Web Pt 2

'; DROP TABLE lectures; --

Trivia

- Problems this week may be late
- Also: there's a CTF this weekend!
    - You're welcome to come (but you don't have to)
    - CIC 2101, Friday at 17:00 o'clock
        - Competition starts at 13:30, but class
    - Lots of binary problems, but some others as well
    - should probably have food?

Databases

- Most properties on the web that are interesting to attack are dynamic
  - as in, they change with user input
  - eg blogs, forums, wikis, reddit
- Most dynamic pages make use of some database
  - Generally, a relational database
  - generally, a SQL database

SQL

- *Structured Query Language*
  - make queries about particular structured data
- Basic syntax:
  - command table [arguments];
  - Command: usually INSERT, UPDATE, SELECT, REPLACE or DELETE
  - table: something like lectures
  - arguments: varies by command
  - eg:
    - SELECT * FROM 98212_students;
    - INSERT INTO foods VALUES ("bacon","tasty");

SQL

- A lot of databases store strings
- SQL "handles" strings by 'quoting!'
- many poorly written sites do something like:

```
$query  = "SELECT * FROM users WHERE
              username='" . $username . "';"
run_sql_queries($query);
```

SQL

- This is bad
  - very, very bad
- Why?

```
$username = "'; UPDATE users SET
    admin=1 WHERE username='hacker'; -- ";
```

Some mySQL nonsense

- DATABASE()
- information_schema
  - SCHEMATA
    - SCHEMA_NAME
  - TABLES
    - TABLE_NAME, TABLE_SCHEMA
  - COLUMNS
    - COLUMN_NAME, TABLE_NAME, TABLE_SCHEMA
- CONCAT(); LIMIT k,n
- mysqli_multi_query

Injection

- setting fields with "special" data that leads to executing a user-controlled query
- often involves bypassing some form of filtering or escaping
- Objective: read data you're not supposed to be able to read, or write data you shouldn't be able to write

Standard Procedure

- Check for injection
- Extract information about database format
- Extract data desired/write data desired

Example

How do you remember all that?

- You don't
- you google "sql injection cheat sheet"

So... Filtering...

- People who are bad (or who run CTFs) often filter incompletely
    - strip spaces & tabs but not newlines or vertical tabs
    - disallow JOIN but not UNION
    - disallow more than one '
    - disallow "
- All of this can be worked around!
    - use abnormal whitespace
    - use "weird" keywords, or include comments mid-keyword
    - Unicode

Escaping works though right?

- Sometimes
- PHP
    - mysql_escape_string (deprecated)
    - mysql_real_escape_string (deprecated)
    - mysqli_escape_string (discouraged)
    - mysqli_real_escape_string (discouraged, secretly same as above)
    - mysqli_real_please_really_escape_string_for_real
        - not actually a thing
    - PDO::quote
- Avoid needing to do this; use prepared statements instead

Blind Injection

- SQL injection, with a catch...
- We don't get any "free" data
  - Everything has to be leaked out bit by bit.
  - And sometimes it's worse!
- For example: no data is ever shown on the page
  - How do we then extract data?

Badness

- Effects of SQL injection
  - You might be able to write files
    - SELECT ... INTO OUTFILE ...
    - combined with a file inclusion bug or a poor setup, this can be deadly
  - You may be able to destroy or tamper with data
- Effects of remote code execution
  - all of the above
  - plus you can (often) take full control of the machine

Command Injection

- Similar to SQL injection, but...
- Command line or code instead of SQL
- eg:
  - exec("mv userfile.txt $uservariable")
- Not as common, but *even deadlier*
  - note: usually you only get the web user's privs

Remote File Inclusion

- a lot of software projects use "modules" the same way C does
  - as in... they don't, really
  - they just have an include system
- Can we get them to include a user-controlled file?
  - If we can, how?
- Example (actually "paste" from pCTF 2012)

Misc

- This week's problems should be up on Friday
- Next week will probably be an assembly "refresher"
- If you:
    - haven't taken 213 AND
    - are not currently taking 213, come talk to me for a second
- We will probably focus on x86 (not x86_64)
- Getting into our favorite topics