

Incident Report: Suspicious activity in Web Server

Incident ID: IR-2025-004

Attack Type: Bruteforce - TryHackme

Date: Dec 21, 2025

Analyst: BALA KOTESWARA REDDY REDDYMALLI

Severity: High

Status: Closed - True Positive

1. Executive Summary

A Brute force attack against the WordPress admin login page was detected. The attacker performed the Bruteforce by using Hydra from an external IP 167.172.41.141 and has successfully compromised the account.

2. Scenario Context

Scenario: You are an SOC Level 1 Analyst on shift and have received an alert indicating a spike in activity on the organisation's web server.

Your task is to dive into the logs and determine exactly what happened.

Environment	Details
Target System	Web Server

3. Incident Timeline

Time	Event Description
27/06/2025 21:20:27	Attacker started the Bruteforce attack against /wp-login.php
27/06/2025 21:20:42	BruteForce Attack successful and wordpress admin account compromised. 302 Login Redirection Detected.

4. Investigation Methodology

My Approach:

1. Begin by analyzing common indicators such as User Agents, HTTP Methods, and URI Paths ("low-hanging fruit").
2. Generate count statistics for the web traffic, grouping the data by HTTP method and URI path to identify anomalies
3. Trace the suspicious web requests by grouping them based on the client IP that generated a high count of requests to specific URI paths(Obtained in previous step).
4. Conduct a detailed investigation associated with suspicious user agents.
5. Determine if the attack was successful by examining web server status codes(302 Redirection)
6. Extracted IOCs for threat hunting

5. Technical Analysis

Detection queries(SPL):

Displays all user agents involved:

```
index="task6"  
| dedup useragent  
| table useragent
```

Count statistics of web traffic, grouping by http method and uri_path:

```
index=task6 status=200  
| stats count by method,uri_path  
| sort -count
```

Count statistics of web requests grouping them based on client ip for specific uri_path:

```
index=task6 method=POST uri_path="/wp-login.php"  
| stats values(referer_domain) as referer_domain values(status) as status values(useragent) as  
UserAgent values(uri_path) as uri_path values(method) as method count by clientip  
| table referer_domain clientip UserAgent uri_path count method status
```

Detailed Investigation of events by individual suspicious user agents:

```
index=task6 method=POST uri_path="/wp-login.php" useragent=*Hydra*
```

```
index=task6 method=POST uri_path="/wp-login.php" useragent=*Hydra*  
| stats values(bytes) as bytes values(clientip) as clientip values(status) as status count by useragent  
| table useragent clientip status bytes count
```

```
index=task6 method=POST uri_path="/wp-login.php" useragent=*WPscan*
```

```
index=task6 method=POST uri_path="/wp-login.php" useragent=*WPscan*  
| stats values(bytes) as bytes values(clientip) as clientip values(status) as status count by useragent  
| table useragent clientip status bytes count
```

Determining if attack was successful:

index=task6 method=POST uri_path="/wp-login.php" status!=200

Key Findings:

- Multiple suspicious User agents found(Hydra,WPscan,curl,python scripts)
- Higher number of Post request are found to be sent to uri path named "/wp-login.php"
- Bruteforce Attack observed against wordpress admin login using Hydra.
- The Bruteforce attack is successfully completed.(Based on 302 Redirection)

6. Indicators of Compromise (IOCs)

Indicator Type	Value	Context
IP Address	167.172.41.141	Attacker IP
Tool	Hydra	Password Bruteforce
Target URI Path	/wp-login.php	Wordpress admin login page

7. MITRE ATT&CK Mapping

- **T1110 (Bruteforce):** The attacker used Hydra to systematically guess passwords
- **T1588 (Obtain Capabilities):** The attacker utilized Hydra, a known credential cracking tool, for the attack.

8. Evidence Screenshots

Splunk Query showing list of user agents:

✓ 26 events (before 12/23/25 7:15:17.000 AM)No Event Sampling

Job

||

Smart Mode

EventsPatternsStatistics (26)Visualization

Show: 20 Per PageFormatPreview: On

< Prev

1

2

Next >

useragent

Apache/2.4.58 (Ubuntu) (internal dummy connection)

WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36

WordPress/6.8.1; http://10.10.28.135

WordPress/6.8.2; http://10.10.28.135

curl/8.1.2

-

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

Mozilla/5.0

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36

Mozilla/5.0 (compatible; InternetMeasurement/1.0; +https://internet-measurement.com/)

WordPress/6.8.1; http://172.16.8.239

Mozilla/5.0 (Hydra)

Expanse, a Palo Alto Networks company, searches across the global IPv4 space multiple times per day to identify customers's presences on the Internet. If you would like to be excluded from our scans, please send IP addresses/domains to: scaninfo@paloaltonetworks.com

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.140 Safari/537.36

python-requests/2.27.1

Mozilla/5.0 zgrab/0.x

Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:71.0) Gecko/20100101 Firefox/71.0

python-requests/2.32.4

Splunk Query showing Count stats grouping by http method and uripath:

splunk>enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

New Search

Save As ▾ Create Table View Close

```

1 index=task6 status=200
2 | stats count by method,url_path
3 | sort -count
  
```

All time 🔍

✓ 987 events (before 12/23/25 7:30:54.000 AM) No Event Sampling ▾ Job ▾ || ■ → 📄 ⬇️ ? Smart Mode ▾

Events Patterns **Statistics (27)** Visualization

Show: 50 Per Page ▾ ↗ Format ▾ Preview: On

method ⇅	uri_path ⇅	count ⇅
POST	/wp-login.php	741
GET	/wp-login.php	163
GET	/	25
OPTIONS	*	14
POST	/wp-cron.php	7
GET	/wp-admin/load-styles.php	5
POST	/wp-admin/admin-ajax.php	5
GET	/wp-admin/images/wordpress-logo.svg	3
GET	/wp-admin/load-scripts.php	3
GET	/wp-admin/theme-editor.php	3
POST	/xmlrpc.php	2
GET	/2025/06/23/hello-world/	1
GET	/author/admin/	1
GET	/comments/feed/	1

Splunk Query showing Count stats grouping by clientip:

splunk>enterprise

Apps

1 Messages

Settings

Activity

Help

Find

Search

Analytics

Datasets

Reports

Alerts

Dashboards

Search & Reporting

New Search

1 index=task6 method=POST uri_path="/wp-login.php"

2 | stats values(referer_domain) as referer_domain values(status) as status values(useragent) as UserAgent values(uri_path) as uri_path values(method) as method count by clientip

3 | table referer_domain clientip UserAgent uri_path count method status

All time

✓ 743 events (before 12/23/25 7:35:09.000 AM) No Event Sampling

Job ||| → ⌵ ⌴ Smart Mode

Events

Patterns

Statistics (2)

Visualization

Show: 50 Per Page

Format

Preview: On

referer_domain	clientip	UserAgent	uri_path	count	method	status
http://10.10.28.135	10.10.243.134	WPScan v3.8.28 (https://wpscan.com/wordpress-security-scanner)	/wp-login.php	583	POST	200
http://demo-web.deceptitech.thm	167.172.41.141	Mozilla/5.0 (Hydra) Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36	/wp-login.php	160	POST	200 302

Splunk Query showing Bruteforce Events:

Start Event:

New Search

index=task6 method=POST url_path="/wp-login.php" useragent="hydra"

158 events (before 12/23/25 7:36:06.000 AM) No Event Sampling

Timeline format Zoom Out Zoom to Selection Deselect 100 milliseconds per column

Format Show: 50 Per Page View: List Prev 1 2 3 4 Next

	< Hide Fields	All Fields	#	Time	Event
SELECTED FIELDS # host 1 # source 1 # sourcetype 1			>	6/27/25 9:20:28.000 PM	167.172.41.141 - [27/Jun/2025:21:20:28 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
			>	6/27/25 9:20:28.000 PM	167.172.41.141 - [27/Jun/2025:21:20:28 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
			>	6/27/25 9:20:28.000 PM	167.172.41.141 - [27/Jun/2025:21:20:28 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
			>	6/27/25 9:20:28.000 PM	167.172.41.141 - [27/Jun/2025:21:20:28 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
INTERESTING FIELDS # bytes 2 # date_hour 1 # date_mday 1 # date_minute 1 # date_month 1 # date_second 16 # date_wday 1 # date_year 1 # date_zone 1 # file 1 # ident 1 # index 1 # linecount 1 # method 1 # punct 1			>	6/27/25 9:20:27.000 PM	167.172.41.141 - [27/Jun/2025:21:20:27 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
			>	6/27/25 9:20:27.000 PM	167.172.41.141 - [27/Jun/2025:21:20:27 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
			>	6/27/25 9:20:27.000 PM	167.172.41.141 - [27/Jun/2025:21:20:27 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
			>	6/27/25 9:20:27.000 PM	167.172.41.141 - [27/Jun/2025:21:20:27 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
			>	6/27/25 9:20:27.000 PM	167.172.41.141 - [27/Jun/2025:21:20:27 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
			>	6/27/25 9:20:27.000 PM	167.172.41.141 - [27/Jun/2025:21:20:27 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
			>	6/27/25 9:20:27.000 PM	167.172.41.141 - [27/Jun/2025:21:20:27 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
			>	6/27/25 9:20:27.000 PM	167.172.41.141 - [27/Jun/2025:21:20:27 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined

End Event:

The screenshot shows the Splunk Enterprise interface with a search query: `index=task6 method=POST uri_path="/wp-login.php" useragent=*hydra*`. The search results show 158 events. The timeline view is active, showing a series of green bars representing events. The table view is also visible, showing the following data:

i	Time	Event
>	6/27/25 9:20:42.000 PM	167.172.41.141 - - [27/Jun/2025:21:20:42 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" "Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
>	6/27/25 9:20:42.000 PM	167.172.41.141 - - [27/Jun/2025:21:20:42 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" "Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
>	6/27/25 9:20:42.000 PM	167.172.41.141 - - [27/Jun/2025:21:20:42 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" "Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
>	6/27/25 9:20:42.000 PM	167.172.41.141 - - [27/Jun/2025:21:20:42 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" "Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
>	6/27/25 9:20:41.000 PM	167.172.41.141 - - [27/Jun/2025:21:20:41 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" "Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined
>	6/27/25	167.172.41.141 - - [27/Jun/2025:21:20:41 +0000] "POST /wp-login.php HTTP/1.0" 200 5244 "-" "Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined

Splunk Query determining whether the brute force is successful or not:

The screenshot shows the Splunk Enterprise interface with a search query: `index=task6 method=POST uri_path="/wp-login.php" status!=200`. The search results show 2 events. The timeline view is active, showing a series of green bars representing events. The table view is also visible, showing the following data:

i	Time	Event
>	6/27/25 9:21:27.000 PM	167.172.41.141 - - [27/Jun/2025:21:21:27 +0000] "POST /wp-login.php HTTP/1.1" 302 1191 "http://demo-web.deceptitech.thm/wp-login.php" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36" host = ce-splunk source = access.log sourcetype = access_combined
>	6/27/25 9:20:42.000 PM	167.172.41.141 - - [27/Jun/2025:21:20:42 +0000] "POST /wp-login.php HTTP/1.0" 302 1154 "-" "Mozilla/5.0 (Hydra)" host = ce-splunk source = access.log sourcetype = access_combined

8. Recommendations & Remediation

- Isolate Machine from network
- Reset wordpress account credentials
- Block the IP 162.172.41.141 in the firewall.