LOG ANALYSIS FORENSIC

SQLI, XSS, BRUTE FORCE

2502064303 – BETRAND GABRIALDI L | 2540123403 – BERTRAND REDONDO M | 2540123100 – VICTOR BENAYA | 2540125024 – FELYSIA MEYTRI

BACK TO AGENDA PAGE

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; Win
dows 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/2016:08:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid
=(SELECT 7505 FROM(SELECT COUNT(*),CONCAT(0x7171787671,(SELECT (ELT(7505=7505,1))),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/2016:08:22:13 0100] "GET /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid
=(SELECT CONCAT(0x7171787671,(SELECT (ELT(1399=1399,1))),0x71707a7871)) HTTP/1.1" 200 166 "-" "Mozilla/5.0 (Windo
ws; 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 "-" "M
ozilla/5.0 (Windows; U; Windows NT 6.1; ru; rv:1.9.2.3) Gecko/20100401 Firefox/4.0 (.NET CLR 3.5.30729)"
```

Log ini merupakan upaya SQLi dari IP 84.55.41.57 pada tanggal 14 April 2016. Attacker melakukan SQLi pada /wordpress/wp-content/plugins/custom_plugin/check_user.php?userid=…". SQLi terjadi pada page check_user.php dan vulnerability terdapat pada parameter user_id. Attacker melakukan Blind SQLi. Pada log pertama, angka 6810 digunakan untuk mengkonfirmasi/ menyangkal suatu kondisi. (SELECT (ELT(6810=6810,1))) akan menghasilkan '1' jika true dan ' ' jika false. COUNT & CONCAT merupakan fungsi untuk menghitung jumlah baris dan menggabungkan hasil tabel. Response yang diberikan adalah 200 yang artinya serangan blind sqli berhasil dengan response size 166 bytes

CROSS SITE SCRIPTING

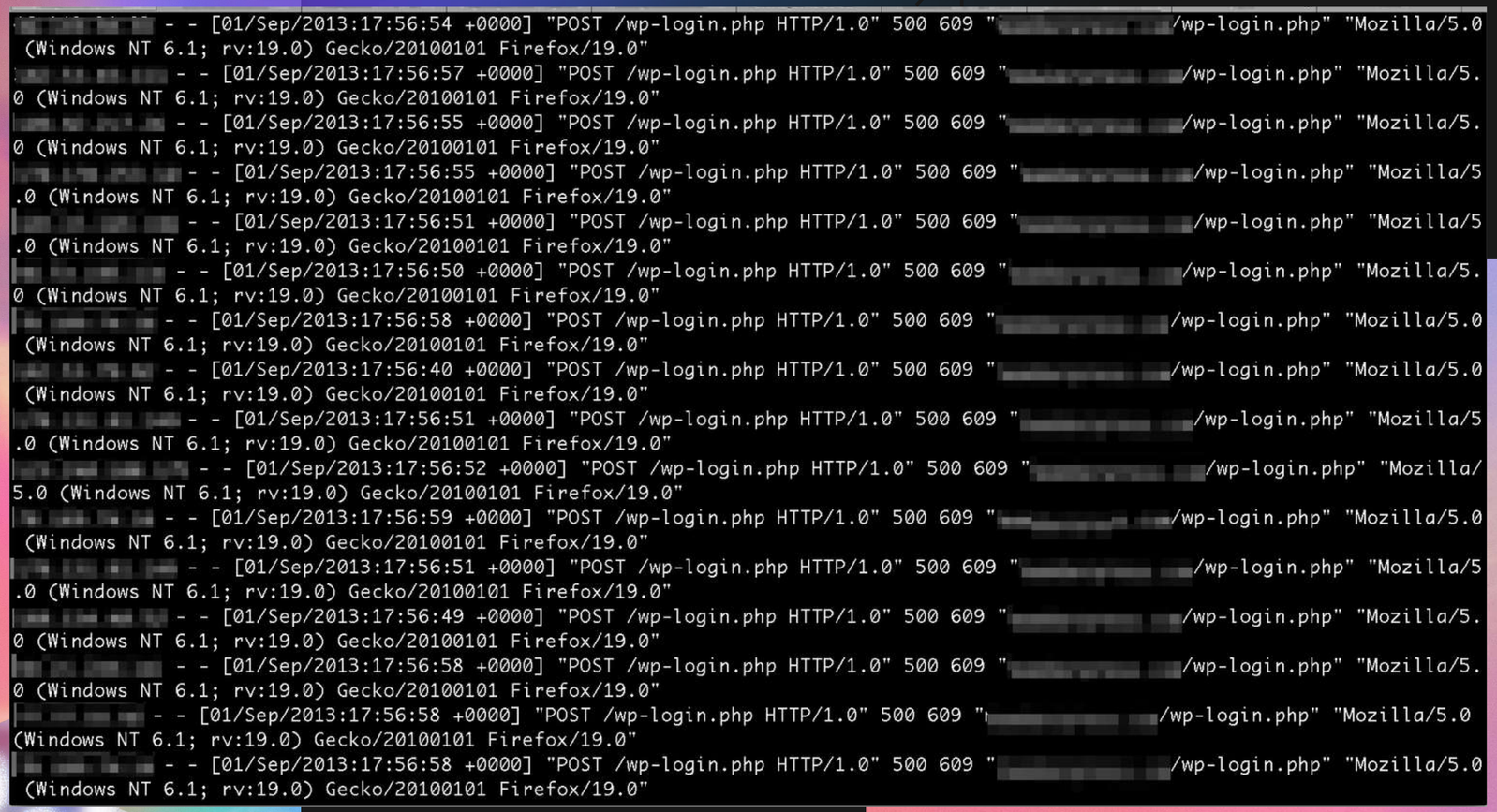
192.168.0.252 – – [05/Aug/2009:15:16:42 -0400] “GET /%27%27;!–%22%3CXSS%3E=&{()} HTTP/1.1” 404 310 “-” “Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12) Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12”

Log ini merupakan upaya XSS dari IP 192.168.0.252 yang dilakukan pada tanggal 5 Agustus 2009 jam 15:16:42. Attacker melakukan get request untuk mendapatkan /%27%27;!–%22%3CXSS%3E=&{()} menggunakan protokol HTTP/1.1. Ketika didecode hasilnya adalahGET /";!"<XSS>=&{()}.

Upaya penyerangan ini menghasilkan response 404 yang artinya halaman yang diminta attacker tidak ditemukan di server dan upaya XSS ini gagal

BACK TO AGENDA PAGE

BRUTE FORCE ATTACK



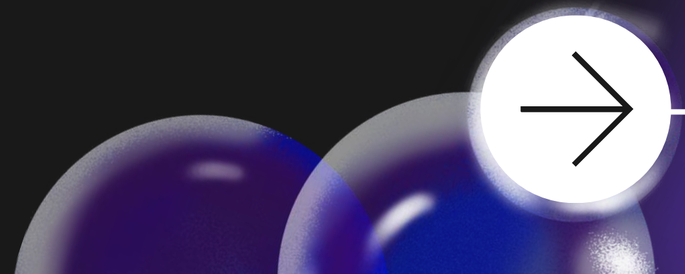
```
[redacted] - - [01/Sep/2013:17:56:54 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5.0
 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:57 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5.
0 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:55 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5.
0 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:55 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5
.0 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:51 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5
.0 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:50 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5.
0 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:58 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5.0
 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:40 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5.0
 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:51 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5
.0 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:52 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/
5.0 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:59 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5.0
 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:51 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5
.0 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:49 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5.
0 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:58 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5.
0 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:58 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5.0
(Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
[redacted] - - [01/Sep/2013:17:56:58 +0000] "POST /wp-login.php HTTP/1.0" 500 609 "[redacted]/wp-login.php" "Mozilla/5.0
 (Windows NT 6.1; rv:19.0) Gecko/20100101 Firefox/19.0"
```

Log tersebut merupakan brute force attack pada wp-login.php, dimana attacker mencoba melakukan bruteforce pada credentials email dan password (kemungkinan menggunakan automasi scripting/tool). Sayangnya upaya brute force ini belum berhasil

BACK TO AGENDA PAGE

LET'S BRAINSTORM

THANK YOU



A world without the possibility of crime is a world where you cannot prove you are not a criminal. A technology that can give you everything you want is a technology that can take away everything that you have.