Week 3 – Misc. Things

Introduction to Offensive Security

Announcements

- This is the last full week of web stuff; RE starts next week
  - Grab binja if you haven't already
  - Or the IDA freeware version
- Start looking for CTFs to play!
  - Email writeup to me and/or the TA within 1 week of the CTF
  - If it looks good, we'll give you a flag for the newly created one point "CTF Writeup" challenge
  - *Don't leave this until the last minute!!*

Errata

- MySQL's SUBSTR actually starts at index 1
  - `SELECT IF(SUBSTR(name, 1, 1) = 'A', SLEEP(1), 0);`
  - However `OFFSET n` still starts at 0
  - Who needs consistency in their database anyways…
- String comparisons against INFORMATION_SCHEMA.SCHEMATA and INFORMATION_SCHEMA.TABLES are case sensitive
  - Most of the time
  - Depends on the underlying filesystem

Errata

- Not mentioned, but if you want to leak result from GROUP_CONCAT:
  - `SELECT … HAVING SUBSTR(GROUP_CONCAT(name SEPARATOR ','), 1, 1) = 'a'`
  - The HAVING clause lets you filter after data has been "reduced"

Common HW Questions

- Clarifying challenge types:
  - Log Me In − Simple SQLi; bypass email and password check to log in as 'admin'
  - Log Me In Again − Blind SQLi; discover and dump another table in the DB
  - SVG Text Extractor − XXE; read the flag file at '/flag.txt'
- Some text editors are trying to format your SQL with "nice" single quotes (‘)
  - These will not work with MySQL! They need to be normal single quotes
  - Best solution is to use a text editor meant for coding
- Need a space after --
  - Common solution is to put an extra char after so nothing strips the space
  - E.g. `; -- a`

Log Me In (Again)

Log Me In (Again)

- Source code is often not given for SQL challenges
- Try to imagine what the query running server side looks like based off
  - The inputs you have
  - What a typical model for the object might look like
  - Number of columns
    - Determine by trying `UNION SELECT 1 -- , UNION SELECT 1,1 -- , UNION SELECT 1,1,1 -- …`

Log Me In (Again)

- So you were supposed to need to change the email field to regular text
  - Never trust the client!
  - But `admin'or'1'='1--@gmail.com` actually works…
- AND/OR precendence
  - AND is evaluated before OR

Log Me In (Again)

```
$hashpass = sha1($password);

SELECT id,email,password FROM users
     WHERE email='$email'
     AND password='$hashpass';
```

Nevernote CSP

- Public note app – log in to post, anyone can see all posted notes
- Vulnerable to XSS in both the title and content
  - But CSP disallows running most scripts…
  - Content-Security-Policy: script-src 'self' cdn.jsdelivr.net *.google.com; img-src *; default-src 'self'; style-src 'self' cdn.jsdelivr.net; report-uri /csp_report
- Solving:
  - How can we inject JavaScript that will run despite the CSP?
  - How can we get the admin to visit a page with our injected XSS?
  - What should we inject to leak the flag somewhere we can see it?

SVG Text Extractor

- A simple webapp that extracts the content of <text> tags from SVG images
- SVG images are XML documents…
- So this is an XXE challenge
- The hardest part of this one is just finding a minimal, well-formed SVG that has a <text> tag
- Then just add:
  <!DOCTYPE bar [<!ENTITY foo SYSTEM "file:///flag.txt">]>
  <text> &foo; </text>