Apache Log

Cyber Attack Type

Anggota

2501981270

AGUSTINUS LEONARDO DWITAMA

2501965052

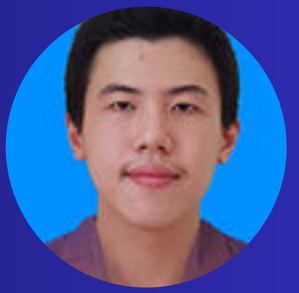
KEVIN MORRIS ARMANDO

2502001864

RAVI DEEVAN SATYAKI

2501989550

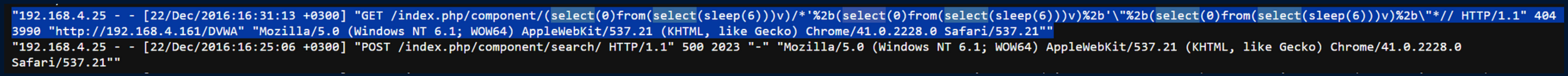
MUHAMAD DWI APRIYANTO



2501983723

NATANAEL FRANSISCO

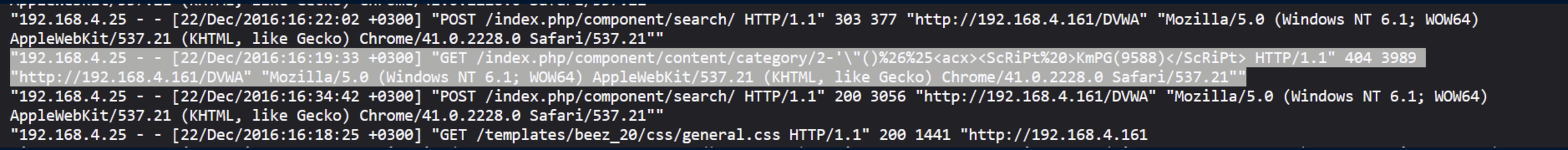
SQL INJECTION



SQL injection
Client : 192.168.4.25
Timestamp: 22 December 2016
Terdapat suatu percobaan injeksi query sql pada url directory
(select(0)from(select(sleep(6)))v)/*'%2b(select(0)from(select(sleep(6)))v)%2b'\"%2b(select(0)from(select(sleep(6)))v)%2b

"select(0)from(select(sleep(6)))v": Ini adalah contoh payload SQL Injection yang mencoba untuk menyisipkan perintah SQL "SELECT" dengan perintah "SLEEP(6)" ke dalam query. Perintah "SLEEP(6)" akan menghentikan eksekusi query selama 6 detik, sehingga penyerang mencoba untuk mengukur reaksi aplikasi terhadap penundaan.

XSS



XSS

Client : 192.168.4.25

Timestamp: 22 December 2016

Disini ada serangan XSS injection

<ScRiPt%20>KmPG(9588)</ScRiPt>

"<ScRiPt%20>KmPG(9588)</ScRiPt>": Ini adalah contoh payload serangan XSS yang dimana penulisan tag javascriptnya di variasikan kapitalnya dengna tujuan untuk menghindari validasi agar script XSS tetap jalan.

BRUTE FORCE URL

Directory Transversal

Client : 192.168.4.25

Timestamp: 22 December 2016 16:33

Merupakan salah satu cara brute force dengan menggunakan "../" untuk naik ke direktori atas, melewati batasan yang seharusnya ada. Penyerang mencoba kombinasi path yang berbeda secara brute force untuk menemukan file sensitif seperti /etc/passwd. Serangan ini mencoba mengakses file dan direktori di luar document root yang seharusnya tidak bisa diakses langsung melalui URL.

BRUTE FORCE URL

Client : 66.249.75.77

Timestamp: 30 September 2015 18:43

Attacker melakukan teknik brute force dengan mencoba mencari url dengan wordlist yang telah dibuat, dengan harap menemukan url yang secara tidak diketahui oleh pihak user dan developer bisa dibuka secara publik.

```
66.249.75.77 - - [30/Sep/2015:18:43:04 -0400] "GET /wp-content/plugins/formcraft/file-upload/server/content/upload.php
HTTP/1.1" 404 407 "-" "Mozilla/5.0 (Linux; Android 5.1.1; Nexus 5 Build/LMY48B; wv) AppleWebKit/537.36 (KHTML, like Gecko)
Version/4.0 Chrome/43.0.2357.65 Mobile Safari/537.36"
66.249.75.77 - - [30/Sep/2015:18:43:06 -0400] "GET /wp-content/plugins/formcraft/file-upload/server/php/upload.php HTTP/1.1"
404 407 "-" "Mozilla/5.0 (Linux; Android 5.1.1; Nexus 5 Build/LMY48B; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
Chrome/43.0.2357.65 Mobile Safari/537.36"
66.249.75.77 - - [30/Sep/2015:18:43:06 -0400] "GET /wp-content/plugins/formcraft/file-upload/server/upload.php HTTP/1.1" 404
407 "-" "Mozilla/5.0 (Linux; Android 5.1.1; Nexus 5 Build/LMY48B; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
Chrome/43.0.2357.65 Mobile Safari/537.36"
66.249.75.77 - - [30/Sep/2015:18:43:07 -0400] "GET /wp-content/plugins/formcraft/file-upload/server/php5/upload.php HTTP/1.1"
404 407 "-" "Mozilla/5.0 (Linux; Android 5.1.1; Nexus 5 Build/LMY48B; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
Chrome/43.0.2357.65 Mobile Safari/537.36"
```


THANK YOU