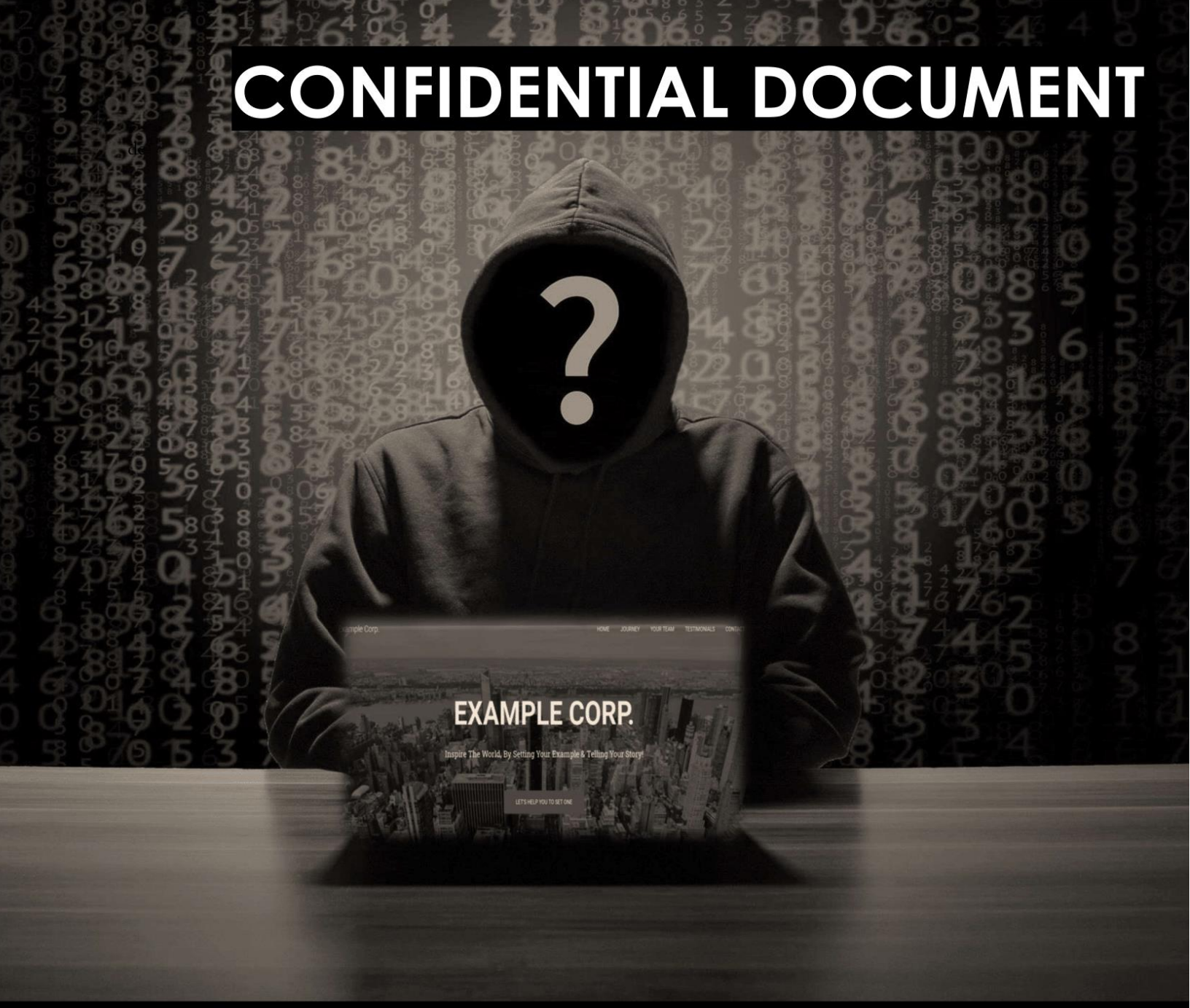
CONFIDENTIAL DOCUMENT



Network Vulnerability Assessment Report

Quarter 3, 2021

Document Control

Document Version	Owner & Role	Status & comments
v1.0	Andrew Pham – Security Analyst	Internal Draft {Restricted Scope)

Legal Disclaimer

The content of this report is highly confidential and may include critical information on Example Corp systems, network, and applications. The report should be shared only with intended parties.

Although maximum effort has been applied to make this report accurate, Example Corp, Security Audit Team cannot be held responsible for inaccuracies or system changes after the report has been issued since new vulnerabilities may be found once the tests are completed.

Guidance should be taken from a Legal Counsel, CISO and Blue Team on how best to implement the recommendations.

All other information and the formats, methods, and reporting approaches is the intellectual property of Example Corp and is considered proprietary information and is provided for the purpose of internal use only.

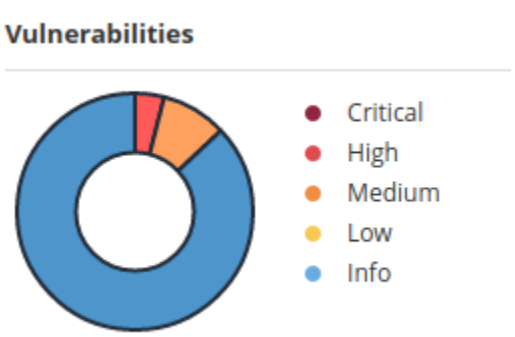
Any copying, distribution, or use of any of the information set forth herein or in any attachments hereto form outside of Example Corp authorized representatives is strictly prohibited.

Table of Contents

1. Executive Summary

An audit of Example Corp revealed no major vulnerabilities. The few vulnerability findings can be corrected with minor updates and only have minor confidentiality impacts.

2. A Glance Through Target Security Posture



Our Faraday automated scan revealed 1 high vulnerability and 2 medium level vulnerabilities. We imported these results into Nessus for tracking.

The high-level vulnerability appeared to allow for database admin control. Upon further investigation of the vulnerability, we believe it to be a false positive since we were unable to gain access to the control panel on the exploited URL.

The next two medium vulnerabilities exposed information on our server but provided no access to change that information. If those features are not actively needed for debugging, it's recommended to disable them.

An nMap test revealed an SSH and FTP server, attempting the developer credentials from the phishing was unsuccessful as well as default usernames and passwords. The nMap also revealed an us-srv server that has a known DDOS exploit via malformed request but we were unable to replicate the exploit.

OSINT revealed that the website is running on a stack with Ubuntu operating system, running an Apache webserver, with a WordPress content management system. OSINT revealed potential security vulnerabilities in file uploads, Apache webserver auth codes, and webserver firewalls.

In the phishing test we gained 10 sets of credentials from various employees.

Using the OSINT and phishing credentials together we find

1. the WordPress admin panel, the URL was unchanged from the default, none of the "phished" credentials worked on the panel.

2. the secure app login, phished credentials worked on the login here

From the secure app login, we find an unlisted contact us page on the site. OSINT clues us in to attempt single file upload, content type file upload, and double extension file upload. Using BurpSuite to intercept and modify requests, we attempt these exploits to upload a backdoor but it does not accept the files even with modified headers. Php files with modified extensions are uploaded suggesting that there is no check for image content such as using mime content type, php getimagesize, or the fileinfo extension.

It is possible to run .php.jpg files using AddType or AddHandler in .htaccess to run all .png as .php; however planting the .htaccess file does not seem possible.

We were unable to exploit the file upload system using double extension, content type, single file, or null byte and therefore could not create a backdoor by executing PHP code. This secure app should still be enclosed within the firewall to prevent possible exploitation from chaining other vulnerabilities.

Recommendations:

1. Disable HTTP Trace and mod_status
2. Change WordPress admin panel URL
3. Move /secureapp within the firewall
4. Add image content checking for file upload on secureapp's contact us form and ensure to prevent any code execution from the uploads folder

Overall Security Rating – Some Action Should Be Considered

3. Testing Methodology

1. Automated scans
2. Manual audit of found vulnerabilities
3. Research into existing proof of concept exploits for vulnerabilities found
4. Research OSINT and Phishing Data
5. Attempt to chain vulnerabilities

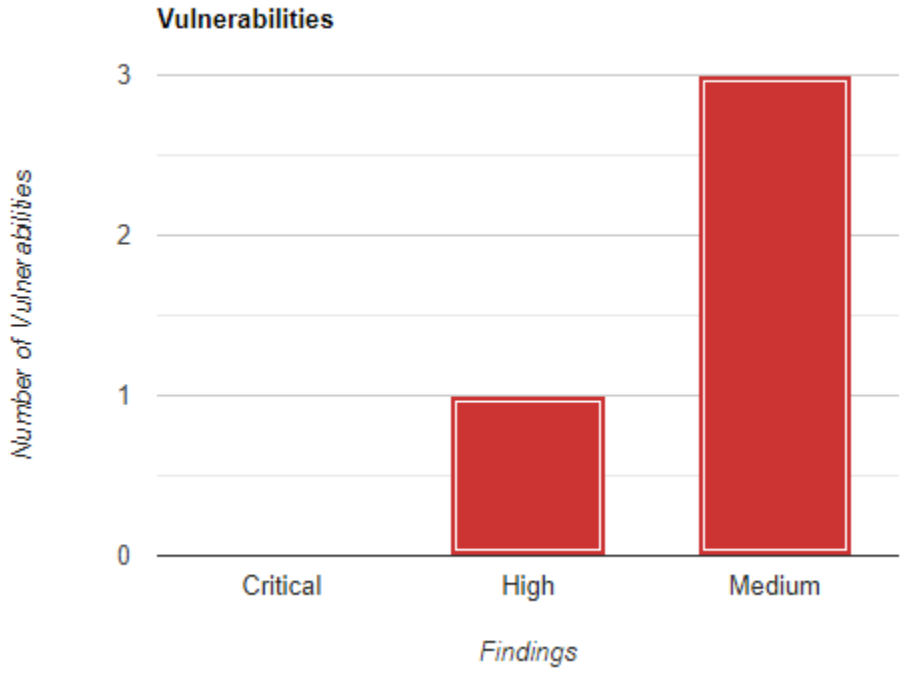
4. Tools & Websites Used

- Nessus
- Faraday
- Firefox
- Curl
- goPhish
- Nmap
- BurpSuite

Detailed Technical Reports (Scope Limited)

example.com

This host contains 1 high and 3 medium vulnerabilities.



Total Findings	Critical	High	Medium
3	0	1	3

Finding X: Apache CouchDB Unauthenticated Administrative Access on port 5984 TCP– High

Vulnerability Description:

Nessus was able to perform administrative actions on the remote CouchDB server without providing authentication. A remote attacker could exploit this to take control of the CouchDB server.

Risk Information:

CVSS Score Source: Tenable

CVSS v2 Calculations

Risk Factor: High

Base Score: 7.5

Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Exposure/Analysis:

Manual attempts at gaining access to “http://10.10.10.10:5984/_config” through the web browser failed. Vulnerability is unconfirmed, flagged as a false positive.

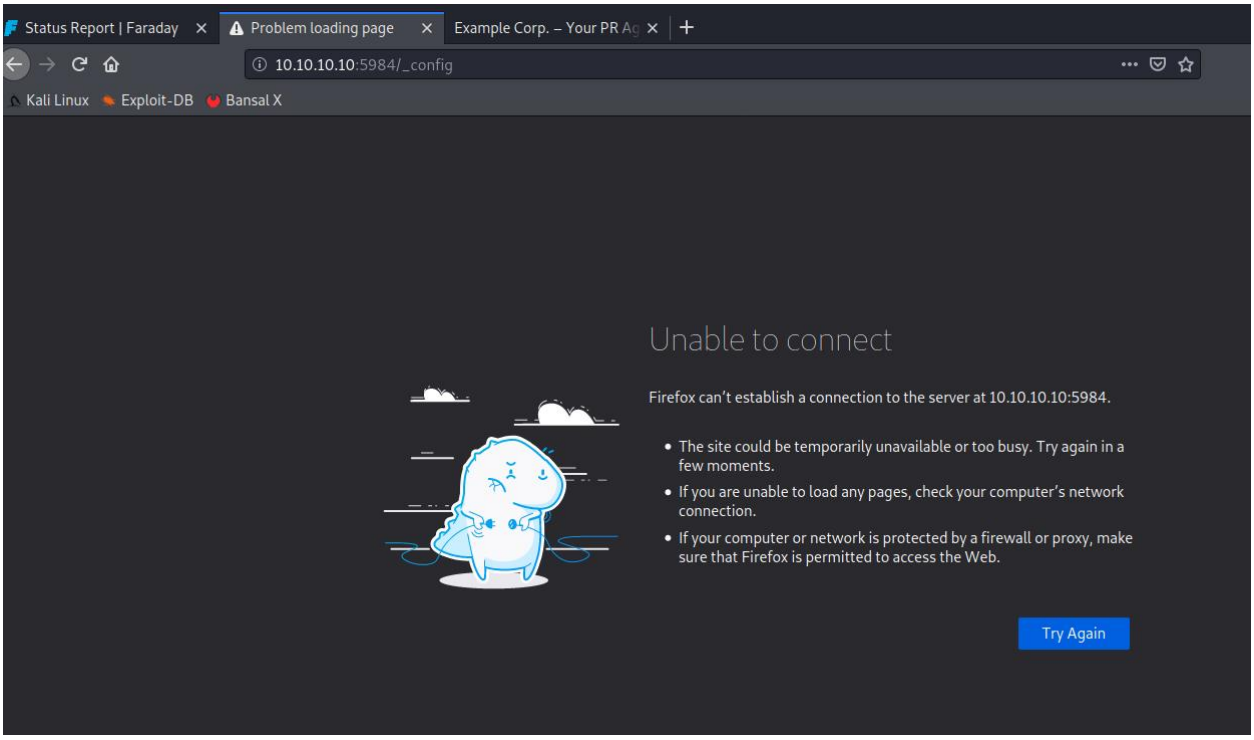
Recommendations:

Secure the CouchDB installation with an administrative account if not done so already.

Steps to Reproduce

Note: vulnerability unconfirmed

1. Navigate to http://10.10.10.10:5984/_config



Finding X: HTTP TRACE / TRACK Methods Allowed on port 80 and 443 TCP– Medium

*technically counts as 2 vulnerabilities since it can be found on two separate ports

Vulnerability Description:

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Risk Information:

Score Source: CVE-2004-2320

CVSS v3.1 Calculations

Risk Factor: Medium

Base Score: 5.3

Temporal Score: 4.6

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Temporal Vector: E:U/RL:O/RC:C

Exposure/Analysis:

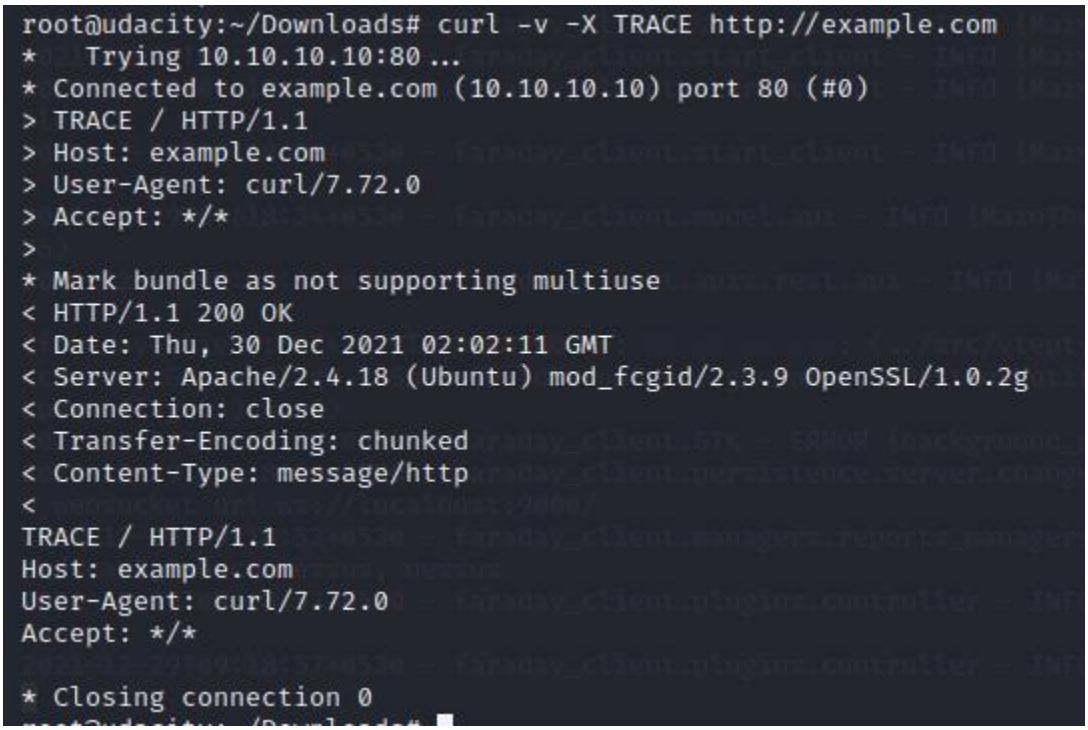
Debugging features have been left on and were confirmed manually with curl TRACE. While this does not allow the attacker a point of entry, it gives them extra information about our systems that can be utilized with other exploits.

Recommendations:

Disable these HTTP methods.

Steps to Reproduce

1. Curl -v -X TRACE example.com



Finding X: Apache mod_status /server-status Information Disclosure on port 443 TCP– Medium

Vulnerability Description:

A remote unauthenticated attacker can obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

Risk Information:

Score Source: Tenable

CVSS v3.1 Calculations

Risk Factor: Medium

Base Score: 5.3

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Exposure/Analysis:

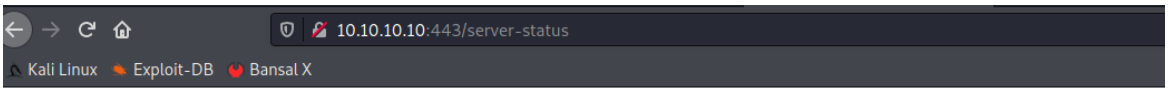
A vulnerability has been confirmed where the server's status is publicly accessible through the server status URL. While this information provides no access by itself, it does provide excess information to attackers to use with other exploits.

Recommendations:

Update Apache's configuration file(s) to either disable mod_status or restrict access to specific hosts.

Steps to Reproduce

1. http://10.10.10.10:443/server-status



Apache Server Status for 10.10.10.10 (via 10.10.10.10)

Server Version: Apache/2.4.18 (Ubuntu) mod_fcgid/2.3.9 OpenSSL/1.0.2g
Server MPM: prefork
Server Built: 2020-08-12T21:35:50

Current Time: Thursday, 30-Dec-2021 07:59:50 IST
Restart Time: Wednesday, 29-Dec-2021 03:15:01 IST
Parent Server Config. Generation: 1
Parent Server MPM Generation: 0
Server uptime: 1 day 4 hours 44 minutes 49 seconds
Server load: 0.00 0.00 0.00
Total accesses: 5794 - Total Traffic: 57.3 MB
CPU Usage: u18.28 s28.86 cu0 cs0 - .0456% CPU load
.056 requests/sec - 580 B/second - 10.1 kB/request
1 requests currently being processed, 9 idle workers

_W____.__.....
.....
.....

Scoreboard Key:
"_" Waiting for Connection, "S" Starting up, "R" Reading Request,
"W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
"C" Closing connection, "L" Logging, "G" Gracefully finishing,
"I" Idle cleanup of worker, "." Open slot with no current process

Srv	PID	Acc	M	CPU	SS	Req	Conn	Child	Slot	Client	VHost	Request
0-0	30682	0/598/598	_	6.16	588	0	0.0	6.19	6.19	127.0.0.1	infra.example.com:8081	GET /server-status HTTP/1.1
1-0	30683	0/631/631	**W**	7.47	0	0	0.0	6.58	6.58	10.10.10.7	infra.example.com:443	GET /server-status HTTP/1.1
2-0	11914	0/235/580	_	2.22	889	0	0.0	2.32	5.66	127.0.0.1	infra.example.com:8081	GET /server-status HTTP/1.1
3-0	11915	0/207/494	_	2.23	1188	0	0.0	2.24	4.93	127.0.0.1	infra.example.com:8081	GET /server-status HTTP/1.1
4-0	30686	0/643/643	_	6.58	1789	0	0.0	6.39	6.39	127.0.0.1	infra.example.com:8081	GET /server-status HTTP/1.1
5-0	9489	0/646/646	_	5.98	2089	0	0.0	5.97	5.97	127.0.0.1	infra.example.com:8081	GET /server-status HTTP/1.1
6-0	9547	0/389/639	_	3.37	2004	0	0.0	3.22	5.87	10.10.10.7	infra.example.com:443	GET /server-status HTTP/1.1

Appendixes

Appendix A:
Vulnerability Score Analysis – CVSS 3.0

1. CVE-2004-2320
https://example.com

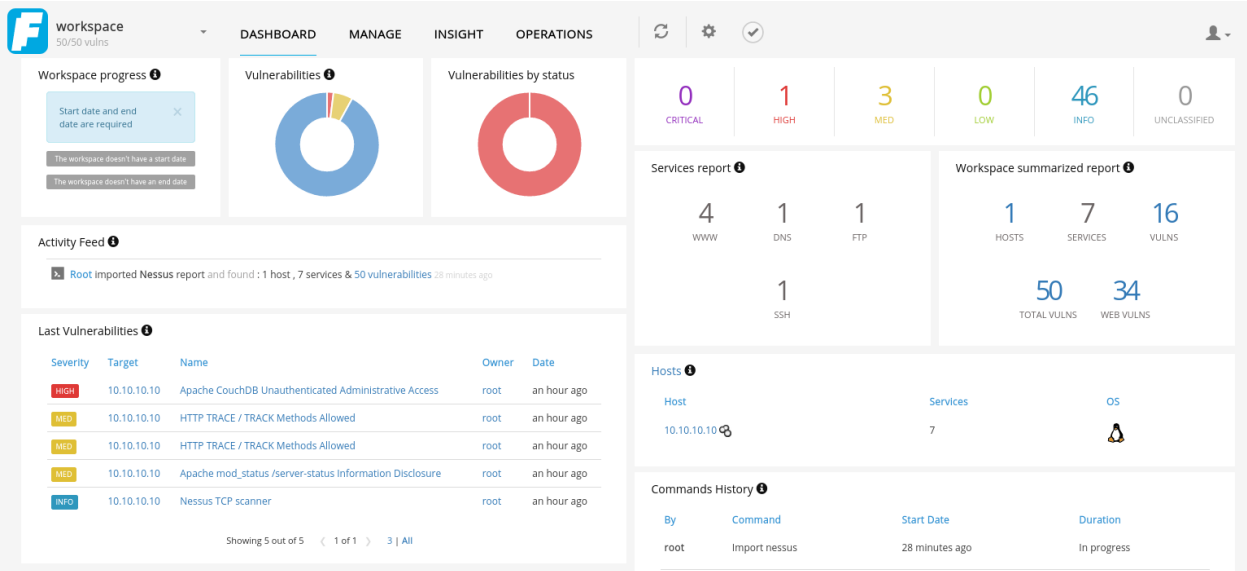
Final Vector:
AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O/RC:C/CR:L/IR:L/AR:L/MAV:N/MAC:X/MPR:N/MUI:N/MS:U/MC:L/MI:N/MA:N

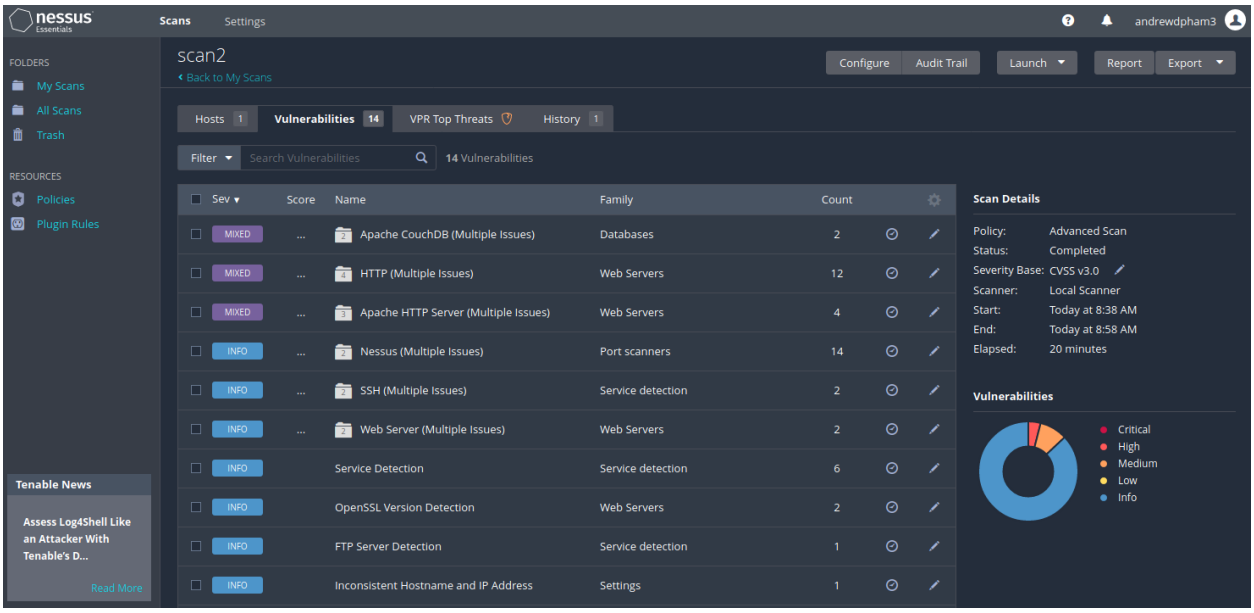
Adjusted Scores:
CVSS Base Score: 5.3
Impact Subscore: 1.4
Exploitability Subscore: 3.9
CVSS Temporal Score: 4.6
CVSS Environmental Score: 4.0
Modified Impact Subscore: 0.7
Overall CVSS Score: 4.0
Risk Rating – Low

Appendix B:
Modified Exploit Code For CVE-XXXX-XXXXX

Only one vulnerability had a CVE number and no exploit code was found.

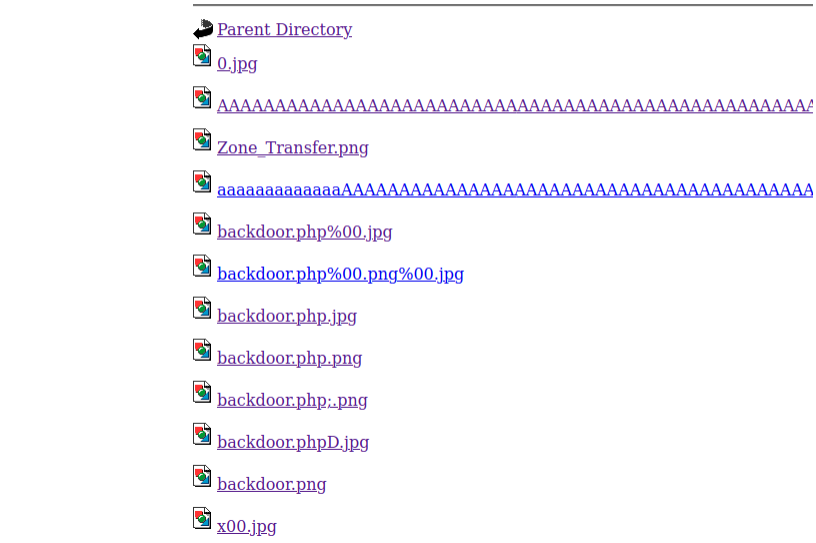
Appendix C:
Screenshots For Nessus & Faraday

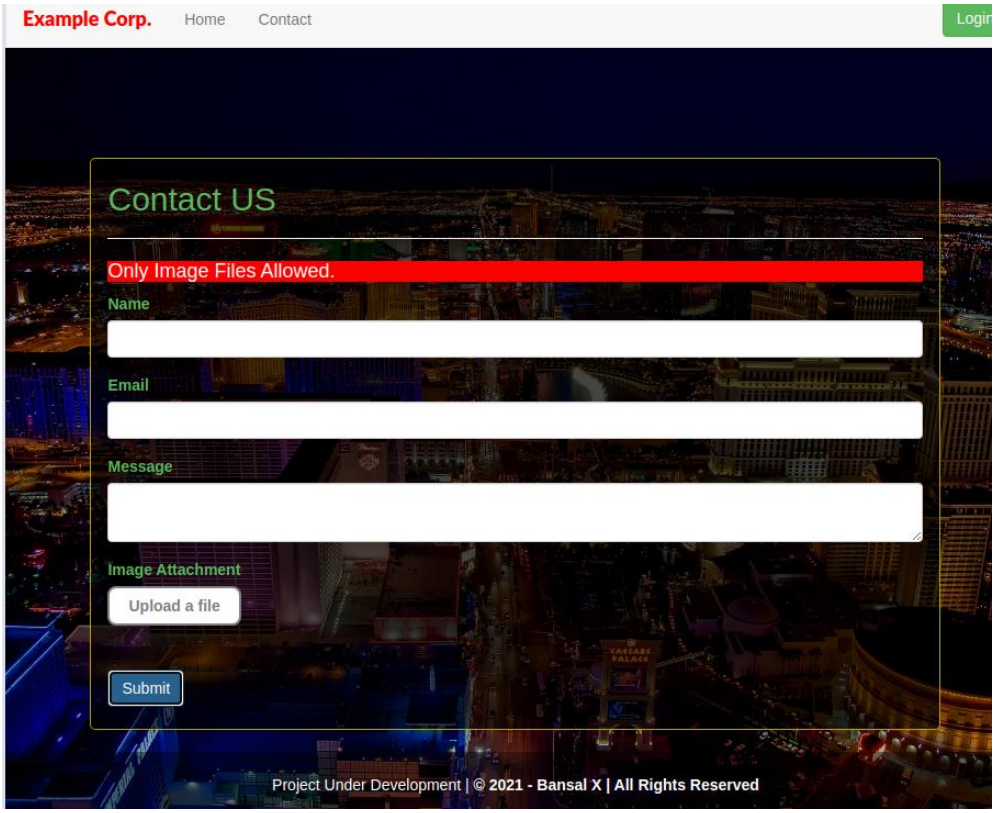




Appendix D:
Screenshots Of Exploited Web App

Index of /secureapp/uploads





Appendix E:
OSINT / Phishing Results Data Used

Details

Show 10 entries

Search:

First Name	Last Name	Email	Position	Status	Reported
Martin	Walters	martin@example.com	Developer	Submitted Data	
Tabitha	Yang	tabitha@example.com	Developer	Submitted Data	
Edwina	Jimenez	edwina@example.com	Employee	Submitted Data	
King	Farley	king@example.com	Employee	Submitted Data	
Pauline	Frey	pauline@example.com	Employee	Submitted Data	
Rose	Underwood	rose@example.com	Employee	Submitted Data	
sagar	bansal	sagar@example.com	Instructor	Submitted Data	✓
Christine	Mcdonald	christine@example.com	Management	Submitted Data	
Liz	Hoover	liz@example.com	Management	Submitted Data	
Millard	Wang	millard@example.com	Management	Submitted Data	✓

Appendix F:
Nmap Found Services

```
root@udacity:~/Desktop# nmap example.com -p-
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-30 10:41 IST
Nmap scan report for example.com (10.10.10.10)
Host is up (0.00052s latency).
Not shown: 65528 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
53/tcp   open   domain
80/tcp   open   http
443/tcp  open   https
5984/tcp closed couchdb
8083/tcp open   us-srv
MAC Address: 08:00:27:5C:99:0E (Oracle VirtualBox virtual NIC)
```