**Apache HTTP**

**\*\*\*Things to note\*\*\***

1. **Default apache runs on 2.4.55**
2. **Using “sudo systemctl apache2” will start that version**
   1. **Check out step by step for how to start 2.4.49**
3. **If apache.service is started from boot and it’s not the correct version**
   1. **Steps to take**
      1. **sudo systemctl stop apache2 / sudo service apache2 stop**
      2. **sudo system disable apache2 / sudo update-rc.d apache2 disable**
4. **↑↑↑Security Measures↓↓↓**

**Apache 2.4.49 Vulnerable Web-app -- Exploit-DB**

* [**https://www.exploit-db.com/exploits/50383**](https://www.exploit-db.com/exploits/50383)

**Installation Step by step**

* **Wget** [**https://www.exploit-db.com/apps/1edb1895661473ea530209e29b83a982-httpd-2.4.49.tar.gz**](https://www.exploit-db.com/apps/1edb1895661473ea530209e29b83a982-httpd-2.4.49.tar.gz)
* **Following download completion**
  + **tar -xvf**
* **Once extracted the extracted directory is named httpd-2.4.49**
  + **cd into the directory**
  + **sudo apt-get install libapr1-dev libaprutil1-dev**
  + **sudo apt-get install libpcre3-dev**
* **./configure**
* **After configuration complete**
  + **sudo make**
  + **sudo make install**
* **Host the Apache service by running the command:**
  + **sudo /usr/local/apache2/bin/apachectl start**
* **php code should be in /usr/local/apache2/htdocs/**
  + **blog directory should be made here**
    - **“renamethis”.php should be in this directory**

**How does this did we configure this to work properly**

**Vulnerable configuration:**

**httpd.conf**

**mod\_cgi**

**Why is it vulnerable?**

1. **The vulnerability lies within the httpd.conf file**
2. **The misconfigured file has this following code**
   1. **<Directory /> Require all granted</Directory>**
3. **By chaining ../ with url encoding .%2e , this allows the attacker to read arbitrary files such as /etc/passwd**
4. **Ex. /cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/etc/passwd**
5. **This command is used within the linux cli with the curl command.**

**Remote code execution vulnerability**

1. **The RCE vulnerability takes place at the mod\_cgi**
2. **This module is enabled on the apache server and has the following:**
   1. **<IfModule !mpm\_prefork\_module> LoadModule cgid\_module modules/mod\_cgid.so </IfModule>**
3. **This allows the attacker to use the same technique demonstrated above and call any binary on the system using HTTP POST requests**
4. **Ex. /cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/sh**
5. **This is also used within the linux cli with the curl command**

**URL Encoding explanation:**

**Conversion: dot ( . ) → %2e → %%32%65**

* **2 is encoded to %32**
* **e is encoded to %65**
* **Original % remained the same**

**Source:** [**https://httpd.apache.org/security/vulnerabilities\_24.html#CVE-2021-41773**](https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2021-41773)

**Proof of concept:**

**Exploit: Testing using 2 separate virtual boxes**

**Victim ip = 192.168.56.117 - kali**

**Attacker ip = 192.168.56.107 - parrot**

**According to the source above ↑↑ this vulnerability allows us to exploit the cgi-bin folder and the mod\_cgi using path transversal and remote code execution techniques.**

**\*\*DEMO HERE\*\***

**\_\_\_\_**

**php code for website building ↓↓**

**index.html**

**<!DOCTYPE html>**

**<html>**

**<head>**

**<title>Project Magenta</title>**

**<style>**

**/\* Add some basic styles \*/**

**body {**

**font-family: Arial, sans-serif;**

**margin: 0;**

**padding: 0;**

**background-color: #f5f5f5;**

**}**

**header {**

**background-color: #333;**

**color: #fff;**

**padding: 20px;**

**text-align: center;**

**display: flex;**

**justify-content: space-between;**

**align-items: center;**

**}**

**h1 {**

**margin: 0;**

**font-size: 36px;**

**letter-spacing: 2px;**

**}**

**main {**

**margin: 20px;**

**padding: 20px;**

**background-color: #fff;**

**box-shadow: 0px 0px 5px rgba(0,0,0,0.3);**

**}**

**p {**

**font-size: 18px;**

**line-height: 1.5;**

**}**

**.login-button {**

**background-color: #4CAF50; /\* Green \*/**

**border: none;**

**color: white;**

**padding: 10px 20px;**

**text-align: center;**

**text-decoration: none;**

**display: inline-block;**

**font-size: 16px;**

**margin: 4px 2px;**

**cursor: pointer;**

**border-radius: 4px;**

**}**

**</style>**

**</head>**

**<body>**

**<header>**

**<h1>Welcome to Project Magenta!</h1>**

**<a class="login-button" href="login.php">Login</a>**

**</header>**

**<main>**

**<h2>About us</h2>**

**<p>Project Magenta is created for us to demonstrate our skills and abilities we learned at Fullstack Academy</p>**

**<h2>Check out the link below for our Blog posts!</h2>**

**<a href="blog/blog.php">Click here to check out our Blog posts!</a>**

**</main>**

**</body>**

**</html>**

**login.php**

**<!DOCTYPE html>**

**<html>**

**<head>**

**<title>Login</title>**

**<style>**

**/\* Add some basic styles \*/**

**body {**

**font-family: Arial, sans-serif;**

**margin: 0;**

**padding: 0;**

**background-color: #f5f5f5;**

**}**

**header {**

**background-color: #333;**

**color: #fff;**

**padding: 20px;**

**text-align: center;**

**}**

**h1 {**

**margin: 0;**

**font-size: 36px;**

**letter-spacing: 2px;**

**}**

**main {**

**margin: 20px;**

**padding: 20px;**

**background-color: #fff;**

**box-shadow: 0px 0px 5px rgba(0,0,0,0.3);**

**}**

**p {**

**font-size: 18px;**

**line-height: 1.5;**

**}**

**form {**

**display: flex;**

**flex-direction: column;**

**align-items: center;**

**}**

**input[type="text"],**

**input[type="password"],**

**input[type="submit"] {**

**width: 100%;**

**padding: 10px;**

**margin: 10px 0;**

**border-radius: 5px;**

**border: 1px solid #ccc;**

**font-size: 18px;**

**text-align: center;**

**}**

**input[type="submit"] {**

**background-color: #333;**

**color: #fff;**

**cursor: pointer;**

**transition: all 0.2s ease-in-out;**

**}**

**input[type="submit"]:hover {**

**background-color: #fff;**

**color: #333;**

**}**

**.register {**

**text-align: center;**

**margin-top: 20px;**

**}**

**</style>**

**</head>**

**<body>**

**<header>**

**<h1>Login</h1>**

**</header>**

**<main>**

**<form action="checkpoint.php" method="post">**

**<label for="username">Username:</label>**

**<input type="text" id="username" name="username" required>**

**<label for="password">Password:</label>**

**<input type="password" id="password" name="password" required>**

**<input type="submit" value="Login">**

**</form>**

**<div class="register">**

**<p>Don't have an account?</p>**

**<a href="register.php">Register here</a>**

**</div>**

**</main>**

**</body>**

**</html>**

**register.php**

**<!DOCTYPE html>**

**<html>**

**<head>**

**<title>Register</title>**

**<style>**

**body {**

**font-family: Arial, sans-serif;**

**margin: 0;**

**padding: 0;**

**background-color: #f5f5f5;**

**}**

**header {**

**background-color: #333;**

**color: #fff;**

**padding: 20px;**

**text-align: center;**

**}**

**h1 {**

**margin: 0;**

**font-size: 36px;**

**letter-spacing: 2px;**

**}**

**main {**

**margin: 20px;**

**padding: 20px;**

**background-color: #fff;**

**box-shadow: 0px 0px 5px rgba(0,0,0,0.3);**

**border-radius: 5px;**

**}**

**label {**

**display: block;**

**margin-bottom: 10px;**

**font-size: 18px;**

**}**

**input[type="text"], input[type="email"], input[type="password"] {**

**padding: 10px;**

**font-size: 16px;**

**border-radius: 5px;**

**border: 1px solid #ccc;**

**width: 100%;**

**box-sizing: border-box;**

**margin-bottom: 20px;**

**}**

**input[type="submit"] {**

**padding: 10px 20px;**

**background-color: #333;**

**color: #fff;**

**font-size: 18px;**

**border: none;**

**border-radius: 5px;**

**cursor: pointer;**

**}**

**.error {**

**color: red;**

**margin-bottom: 10px;**

**font-size: 16px;**

**}**

**</style>**

**</head>**

**<body>**

**<header>**

**<h1>Register</h1>**

**</header>**

**<main>**

**<?php if (!empty($errors)): ?>**

**<div class="error">**

**<?php foreach ($errors as $error): ?>**

**<p><?php echo $error; ?></p>**

**<?php endforeach; ?>**

**</div>**

**<?php endif; ?>**

**<form action="verification.php" method="post">**

**<label for="username">Username:</label>**

**<input type="text" id="username" name="username" required>**

**<label for="email">Email:</label>**

**<input type="email" id="email" name="email" required>**

**<label for="password">Password:</label>**

**<input type="password" id="password" name="password" required>**

**<input type="submit" value="Register">**

**</form>**

**</main>**

**</body>**

**</html>**

**verification.php**

**<!DOCTYPE html>**

**<html>**

**<head>**

**<title>Register</title>**

**<style>**

**body {**

**font-family: Arial, sans-serif;**

**margin: 0;**

**padding: 0;**

**background-color: #f5f5f5;**

**}**

**header {**

**background-color: #333;**

**color: #fff;**

**padding: 20px;**

**text-align: center;**

**}**

**h1 {**

**margin: 0;**

**font-size: 36px;**

**letter-spacing: 2px;**

**}**

**main {**

**margin: 20px;**

**padding: 20px;**

**background-color: #fff;**

**box-shadow: 0px 0px 5px rgba(0,0,0,0.3);**

**border-radius: 5px;**

**}**

**label {**

**display: block;**

**margin-bottom: 10px;**

**font-size: 18px;**

**}**

**input[type="text"], input[type="email"], input[type="password"] {**

**padding: 10px;**

**font-size: 16px;**

**border-radius: 5px;**

**border: 1px solid #ccc;**

**width: 100%;**

**box-sizing: border-box;**

**margin-bottom: 20px;**

**}**

**input[type="submit"] {**

**padding: 10px 20px;**

**background-color: #333;**

**color: #fff;**

**font-size: 18px;**

**border: none;**

**border-radius: 5px;**

**cursor: pointer;**

**}**

**.error {**

**color: red;**

**margin-bottom: 10px;**

**font-size: 16px;**

**}**

**</style>**

**</head>**

**<body>**

**<header>**

**<h1>Register</h1>**

**</header>**

**<main>**

**<?php if (!empty($errors)): ?>**

**<div class="error">**

**<?php foreach ($errors as $error): ?>**

**<p><?php echo $error; ?></p>**

**<?php endforeach; ?>**

**</div>**

**<?php endif; ?>**

**<form action="verification.php" method="post">**

**<label for="username">Username:</label>**

**<input type="text" id="username" name="username" required>**

**<label for="email">Email:</label>**

**<input type="email" id="email" name="email" required>**

**<label for="password">Password:</label>**

**<input type="password" id="password" name="password" required>**

**<input type="submit" value="Register">**

**</form>**

**</main>**

**</body>**

**</html>**

**success.php**

**<!DOCTYPE html>**

**<html>**

**<head>**

**<title>Login Success</title>**

**</head>**

**<body>**

**<h1>Login Success!</h1>**

**<p>Click <a href="index.html">here</a> to return home.</p>**

**</body>**

**</html>**

**failed.php**

**<!DOCTYPE html>**

**<html>**

**<head>**

**<title>Login Failed</title>**

**</head>**

**<body>**

**<h1>Login Failed</h1>**

**<p>Click <a href="login.php">here</a> to try again.</p>**

**</body>**

**</html>**

**Checkpoint.php - Currently non-functional**

**<?php**

**// Function to check if a user exists in user.csv with matching username and password**

**function checkUser($username, $password) {**

**// Open the user.csv file for reading**

**$file = fopen('/usr/local/apache2/htdocs/user.csv', 'r');**

**// Loop through each line in the file**

**while (($line = fgetcsv($file)) !== false) {**

**// If the username and password match the current line, return true**

**if ($line[0] === $username && $line[1] === $password) {**

**fclose($file);**

**return true;**

**}**

**}**

**// If no matching user is found, return false**

**fclose($file);**

**return false;**

**}**

**// Check if the login form has been submitted**

**if (isset($\_POST['username']) && isset($\_POST['password'])) {**

**$username = $\_POST['username'];**

**$password = $\_POST['password'];**

**// If the user exists, redirect to success.php**

**if (checkUser($username, $password)) {**

**header('Location: success.php');**

**exit;**

**} else {**

**// If the user doesn't exist, redirect to failed.php**

**header('Location: failed.php');**

**exit;**

**}**

**}**

**?>**

**/blog/ → must be in /usr/local/apache2/htdocs**

**blog.php**

**<?php**

**// Read the current blog posts from the file**

**$file = 'blog\_posts.json';**

**$blog\_posts = json\_decode(file\_get\_contents($file), true);**

**?>**

**<!DOCTYPE html>**

**<html>**

**<head>**

**<title>Welcome to the Blog of Project Magenta</title>**

**<style>**

**/\* Add some basic styles \*/**

**body {**

**font-family: Arial, sans-serif;**

**margin: 0;**

**padding: 0;**

**background-color: #f5f5f5;**

**}**

**header {**

**background-color: #333;**

**color: #fff;**

**padding: 20px;**

**text-align: center;**

**}**

**h1 {**

**margin: 0;**

**font-size: 36px;**

**letter-spacing: 2px;**

**}**

**main {**

**margin: 20px;**

**padding: 20px;**

**background-color: #fff;**

**box-shadow: 0px 0px 5px rgba(0,0,0,0.3);**

**}**

**p {**

**font-size: 18px;**

**line-height: 1.5;**

**}**

**</style>**

**</head>**

**<body>**

**<header>**

**<h1>Project Magenta</h1>**

**</header>**

**<main>**

**<h2>Welcome to The Blog of Project Magenta</h2>**

**<p>Here you will find our latest posts and musings on a variety of topics.</p>**

**<h2>Latest Posts</h2>**

**<ul>**

**<li><a href="Chandler.php">Chandler's Post</a></li>**

**<li><a href="Stephanie.php">Stephanie's Post</a></li>**

**<li><a href="Jeremy.php">Jeremy's Post</a></li>**

**<li><a href="Jay.php">Jay's Post<a></li>**

**</ul>**

**</main>**

**</body>**

**</html>**

**“renamethis”.php**

**<!DOCTYPE html>**

**<html>**

**<head>**

**<title>edit this</title>**

**<style>**

**/\* Add some basic styles \*/**

**body {**

**font-family: Arial, sans-serif;**

**margin: 0;**

**padding: 0;**

**background-color: #f5f5f5;**

**}**

**header {**

**background-color: #333;**

**color: #fff;**

**padding: 20px;**

**text-align: center;**

**}**

**h1 {**

**margin: 0;**

**font-size: 36px;**

**letter-spacing: 2px;**

**}**

**main {**

**margin: 20px;**

**padding: 20px;**

**background-color: #fff;**

**box-shadow: 0px 0px 5px rgba(0,0,0,0.3);**

**}**

**p {**

**font-size: 18px;**

**line-height: 1.5;**

**}**

**</style>**

**</head>**

**<body>**

**<header>**

**<h1>Post 4</h1>**

**</header>**

**<main>**

**<p>This is the content of Post (edit this)</p>**

**</main>**

**</body>**

**</html>**