



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

```
"192.168.4.25 - - [22/Dec/2016:16:31:13 +0300] "GET /index.php/component/(*%2b(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\"*// HTTP/1.1" 404
3990 "http://192.168.4.161/DVWA" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21"
"192.168.4.25 - - [22/Dec/2016:16:25:06 +0300] "POST /index.php/component/search/ HTTP/1.1" 500 2023 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0
Safari/537.21"
```

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

```
"192.168.4.25 - - [22/Dec/2016:16:22:02 +0300] "POST /index.php/component/search/ HTTP/1.1" 303 377 "http://192.168.4.161/DVWA" "Mozilla/5.0 (Windows NT 6.1; WOW64)  
AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21"  
"192.168.4.25 - - [22/Dec/2016:16:19:33 +0300] "GET /index.php/component/content/category/2-'\"()%26%25<acx><ScRiPt%20>KmPG(9588)</ScRiPt> HTTP/1.1" 404 3989  
"http://192.168.4.161/DVWA" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21"  
"192.168.4.25 - - [22/Dec/2016:16:34:42 +0300] "POST /index.php/component/search/ HTTP/1.1" 200 3056 "http://192.168.4.161/DVWA" "Mozilla/5.0 (Windows NT 6.1; WOW64)  
AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21"  
"192.168.4.25 - - [22/Dec/2016:16:18:25 +0300] "GET /templates/beez_20/css/general.css HTTP/1.1" 200 1441 "http://192.168.4.161
```

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 dengan 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 UR

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"
```

A woman with long dark hair is sitting at a desk in an office, stretching her arms above her head. She is wearing a blue button-down shirt. On her desk, there is a computer monitor displaying a cityscape, a lamp, a potted plant, and some papers. The background shows shelves with books and other office equipment.

THANK YOU
