

Security Assessment Findings Report

Final Report

Business Confidential

Date: April 18th, 2022

Project: Blunder\_Tiffin\_001

Version 2.0

# Version History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Description** |
| 1.0 | April 14th 2022 | Francesco Elisa | Initial Version |
| 1.1 | April 15th 2022 | Francesco Elisa | Introductory Sections |
| 1.2 | April 16th 2022 | Francesco Elisa | Penetration Test Findings and Annexes |
| 1.3 | April 17th 2022 | Francesco Elisa | Executive Summary and Security Weaknesses |
| 2.0 | April 18th 2022 | Francesco Elisa | Final Review |

# Table of Contents

[Version History 2](#_Toc101217378)

[Table of Contents 3](#_Toc101217379)

[Confidentiality Statement 5](#_Toc101217380)

[Disclaimer 5](#_Toc101217381)

[Contact Information 5](#_Toc101217382)

[Assessment Overview 6](#_Toc101217383)

[Assessment Components 6](#_Toc101217384)

[Finding Severity Ratings 7](#_Toc101217385)

[Scope 8](#_Toc101217386)

[Scope Exclusions 8](#_Toc101217387)

[Client Allowances 8](#_Toc101217388)

[Executive Summary 9](#_Toc101217389)

[Attack Summary 9](#_Toc101217390)

[Security Weaknesses 10](#_Toc101217391)

[Information Disclosure through Headers 10](#_Toc101217392)

[Unrestricted Login Attempts 10](#_Toc101217393)

[Login Portal Username Enumeration 10](#_Toc101217394)

[Password Recovery Username and Email Enumeration 11](#_Toc101217395)

[Directory Transversal and Read access to Web Server Files 11](#_Toc101217396)

[Password Reutilization 11](#_Toc101217397)

[Legacy Polkit Version 11](#_Toc101217398)

[Legacy WordPress Version 11](#_Toc101217399)

[Default Apache HTTP Test Page and Files 11](#_Toc101217400)

[Vulnerabilities by Impact 12](#_Toc101217401)

[Internal Penetration Test Findings 13](#_Toc101217402)

[Possibility to Brute Force User Credentials in the Login Portal 17](#_Toc101217403)

[Legacy Polkit Version Vulnerable to CVE-2021-3560 13](#_Toc101217404)

[SSL Self-Signed Certificate/SSL Certificate Cannot Be Trusted 14](#_Toc101217405)

[Legacy WordPress Version Vulnerable to CVE-2019-17671 16](#_Toc101217406)

[HTTP TRACE / TRACK Methods Allowed 18](#_Toc101217407)

[Browsable Web Directories 18](#_Toc101217408)

[Directory Transversal and Read access to Web Server Files 23](#_Toc101217409)

[WordPress User and Email Enumeration 19](#_Toc101217410)

[Information Disclosure through the “X-Backend-Server” Header 22](#_Toc101217411)

[Web Server Transmits Cleartext Credentials 25](#_Toc101217412)

[Web Server Allows Password Auto-Completion 25](#_Toc101217413)

[SSH Server CBC Mode Ciphers Enabled 26](#_Toc101217414)

[SSH Weak KXPTO Exchange Algorithms Enabled 24](#_Toc101217415)

[HSTS Missing from HTTPS Server 27](#_Toc101217416)

[HTTP Cookies Web Application Cookies Not Marked HttpOnly 27](#_Toc101217417)

[HTTP Cookies Web Application Cookies Not Marked Secure 27](#_Toc101217418)

[WordPress Detection 28](#_Toc101217419)

[Additional Reports and Scans (Informational) 28](#_Toc101217420)

# Confidentiality Statement

This document is the exclusive property of XPTO Portugal (XPTO) and Blunder Tiffin Inc. (BT). This document holds proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both XPTO and BT.

XPTO may share this document with auditors under non-disclosure agreements to display 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. XPTO prioritized the assessment to find the weakest security controls an attacker would exploit. XPTO recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

# Contact Information

|  |  |
| --- | --- |
|  |  |

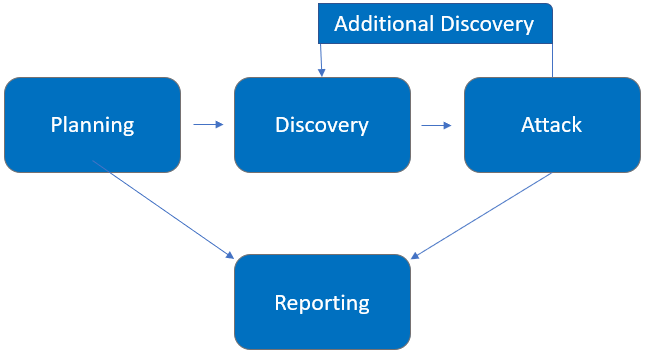
|  |  |  |
| --- | --- | --- |
| Name | Title | Contact Information |
| **Blunder Tiffin Inc.** | | |
| Michael Scott | CISO | Office: (+351) 912 345 678  Email: [michael.scott@bt.com](mailto:michael.scott@bt.com) |
| Dwight Schrute | IT Manager | Office: (+351) 919 876 543  Email: [dwight.shrute@bt.com](mailto:dwight.shrute@bt.com) |
| **TCM Security** | | |
| Francesco Elisa | Lead Penetration Tester | Office: (+351) 918 102 385  Email: [francesco.elisa@xpto.com](mailto:francesco.elisa@xpto.com) |

# Assessment Overview

From April 9th, 2022, to April 18th, 2022, BT engaged XPTO 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 the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4)* which includes the *OWASP Web Security Testing Guide*, *OWASP Top Ten Web* and the *Common Vulnerability Scoring System (CVSS)*.

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 added discovery upon new access.
* Reporting – Document all found vulnerabilities and exploits, failed attempts, and company security weaknesses.



# Assessment Components

**Internal Penetration Test**

An internal network penetration test is performed to help gauge what an attacker could achieve with initial access to a network. This assessment has the purpose of identifying what could be accomplished by an intruder who has gained internal access to the network. After the vulnerability identification stage, penetration testes exploit these vulnerabilities to gauge the impact of the vulnerability and highlight possible entry points. It usually comes into picture after the execution of an external penetration test, but in the case of our assessment, this phase was omitted since XPTO was granted access to the internal network.

# 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. |
| Medium | 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 | 10.10.11.143 |

* Full scope information provided in “**Blunder\_Tiffin\_001\_Full\_Findings.xslx”**

## Scope Exclusions

XPTO deployed a vulnerability management tool to automatically detect common vulnerabilities which the server could be vulnerable to. The server holds a default Apache HTTP Test page, but since the main target of this assessment is not the HTTP server’s test page, this report will focus on the remaining vulnerabilities.

Per client request, XPTO did not perform any Denial-of-Service attacks during testing.

## Client Allowances

BT did not provide any allowances to assist the testing.

# Executive Summary

XPTO evaluated BT’s external security posture through an internal network penetration test from April 9th, 2022, to April 19th, 2022. By leveraging a series of attacks, XPTO found high level vulnerabilities that allowed complete control over BT’s target machine. It is highly recommended that BT address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

## Attack Summary

The following table describes how XPTO gained root level access over the target system, step by step:

|  |  |  |
| --- | --- | --- |
| Step | Action | Recommendation |
| 1 | Discovered the “X-Backend-Server" Header that disclosed the internal/hidden domain **office.paper** | Reconfigure HTTP responses to not send this header |
| 2 | Simple enumeration techniques and HTML code inspection were able to **identify the WordPress version** in use by the web application.  Additionally, despite not being directly relevant for this attack chain it was verified that an attacker can perform unrestricted login attempts to the web application in **office.paper.** | Installing the “WP-Hardening” plugin allows to easily hide the WordPress version in use. Alternatively, BT may also perform this step manually using “secure by obscure” mechanisms to remove the vulnerability.  Restricting login attempts by setting a timeout or blacklisting the IP would be a recommended approach to tackle this vulnerability. |
| 3 | Through the identification of the WordPress version, we were able to identify that the web application was susceptible to CVE-2019-17671. This vulnerability allows the viewing of unauthenticated private posts which enabled us to discover a new subdomain **chat.office.paper** | XPTO recommends upgrading WordPress to version 5.2.4 or above (ideally the latest stable version) |
| 4 | Extracted “recyclops” credentials which were later used to **obtain a shell** through SSH | Restricting directory transversal and read access to the files outside the “sales” folder. |
| 5 | Leveraged valid credentials to **log into SSH** | Changing the password of the user “dwight” to a different and more secure one is recommended. It was verified that the current password is identical to the password of the user “recyclops” in the chat application. Furthermore, BT can also [set up SSH to use multi-factor authentication](https://www.digitalocean.com/community/tutorials/how-to-set-up-multi-factor-authentication-for-ssh-on-ubuntu-16-04). |
| 6 | Server’s Polkit version vulnerable to **CVE-2021-3560**, which allows an authenticated user to gain a root level access on the system without passing the authentication requirements | To fix the exploit you can download the fixed packages from the Linux distribution websites.  **NOTE: Recently it was discovered a new privilege escalation vulnerability (CVE-2021-4034). We highlight the importance of updating to the latest version.** |

# Security Weaknesses

## Information Disclosure through Headers

During the information gathering phase of the assessment, XPTO was able to identify headers that disclosed information regarding server details, technologies, WordPress API and an internal domain.

* Server details: “Server” Header
* Technologies: “Powered-by” Header
* WordPress API: “Link” Header
* Internal domain: “X-Backend-Server” Header

## Unrestricted Login Attempts

During the assessment, XPTO performed multiple authentication attacks against the login form found on the web application. For all logins, unlimited attempts were allowed, which serves as a proof-of-concept that an attacker with enough time and resource could login with valid account credentials to **office.paper**. This would further open the attack landscape as the attacker would be able to login in the web application.

## Login Portal Username Enumeration

XPTO was able to detect the possibility of enumerating usernames in the **office.paper** web application login portal.

## Password Recovery Username and Email Enumeration

XPTO was able to detect the possibility of enumerating usernames and email addresses in the **office.paper** web application password recovery portal.

## Directory Transversal and Read access to Web Server Files

A user authenticated in the rocket chat web application (**chat.office.paper**) can leverage the “recyclops” bot functionalities to list and read some of the web server’s files. This vulnerability was leveraged to extract credentials to login with SSH as user “dwight”.

## Password Reutilization

XPTO was able to successfully obtain a shell by logging into SSH, because of the existence of password reutilization between the system user “dwight” and the chat application user “recyclops”.

## Legacy Polkit Version

XPTO leveraged a vulnerability in Polkit to obtain root level access to the target system by escalating dwight’s privileges in an SSH shell.

## Legacy WordPress Version

XPTO leveraged a vulnerability in WordPress that returns all pages from the database (including password protected, pending and drafts), thus leaking its secret content. This vulnerability allowed to discover a new subdomain.

## Default Apache HTTP Test Page and Files

It is not recommended to have the default HTTP Apache Test Page or the default files of Apache in a live web server environment. This can be used to fingerprint the Apache version and even the operating system. To highlight this aspect, Nessus detected a wide array of vulnerabilities related to this test page and the files it exposes which can be consulted in the **Blunder\_Tiffin\_001\_Full\_Findings.xslx**.

# Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

*Figure 1: Bar chart displaying the distribution of Vulnerabilities by Impact*

*Figure 1: Pie chart displaying the distribution of Vulnerabilities by Impact*

## Internal Penetration Test Findings

**Enumeration**

The enumeration of information relating to BT's internal network was conducted using active recognition tools, such as port scanners, which allow for the mapping of all exposed services and ports of the asset being covered in this assessment.

|  |  |
| --- | --- |
| IP Address | **Ports/Protocols** |
| 10.10.11.143 | 22/tcp, 80/tcp, 443/tcp, 5353/udp |

**Vulnerabilities**

For the process of enumeration, vulnerability assessment and exploitation, BT provided XPTO with a VPN access to conduct their tests.

Legacy Polkit Version Vulnerable to CVE-2021-3560

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | High | **CVSSv3 Classification** | 7.8 |
| Description | Polkit is a small toolkit used for defining and handling authorizations on Unix/Linux platforms. In short, by helping unprivileged process securely communicate with privileged processes, it stops unprivileged users from executing admin tasks. | | |
| CVSSv3  Criteria | **Attack Vector**: Local  **Attack** **Complexity**: Low  **Privileges** **Required**: Low  **User** **Interaction**: None  **Scope**: Unchanged  **Confidentiality**: High  **Integrity**: High  **Availability**: High | | |
| System | 10.10.11.143 | | |
| Risk | If the attacker has local access to the machine (e.g., SSH) and the machine is vulnerable to the exploit, the attacker can obtain root level access without passing the authentication. | | |
| Proof-of-Concept | XPTO took advantage of [this proof-of-concept script](https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Esclation) to get root level access on the victim. Basically, the script tricks the system into executing a request as UID 0 (root) by taking advantage of how polkit treats the UID of a connection with a bus identifier that no longer exists.  Steps:   * Execute the script (creates a new username in the system) * Switch user to the created username * Run "bash" as the super user (root) | | |
| Part played  towards Flag | By being able to gain root level access to the machine XPTO was able to read the content of the /root/root.txt flag. | | |
| Recommendation | BT can patch the vulnerability by downloading the fixed packages from the Linux distribution websites.  **NOTE**: Recently it was discovered a new privilege escalation vulnerability (CVE-2021-4034). XPTO highlights the importance of updating to the latest version. | | |
| References | https://github.com/secnigma/CVE-2021-3560-Polkit-Privilege-Esclation | | |

SSL Self-Signed Certificate/SSL Certificate Cannot Be Trusted

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Medium | **CVSSv3 Classification** | 6.5 |
| Description | The server's X.509 certificate cannot be trusted because it is self-signed. | | |
| CVSSv3  Criteria | **Attack Vector**: Network  **Attack** **Complexity**: Low  **Privileges** **Required**: None  **User** **Interaction**: None  **Scope**: Unchanged  **Confidentiality**: Low  **Integrity**: Low  **Availability**: None | | |
| System | 10.10.11.143 | | |
| Risk | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production , this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. | | |
| Proof-of-Concept | The following certificate was found at the top of the certificate chain sent by the remote host, but it is self-signed and was not found in the list of known certificate authorities. | | |
| Part played  towards Flag | N/a | | |
| Recommendation | BT may purchase or generate a proper SSL certificate for this service from a Certified Authority if thXPTO plan to publish this application to be accessible via the Internet. | | |
| References | [OWASP Web Security Testing Guide: Testing for Weak SSL TLS Ciphers Insufficient Transport Layer Protection](https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/01-Testing_for_Weak_SSL_TLS_Ciphers_Insufficient_Transport_Layer_Protection) | | |

Legacy WordPress Version Vulnerable to CVE-2019-17671

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Medium | **CVSSv3 Classification** | 5.3 |
| Description | Unauthenticated viewing of certain content is possible because the static query property is mishandled. | | |
| CVSSv3  Criteria | **Attack Vector**: Network  **Attack** **Complexity**: Low  **Privileges** **Required**: None  **User** **Interaction**: None  **Scope**: Unchanged  **Confidentiality**: Low  **Integrity**: None  **Availability**: None | | |
| System | 10.10.11.143 ([http://office.paper/](http://office.paper/wp-login.php) ) | | |
| Risk | Adding ?static=1 to a WordPress URL returns all pages from the database (including password protected, pending and drafts), thus leaking its secret content. | | |
| Proof-of-Concept | XPTO detected that the Wordpress version being used by the web application was vulnerable to CVE-2019-17671. Hence, by adding the static query parameter with value 1 XPTO was able to discover a registration page for the web application stored in the subdomain **chat.paper.office**, further widening their attack surface.  Uma imagem com texto  Descrição gerada automaticamente | | |
| Part played  towards Flag | By having access to the chat web application, XPTO was later able to meet “recyclops”, a bot developed by Dwight. Through chatting with the bot, XPTO was able to extract user credentials (username and **password** of recyclops in the rocket chat application) that could be used in combination with **“dwight”** username to obtain an SSH shell and read the user flag stored in the user.txt file. | | |
| Recommendation | BT should update Wordpress to the latest version so that the web application is no longer vulnerable to this exploit. | | |
| References | [NIST: CVE-2019-17671](https://nvd.nist.gov/vuln/detail/CVE-2019-17671)  [Exploit Database: CVE-2019-17671](https://www.exploit-db.com/exploits/47690) | | |

Possibility to Brute Force User Credentials in the Login Portal

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Medium | **CVSSv3 Classification** | 6.5 |
| Description | BT does not restrict the number of authentication attempts against their **office.paper** web application login portal. This configuration allows the possibility to brute force user credentials. | | |
| CVSSv3  Criteria | **Attack Vector**: Network  **Attack** **Complexity**: Low  **Privileges** **Required**: None  **User** **Interaction**: None  **Scope**: Unchanged  **Confidentiality**: Low  **Integrity**: Low  **Availability**: None | | |
| System | 10.10.11.143 (<http://office.paper/wp-login.php>) | | |
| Risk | The risk of being able to brute force user credentials is that an attacker may be able to compromise all user accounts including ones with higher privileges. This is especially dangerous because it compromises the principles of confidentiality, integrity, and availability of data. | | |
| Proof-of-Concept | For demonstration purposes, through Hydra XPTO was able to perform an authentication attack using a large wordlist. As you can see in the image below the target did not perform any type of filtering or apply any restriction to the attacker’s IP.  Hence, if an threat actor performed a brute force attack instead, he would eventually be able to gain access to every user’s account. Furthermore, the attacker would not even have to try to brute force usernames, since the web application is also vulnerable to user enumeration. | | |
| Part played  towards Flag | N/a | | |
| Recommendation | Mitigation techniques recommended to implement:   * Locking out accounts after a certain number of incorrect password attempts; * Limit failed login attempts; * Use a Captcha mechanism; * Limit logins to a specified IP address or range; * Employ Multi-factor authentication. | | |
| References: | [OWASP TOP 10 A07 2021- Identification and Authentication Failures](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/)  [NIST SP800-53r5 AC-7](https://nvd.nist.gov/800-53/Rev4/control/AC-7#enhancement-1) - Unsuccessful Logon Attempts |Automatic Account Lock | | |

HTTP TRACE / TRACK Methods Allowed

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Medium | **CVSSv3 Classification** | 5.3 |
| Description | The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. | | |
| CVSSv3  Criteria | **Attack Vector**: Network  **Attack** **Complexity**: Low  **Privileges** **Required**: None  **User** **Interaction**: None  **Scope**: Unchanged  **Confidentiality**: Low  **Integrity**: None  **Availability**: None | | |
| System | 10.10.11.143 | | |
| Risk | An attacker could steal credentials by using a client-side attack, such as cross-site scripting to steal a cookie even being able to bypass the HTTPOnly header. | | |
| Proof-of-Concept | N/a | | |
| Part played  towards Flag | N/a | | |
| Recommendation | BT should disable these HTTP methods by adding the following to the Apache httpd.conf file: “TraceEnable Off” | | |
| References | N/a | | |

Browsable Web Directories

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Medium | **CVSSv3 Classification** | 5.3 |
| Description | Directories on the remote web server are browsable. | | |
| CVSSv3  Criteria | **Attack Vector**: Network  **Attack** **Complexity**: Low  **Privileges** **Required**: None  **User** **Interaction**: None  **Scope**: Unchanged  **Confidentiality**: Low  **Integrity**: None  **Availability**: None | | |
| System | 10.10.11.143 | | |
| Risk | Could allow XPTO to perform directory transversal attacks by viewing “hidden files”, such as CGI scripts, data files or backup pages. | | |
| Proof-of-Concept | XPTO detected that a couple of resources of the web application were browsable such as:   * http://10.10.11.143/icons/ * http://10.10.11.143/manual/ * http://10.10.11.143/manual/images/ * http://10.10.11.143/manual/style/ * http://10.10.11.143/manual/style/css/ * http://10.10.11.143/manual/style/lang/ * http://10.10.11.143/manual/style/latex/ * http://10.10.11.143/manual/style/scripts/ * http://10.10.11.143/manual/style/xsl/ | | |
| Part played  towards Flag | N/a | | |
| Recommendation | BT should ensure that those directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing is recommended. | | |
| References | N/a | | |

WordPress User and Email Enumeration

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Medium | **CVSSv3 Classification** | 5.3 |
| Description | The remote web server contains a PHP application that is affected by an information disclosure vulnerability. | | |
| CVSSv3  Criteria | **Attack Vector**: Network  **Attack** **Complexity**: Low  **Privileges** **Required**: None  **User** **Interaction**: None  **Scope**: Unchanged  **Confidentiality**: Low  **Integrity**: None  **Availability**: None | | |
| System | 10.10.11.143 (<http://office.paper/wp-login.php>)  10.10.11.143 (<http://office.paper/wp-login.php?action=lostpassword>) | | |
| Risk | The version of WordPress hosted on the remote web server is affected by a user enumeration vulnerability. An unauthenticated, remote attacker can exploit this to learn the names of valid WordPress users and emails. | | |
| Proof-of-Concept | **Login Portal**  The web application returns different errors in the login portal if the username exists or not.  Logging in as “prisonmike”:    Logging in as an invalid username:    **Password Recovery**  Application returns different error if the username/email address exist or not.  Testing with an invalid username:      Testing with “prisonmike”: | | |
| Part played  towards Flag | N/a | | |
| Recommendation | Installing the “WP-Hardening” or the “Stop User Enumeration” plugins help to mitigate this vulnerability. Alternatively, BT may also provide generic response to every failed login attempt (“Invalid credentials”) and for every password reset (“If your username/email exists check your inbox to reset your password”). | | |
| References | [OWASP TOP 10 A07 2021- Identification and Authentication Failures](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/) | | |

Information Disclosure through the “X-Backend-Server” Header

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Medium | **CVSSv3 Classification** | 5.3 |
| Description | Information Disclosure through the “X-Backend-Server” header discloses hidden resource. | | |
| CVSSv3  Criteria | **Attack Vector**: Network  **Attack** **Complexity**: Low  **Privileges** **Required**: None  **User** **Interaction**: None  **Scope**: Unchanged  **Confidentiality**: Low  **Integrity**: None  **Availability**: None | | |
| System | 10.10.11.143 | | |
| Risk | XPTO was able to further widen the attack surface by extracting the existing domain **office.paper** through the header “X-Backend-Server”. | | |
| Proof-of-Concept | Performing a simple HTTP request to the server provides a response which contains the “X-Backend-Server” Header. | | |
| Part played  towards Flag | This was the first major step towards indirectly being able to exploit the server. This allowed XPTO to discover a resource which later was found to be vulnerable to an exploit. | | |
| Recommendation | BT should ensure that those directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing is recommended. | | |
| References | [OWASP TOP 10 A05 2021 – Security Misconfiguration](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/) | | |

Directory Transversal and Read access to Web Server Files

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Medium | **CVSSv3 Classification** | 5 |
| Description | Directories on the remote web server are browsable and files are readable through exploiting the rocket chat bot’s functionalities. | | |
| CVSSv3  Criteria | **Attack Vector**: Network  **Attack** **Complexity**: Low  **Privileges** **Required**: Low  **User** **Interaction**: None  **Scope**: Changed  **Confidentiality**: Low  **Integrity**: None  **Availability**: None | | |
| System | 10.10.11.143 (chat.office.paper) | | |
| Risk | Through this vulnerability XPTO was able to have read access to the “.env” file stored in the “hubot” folder which holds **“recyclops”’s credentials** in the rocket chat app. | | |
| Proof-of-Concept | By running the command “list ../hubot/” XPTO was able to list the folder contents. Afterwards using the command “file .env” we extract the bot’s credentials.  Uma imagem com texto  Descrição gerada automaticamente | | |
| Part played  towards Flag | The bot’s password is the same as Dwight’s password in the server. Therefore, XPTO was able to obtain shell using SSH. | | |
| Recommendation | BT should ensure that the bot is only able to list and read the files inside the sales directory. | | |
| References | N/a | | |

SSH Weak KXPTO Exchange Algorithms Enabled

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Low | **CVSSv3 Classification** | 3.7 |
| Description | The remote SSH server is configured to allow weak kXPTO exchange algorithm diffie-hellman-group-exchange-sha1. | | |
| CVSSv3  Criteria | **Attack Vector**: Network  **Attack** **Complexity**: High  **Privileges** **Required**: None  **User** **Interaction**: None  **Scope**: Unchanged  **Confidentiality**: Low  **Integrity**: None  **Availability**: None | | |
| System | 10.10.11.143 | | |
| Risk | The IETF draft document KXPTO Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) states that the diffie-hellman-group-exchange-sha1 should not be enabled. This is because SHA-1 is considered deprecated and has security concerns. | | |
| Proof-of-Concept | N/a | | |
| Part played  towards Flag | N/a | | |
| Recommendation | BT should disable the weak algorithms. | | |
| References | [KXPTO Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH)](https://www.ietf.org/archive/id/draft-ietf-curdle-ssh-kex-sha2-12.html)  [Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms](https://www.rfc-editor.org/info/rfc6194)  [OWASP Web Security Testing Guide: Testing for Weak SSL TLS Ciphers Insufficient Transport Layer Protection](https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/01-Testing_for_Weak_SSL_TLS_Ciphers_Insufficient_Transport_Layer_Protection) | | |

Web Server Transmits Cleartext Credentials

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Low | **CVSSv3 Classification** | 3.1 |
| Description | The remote web server contains HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext. | | |
| CVSS  Vector String | **Attack Vector**: Network  **Attack** **Complexity**: High  **Privileges** **Required**: None  **User** **Interaction**: Required  **Scope**: Unchanged  **Confidentiality**: Low  **Integrity**: None  **Availability**: None | | |
| System | 10.10.11.143 | | |
| Risk | An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users. | | |
| Proof-of-Concept | N/a | | |
| Part played  towards Flag | N/a | | |
| Recommendation | Make sure that every sensitive form transmits content over HTTPS. Enforce encryption using directives like HTTP Strict Transport Security (HSTS). | | |
| References | [OWASP TOP 10 A02 2021 – Cryptographic Failures](https://owasp.org/Top10/A02_2021-Cryptographic_Failures/) | | |

Web Server Allows Password Auto-Completion

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Low | **CVSSv3 Classification** | 3.1 |
| Description | The 'autocomplete' attribute is not disabled on password fields. | | |
| CVSSv3  Criteria | **Attack Vector**: Network  **Attack** **Complexity**: High  **Privileges** **Required**: None  **User** **Interaction**: Required  **Scope**: Unchanged  **Confidentiality**: Low  **Integrity**: None  **Availability**: None | | |
| System | 10.10.11.143 | | |
| Risk | Could lead to a loss of confidentiality on their saved passwords if any of the users use a shared host or if their machine is compromised at some point. | | |
| Proof-of-Concept | N/a | | |
| Part played  towards Flag | N/a | | |
| Recommendation | BT should add the attribute 'autocomplete=off' to password fields to prevent browsers from caching credentials. | | |
| References | [CWE-200: Information Exposure](https://cwe.mitre.org/data/definitions/200.html) | | |

SSH Server CBC Mode Ciphers Enabled

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Low | **CVSSv3 Classification** | 3.1 |
| Description | The SSH server is configured to use Cipher Block Chaining, which historically has been proven insecure. | | |
| CVSSv3  Criteria | **Attack Vector**: Network  **Attack** **Complexity**: High  **Privileges** **Required**: None  **User** **Interaction**: Required  **Scope**: Unchanged  **Confidentiality**: Low  **Integrity**: None  **Availability**: None | | |
| System | 10.10.11.143 | | |
| Risk | Usage of CBC makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session. | | |
| Proof-of-Concept | N/a | | |
| Part played  towards Flag | N/a | | |
| Recommendation | BT should disable CBC mode cipher encryption and enable CTR or GCM cipher mode encryption. | | |
| References | [OWASP TOP 10 A02 2021 – Cryptographic Failures](https://owasp.org/Top10/A02_2021-Cryptographic_Failures/)  [NIST Vulnerability Database: CVE-2008-5161](https://nvd.nist.gov/vuln/detail/CVE-2008-5161) | | |

HSTS Missing from HTTPS Server

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Informational | **CVSSv3 Classification** | - |
| Description | The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. | | |
| CVSSv3  Criteria | N/a | | |
| System | 10.10.11.143 | | |
| Risk | The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks and weakens cookie-hijacking protections. | | |
| Proof-of-Concept | N/a | | |
| Part played  towards Flag | N/a | | |
| Recommendation | Configure the remote web server to use HSTS ("Strict-Transport-Security" header). | | |
| References | [OWASP TOP 10 A02 2021 – Cryptographic Failures](https://owasp.org/Top10/A02_2021-Cryptographic_Failures/)  [OWASP Web Security Testing Guide: Testing for Weak SSL TLS Ciphers Insufficient Transport Layer Protection](https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/01-Testing_for_Weak_SSL_TLS_Ciphers_Insufficient_Transport_Layer_Protection) | | |

HTTP Cookies Web Application Cookies Not Marked HttpOnly

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Informational | **CVSSv3 Classification** | - |
| Description | The HttpOnly flag is a security mechanism to protect against cross-site scripting attack. | | |
| CVSSv3  Criteria | N/a | | |
| System | 10.10.11.143 | | |
| Risk | HTTP session cookies might be vulnerable to cross-site scripting attacks. A malicious client-side script, such as JavaScript, could read a user’s cookies. | | |
| Proof-of-Concept | N/a | | |
| Part played  towards Flag | N/a | | |
| Recommendation | BT should review each cookie to determine if it contains sensitive data or is relied upon for a security decision. If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data. | | |
| References | [CWE:1004](https://cwe.mitre.org/data/definitions/1004.html)  [OWASP HTTPOnly](https://owasp.org/www-community/HttpOnly)  [OWASP Web Security Testing Guide: Testing for Weak SSL TLS Ciphers Insufficient Transport Layer Protection](https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/01-Testing_for_Weak_SSL_TLS_Ciphers_Insufficient_Transport_Layer_Protection) | | |

HTTP Cookies Web Application Cookies Not Marked Secure

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Informational | **CVSSv3 Classification** | - |
| Description | The Secure flag is a security mechanism to prevent the transmission of a cookie over an unencrypted channel. | | |
| CVSSv3  Criteria | N/a | | |
| System | 10.10.11.143 | | |
| Risk | HTTP session cookies are transmitted in cleartext which would let a remote attacker intercept them. | | |
| Proof-of-Concept | N/a | | |
| Part played  towards Flag | N/a | | |
| Recommendation | BT should review each cookie to determine if it contains sensitive data or is relied upon for a security decision. If possible, add the ‘Secure’ attribute to all session cookies and any cookies containing sensitive data. | | |
| References | [OWASP Secure Cookie Attribute](https://owasp.org/www-community/controls/SecureCookieAttribute)  [OWASP Web Security Testing Guide: Testing for Weak SSL TLS Ciphers Insufficient Transport Layer Protection](https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/09-Testing_for_Weak_Cryptography/01-Testing_for_Weak_SSL_TLS_Ciphers_Insufficient_Transport_Layer_Protection) | | |

WordPress Detection

|  |  |  |  |
| --- | --- | --- | --- |
| Severity | Informational | **CVSSv3 Classification** | - |
| Description | The remote web server contains a blog application written in PHP. | | |
| CVSSv3  Criteria | N/a | | |
| System | 10.10.11.143 | | |
| Risk | The remote host is running WordPress, a free blog application written in PHP with a MySQL back-end. | | |
| Proof-of-Concept | XPTO was able to retrieve the technology and version used by the web application by HTML code inspection. | | |
| Part played  towards Flag | XPTO was able to later find a vulnerability through this information. | | |
| Recommendation | Installing the “WP-Hardening” plugin allows to easily hide the WordPress version in use. Alternatively, BT may also perform this step manually using “secure by obscure” mechanisms to mitigate the vulnerability. | | |
| References | N/a | | |

Additional Reports and Scans (Informational)

XPTO provides all clients with all report information gathered during testing. This includes vulnerability scans and a detailed findings spreadsheet. For more information, please see the following documents:

**Vulnerability Scans:**

* Blunder\_Tiffin\_001\_Full\_Findings.xslx
* Blunder\_Tiffin\_001\_Vulnerability\_Scan\_Summary.pdf
* Blunder\_Tiffin\_001\_Vulnerability\_Scan\_By\_Host.pdf

**Enumeration of Services and Open ports:**

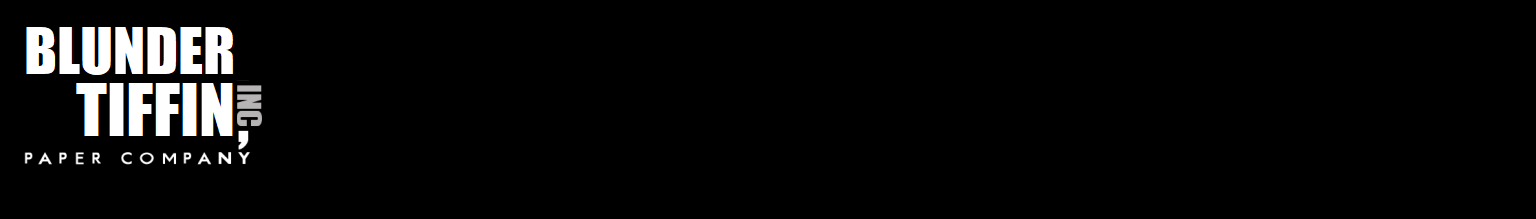
* initial\_paper\_scan.nmap
* full\_paper\_tcp\_scan.nmap
* scripted\_scan.nmap
* paper\_nmap\_http\_enum.nmap

**File Directory Enumeration:**

* gobuster\_enum\_office.txt

**Scripts for Privilege Escalation:**

* LinEnum.sh
* Linpeas.sh
* file.sh



Last Page