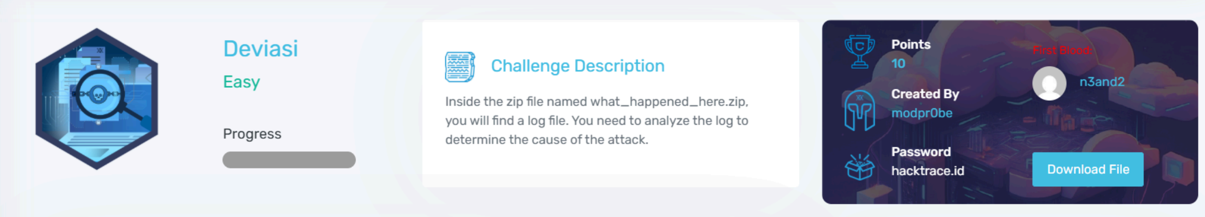
Write-Up Hacktrace Defensive : DEVIASI
(NafyCat69/BetaBot34 a.k.a Opel)

Deskripsi :
Inside the zip file named what_happened_here.zip, you will find a log file. You need to analyze the log to determine the cause of the attack.



Deviasi
Easy
Progress

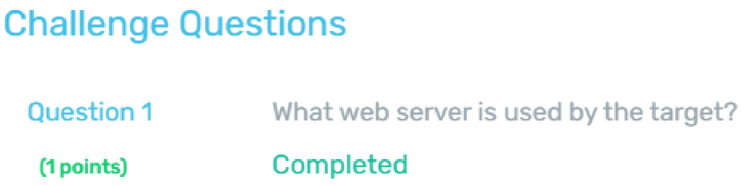
Challenge Description

Inside the zip file named what_happened_here.zip, you will find a log file. You need to analyze the log to determine the cause of the attack.

Points
10
Created By
modpr0be
Password
hacktrace.id
First Blood:
n3and2

Chall :

1. **Web Server Target**

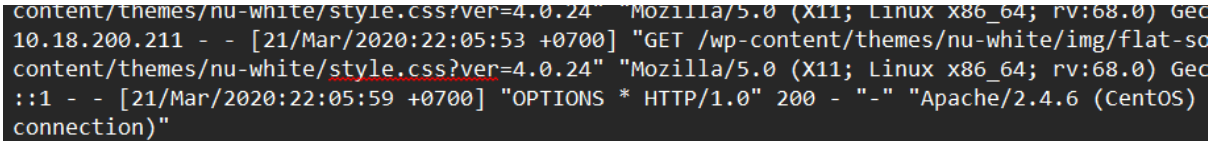


Challenge Questions

Question 1
(1 points)

What web server is used by the target?
Completed

Pada pertanyaan pertama, apa web server yang digunakan oleh korban pada file log.txt



```
content/themes/nu-white/style.css?ver=4.0.24" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gec
10.18.200.211 - - [21/Mar/2020:22:05:53 +0700] "GET /wp-content/themes/nu-white/img/flat-so
content/themes/nu-white/style.css?ver=4.0.24" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gec
::1 - - [21/Mar/2020:22:05:59 +0700] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.6 (CentOS)
connection)"
```

Pada log.txt dapat diketahui terdapat entries “::1” yang artinya terdapat sebuah request berasal dari komputer itu sendiri, dan disini kita dapat melihat bahwa webserver yang digunakan oleh korban adalah

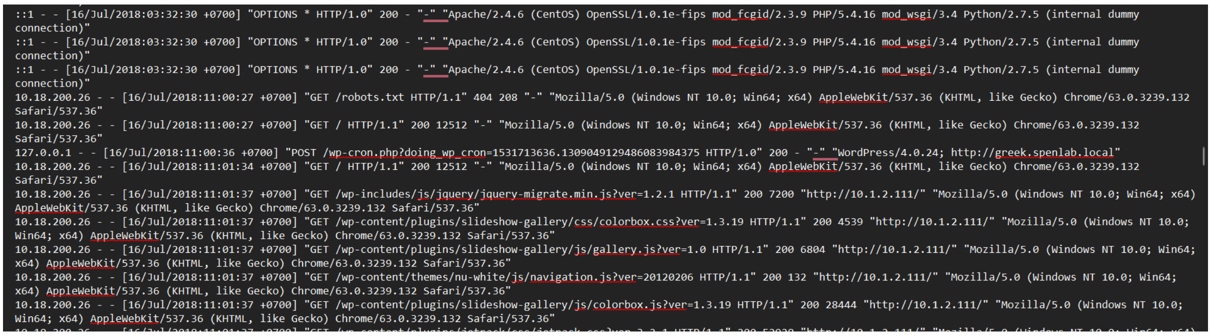
Jawaban : **Apache/2.4.6**

2. **Hacker IP Address**

Question 2
(2 points)

What is the IP address of the hacker?
Completed

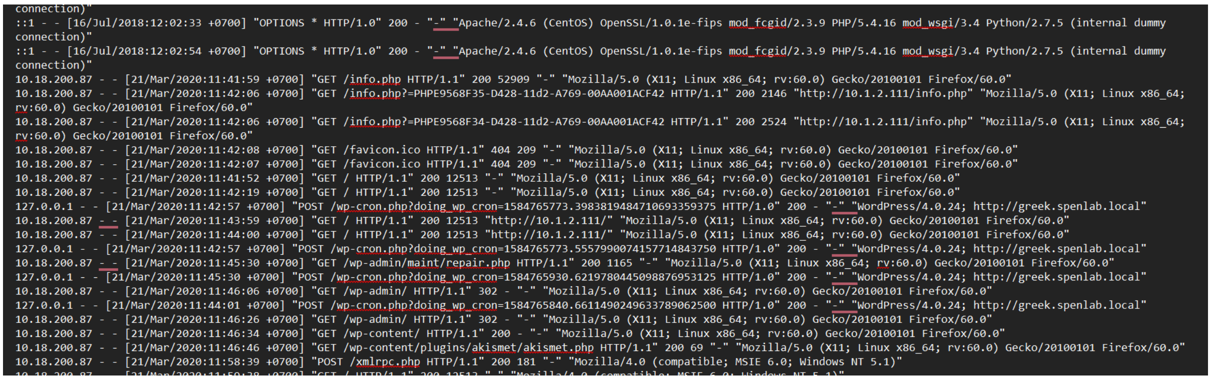
Soal ke-2 dapat kita ketahui jawabannya setelah kita cek log.txt pada bagian berikut



```
::1 - - [16/Jul/2018:03:32:30 +0700] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16 mod_wsgi/3.4 Python/2.7.5 (internal dummy
connection)"
::1 - - [16/Jul/2018:03:32:30 +0700] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16 mod_wsgi/3.4 Python/2.7.5 (internal dummy
connection)"
::1 - - [16/Jul/2018:03:32:30 +0700] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16 mod_wsgi/3.4 Python/2.7.5 (internal dummy
connection)"
10.18.200.26 - - [16/Jul/2018:11:00:27 +0700] "GET /robots.txt HTTP/1.1" 404 208 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132
Safari/537.36"
10.18.200.26 - - [16/Jul/2018:11:00:27 +0700] "GET / HTTP/1.1" 200 12512 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132
Safari/537.36"
127.0.0.1 - - [16/Jul/2018:11:00:36 +0700] "POST /wp-cron.php?doing_wp_cron=1531713636.1309049129486083984375 HTTP/1.0" 200 - "-" "WordPress/4.0.24; http://greek.spenlab.local"
10.18.200.26 - - [16/Jul/2018:11:01:34 +0700] "GET / HTTP/1.1" 200 12512 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132
Safari/537.36"
10.18.200.26 - - [16/Jul/2018:11:01:37 +0700] "GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HTTP/1.1" 200 7200 "http://10.1.2.111/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36"
10.18.200.26 - - [16/Jul/2018:11:01:37 +0700] "GET /wp-content/plugins/slideshow-gallery/css/colorbox.css?ver=1.3.19 HTTP/1.1" 200 4539 "http://10.1.2.111/" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36"
10.18.200.26 - - [16/Jul/2018:11:01:37 +0700] "GET /wp-content/plugins/slideshow-gallery/js/gallery.js?ver=1.0 HTTP/1.1" 200 6804 "http://10.1.2.111/" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36"
10.18.200.26 - - [16/Jul/2018:11:01:37 +0700] "GET /wp-content/themes/nu-white/js/navigation.js?ver=20120206 HTTP/1.1" 200 132 "http://10.1.2.111/" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36"
10.18.200.26 - - [16/Jul/2018:11:01:37 +0700] "GET /wp-content/plugins/slideshow-gallery/js/colorbox.js?ver=1.3.19 HTTP/1.1" 200 28444 "http://10.1.2.111/" "Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36"
```

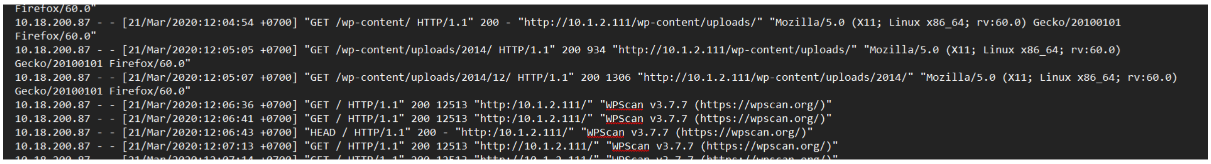
Pada gambar diatas terdapat beberapa aktivitas mencurigakan seperti entries pada /robots.txt pada tanggal 16/Jul/2018:11:00:27. Lalu ada beberapa kali request entries setelahnya seperti POST pada wp-cron.php yang berfungsi untuk sebagai sistem penjadwalan tugas otomatis di WordPress yang menjalankan tugas secara berkala saat halaman website dimuat.

lalu kurang lebih 2 tahun kemudian pada 21/Mar/2020:11:41:59 terdapat aktivitas mencurigakan kembali dari IP yang berbeda. Maka ada kemungkinan ada 2 Hacker yang menyerang namun dengan jangka waktu yang relative beda dan lama.



```
connection)"
::1 - - [16/Jul/2018:12:02:33 +0700] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16 mod_wsgi/3.4 Python/2.7.5 (internal dummy
connection)"
::1 - - [16/Jul/2018:12:02:54 +0700] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16 mod_wsgi/3.4 Python/2.7.5 (internal dummy
connection)"
10.18.200.87 - - [21/Mar/2020:11:41:59 +0700] "GET /info.php HTTP/1.1" 200 52909 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:11:42:06 +0700] "GET /info.php?=PHPE9568F35-D428-11d2-A769-00AA001ACF42 HTTP/1.1" 200 2146 "http://10.1.2.111/info.php" "Mozilla/5.0 (X11; Linux x86_64;
rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:11:42:06 +0700] "GET /info.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42 HTTP/1.1" 200 2524 "http://10.1.2.111/info.php" "Mozilla/5.0 (X11; Linux x86_64;
rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:11:42:08 +0700] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:11:42:07 +0700] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:11:41:52 +0700] "GET / HTTP/1.1" 200 12513 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:11:42:19 +0700] "GET / HTTP/1.1" 200 12513 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [21/Mar/2020:11:42:57 +0700] "POST /wp-cron.php?doing_wp_cron=1584765773.3983819484710693359375 HTTP/1.0" 200 - "-" "WordPress/4.0.24; http://greek.spenlab.local"
10.18.200.87 - - [21/Mar/2020:11:43:59 +0700] "GET / HTTP/1.1" 200 12513 "http://10.1.2.111/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:11:44:00 +0700] "GET / HTTP/1.1" 200 12513 "http://10.1.2.111/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [21/Mar/2020:11:42:57 +0700] "POST /wp-cron.php?doing_wp_cron=1584765773.5557990074157714843750 HTTP/1.0" 200 - "-" "WordPress/4.0.24; http://greek.spenlab.local"
10.18.200.87 - - [21/Mar/2020:11:45:30 +0700] "GET /wp-admin/maint/repair.php HTTP/1.1" 200 1165 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [21/Mar/2020:11:45:30 +0700] "POST /wp-cron.php?doing_wp_cron=1584765930.6219780445098876953125 HTTP/1.0" 200 - "-" "WordPress/4.0.24; http://greek.spenlab.local"
10.18.200.87 - - [21/Mar/2020:11:46:06 +0700] "GET /wp-admin/ HTTP/1.1" 302 - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
127.0.0.1 - - [21/Mar/2020:11:44:01 +0700] "POST /wp-cron.php?doing_wp_cron=1584765840.6611490249633789062500 HTTP/1.0" 200 - "-" "WordPress/4.0.24; http://greek.spenlab.local"
10.18.200.87 - - [21/Mar/2020:11:46:26 +0700] "GET /wp-admin/ HTTP/1.1" 302 - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:11:46:34 +0700] "GET /wp-content/ HTTP/1.1" 200 - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:11:46:46 +0700] "GET /wp-content/plugins/akismet/akismet.php HTTP/1.1" 200 69 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:11:58:39 +0700] "POST /xmlrpc.php HTTP/1.1" 200 181 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

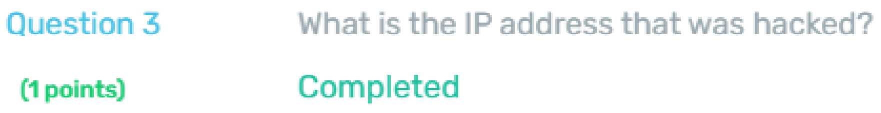
Indikasi hacker melakukan recon menggunakan tools WpScan



```
Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:12:04:54 +0700] "GET /wp-content/ HTTP/1.1" 200 - "http://10.1.2.111/wp-content/uploads/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:12:05:05 +0700] "GET /wp-content/uploads/2014/ HTTP/1.1" 200 934 "http://10.1.2.111/wp-content/uploads/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:12:05:07 +0700] "GET /wp-content/uploads/2014/12/ HTTP/1.1" 200 1306 "http://10.1.2.111/wp-content/uploads/2014/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:12:06:36 +0700] "GET / HTTP/1.1" 200 12513 "http:/10.1.2.111/" "WPScan v3.7.7 (https://wpscan.org/)"
10.18.200.87 - - [21/Mar/2020:12:06:41 +0700] "GET / HTTP/1.1" 200 12513 "http:/10.1.2.111/" "WPScan v3.7.7 (https://wpscan.org/)"
10.18.200.87 - - [21/Mar/2020:12:06:43 +0700] "HEAD / HTTP/1.1" 200 - "http:/10.1.2.111/" "WPScan v3.7.7 (https://wpscan.org/)"
10.18.200.87 - - [21/Mar/2020:12:07:13 +0700] "GET / HTTP/1.1" 200 12513 "http://10.1.2.111/" "WPScan v3.7.7 (https://wpscan.org/)"
```

Jawaban : **10.18.200.26, 10.18.200.87**

3. Victim IP Address

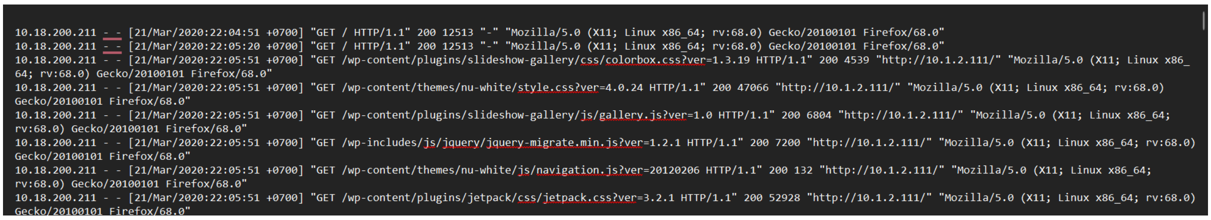


Question 3 (1 points)

What is the IP address that was hacked?

Completed

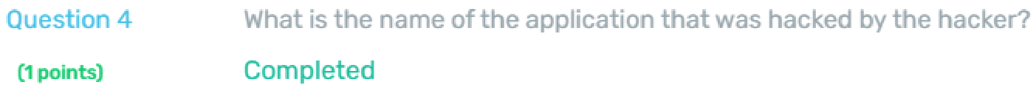
Pertanyaan selanjutnya berkaitan dengan DNS dari korban



```
10.18.200.211 - - [21/Mar/2020:22:04:51 +0700] "GET / HTTP/1.1" 200 12513 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.18.200.211 - - [21/Mar/2020:22:05:20 +0700] "GET / HTTP/1.1" 200 12513 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.18.200.211 - - [21/Mar/2020:22:05:51 +0700] "GET /wp-content/plugins/slideshow-gallery/css/colorbox.css?ver=1.3.19 HTTP/1.1" 200 4539 "http://10.1.2.111/" "Mozilla/5.0 (X11; Linux x86_
64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.18.200.211 - - [21/Mar/2020:22:05:51 +0700] "GET /wp-content/themes/nu-white/style.css?ver=4.0.24 HTTP/1.1" 200 47066 "http://10.1.2.111/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0)
Gecko/20100101 Firefox/68.0"
10.18.200.211 - - [21/Mar/2020:22:05:51 +0700] "GET /wp-content/plugins/slideshow-gallery/js/gallery.js?ver=1.0 HTTP/1.1" 200 6804 "http://10.1.2.111/" "Mozilla/5.0 (X11; Linux x86_64;
rv:68.0) Gecko/20100101 Firefox/68.0"
10.18.200.211 - - [21/Mar/2020:22:05:51 +0700] "GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HTTP/1.1" 200 7200 "http://10.1.2.111/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0)
Gecko/20100101 Firefox/68.0"
10.18.200.211 - - [21/Mar/2020:22:05:51 +0700] "GET /wp-content/themes/nu-white/js/navigation.js?ver=20120206 HTTP/1.1" 200 132 "http://10.1.2.111/" "Mozilla/5.0 (X11; Linux x86_64;
rv:68.0) Gecko/20100101 Firefox/68.0"
10.18.200.211 - - [21/Mar/2020:22:05:51 +0700] "GET /wp-content/plugins/jetpack/css/jetpack.css?ver=3.2.1 HTTP/1.1" 200 52928 "http://10.1.2.111/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0)
Gecko/20100101 Firefox/68.0"
```

Pada baris awal kita dapat melihat beberapa entries request yang menuju ke IP 10.1.2.111
Jawaban : **10.1.2.111**

4. Application Hacked By Hacker



Question 4 (1 points)

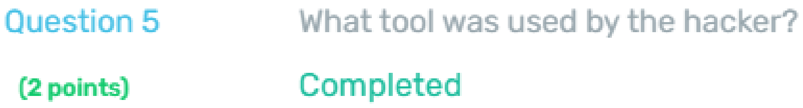
What is the name of the application that was hacked by the hacker?

Completed

Kita dapat menjawab pertanyaan ini jika kita sudah menganalisis pertanyaan no.2. Terdapat tools WpScan. Maka dapat ditarik kesimpulan bahwa aplikasi yang di hack oleh hacker adalah wordpress karena WpScan di gunakan untuk scanning atau recon wordpress

Jawaban : **Wordpress**

5. Tool Used by Hacker



Question 5 (2 points)

What tool was used by the hacker?

Completed

Karena kita sudah menganalisis dan menjawab pertanyaan nomor 2 maka dapat disimpulkan jawabannya adalah Wpscan

Jawab : **Wpscan**

6. Breached

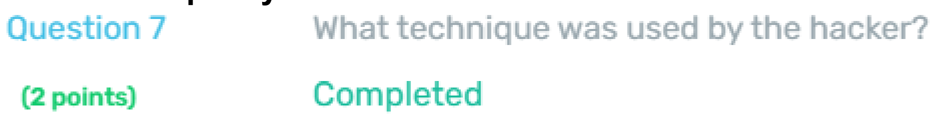
Question 6 How many hackers breached the target?

(1 points) Completed

Karena tadi kita sudah menganalisis bahwa terdapat 2 Hacker yang menyerang dalam jangka waktu yang lama. Maka dapat kesimpulan bahwa target terserang 2 kali

Jawaban : **2**

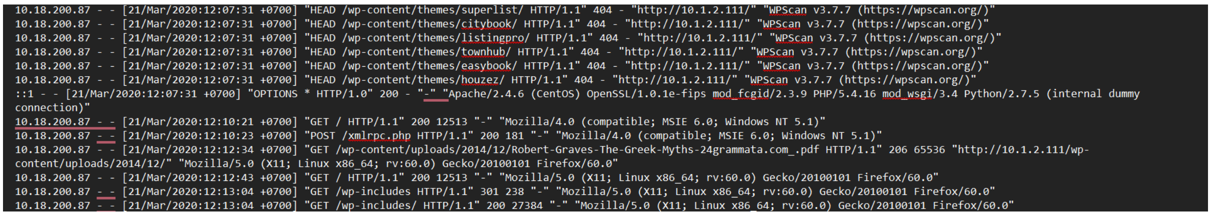
7. Technique by Hacker



Question 7 What technique was used by the hacker?

(2 points) Completed

Last Question teknik yang digunakan oleh hacker



```
10.18.200.87 - - [21/Mar/2020:12:07:31 +0700] "HEAD /wp-content/themes/superlist/ HTTP/1.1" 404 - "http://10.1.2.111/" "WPScan v3.7.7 (https://wpscan.org/)"
10.18.200.87 - - [21/Mar/2020:12:07:31 +0700] "HEAD /wp-content/themes/citybook/ HTTP/1.1" 404 - "http://10.1.2.111/" "WPScan v3.7.7 (https://wpscan.org/)"
10.18.200.87 - - [21/Mar/2020:12:07:31 +0700] "HEAD /wp-content/themes/listingpro/ HTTP/1.1" 404 - "http://10.1.2.111/" "WPScan v3.7.7 (https://wpscan.org/)"
10.18.200.87 - - [21/Mar/2020:12:07:31 +0700] "HEAD /wp-content/themes/townhub/ HTTP/1.1" 404 - "http://10.1.2.111/" "WPScan v3.7.7 (https://wpscan.org/)"
10.18.200.87 - - [21/Mar/2020:12:07:31 +0700] "HEAD /wp-content/themes/easybook/ HTTP/1.1" 404 - "http://10.1.2.111/" "WPScan v3.7.7 (https://wpscan.org/)"
10.18.200.87 - - [21/Mar/2020:12:07:31 +0700] "HEAD /wp-content/themes/houzez/ HTTP/1.1" 404 - "http://10.1.2.111/" "WPScan v3.7.7 (https://wpscan.org/)"
::1 - - [21/Mar/2020:12:07:31 +0700] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16 mod_wsgi/3.4 Python/2.7.5 (internal dummy
connection)"
10.18.200.87 - - [21/Mar/2020:12:10:21 +0700] "GET / HTTP/1.1" 200 12513 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.18.200.87 - - [21/Mar/2020:12:10:23 +0700] "POST /xmlrpc.php HTTP/1.1" 200 181 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
10.18.200.87 - - [21/Mar/2020:12:12:34 +0700] "GET /wp-content/uploads/2014/12/Robert-Graves-The-Greek-Myths-24grammata.com_.pdf HTTP/1.1" 206 65536 "http://10.1.2.111/wp-
content/uploads/2014/12/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:12:12:43 +0700] "GET / HTTP/1.1" 200 12513 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:12:13:04 +0700] "GET /wp-includes HTTP/1.1" 301 238 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.18.200.87 - - [21/Mar/2020:12:13:04 +0700] "GET /wp-includes/ HTTP/1.1" 200 27384 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
```

Pada 21/Mar/2020:12:07:31 Hacker menggunakan Wpscan untuk scanning tema yang digunakan pada website, maka dapat ditarik kesimpulan bahwa teknik yang digunakannya adalah themes enumeration

Jawaban : **themes enumeration**