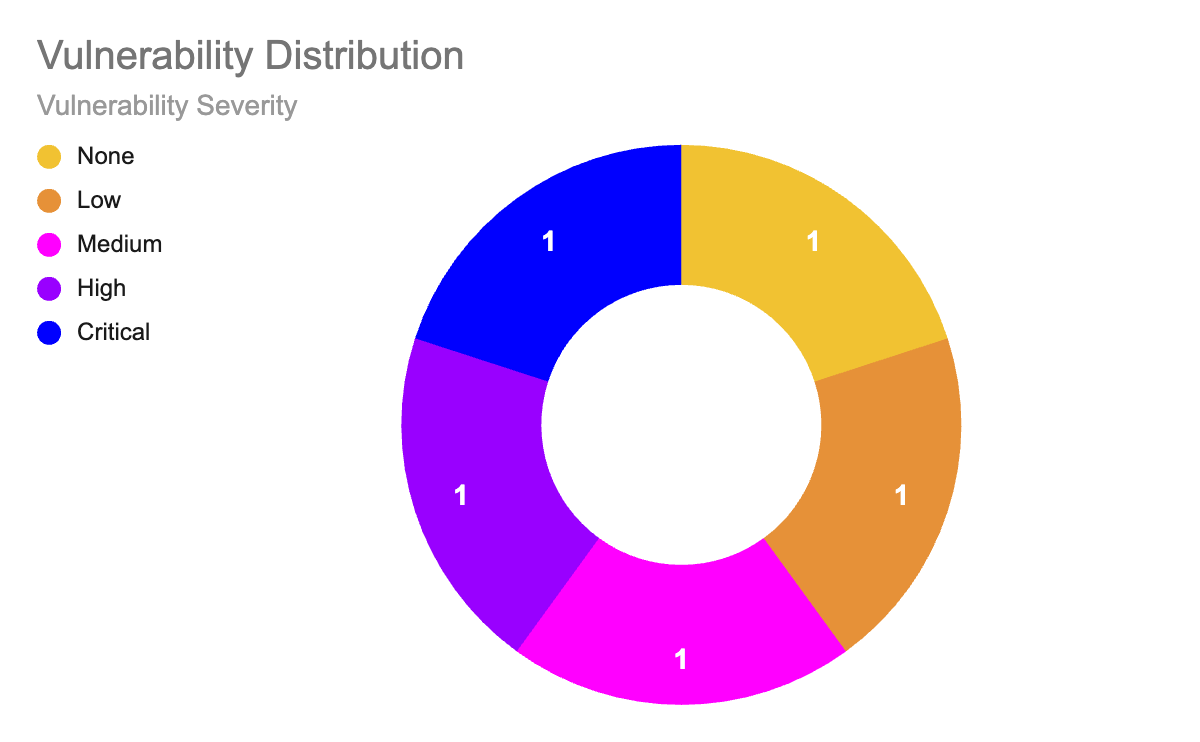
All other attacks not specified above were covered in penetration testing of the domain.

| Assessment | Details |
| --- | --- |
| Out-of-Scope Networks | VDI |
| Out-of-Scope Networks | VPN |
| Out-of-Scope Networks | RIT Cyber Range |
| Out-of-Scope Networks | Regional Host/University Environment |
| Out-of-Scope Tools | Our technology partner's deployment tool (LaForge) |

10. Executive Summary

Xploit Cyber Security evaluated Demo Corp's web application security posture through an external penetration test following sections provide a high-level overview of

from <month> xth, 20XX to <month> Yth, 20XX. The

vulnerabilities discovered, successful and unsuccessful Security Rating attempts, and strengths and weaknesses.

## 10.1 Scope Topology

## 10.2 Testing Summary

*The web application assessment evaluated democorp.com's security posture. The Xploit Cyber Security team performed vulnerability scanning against the domains mentioned in the scope.*

*Unrestricted File Upload was found on the domain democorp.com, resulting in an attacker being able to execute commands on the server. This vulnerability can let an attacker discover sensitive files like databases, password files, and configuration files which can help an attacker potentially gain access to the server.*

*Also, it was found that the domain* ***example.com*** *does not implement strict HSTS which means all of the communications between the user and the webserver are unencrypted. This can aid an attacker to gain login credentials, credit/debit card numbers, etc. By performing MITM (man in the middle) attacks.*

*An outdated “js\_composer” was found on democorp.com, the version “js\_composer 5.0.1” which is implemented is known to be vulnerable to authenticated stored XSS, this vulnerability can be utilized by an attacker to execute arbitrary JavaScript on the victim's browser.*

*There were also some vulnerable old Jquery libraries being implemented on the website. Usage of these libraries can result in new vulnerabilities arising late*

# 11. Key Strengths and Weaknesses

# 12. Vulnerability Distribution Table

The following table illustrates the vulnerabilities found by severity and recommended remediations:

| Findings | Severity | Recommendations |
| --- | --- | --- |
| WPT-001: example.txt | Critical | Update the sample file plugin to the latest version |
| WPT-002 | Medium | Enable js\_composer to the latest version |
| WPT-003 | Low | Enable HTTP strict transport security (HSTS) by adding a response hear |
| WPT-004 | Informational | Implement the latest Jquery libraries |

# 13. Vulnerability Application Penetration Testing

### WPT-001: example.txt

| Description |  |
| --- | --- |
| URL: |  |
| Approach: |  |
| Tools Used: |  |
| References: |  |

### Evidence

By visiting the URL we can get the version number of “text.txt” inside the source.

\*\*\*\*\* Insert Image\*\*\*\*\*\*\*\*

### Risk

#### Likelihood

If the website is providing the functionality of file upload then it’s highly likely that this vulnerability can be exploited.

* Impact

### Remediation

* + More Information
    - Links

# FindingsWPT-002: example.txt

| Description |  |
| --- | --- |
| URL: |  |
| Approach: |  |
| Tools Used: |  |
| References: |  |

### Evidence

By visiting the URL we can get the version number of “text.txt” inside the source.

\*\*\*\*\* Insert Image\*\*\*\*\*\*\*\*

### Risk

* Likelihood

If the website is providing the functionality of file upload then it’s highly likely that this vulnerability can be exploited.

* Impact

### Remediation

* + More Information
    - Links

# FindingsWPT-003: example.txt

| Description |  |
| --- | --- |
| URL: |  |
| Approach: |  |
| Tools Used: |  |
| References: |  |

### Evidence

By visiting the URL we can get the version number of “text.txt” inside the source.

\*\*\*\*\* Insert Image\*\*\*\*\*\*\*\*

### Risk

* Likelihood`

If the website is providing the functionality of file upload then it’s highly likely that this vulnerability can be exploited.

* Impact

### Remediation

* + More Information
    - Links

# Findings

## Network

## Approach

Briefly supply methodology and tools used

Xploit Cybersecurity is authorized by Flakebook to perform a penetration test on the External and Internal networks owned and operated by Flakebook. The External IPs in scope are to be provided before the beginning of the penetration test period, and Xploit Cybersecurity agrees to limit testing to these IPs only. Should Xploit Cybersecurity find entry into the internal networks and systems owned by Fakebook, we will continue to assess these resources for vulnerabilities and append them to our report. Xploit Cybersecurity will use a variety of tools to perform these tests, but testing will be limited to tools and methods which will not cause disruption of service, loss or publishing of confidential and proprietary data, or loss of access to systems for employees and contractors. These tools will fingerprint the environment using network and vulnerability scanners such as Nmap, OpenVas, Nikto, and more. There will be an increase of activity on the network due to these scans, however our testing assures us that we can do so without depriving access to resources to customers and employees. Our tests will also include testing web applications manually and through the use of tools such as BurpSuite, Postman, and more. These tools manipulate web requests but will be done with care to assure that legitimate traffic to these web application is not impeded. In certain cases our team may use known exploit code to confirm vulnerabilities found, in which case Xploit Cybersecurity will review and approve code that will not negatively impact Flakebook’s systems and business practices. Similarly, any internal testing will be done with a combination of native binaries and tools suited to test vulnerabilities on operating systems and domains within our scope. Xploit Cybersecurity will do so without impeding employee access to systems and internal resources. Also, as part of our service we will clean up any tools and files we may import into the environment and all actions such as these will be available in this document.

# Network Penetration Test Assessment Summary

# Summary of Findings

\*\*add numbered table with x number of high, x number of medium, x number of low

Overview

Findings per platform:

Naming Convention:

Findings -

BoxDNS\_IP\_Finding\_SEVERITY.txt

Box DNS = DNS Name

IP = IP Address

Finding (CVE / Desc.)

Severity = (Crit,High,Med,Low)

# References

## Work Cited

SANS. “NVD - Vulnerability Metrics.” *What is Common Vulnerability Scoring System (CVSS Score)*, 22 May 2023, https://nvd.nist.gov/vuln-metrics/cvss. Accessed 9 November 2024.

# Appendices

# Glossary

Data Classification - The process of grouping information on a basis of sensitivity, type and business context.



XPLOIT Cyber Security

Guarding tomorrow’s digital code one line of code at a time.