IT Blog

Vulnerability Assessment and Penetration Test

Findings Report

Date: Jun 22, 2021
Project: CL002

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

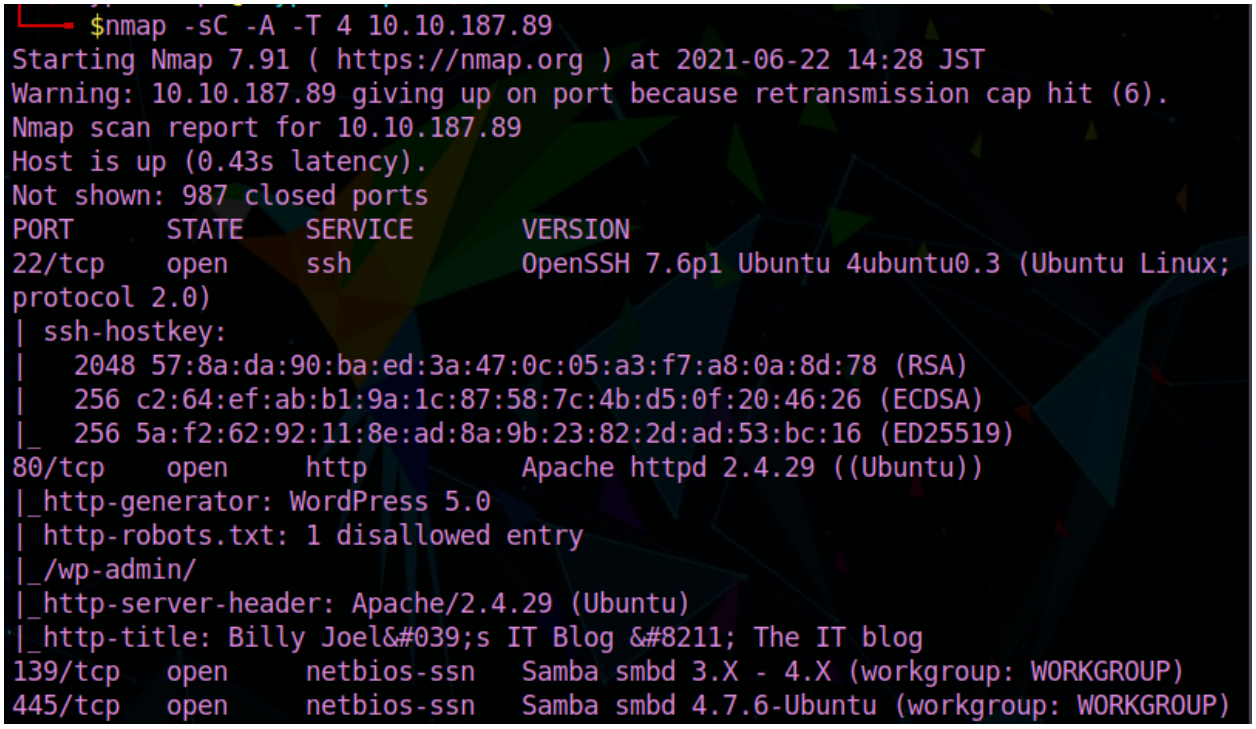

Figure 1: nmap scan

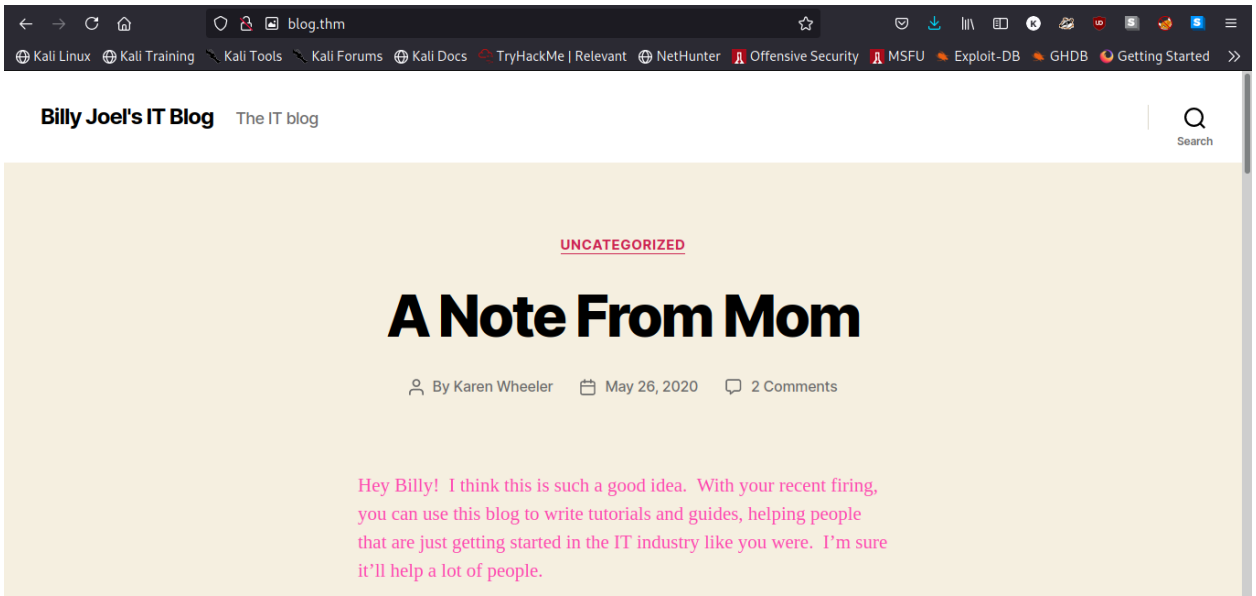

Figure 2: non secure web application's home page

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

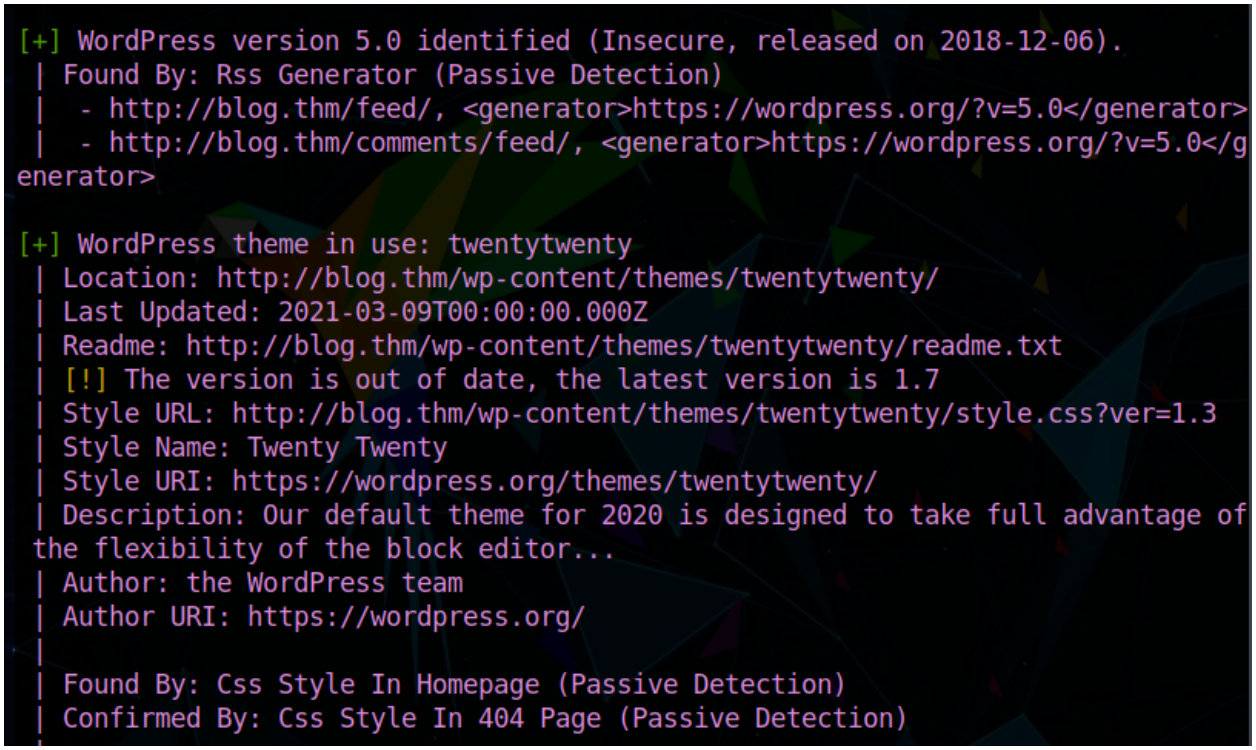

Figure 3: wpscan output

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

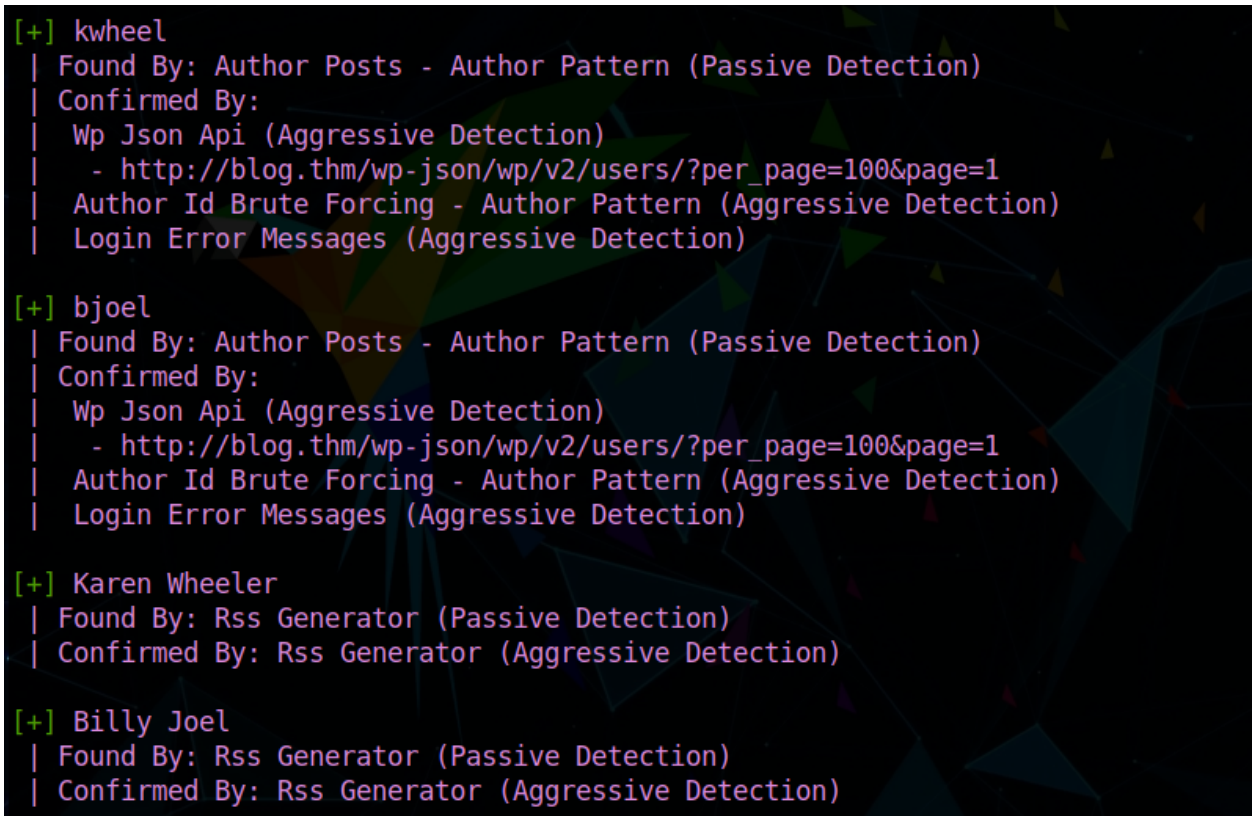

Figure 4: penetration tester identified users through wpscan

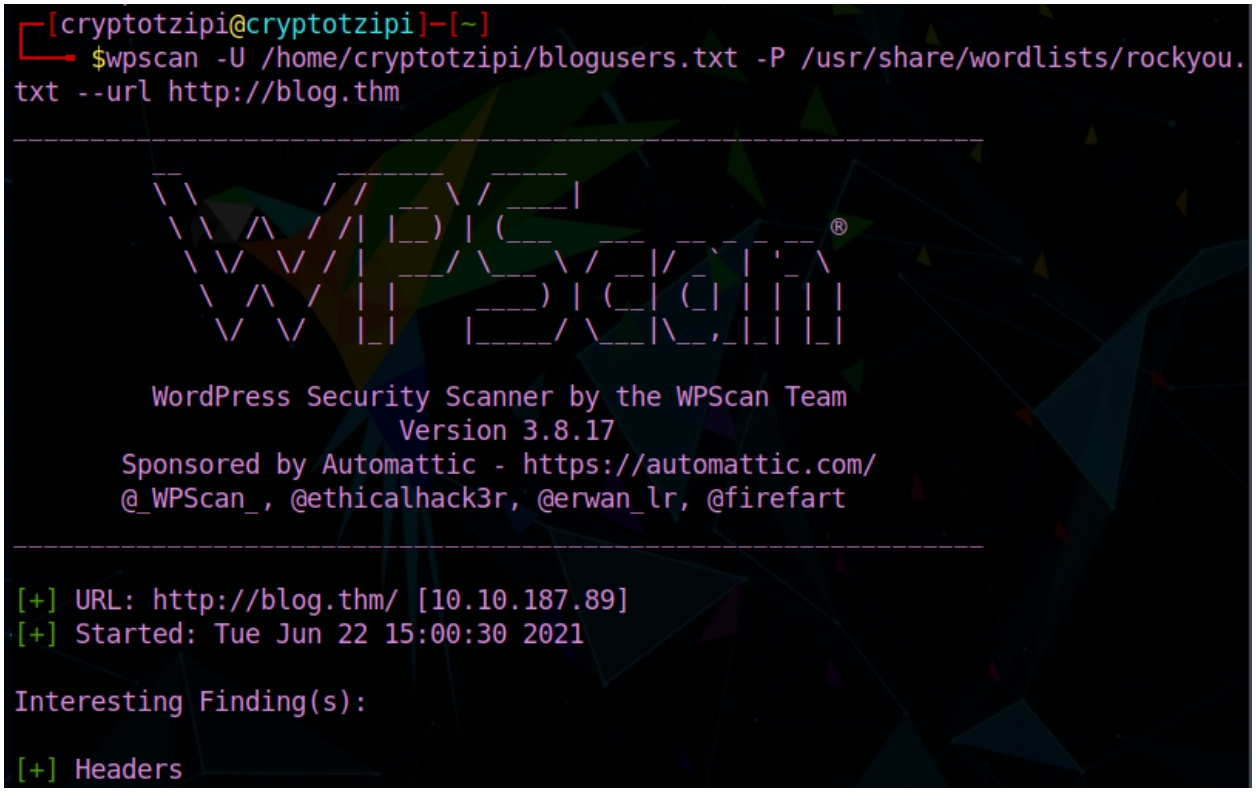

Figure 5: penetration tester used wpscan to find a complete set of credentials

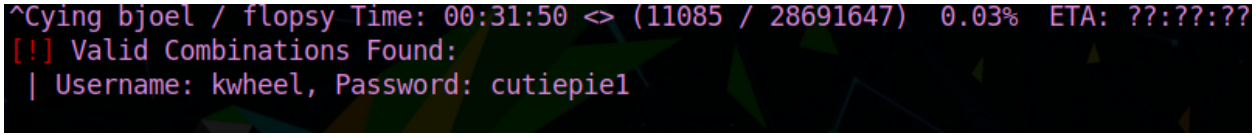

Figure 6: set of credentials found

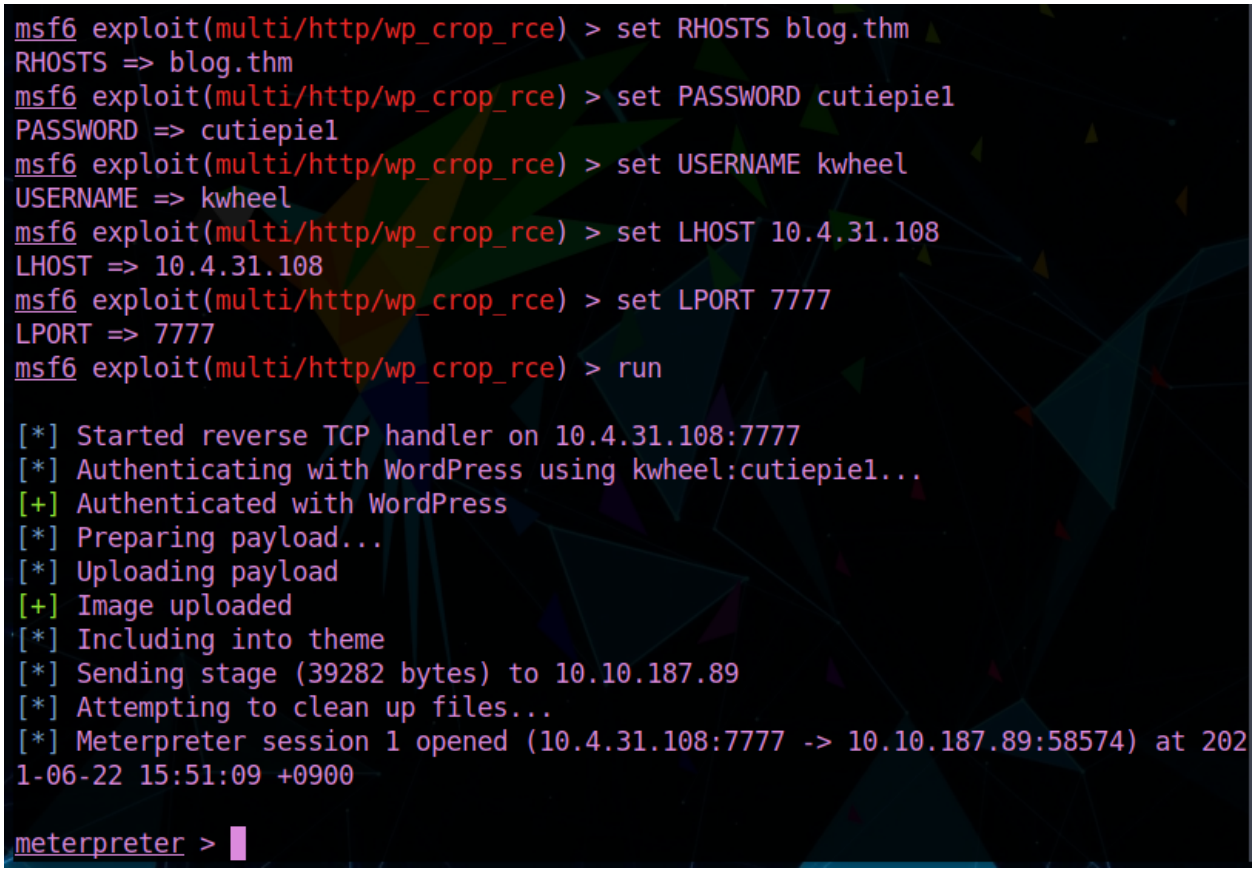

Figure 7: A meterpreter shell was obtained through metasploit using the credentials obtained previously

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

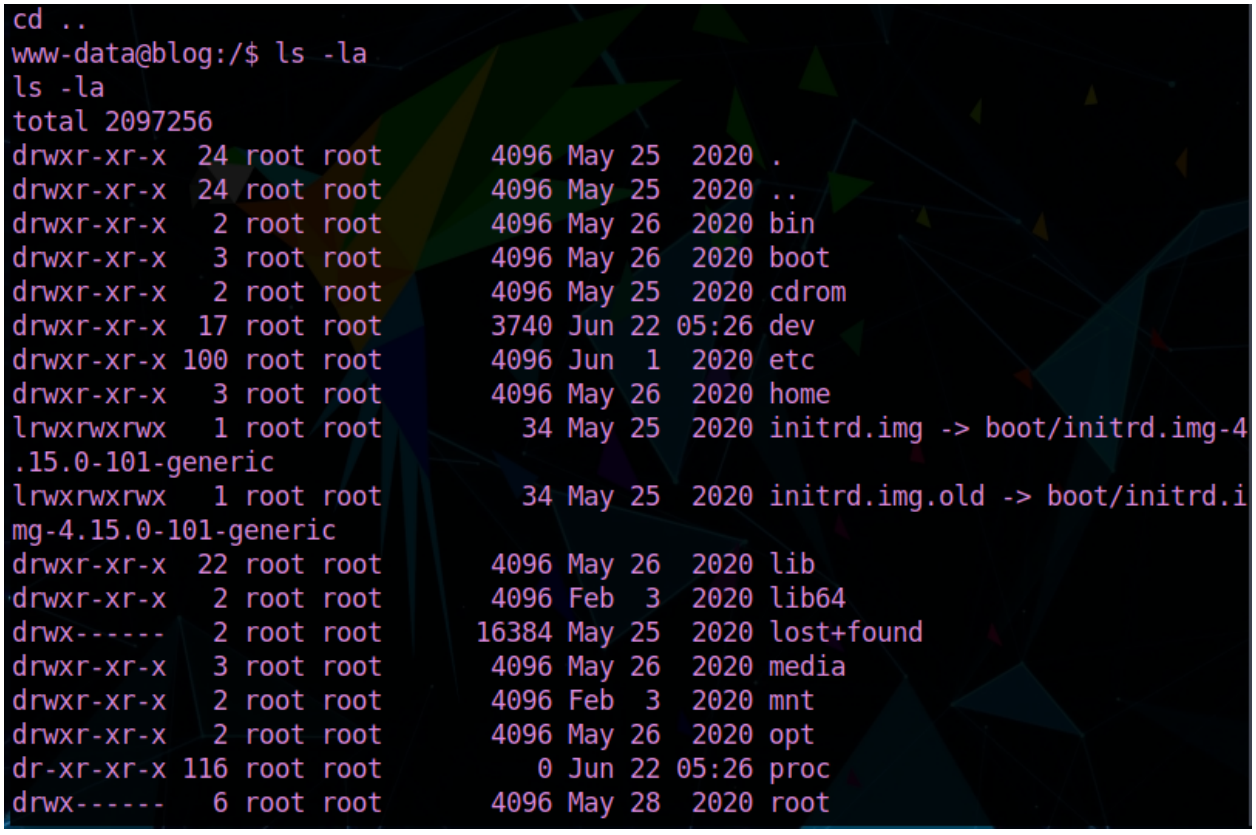

Figure 8: penetration tester performing manual enumeration

```
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.