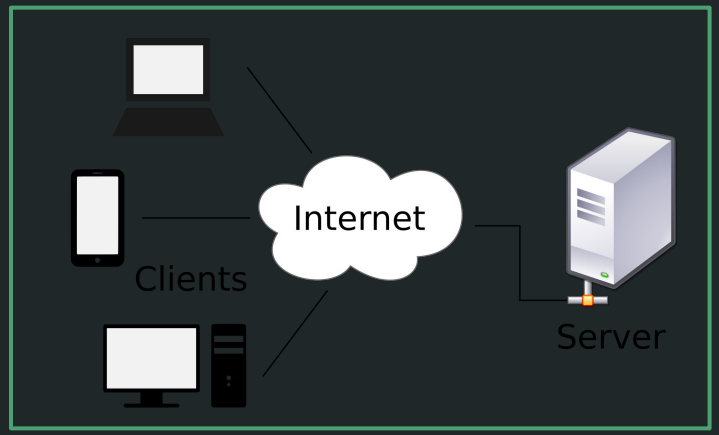
Web Application Testing

IceBear

What is a web app?

- Software that runs on a server
- Accessed over the internet via browser
- Client/server relationship
- Languages:
  - Python
  - Ruby
  - PHP
  - Node.js
  - Etc...



Example Flask app

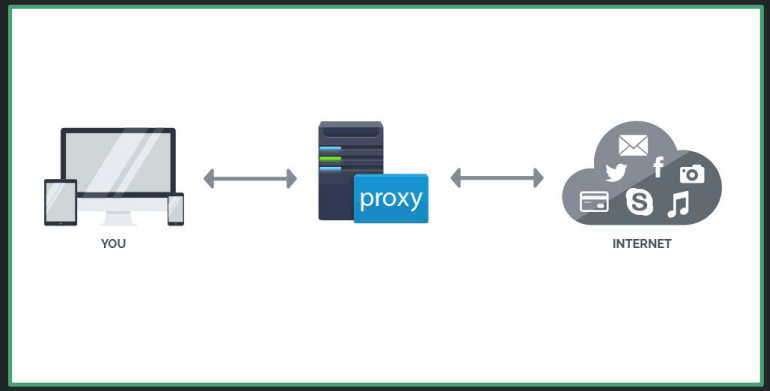
```python
@app.route('/login', methods=['GET', 'POST'])
def login():
    if request.method == 'POST':
        # Get Form Fields
        username = request.form['username']
        password = request.form['password']

        # Fetch the user from the database
        db = local_session()
        user = db.query(User).filter(User.username == username).first()
        db.close()

        if user and check_password_hash(user.password, password):
            session['logged_in'] = True
            session['username'] = username
            return redirect(url_for('index'))
```

What is a web app vulnerability?

- There are tons... and they all have cool names
  - XSS - Cross Site Scripting (blog site)
    - `<script>alert(‘1’)</script>`
  - SSTI - Server Side Template Injection
    - {{ 3 * 3 }}
  - CSRF - Cross Site Request Forgery
    - `www.mybank.com/?from=1234&to=4321&amount=99999`
  - SQLi - SQL Injection
    - `‘ or ‘1’ = ‘1`
  - XXE Injection - XML External Entity Injection
    - `<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>`
  - IDOR - Insecure Direct Object Reference
    - `/loadAccount?id=123`

Burp Suite

- All in one testing tool kit
- Proxy
  - See/edit all requests being made
- Repeater
  - Send same request with different values
- Intruder
  - Perform attacks like password spraying
- Extensive Addons
  - Autorizor
- Scope definition
  - Only analysis what you care about




```
POST /login HTTP/1.1
Host: dvwa.davidjwolfe.com:4321
Content-Length: 34
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dvwa.davidjwolfe.com:4321
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
Accept:
text/html,application/xhtml+xml,application/xml;
Referer: http://dvwa.davidjwolfe.com:4321/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

username=$admin$&password=$password123$
```

Extensions

- Open Source community
- Plugins for pretty much everything
- Requires jython?
- Autorize is my favorite
  - Test for unauthenticated pages
  - Useful on pen tests, not ctfs
  - Little complex to setup
- Logger++
  - Log everything!
  - Saves time later

Demo Time

Postman

- Easy API testing
- UI for crafting web requests
- Assign cookies
- Send JSON/Form data
- Free to use
  - https://www.postman.com/downloads/

Demo Time