Pwning Web Backends

PWNY B-I-G-O

sigpwny{not_bigo_notation}

2018game.picoctf.com

Team: SIGPWNY

Password: toor

HTTP

- The protocol used to communicate (the majority of) data across the web.
- Verbs:
  - **GET** - used to *get* a resource from the server
  - **POST** - used to *send* data to the server
  - Others: UPDATE, PUT, DELETE, HEAD, OPTIONS
- When you open up a website, your browser sends a ***GET*** request to the server to fetch the HTML file, and ***GET*** requests for the required Javascript and CSS files.
- When you enter data into a form on a website and hit submit, your browser sends a ***POST*** request to the server, containing the data you entered. The server can then process the data you send it.

CSRF

- Trick the user’s browser into accessing resources from another site or sending data to another site
- Example:
  - Netflix, Youtube, several big sites were vulnerable to this sort of attack
    - Server has a route to process POST /change-password
    - Attacker creates a website with a HTML form
    - Simply need to trick the user into visiting the attackers website, and clicking a button.
    - The POST request could also be automatically sent with JavaScript

XSS

- Website with dynamic content:

```
from flask import Flask
app = Flask(__name__)

@app.route('/search')
def search():
    query= request.args.get('q', '')
    return '<html><body>Search results for:'+query+':'+do_search(query)+'</body></html>
```

- What happens if we send a GET request to `/search?q=<script>alert("pwn'd");</script>`
- The result becomes:

```
<html>
  <body>
    Search results for: <script> alert("pwn'd"); </script>:
    Example Result
  </body>
</html>
```

SQL Basics

- SQL (Structured Query Language) - a language used to store, manipulate, and retrieve data from a database.
- Data is organized into tables, which have column names. Each record in the table is a row.
- `SELECT * FROM Users` --return all records from the “Users” table
- `SELECT * FROM Users WHERE username='bob'`--return all records from the “Users” table where the “name” column is bob.
- `SELECT userId FROM Users WHERE name='bob'`--return the “userId” column of all records from the “Users” table where the “name” column is “bob”.

SQL Injections

- SQL is a separate language. Other languages have to interface with it, and execute it. This often leads to some messy solutions
- Most common offender: PHP

```
mysql_connect("$host", "$username", "$password");
uname = $_POST['username'];
passwd = $_POST['password'];
$result = mysql_query("SELECT id FROM users WHERE username='"+uname+"' AND password='"+passwd+"'");
if (mysql_num_rows($result) == 1) {
  echo "Logged in!";
} else {
  echo "Incorrect!";
}
```

- What happens if we set the username to `' OR 1=1 OR ''='` ?
- Try it!: https://hack.me/102131/very-basic-sql-injection.html

SQL Injections

- Simple mistake, but extremely common and dangerous
- Most password dumps and leaks are due to SQL injection vulnerabilities
- Prevention:
  - Sanitize inputs! Use PreparedStatements for your queries.