**Response to feedback and request for assistance from the grader:**

**1. Managing Vulnerability Lifestyle – Appendix C**

My Nessus results did not reveal a critical vulnerability. Please check my scan here:

Graphical user interface, application

Description automatically generated

* Do not ping the host
* Scanning Fragile devices is not allowed

Graphical user interface, text, application

Description automatically generated

* Scan all ports

Graphical user interface, application

Description automatically generated

* Do not use local enumerators

Graphical user interface, text, application, email

Description automatically generated

* Scan over tcp syn and udp

Graphical user interface, text, application, email

Description automatically generated

* Disable ssl/tls

A picture containing logo

Description automatically generated

* Scan for database related issues



* Scan for Debian specific issues



* Scan for ubuntu specific issues



* Scan for firewall specific issues



* Scan for cgi related abuses

A screenshot of a computer

Description automatically generated with low confidence

* Scan for webserver related issues



* Scan for remote shell possibilities



* Scan for default accounts



* Scan for backdoors



* Scan for dos



* Scan for service



* Scan for settings



Resulted in only one high vulnerability and no critical vulnerabilities:

A screenshot of a computer screen

Description automatically generated with medium confidence

**2. Managing Vulnerability Lifestyle – Appendix A**

In the one high vulnerability I found, there was no related cvss source score or CVE, only CVSSv2 risk information on the tenable site:

Graphical user interface, text, website

Description automatically generated

A screenshot of a computer

Description automatically generated

Where do I go from here to find the CVE?

**3. Managing Security Awareness Programs – Appendix E**

I’ve included an appendix with a screenshot of the csv results. However, it does not show usernames and passwords on the default export. Am I meant to create the document myself or is there a way to export the results with the passwords?

Graphical user interface, application, table, Excel

Description automatically generated

**3. OSINT – Public Exposure Audit – Appendix E**

I’ve added the screenshots that were useful to me in uploading the backdoor.

Could you give me a hint on how I’m supposed to use the information in the zone transfer and whois? I think this could be used to spoof emails from their domain but I’m unsure of how to use that in this project.

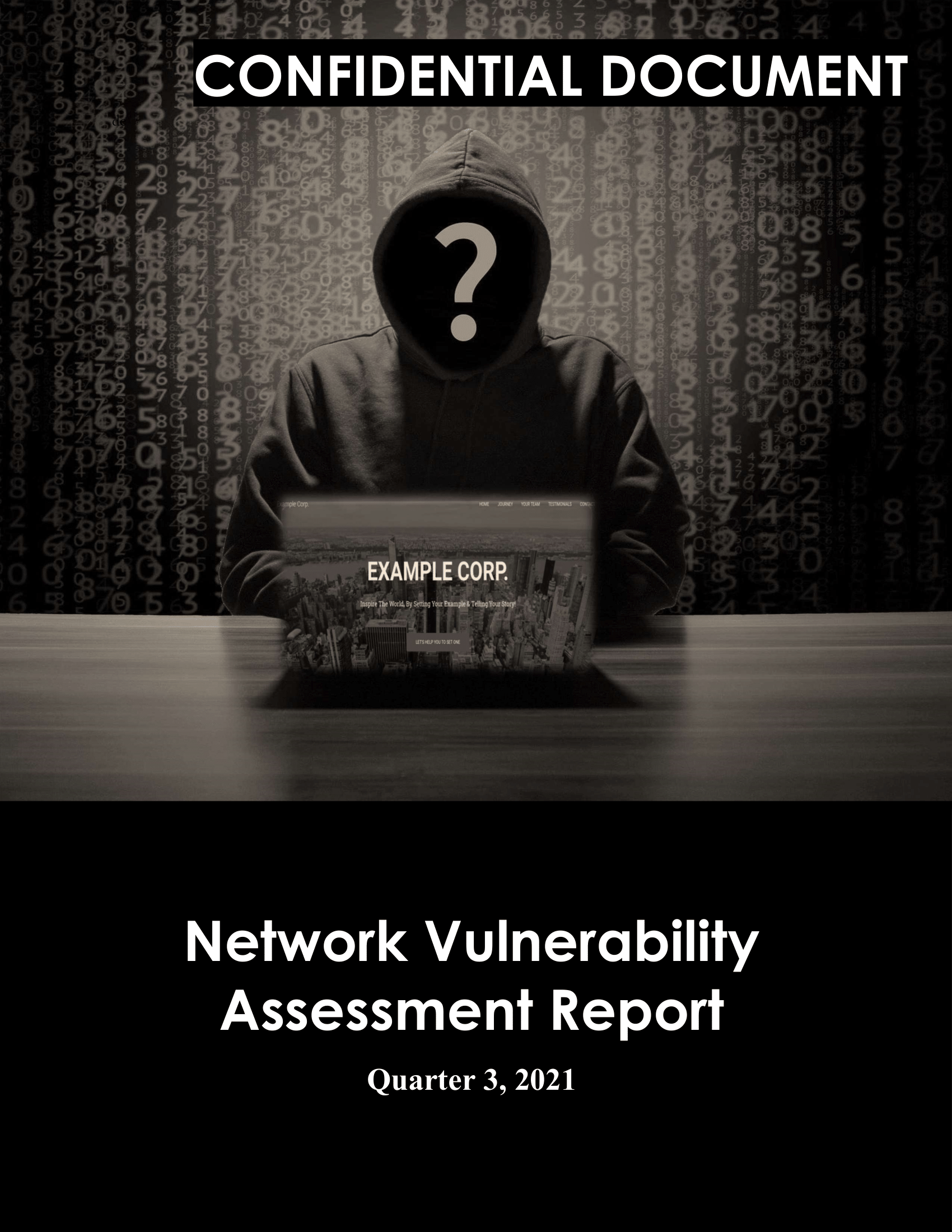
**4. Auditing Systems & Applications – Appendix E**

The CouchDB port doesn’t seem to be accepting connections for me. Is this the correct usage of NetCat?

Text

Description automatically generated

**1**

**de**

# 

# 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

[**Document Control 2**](#_heading=h.30j0zll)

[**Legal Disclaimer 3**](#_heading=h.3znysh7)

[**Table of Contents 4**](#_heading=h.2et92p0)

[**1.**](#_heading=h.tyjcwt) **10**

[**2.**](#_heading=h.1t3h5sf) **10**

[**3.**](#_heading=h.2s8eyo1) Error! Bookmark not defined.

[**4.**](#_heading=h.17dp8vu) **12**

[**Detailed Technical Reports (Scope Limited) 8**](#_heading=h.26in1rg)

[**Appendixes 16**](#_heading=h.4i7ojhp)

[**Appendix A: Vulnerability Score Analysis – CVSS 3.0 17**](#_heading=h.2xcytpi)

[**Appendix B: Modified Exploit Code For CVE-XXXX-XXXXX 18**](#_heading=h.1ci93xb)

[**Appendix C: Screenshots For Nessus & Faraday 19**](#_heading=h.3whwml4)

[**Appendix D: Screenshots Of Exploited Web App 20**](#_heading=h.2bn6wsx)

[**Appendix E: OSINT / Phishing Results Data Used 21**](#_heading=h.qsh70q)

[**Appendix F: NMAP Services 22**](#_heading=h.qsh70q)

# 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. For context our assessment audited the company’s website, example.com. We have found TODO critical vulnerabilities, TODO high vulnerabilities and TODO medium vulnerabilities. We also observed that there were some public exposures revealing security related information and we collected some credentials through phishing. We discovered a major problem with CouchDB allowing us to create a back door and gain access to the site. We propose that TODO**

# A Glance Through Target Security Posture

**Chart

Description automatically generated with low confidence****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 – Immediate action is required.**

# 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**

# 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.**

**Chart, bar chart

Description automatically generated**

|  |  |  |  |
| --- | --- | --- | --- |
| **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**

**Graphical user interface, text

Description automatically generated**

## 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**

**Text

Description automatically generated**

## 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**

**Text

Description automatically generated with medium confidence**

# 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

**Graphical user interface

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

# Appendix D: Screenshots Of Exploited Web App

**A picture containing table

Description automatically generated**

**A screenshot of a computer

Description automatically generated with medium confidence**

# Appendix E: OSINT / Phishing Results Data Used

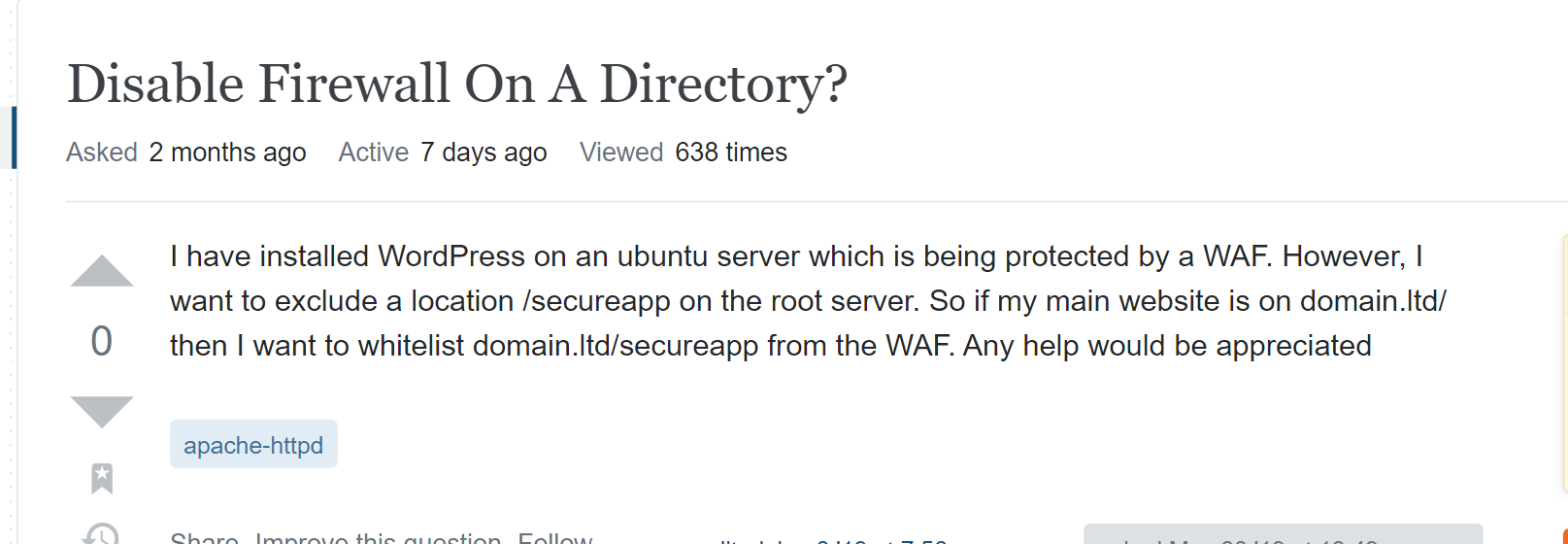
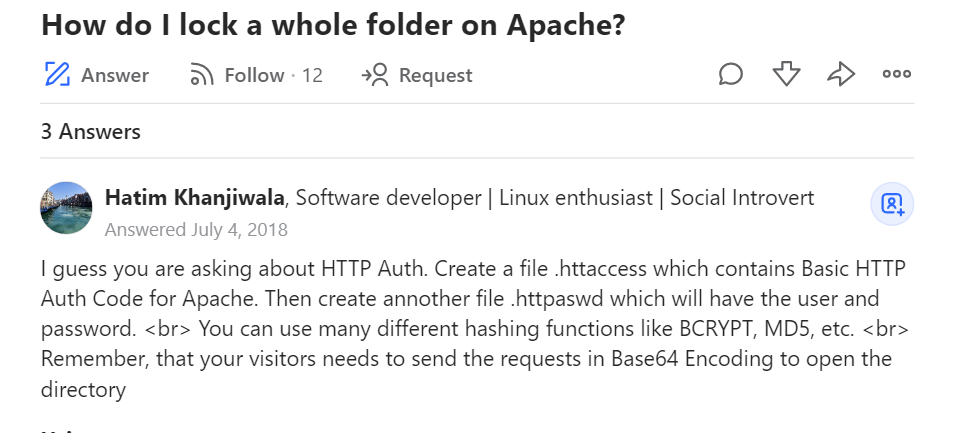
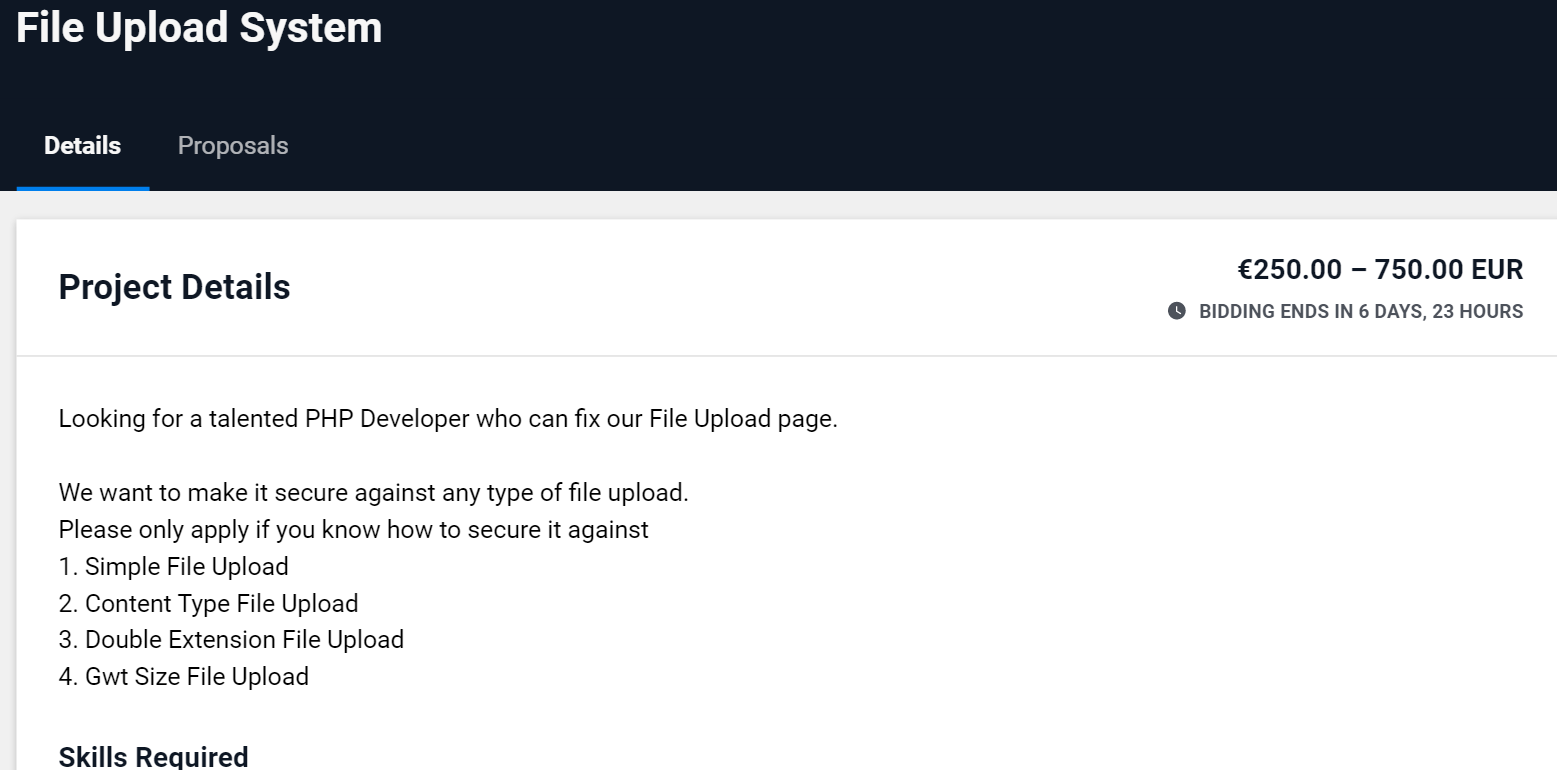
**Graphical user interface, application

Description automatically generated**

Graphical user interface, application, table, Excel

Description automatically generated

OSINT for uploading backdoor file:

****

# Appendix F: Nmap Found Services

**Text

Description automatically generated**