Stealing Web Browser Cookies

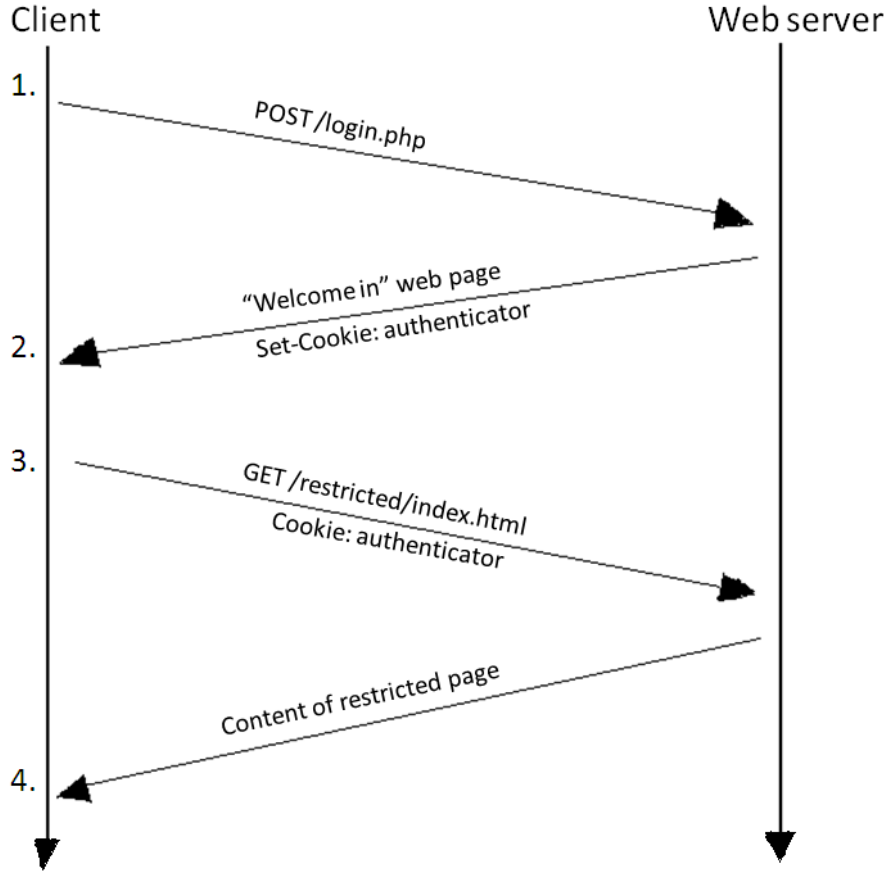
ben-holland.com

What’s a cookie?

Web 2.0 – Cookies provide state

Examples:

- Items in shopping cart
- Authentication!



Cookies ≥ Passwords!

- Username + Password = Cookie
- If I know your authentication cookie value I don’t need your password!
- Sometimes cookies don’t expire for a really long time…

How can I get your cookies?

- Packet sniffing (wiretapping)
  - Wired networks
  - Wireless networks
    - (IASTATE vs eduroam)
  - HTTP vs. HTTPS
  - https://www.cookiecadger.com/
  - https://github.com/benjholla/tssk

How can I get your cookies?

- XSS (Cross Site Scripting) Attacks
  - How about you just send me your cookies…
  - HTTP Only Flag

How can I get your cookies?

- Client Side Attacks
  - Browsers store cookies in a file…
  - https://github.com/benjholla/CookieMonster