



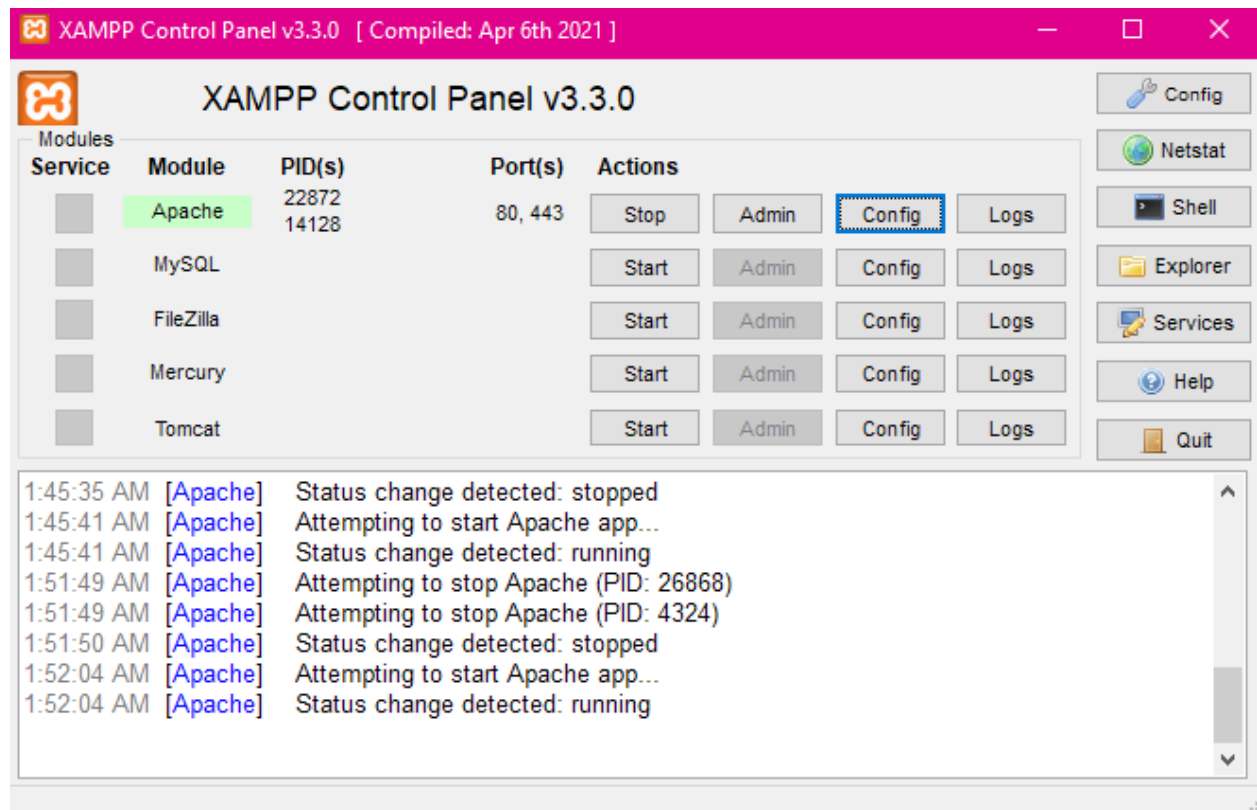
CCS6224: Network Security

Question 0

Num.	ID	Student Name
1	1221302093	Ahmad Fikri Bin Sharudin
2	1211102757	Sri Raam A/L Gunalingam

Tutorial Day: Wednesday
Tutorial Time: 10 AM - 12 PM
Tutorial Section: TT1L

Setting Up an Apache Web Server using XAMPP



Setting up an Apache web server is essential for web development. Using XAMPP simplifies this process, as it includes Apache, MariaDB, PHP, and Perl, providing a comprehensive environment for local web development and testing.

Start Apache Server:

- Open the XAMPP Control Panel.
- Click "Start" next to "Apache" and ensure it shows "Running".

Verify Installation:

- Open a web browser and go to <http://localhost>



Index of /

Name	Last modified	Size	Description
LICENSE	2024-04-05 08:25	1.0K	
_gdscmmu_theme/	2024-04-24 10:36	-	
app/	2024-04-05 08:25	-	
artisan	2024-04-05 08:25	1.6K	
bootstrap/	2024-04-05 08:25	-	
composer.json	2024-04-05 08:25	1.8K	
composer.lock	2024-04-05 08:25	292K	
config/	2024-04-05 08:25	-	
database/	2024-04-05 08:25	-	
package.json	2024-04-05 08:25	248	
phpunit.xml	2024-04-05 08:25	1.1K	
public/	2024-04-05 08:25	-	
resources/	2024-04-05 08:25	-	
routes/	2024-04-24 10:36	-	
storage/	2024-04-05 08:25	-	
tests/	2024-04-05 08:25	-	
vendor/	2024-04-05 08:32	-	
vite.config.js	2024-04-05 08:25	263	

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at localhost Port 80

Creating User Login on Web Server

1. Created .htaccess file to define rules of authentication

```
AuthType Basic
AuthName "Restricted Area"
AuthUserFile "C:/xampp/htdocs/protected/.htpasswd"
Require valid-user
```

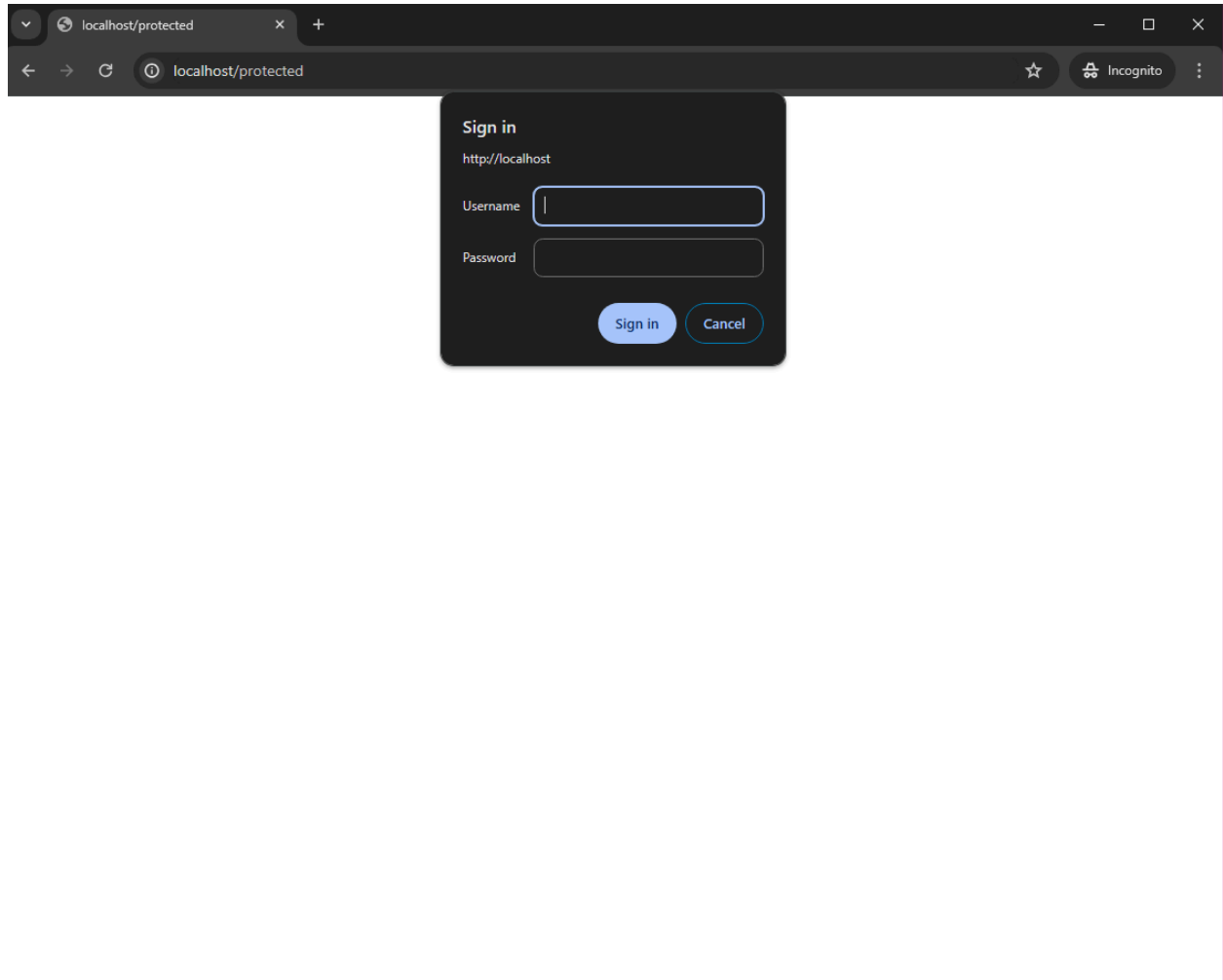
2. Created .htpasswd file to store encrypted username and password
username : admin
password : password

By using a .htpasswd generator online, an encrypted username and password was created

```
admin:$2y$10$xU607r1QgKDzLxIYV0E79usUN9PKJWai8kTpAUfWi0zkYdwq2GxSy
```

Which later stored in .htpasswd file

Output of authentication and web server running



Setting up Error Logs for Web Server

1. Defined path for errorlogs

```
httpd.conf - Notepad
File Edit Format View Help
# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog "C:/xampp/apache/logs/error.log"
```

2. When inputting wrong credentials, errors would show up in error logs

```
error.log - Notepad
File Edit Format View Help
[Tue Jun 11 01:52:04.598628 2024] [ssl:warn] [pid 22872:tid 444] AH01909: www.example.com:443:0 server certificate does NOT include an ID which matches the server name
[Tue Jun 11 01:52:04.651677 2024] [core:warn] [pid 22872:tid 444] AH00098: pid file C:/xampp/apache/logs/httpd.pid overwritten -- Unclean shutdown of previous Apache run?
[Tue Jun 11 01:52:04.654679 2024] [ssl:warn] [pid 22872:tid 444] AH01909: www.example.com:443:0 server certificate does NOT include an ID which matches the server name
[Tue Jun 11 01:52:04.695717 2024] [mpm_winnt:notice] [pid 22872:tid 444] AH00455: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 configured -- resuming normal operations
[Tue Jun 11 01:52:04.695717 2024] [core:notice] [pid 22872:tid 444] AH00094: Command line: 'c:\\xampp\\apache\\bin\\httpd.exe -d C:/xampp/apache'
[Tue Jun 11 01:52:04.699721 2024] [mpm_winnt:notice] [pid 22872:tid 444] AH00418: Parent: Created child process 14128
[Tue Jun 11 01:52:05.061560 2024] [ssl:warn] [pid 14128:tid 444] AH01909: www.example.com:443:0 server certificate does NOT include an ID which matches the server name
[Tue Jun 11 01:52:05.117611 2024] [ssl:warn] [pid 14128:tid 444] AH01909: www.example.com:443:0 server certificate does NOT include an ID which matches the server name
[Tue Jun 11 01:52:05.162652 2024] [mpm_winnt:notice] [pid 14128:tid 444] AH00354: Child: Starting 150 worker threads.
[Tue Jun 11 01:55:02.385082 2024] [auth_basic:error] [pid 14128:tid 1836] [client ::1:54524] AH01618: user 0000 not found: /protected
[Tue Jun 11 01:55:24.496440 2024] [auth_basic:error] [pid 14128:tid 1836] [client ::1:54526] AH01617: user admin: authentication failure for "/protected": Password Mismatch
```

Attacking Web Server: Using nmap

```
C:\Users\fudge>nmap -sV 192.168.0.100
Starting Nmap 7.95 ( https://nmap.org ) at 2024-06-12 17:37 Malay Peninsula Standard Time
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 80.00% done; ETC: 17:37 (0:00:03 remaining)
Nmap scan report for 192.168.0.100
Host is up (0.00040s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
443/tcp   open  ssl/http       Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
445/tcp   open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.69 seconds
```

Apache HTTP Server Details

HTTP (Port 80)

- **Service:** HTTP
- **Port:** 80/tcp
- **Server:** Apache HTTP Server 2.4.58
- **OS:** Windows 64-bit
- **OpenSSL Version:** 3.1.3
- **PHP Version:** 8.2.12

HTTPS (Port 443)

- **Service:** HTTPS (SSL/TLS)
- **Port:** 443/tcp
- **Server:** Apache HTTP Server 2.4.58
- **OS:** Windows 64-bit
- **OpenSSL Version:** 3.1.3
- **PHP Version:** 8.2.12

Summary

- **Apache Version:** 2.4.58
- **Operating System:** Windows (64-bit)
- **SSL/TLS Support:** Enabled with OpenSSL 3.1.3
- **PHP Support:** Enabled with PHP 8.2.12

HTTP Status Codes Using curl

curl (short for "Client URL") is a command-line tool and library for transferring data with URLs. It is widely used for interacting with web servers and web services, allowing users to send various types of requests and receive responses over different protocols such as HTTP, HTTPS, FTP, and many others. In this section, curl is used to see HTTP status codes from the web server.

HTTP 200 (OK)

Purpose: Verify that the home page of the web server is accessible and functioning correctly.

```
C:\Users\fudge>curl -i http://192.168.0.100/dashboard/
HTTP/1.1 200 OK
Date: Wed, 12 Jun 2024 10:11:40 GMT
Server: Apache/2.4.58 (win64) OpenSSL/3.1.3 PHP/8.2.12
Last-Modified: Sun, 19 Nov 2023 11:10:25 GMT
ETag: "1443-60a7f6a8cca40"
Accept-Ranges: bytes
Content-Length: 5187
Content-Type: text/html

<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <!-- Always force latest IE rendering engine or request Chrome Frame -->
    <meta content="IE=edge,chrome=1" http-equiv="X-UA-Compatible">
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />

    <!-- Use title if it's in the page YAML frontmatter -->
    <title>Welcome to XAMPP</title>

    <meta name="description" content="XAMPP is an easy to install Apache distribution containing MariaDB, PHP and Perl." />
    <meta name="keywords" content="xampp, apache, php, perl, mariadb, open source distribution" />

    <link href="/dashboard/stylesheets/normalize.css" rel="stylesheet" type="text/css" /><link href="/dashboard/stylesheets/all.css" rel="stylesheet" type="text/css" />
    <link href="//cdnjs.cloudflare.com/ajax/libs/font-awesome/3.1.0/css/font-awesome.min.css" rel="stylesheet" type="text/css" />

    <script src="/dashboard/javascripts/modernizr.js" type="text/javascript"></script>

    <link href="/dashboard/images/favicon.png" rel="icon" type="image/png" />

  </head>

  <body class="index">
    <div id="fb-root"></div>
    <script>(function(d, s, id) {
      var js, fjs = d.getElementsByTagName(s)[0];
      if (d.getElementById(id)) return;
      js = d.createElement(s); js.id = id;
      js.src = "//connect.facebook.net/en_US/all.js#xfbml=1&appId=277385395761685";
      fjs.parentNode.insertBefore(js, fjs);
    })(document, 'script', 'facebook-jssdk');</script>
    <header class="header contain-to-grid">
      <nav class="top-bar" data-topbar>
        <ul class="title-area">
          <li class="name">
            <h1><a href="/dashboard/index.html">Apache Friends</a></h1>
          </li>
          <li class="toggle-topbar menu-icon">
            <a href="#">
              <span>Menu</span>
            </a>
          </li>
        </ul>
      </nav>

      <section class="top-bar-section">
        <!-- Left Nav Section -->
        <ul class="left">
          <li class="item"><a href="/dashboard/faq.html">FAQs</a></li>
          <li class="item"><a href="/dashboard/howto.html">HOW-TO Guides</a></li>
        </ul>
      </section>
    </body>
  </html>
```

Description: Successfully loaded the home page, receiving a 200 OK status code indicating that the request was successful.

HTTP 401 (Unauthorized)

Purpose: Test access control by attempting to access a protected directory without credentials.

```
C:\Users\fudge>curl -i http://192.168.0.100/protected/
HTTP/1.1 401 Unauthorized
Date: Wed, 12 Jun 2024 10:16:57 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
WWW-Authenticate: Basic realm="Restricted Area"
Content-Length: 484
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested. Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
<hr>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at 192.168.0.100 Port 80</address>
</body></html>
```

Description: Attempted to access the protected directory without credentials, resulting in a 401 Unauthorized status code, indicating that authentication is required.

HTTP 403 (Forbidden)

Purpose: Confirm that access is correctly restricted to a specific directory.

```
C:\Users\fudge>curl -i http://192.168.0.100/forbidden
HTTP/1.1 403 Forbidden
Date: Wed, 12 Jun 2024 10:21:55 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Content-Length: 302
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at 192.168.0.100 Port 80</address>
</body></html>
```

Description: Attempted to access a forbidden directory configured with an `.htaccess` file, resulting in a 403 Forbidden status code, indicating that access is correctly restricted.

HTTP 404 (Not Found)

Purpose: Ensure that the server correctly handles requests for non-existent resources.

```
C:\Users\fudge>curl -i http://192.168.0.100/nonexistentpage
HTTP/1.1 404 Not Found
Date: Wed, 12 Jun 2024 10:34:45 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Content-Length: 299
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at 192.168.0.100 Port 80</address>
</body></html>
```

Description: Attempted to access a non-existent page, resulting in a 404 Not Found status code, indicating that the server correctly handles missing resources.

HTTP 500 (Internal Server Error)

Purpose: Verify the server's error handling by triggering a server-side error.

```
C:\Users\fudge>curl -i http://192.168.0.100/
HTTP/1.1 500 Internal Server Error
Date: Wed, 12 Jun 2024 10:39:25 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
Content-Length: 636
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>500 Internal Server Error</title>
</head><body>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error or
misconfiguration and was unable to complete
your request.</p>
<p>Please contact the server administrator at
postmaster@localhost to inform them of the time this error occurred,
and the actions you performed just before this error.</p>
<p>More information about this error may be available
in the server error log.</p>
<hr>
<address>Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at 192.168.0.100 Port 80</address>
</body></html>
```

Description: Triggered a server error by introducing an invalid directive in the .htaccess file, resulting in a 500 Internal Server Error status code, indicating that the server correctly handles internal errors.

Nikto Scan Report

```
perl nikto.pl -h http://192.168.0.100/
Nikto v2.5.0

-----
+ Target IP:      192.168.0.100
+ Target Hostname: 192.168.0.100
+ Target Port:    80
+ Start Time:     2024-06-12 19:17:53 (GMT8)
-----

+ Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
+ Apache/2.4.58 appears to be outdated (current is at least 2.4.59). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/8.2.12 appears to be outdated (current is at least 8.3.0).
+ OpenSSL/3.1.3 appears to be outdated (current is at least 3.2.0). OpenSSL 1.1.1w is current for 1.x and is supported via contract, and 3.0.12 for 3.0.x, and 3.1.4 for 3.1.x.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /nsn/fdir.bas:ShowVolume: You can use ShowVolume and ShowDirectory directly on the Novell server (NW5.1) to view the filesystem without having to log in.
+ /cgi-bin/post32.exe|dir%20c:\: post32 can execute arbitrary commands.
+ /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: Retrieved x-powered-by header: PHP/8.2.12.
+ /phpmyadmin/:X-Frame-Options header is deprecated and has been replaced with the Content-Security-Policy HTTP header with the frame-ancestors directive instead. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /phpmyadmin/: Uncommon header 'x-ob_mode' found, with contents: 1.
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ 8906 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:      2024-06-12 19:19:11 (GMT8) (78 seconds)
-----
+ 1 host(s) tested
```

Overview

The Nikto scan was conducted on the target web server (<http://192.168.0.100/>) to identify potential vulnerabilities and misconfigurations. The scan results provide valuable insights into the security posture of the server and highlight areas for improvement.

Findings

- 1. Server Information:**
 - The server is running Apache version 2.4.58, OpenSSL version 3.1.3, and PHP version 8.2.12.
 - These versions are flagged as potentially outdated, indicating a need for updating to newer versions.
- 2. Vulnerabilities and Misconfigurations:**
 - The X-Content-Type-Options header is not set, potentially allowing content rendering inconsistencies based on MIME type.
 - HTTP TRACE method is active, indicating vulnerability to Cross Site Tracing (XST).

- Directories and files with sensitive information or potential vulnerabilities were identified, including `/nsn/fdir.bas`, `/cgi-bin/post32.exe`, `/phpmyadmin/ChangeLog`, `/phpmyadmin/README`, etc.
- Directory indexing (`/icons/`) is enabled, which could expose directory contents to unauthorized users.
- Various headers, such as `X-Powered-By`, `X-Frame-Options`, and `x-ob_mode`, were observed, with recommendations provided for each.

3. Recommendations:

- Enable the X-Content-Type-Options header to prevent content type sniffing.
- Disable the HTTP TRACE method to mitigate Cross Site Tracing vulnerabilities.
- Secure sensitive directories and files (e.g., `/phpmyadmin/`) by restricting access or implementing additional authentication measures.
- Disable directory indexing to prevent unauthorized access to directory contents.
- Update server software (Apache, OpenSSL, PHP) to the latest versions to address potential security vulnerabilities.
- Implement security headers (e.g., `X-Frame-Options`) to enhance web security and mitigate certain types of attacks.

4. Scan Statistics:

- Total requests: 8906
- Errors encountered: 0
- Start time: 2024-06-12 19:17:53 (GMT8)
- End time: 2024-06-12 19:19:11 (GMT8)
- Duration: (78 seconds)

ZAP Security Testing Report

Summary

Attack had been conducted on the web server using OWASP ZAP (Zed Attack Proxy). The testing aimed to identify vulnerabilities and assess the security posture of the web application.

Findings

```
GET http://192.168.0.100/protected/ HTTP/1.1
host: 192.168.0.100
Proxy-Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic YWRtaW46cGFzc3dvcmQ=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-GB,en;q=0.9
```

Login Credential Capture

During the testing, a login request to the protected area of the web server was intercepted using ZAP. The intercepted request included an Authorization header containing Base64-encoded credentials for HTTP Basic Authentication. Upon decoding the Authorization header, the username and password used for authentication were successfully retrieved

Authorization header using Base64-encoded:


YWRtaW46cGFzc3dvcmQ=

After decoded:

Decode from Base64 format

Simply enter your data then push the decode button.



YWRtaW46cGFzc3dvcmQ=

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8  Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

 **DECODE**  Decodes your data into the area below.

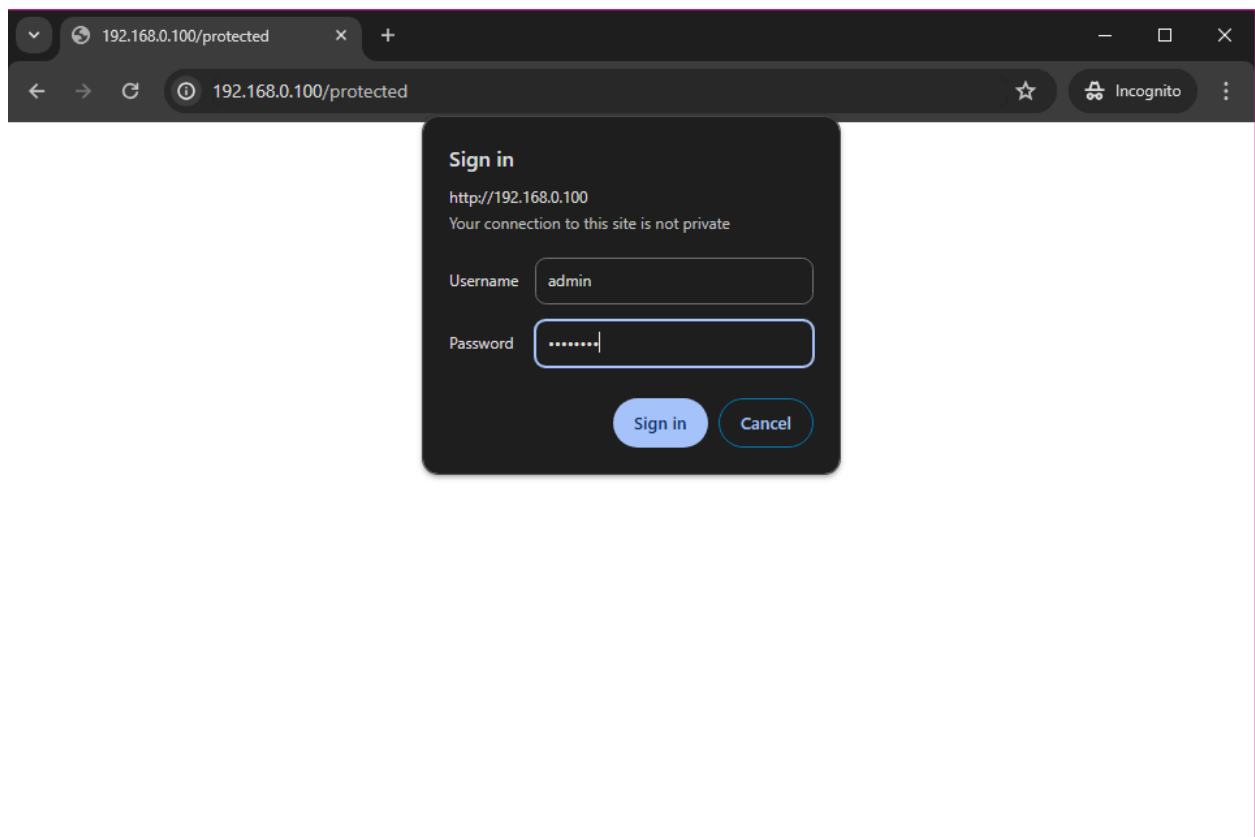
admin:password

Decoded Credentials:

- **Username:** admin
- **Password:** password

Capture Login Packet Using Wireshark

Run webserver and attempt login process



Run wireshark and capture the packets from the login process

For filtering purposes, apply the filter

`http && tcp.port == 80`

```

http &&tcpport==80
No.    time    Source          Destination      Protocol  Length  Info
575 17.173709 192.168.0.100   192.168.0.100   HTTP     317    GET /dashboard/images/social-icons.png HTTP/1.1
577 17.183247 192.168.0.100   192.168.0.100   HTTP     3714   HTTP/1.1 200 OK (PNG)
579 19.809998 192.168.0.100   192.168.0.100   HTTP     401    GET /protected HTTP/1.1
581 19.809998 192.168.0.100   192.168.0.100   HTTP     820    HTTP/1.1 401 Unauthorized (text/html)
640 85.218492 192.168.0.100   192.168.0.100   HTTP     550    GET /protected HTTP/1.1
640 85.271056 192.168.0.100   192.168.0.100   HTTP     570    HTTP/1.1 301 Moved Permanently (text/html)
650 85.273012 192.168.0.100   192.168.0.100   HTTP     551    GET /protected/ HTTP/1.1
652 86.543314 192.168.0.100   192.168.0.100   HTTP     1050   HTTP/1.1 200 OK (text/html)
654 86.554512 192.168.0.100   192.168.0.100   HTTP     471    GET /icons/blank.gif HTTP/1.1
656 86.555660 192.168.0.100   192.168.0.100   HTTP     499    HTTP/1.1 200 OK (GIF89a)
661 86.556441 192.168.0.100   192.168.0.100   HTTP     470    GET /icons/back.gif HTTP/1.1
663 86.557418 192.168.0.100   192.168.0.100   HTTP     568    HTTP/1.1 200 OK (GIF89a)
665 86.582636 192.168.0.100   192.168.0.100   HTTP     467    GET /favicon.ico HTTP/1.1
667 86.583201 192.168.0.100   192.168.0.100   HTTP     31252  HTTP/1.1 200 OK (image/x-icon)

Internet Protocol Version 4, Src: 192.168.0.100, Dst: 192.168.0.100
Transmission Control Protocol, Src Port: 6397, Dst Port: 80, Seq: 507, Ack: 635, Len: 507
Source Port: 6397
Destination Port: 80
[Stream Index: 24]
[Conversation completeness: Complete, MTH_DATA (31)]
[TCP Segment Len: 507]
Sequence Number: 507 (relative sequence number)
Sequence Number (raw): 2241564165
[Next Sequence Number: 1014 (relative sequence number)]
Acknowledgment Number: 635 (relative ack number)
Acknowledgment Number (raw): 1300000065
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 18231
[Calculated window size: 2619136]
Window size scaling factor: 256
Checksum: 0x1485 [Unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (507 bytes)
Hypertext Transfer Protocol
GET /protected/ HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /protected/ HTTP/1.1\r\n]
Request Method: GET
Request URI: /protected/
Request Version: HTTP/1.1
Host: 192.168.0.100\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic YWRtaW46cGFzc3dvcmQ=\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/1537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en;q=0.9\r\n
\r\n
[Full request URI: http://192.168.0.100/protected/]
[HTTP request 2/2]
[Prev. request in frame: 656]
[Response in frame: 662]
[Next request in frame: 664]

```

Login process packet captured

650	85.273012	192.168.0.100	192.168.0.100	HTTP	551 GET /protected/ HTTP/1.1
652	86.543314	192.168.0.100	192.168.0.100	HTTP	1050 HTTP/1.1 200 OK (text/html)
654	86.554512	192.168.0.100	192.168.0.100	HTTP	471 GET /icons/blank.gif HTTP/1.1
656	86.555660	192.168.0.100	192.168.0.100	HTTP	499 HTTP/1.1 200 OK (GIF89a)
661	86.556441	192.168.0.100	192.168.0.100	HTTP	470 GET /icons/back.gif HTTP/1.1
663	86.557418	192.168.0.100	192.168.0.100	HTTP	568 HTTP/1.1 200 OK (GIF89a)
665	86.582636	192.168.0.100	192.168.0.100	HTTP	467 GET /favicon.ico HTTP/1.1

From the packet details, authorization is using base-64 encoded

```

Hypertext Transfer Protocol
GET /protected/ HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /protected/ HTTP/1.1\r\n]
Request Method: GET
Request URI: /protected/
Request Version: HTTP/1.1
Host: 192.168.0.100\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic YWRtaW46cGFzc3dvcmQ=\r\n
Upgrade-Insecure-Requests: 1\r\n

```

authorization: Basic YWRtaW46cGFzc3dvcmQ=

After decoding, the login details for username and password for the webserver is achieved

Decode from Base64 format


Simply enter your data then push the decode button.

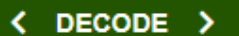

YWRtaW46cGFzc3dvcmQ=

 For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8  Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

 **DECODE**  Decodes your data into the area below.

admin:password

Username : admin

Password : password

Conclusion

Successfully captured and decoded the login credentials using Wireshark. This demonstrates the potential security risks of using basic authentication over HTTP.