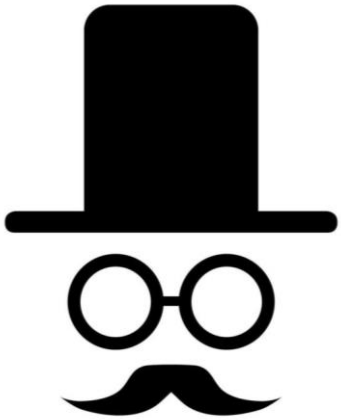


Futura Business Informatique
Security Assessment Findings Report

Business Confidential

Date: September 29th, 2023
Project: 001-01
Version 1.0

Contents

Confidentiality Statement

This document is the exclusive property of Futura Business Informatique (FBI) and Blackhat Security (BS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both FBI and BS.

BS 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. BS prioritized the assessment to identify the weakest security controls an attacker would exploit. BS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

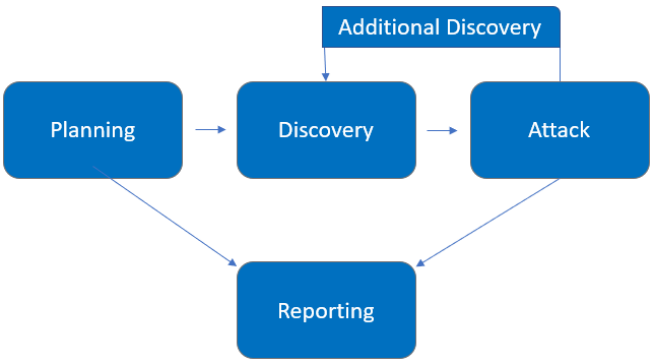
Name	Title	Contact Information
Demo Company		
Rodrigue Masson	IT Administrator	Office: (555) 555-5555 Email: rmasson@futuraBI.fr
TCM Security		
Ulrik Holtan	Lead Penetration Tester	Office: (555) 555-5555 Email: ulho001@student.kristiania.no

Assessment Overview

From November 14th, 2023, to November 29th, 2023, FBI engaged BS to evaluate the security posture of its infrastructure compared to current industry best practices that included a white box 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), and customized testing frameworks*.

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.



Assessment Components

White Box Penetration Test

A white box penetration test provides the tester full access and complete knowledge of the target that is being tested and its features. In this test the tester is given full access to the web server and its login credentials.

Finding Severity Ratings

The following table defines levels of severity.

Severity	Definition
Critical	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	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	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	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	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

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

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.

Scope

Assessment	Details
External Penetration Test	192.168.44.136 *Dates: 18-20.09.23, 22.09.23, 25 -28.09.23*

Client Allowances

FBI was provided with the following users/accounts during testing:

- Server User/PW: osboxes/osboxes.org

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

White Box Penetration Test Findings

1	3	4	3	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
White Box Penetration Test		
WBPT-001: Cross Site Scripting (XSS)	Critical	Follow the OWASP XSS (Cross Site Scripting) Prevention Cheat Sheet.
WBPT-002: Data sent over unencrypted HTTP	High	Make sure data is encrypted
WBPT -003: admin/admin.php visible to web.	High	Hide site from public
WBPT -004: Insufficient Password Complexity	High	Implement CIS Benchmark Password requirements / PAM solution.
WBPT -005: No brute-force protection on login	High	Restrict users to x-amount of tries before needing to contact administrator.
WBPT -006: Content Security Policy (CSP) Header Not Set	Moderate	Ensure that your web server is configured to set the Content-Security-Policy header.
WBPT -007: Anti-clickjacking X-Content-Type-Options header is not present	Moderate	See: Mozilla X-Frame options
WBPT -008: Absence of Anti-CSRF Tokens	Moderate	See: OWASP Absence of Anti-CSRF Tokens
WBPT -009: Apache/2.4.38 is out of date	Low	Update Apache server. Latest is at least 2.4.54.
WBPT -010: Cookie without SameSite attribute	Low	Ensure that SameSite attribute is set to 'lax' or ideally 'strict' for all cookies.
WBPT -011: Cookie PHPSESSID created without the httponly flag	Low	See: Using HTTP cookies
WNPT -012: Apache default file found	Informational	Restrict access to the Apache default files.

Technical Findings

White Box Test Findings

Finding WBPT-001: Cross Site Scripting (XSS) – (Critical)

Description:	Futura Business Informatique does not sanitize their input fields in their registration field, making the website susceptible for injection with malicious scripts.
Risk:	Likelihood: High - Impact: High
System:	All
Tools Used:	Manual Review
References:	OWASP Cross-Site Scripting OWASP XSS (Cross Site Scripting) Prevention Cheat Sheet

Evidence

Figure 1: Input payload in the "Create an account" input fields

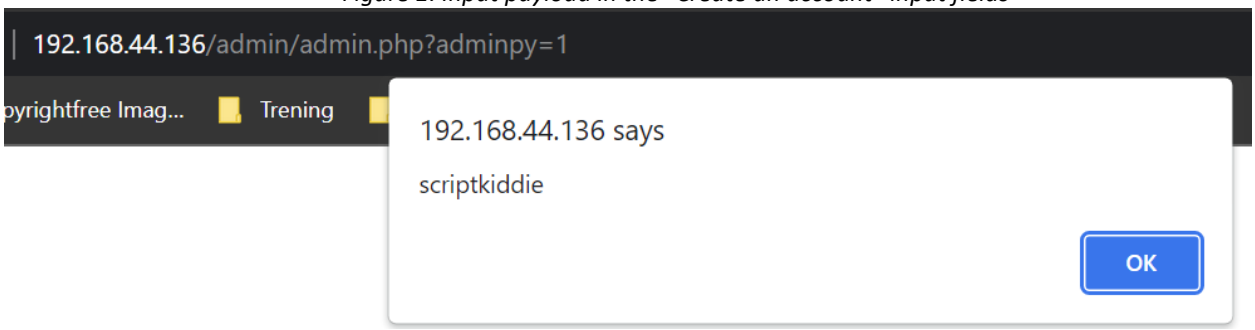


Figure 2: admin/admin.php executes the script once website loads

Remediation

Follow the XSS (Cross Site Scripting) Prevention Cheat Sheet to update the website security.

Finding WBPT-002: Data sent over unencrypted HTTP (High)

Description:	The web-application sends data over unencrypted HTTP on port 80.
Risk:	Likelihood: Medium – Anyone with access to the network, be it other employees, visitors, contractors or unauthorized personnel will be able to listen in on the traffic. Impact: High – If capturing the traffic, one may gain access to login credentials.
System:	All
Tools Used:	NMAP, Nikto, WireShark
References:	

Evidence

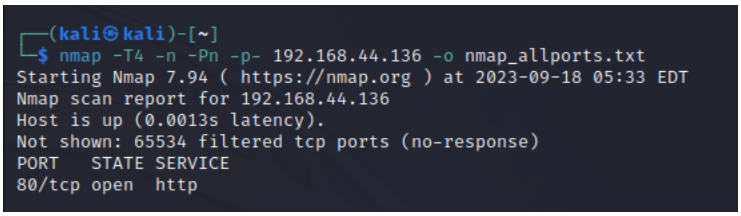


Figure 1: Nmap showing port 80/tcp as open

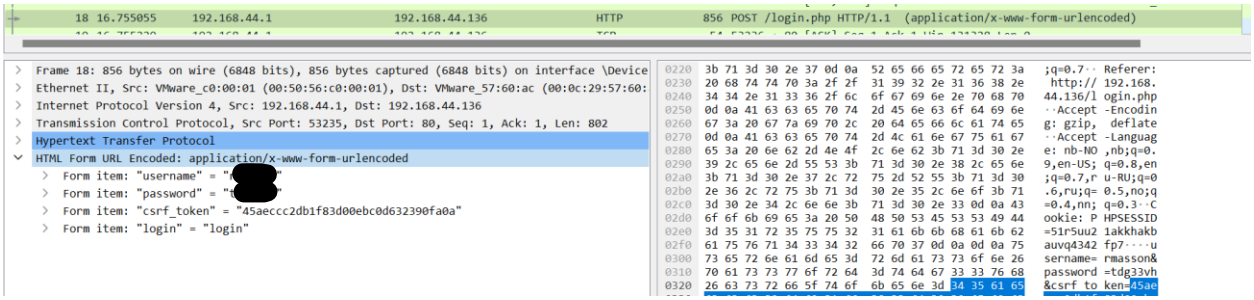


Figure 2: Captured package in Wireshark showing "username" and "password" in cleartext

Remediation

Make sure password and username is encrypted.

Finding WBPT-003: www.futuraBI.fr/admin/admin.php visible to web (High)

Description:	/admin/admin.php and /robots.txt are visible to the web.
Risk:	Likelihood: High – Any simple scan shows the directory open to the web Impact: Medium – The folder shows all user information including full name, username, email account and the user's role in the company. This is valuable information for both brute-forcing an account or spear-phishing.
System:	All
Tools Used:	OWASP Zap Spider, Nmap, Nikto
References:	

Evidence

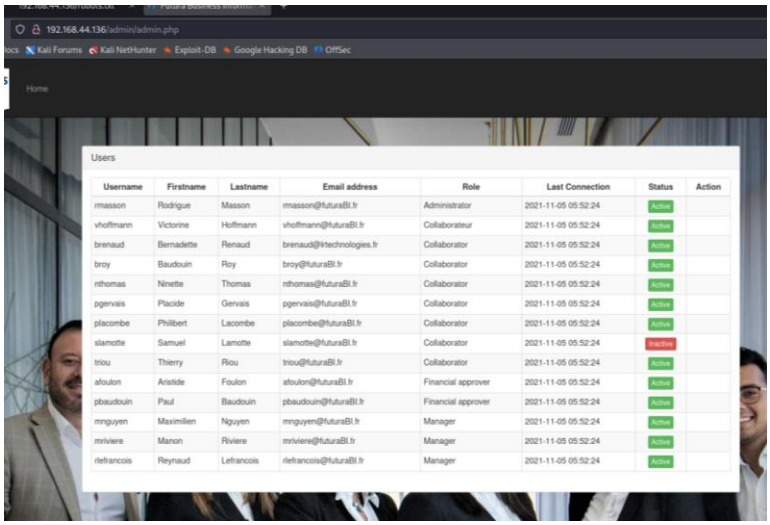


Figure 1: The /admin/admin.php website listing all user information

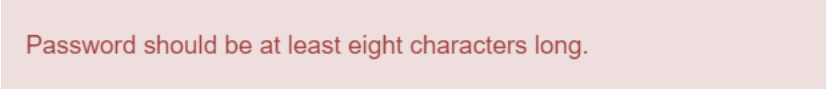
Remediation

Hide directory from anyone without administrator privileges.

Finding WBPT-004: Insufficient Password Complexity (High)

Description:	Users are only required to have an 8-character long password, with no requirements of unique characters, upper or lowercase or numbers.
Risk:	Likelihood: Medium – A sub-optimal password requirement allows for easier brute-forcing of passwords. Impact: High – If an account is compromised as a result of a weak password, unauthorized parties may gain access to company data, or in worse scenarios administrator accounts.
System:	All
Tools Used:	Manual Review
References:	CIS Benchmark Password requirements PAM solution

Evidence



Remediation

Implement CIS Benchmark Password requirements / PAM solution

Finding WBPT-005: No brute-force protection on login (High)

Description:	There are no safety measures in place to prohibit repeat testing of passwords or brute forcing.
Risk:	Likelihood: High – With usernames available online, weak password requirements and no brute-force protection the likelihood that someone wanting to gain access to the system will use brute-force is high. Impact: High – By gaining access to the different users, company data or admin rights may be vulnerable.
System:	All
Tools Used:	OWASP Zap Fuzzer, Manual Review
References:	

Remediation

Limit login attempts per account, to make the user contact the administrator for a reset or other measure.

WBPT-006: Content Security Policy (CSP) Header Not Set (Medium).
See: https://www.zaproxy.org/docs/alerts/10038-1/

WBPT -007: Anti-clickjacking X-Content-Type-Options header is not present (Medium)
See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

WBPT -008: Absence of Anti-CSRF Tokens (Low)
See: https://www.zaproxy.org/docs/alerts/10202/

WBPT -009: Apache/2.4.38 is out of date (Low)
Apache server is out of date, version 2.4.57 is available. Please update to increase security.

WBPT -010: Cookie without SameSite attribute (Low)
See: https://www.zaproxy.org/docs/alerts/10054/

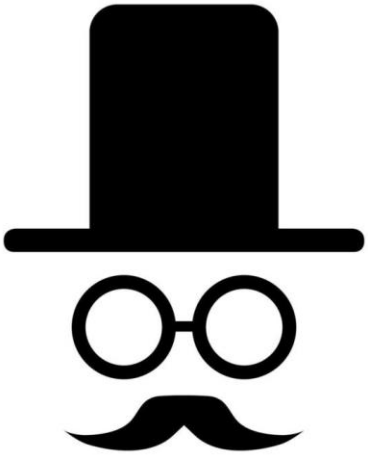
WBPT -011: Cookie PHPSESSID created without the httponly flag (Low)
See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

WNPT -012: Apache default file found (Informational)
Whilst there are no known security risks associated with these files, it is still considered a security risk to have this file viewable on a website.
See: https://vntweb.co.uk/apache-restricting-access-to-iconsreadme/

Additional Reports and Scans (Informational)

BS 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:

- **FBI-001-01 Web App Testing.pdf**
- **FBI-001-01 Network Scan.pdf**



Last Page