**SafeBank**

**Penetration Test Report**

**Nov 2023**

**Purpose & Scope**

The Securify team was engaged to gain an understanding of the Safe Bank external facing website to establish the effectiveness of Cyber Essentials against this asset.

The scope of this test was defined as:

* IP address 10.0.0.3
* All associated ports and their services
* Intrusion and exploration of the internal network if possible.

**Executive Summary**

During the investigation of the Safe Bank external facing website, several misconfigurations were found that allowed for gaining an understanding of the backend services running the website.

Though we were unable to reach the internal network, the lack of effective controls around the “Upload CV” functionality did allow our team to upload malicious documents which could’ve been executed by a member of banking team.

This report will outline the key findings.

**Test Findings**

***Critical: Weak protection against malicious documents being uploaded.***

* CVSS potential: 9.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)
* Endpoint affected: <https://10.0.0.3/upload-file/>

The CVSS potential of 9.6 has been given as it was possible to upload malicious Word documents via the upload CV function that would’ve been likely opened by staff on the Internal network.

Though there were some controls that did stop some of our uploads, this was minimal and common tooling such as msfvenom was able to bypass this easily. There was no callback during our limited testing window (out of business hours), but we are confident that internal controls would likely not have stopped us succeeding in a sustained attack.

***High: Sensitive Information Disclosure: CVs***

* CVSS potential: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
* Endpoint affected: <https://10.0.0.3/wp-content/uploads>
* Evidence:

***A screenshot of a computer

Description automatically generated***

Due to a misconfiguration on the website, uploaded CVs are listed in the given directory. This leads to disclosure of uploaded CVs which can contain addresses, email addresses, as well as full names.

***High: Sensitive Information Disclosure: PHPInfo***

* CVSS potential: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
* Endpoint affected: <http://10.0.0.3/dashboard/phpinfo.php>
* Evidence:

A screenshot of a computer

Description automatically generated

Due to a misconfiguration of the website, port 80 is open and accessible. This led to the discovery of *XAMPP* which by default comes with the endpoints *phpinfo.php* which provided a summary of PHP services as well as the webserver services. From this it could be determined the web server was running as administrator as well as key information on the underlying operating system which would help further an attack.

***Medium: Exposed MSRPC, SMB, WSMAN & MySQL ports***

* CVSS potential: 6.5 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)
* Affected: 10.0.0.3

Though we were unable to bruteforce any credentials during testing, but it only takes a single bad password to allow for this to happen. Ports like MySQL,WSMAN,MSPRC and SMB are a common attack vector and it not a good practice to have these publicly facing on the Internet.

***Medium: SSL misconfiguration & exposed port 80***

* CVSS potential: 4.8 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)
* Affected endpoints: <http://10.0.0.3> & <https://10.0.0.3>
* Evidence:



SSL has been misconfigured on this website leading to warning when visiting by name, and port 80 is accessible to the world.

In both cases these can be further attacked in a mitm attack, though the CVSS has been given as 4.3, this is because there is no login for clients. If this had client login and e-banking functionality, this would be a much more severe finding.

**Recommendations**

We recommend enforcing anti-virus/malware scanning for any uploaded documents through the Upload CV functionality, and a full and through audit of the webserver its configurations to ensure the following of best practices.

We also recommending reducing the attack surface by removing all ports other than the webserver unless absolutely necessary. We would also recommend the implementation of a WAF and/or IPS to stop the possible scanning from common tools.

**Appendix**

***wpscan***

[i] Updating the Database ...

[i] Update completed.

[+] URL: <https://10.0.0.3/> [10.0.0.3]

[+] Started: Fri Nov 17 08:01:05 2023

Interesting Finding(s):

[+] Headers

| Interesting Entries:

| - Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6

| - X-Powered-By: PHP/8.1.6

| Found By: Headers (Passive Detection)

| Confidence: 100%

[+] robots.txt found: <https://10.0.0.3/robots.txt>

| Interesting Entries:

| - /wp-admin/

| - /wp-admin/admin-ajax.php

| Found By: Robots Txt (Aggressive Detection)

| Confidence: 100%

[+] XML-RPC seems to be enabled: <https://10.0.0.3/xmlrpc.php>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

| References:

| - <http://codex.wordpress.org/XML-RPC_Pingback_API>

| - <https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/>

| - <https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/>

| - <https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/>

| - <https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/>

[+] WordPress readme found: <https://10.0.0.3/readme.html>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] Upload directory has listing enabled: <https://10.0.0.3/wp-content/uploads/>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] The external WP-Cron seems to be enabled: <https://10.0.0.3/wp-cron.php>

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - <https://www.iplocation.net/defend-wordpress-from-ddos>

| - <https://github.com/wpscanteam/wpscan/issues/1299>

[+] WordPress version 6.4.1 identified (Latest, released on 2023-11-09).

| Found By: Rss Generator (Passive Detection)

| - <https://10.0.0.3/feed/,> <generator><https://wordpress.org/?v=6.4.1></generator>

| - <https://10.0.0.3/comments/feed/,> <generator><https://wordpress.org/?v=6.4.1></generator>

[+] WordPress theme in use: twentytwentyone

| Location: <https://10.0.0.3/wp-content/themes/twentytwentyone/>

| Latest Version: 2.0 (up to date)

| Last Updated: 2023-11-07T00:00:00.000Z

| Readme: <https://10.0.0.3/wp-content/themes/twentytwentyone/readme.txt>

| Style URL: <https://10.0.0.3/wp-content/themes/twentytwentyone/style.css?ver=2.0>

| Style Name: Twenty Twenty-One

| Style URI: <https://wordpress.org/themes/twentytwentyone/>

| Description: Twenty Twenty-One is a blank canvas for your ideas and it makes the block editor your best brush. Wi...

| Author: the WordPress team

| Author URI: <https://wordpress.org/>

|

| Found By: Css Style In Homepage (Passive Detection)

| Confirmed By: Css Style In 404 Page (Passive Detection)

|

| Version: 2.0 (80% confidence)

| Found By: Style (Passive Detection)

| - <https://10.0.0.3/wp-content/themes/twentytwentyone/style.css?ver=2.0,> Match: 'Version: 2.0'

[+] Enumerating All Plugins (via Passive Methods)

[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] contact-form-7

| Location: <https://10.0.0.3/wp-content/plugins/contact-form-7/>

| Latest Version: 5.8.3 (up to date)

| Last Updated: 2023-11-16T02:59:00.000Z

|

| Found By: Urls In Homepage (Passive Detection)

| Confirmed By: Urls In 404 Page (Passive Detection)

|

| Version: 5.8.3 (90% confidence)

| Found By: Query Parameter (Passive Detection)

| - <https://10.0.0.3/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.8.3>

| Confirmed By: Readme - Stable Tag (Aggressive Detection)

| - <https://10.0.0.3/wp-content/plugins/contact-form-7/readme.txt>

[+] wp-file-upload

| Location: <https://10.0.0.3/wp-content/plugins/wp-file-upload/>

| Latest Version: 4.24.1 (up to date)

| Last Updated: 2023-11-09T14:14:00.000Z

|

| Found By: Urls In Homepage (Passive Detection)

| Confirmed By: Urls In 404 Page (Passive Detection)

|

| Version: 4.24.1 (50% confidence)

| Found By: Readme - ChangeLog Section (Aggressive Detection)

| - <https://10.0.0.3/wp-content/plugins/wp-file-upload/readme.txt>

[+] Enumerating Config Backups (via Passive and Aggressive Methods)

Checking Config Backups - Time: 00:00:14 <================================================================================================================

[i] No Config Backups Found.

[+] WPScan DB API OK

| Plan: free

| Requests Done (during the scan): 1

| Requests Remaining: 21

[+] Finished: Fri Nov 17 08:01:23 2023

[+] Requests Done: 152

[+] Cached Requests: 45

[+] Data Sent: 47.904 KB

[+] Data Received: 17.307 MB

[+] Memory used: 249.055 MB

[+] Elapsed time: 00:00:17

*Nikto*

└─$ nikto -h <http://10.0.0.3>

* Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 10.0.0.3

+ Target Hostname: 10.0.0.3

+ Target Port: 80

+ Start Time: 2023-11-17 08:39:46 (GMT0)

---------------------------------------------------------------------------

+ Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6

+ Retrieved x-powered-by header: PHP/8.1.6

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Root page / redirects to: <http://10.0.0.3/dashboard/>

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ OSVDB-3268: /img/: Directory indexing found.

+ OSVDB-3092: /img/: This might be interesting...

+ OSVDB-3268: /icons/: Directory indexing found.

+ OSVDB-3233: /icons/README: Apache default file found.

+ 8698 requests: 0 error(s) and 9 item(s) reported on remote host

+ End Time: 2023-11-17 08:40:58 (GMT0) (72 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Portions of the server's headers (Apache/2.4.53 PHP/8.1.6) are not in

the Nikto 2.1.6 database or are newer than the known string. Would you like

to submit this information (\*no server specific data\*) to CIRT.net

for a Nikto update (or you may email to sullo@cirt.net) (y/n)?

**https:**

─$ nikto -h <https://10.0.0.3>

* Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 10.0.0.3

+ Target Hostname: 10.0.0.3

+ Target Port: 443

---------------------------------------------------------------------------

+ SSL Info: Subject: /CN=localhost

Ciphers: TLS\_AES\_256\_GCM\_SHA384

Issuer: /CN=localhost

+ Start Time: 2023-11-17 08:45:08 (GMT0)

---------------------------------------------------------------------------

+ Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.1.6

+ Cookie wp\_wpfileupload\_cbc6ae40dcd77c4ef405e17ea2767821 created without the secure flag

+ Cookie wp\_wpfileupload\_cbc6ae40dcd77c4ef405e17ea2767821 created without the httponly flag

+ Retrieved x-powered-by header: PHP/8.1.6

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ Uncommon header 'link' found, with multiple values: (<<https://10.0.0.3/wp-json/>>; rel="<https://api.w.org/>",<<https://10.0.0.3/wp-json/wp/v2/pages/7>>; rel="alternate"; type="application/json",<<https://10.0.0.3/>>; rel=shortlink,)

+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.

+ The site uses SSL and Expect-CT header is not present.

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Uncommon header 'x-redirect-by' found, with contents: WordPress

+ Entry '/wp-admin/' in robots.txt returned a non-forbidden or redirect HTTP code (302)

+ "robots.txt" contains 2 entries which should be manually viewed.

+ Hostname '10.0.0.3' does not match certificate's names: localhost

+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ OSVDB-3268: /icons/: Directory indexing found.

+ OSVDB-3092: /LICENSE.txt: License file found may identify site software.

+ OSVDB-3233: /icons/README: Apache default file found.

+ /wp-links-opml.php: This WordPress script reveals the installed version.

+ OSVDB-3092: /license.txt: License file found may identify site software.

+ OSVDB-3092: /LICENSE.TXT: License file found may identify site software.

+ /wp-app.log: Wordpress' wp-app.log may leak application/system details.

+ /wordpresswp-app.log: Wordpress' wp-app.log may leak application/system details.

+ /: A Wordpress installation was found.

+ /wordpress: A Wordpress installation was found.

+ Cookie wordpress\_test\_cookie created without the httponly flag

+ OSVDB-3268: /wp-content/uploads/: Directory indexing found.

+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information

+ /wp-login.php: Wordpress login found

+ /.well-known/assetlinks.json: Google Asset Links Specification file may contain server info, per RFC-5785. See <https://github.com/google/digitalassetlinks/blob/master/well-known/details.md>

+ 8705 requests: 0 error(s) and 30 item(s) reported on remote host

+ End Time: 2023-11-17 10:00:22 (GMT0) (4514 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested

***Nmap:***

└─$ nmap -p- 10.0.0.3

Starting Nmap 7.92 ( <https://nmap.org> ) at 2023-11-17 08:02 GMT

Illegal character(s) in hostname -- replacing with '\*'

Illegal character(s) in hostname -- replacing with '\*'

Nmap scan report for http:\*\*[www.safebank.com](http://www.safebank.com) (10.0.0.3)

Host is up (0.0011s latency).

Not shown: 65521 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http --> XAMPP

135/tcp open msrpc

139/tcp open netbios-ssn

443/tcp open https

445/tcp open microsoft-ds

3306/tcp open mysql

5985/tcp open wsman

47001/tcp open winrm

49664/tcp open unknown

49665/tcp open unknown

49666/tcp open unknown

49667/tcp open unknown

49668/tcp open unknown

49671/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 104.47 seconds