**Introduction:**

***SafeBank - Security evaluation***

Scope was to evaluate the fictional entity, Safe Bank, for vulnerable threat vectors as well as any wider security concerns; largely this was centred around the external website, the initial evaluation of which, forms the extent of this report.

Efforts were largely focused on the IP 10.0.0.3 and the services / configuration which resigned there.

The intention/scope would have extended beyond this had exploitations of the preliminary issues been successful. Further exploration of the network/systems beyond was considered a stretch objective for this evaluation.

**Findings:**

Rudimentary website was identified.

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

*Host is up (0.00080s latency).*

*Not shown: 994 filtered tcp ports (no-response)*

***PORT STATE SERVICE VERSION***

***80/tcp open http Apache httpd 2.4.53 ((Win64) OpenSSL/1.1.1n PHP/8.1.6)***

***135/tcp open msrpc Microsoft Windows RPC***

***139/tcp open netbios-ssn Microsoft Windows netbios-ssn***

***443/tcp open ssl/http Apache httpd 2.4.53 ((Win64) OpenSSL/1.1.1n PHP/8.1.6)***

***445/tcp open microsoft-ds?***

***3306/tcp open mysql MariaDB (unauthorized)***

*Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows*

A screenshot of a computer

Description automatically generated

***whatweb*** provided some basic information:

*└─$ whatweb https://10.0.0.3/*

*https://10.0.0.3/ [200 OK]* ***Apache[2.4.53]****,* ***Cookies[wp\_wpfileupload\_cbc6ae40dcd77c4ef405e17ea2767821]****, Country[RESERVED][ZZ], HTML5, HTTPServer[Apache/2.4.53 (Win64)* ***OpenSSL/1.1.1n PHP/8.1.6]****, IP[10.0.0.3], JQuery[3.7.1], MetaGenerator[****WordPress 6.4.3****], OpenSSL[1.1.1n], PHP[8.1.6], PoweredBy[--], Script, Title[SafeBank], UncommonHeaders[link], WordPress[6.4.3], X-Powered-By[PHP/8.1.6]*

Probed the main WordPress website at https://10.0.0.3/ in more depth using ***nikto***. Some interesting results from some basic commands/probing. Highlighted output indicative of further areas to investigate.

*nikto -h https://10.0.0.3/ -o scan.txt*

*- 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: 2024-02-18 18:49:33 (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*

*Note: Loading http://10.0.0.3/ (not https) via a web browser takes you straight to the default installation page for XAMPP. Additional valuable information to be gleaned from this including but not limited to the Php.iIni file:*

A screenshot of a computer

Description automatically generated

In parallel also probed the web page at 10.0.0.3 initially using ***dirb*** *default directories*. Some interesting results and directory structures highlighted; directories indicative of further investigation required:

*└─$ dirb https://10.0.0.3/*

*WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt*

***==> DIRECTORY: https://10.0.0.3/contact/***

***==> DIRECTORY: https://10.0.0.3/Contact/***

*…*

***==> DIRECTORY: https://10.0.0.3/shell/***

*…*

***==> DIRECTORY: https://10.0.0.3/contact/0/***

*…*

***==> DIRECTORY: https://10.0.0.3/contact/embed/***

***==> DIRECTORY: https://10.0.0.3/contact/entries/***

***==> DIRECTORY: https://10.0.0.3/contact/feed/***

*…*

*Additional directories discovered such as:*

***==> https://10.0.0.3/upload-file/***

***==> https://10.0.0.3/wp-content/uploads/***

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screen shot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Note: File type uploads seemed enforced via a default setting. Opportunity for a more sophisticated attacker to construct a carefully crafted doc or pdf or other file format to exploit the feature and obtain further access.

Note: Cross site scripting seemed to be restricted within the comments form.

A screenshot of a computer

Description automatically generated

Note: attempts to brute force authentication the WordPress admin portal ([**https://10.0.0.3/wp-login.php**](https://10.0.0.3/wp-login.php)) were not successful. Burp suite and other Kalli linux standard offerings were tried. Simple brute force attempts were undertaken.

A screenshot of a computer

Description automatically generated

***3306/tcp open mysql MariaDB***

**Recommendations:**

**Make it relevant to Cyber Essentials?**

Description of each vulnerability or area of concern discovered.

Severity ratings for each vulnerability (e.g., low, medium, high).

Recommendations for remediation or mitigation.

Suspected weak configuration from almost default initial setup.

Specific actions to address the identified vulnerabilities.

Prioritisation based on risk level.

**+ 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.**

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

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

A screenshot of a computer

Description automatically generated

**Conclusion:**

Summary of key findings and recommendations.

Further security analysis required - high level shows issues so this is reason enough to suspect any underlying issues may present additional problem areas.

**Other/Appendices (Can be omitted):**

─$ sudo arp-scan --interface=eth0 --localnet

[sudo] password for kali:

Interface: eth0, type: EN10MB, MAC: 00:50:56:08:27:39, IPv4: 10.10.10.1

Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)

10.10.10.10 00:50:56:11:7d:d9 VMware, Inc.

10.10.10.200 00:50:56:27:24:8e VMware, Inc.

10.10.10.254 a0:b9:ed:ff:ff:0a Skytap

──(kali㉿host-1)-[~]

└─$ sudo nmap -sV -O -T4 10.10.10.10

Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-27 14:30 GMT

Nmap scan report for 10.10.10.10

Host is up (0.00029s latency).

Not shown: 997 closed tcp ports (reset)

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds?

MAC Address: 00:50:56:11:7D:D9 (VMware)

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:

OS:SCAN(V=7.92%E=4%D=1/27%OT=135%CT=1%CU=41786%PV=Y%DS=1%DC=D%G=Y%M=005056%

OS:TM=65B51383%P=x86\_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=10C%TI=I%CI=I%II=I

OS:%SS=S%TS=U)OPS(O1=M5B4NW8NNS%O2=M5B4NW8NNS%O3=M5B4NW8%O4=M5B4NW8NNS%O5=M

OS:5B4NW8NNS%O6=M5B4NNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70

OS:)ECN(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+

OS:%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T

OS:=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0

OS:%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S

OS:=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R

OS:=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N

OS:%T=80%CD=Z)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated