CodePath

Week 4

Codepath Homework

~~Security Shepherd~~

CTF Homework (check Schedule for details)

*Burp will be **very** useful

Topics

Week 4

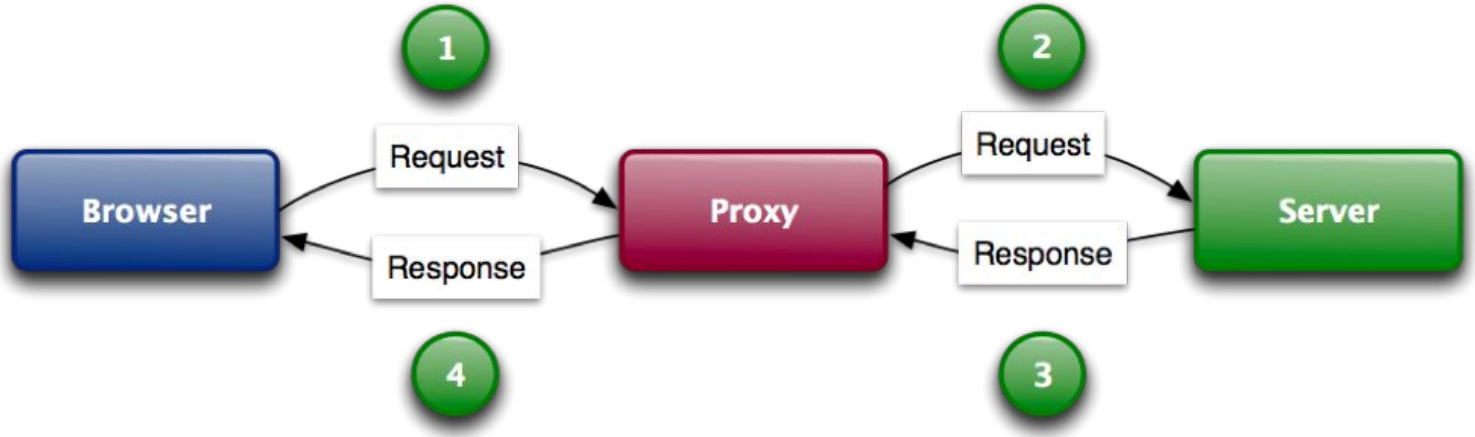
Readings on course website

- Faked Requests
- Cross-Site Request Forgery
- Cookie Theft and Manipulation
- Session Hijacking
- Session Fixation

Sessions

- Recall that cookies are small pieces of data stored on your device
- With respect to communications, it establishes a session
- Sessions act as an alternative to cookies
  - Stored in servers
  - Client sends a session ID (stored on browser as cookie)

What's the vulnerability?



Simple Example

```
<?php
 setcookie(‘user_id’, 42);
 setcookie(‘logged_in’, false);
>?
```

```
HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: user_id=42
Set-Cookie: logged_in=false
```

Session Attacks

- **Session Hijacking**
  - Steal a session ID and use in your requests
- **Session Fixation**
  - Create a session ID and plant it in your victim's browser
  - Victim authenticates with created session ID
  - Use session ID to impersonate that victim

Cross-Site Request Forgery

- An attack in which a user is tricked into performing actions on another site by inadvertently clicking a link or submitting a form
- This can lead to the compromise of Session ID’s

Cross-Site Request Forgery

- Simple attack: Trick user into making a GET (can be POST as well) request to a URL
  - View PDF

- Advanced attack: Place the URL as the image source in an image tag
  - Once the page is loaded, the request is ***automatically*** made
  - No user interaction!
  -

Prevention

- Don’t put sensitive data in cookies
- Make sure that session ID’s are long and unique
- Recall that POST requests should be used only when you want a change
- CSRF Tokens

CSRF Tokens

- Unique CSRF Token upon each session when request is made
- Upon initial authentication, check for CSRF Token and Session ID
- Once authenticated, delete CSRF Token on server so that another user cannot use that same Session ID
    - Reasons why you can’t have multiple tabs on certain websites

Lab 4

CSRF

Office Hours

Monday / Thursday : 5 - 7 PM @ Rice 226