Cross-Site Request Forgery (Sea-Surf)

Wrapping up XSS:

mitigations? Browser features (XSS Auditor)
escaping / validation / sanitization
“Content-Security-Policy” (CSP)

CSP: header sent by server
enforced by browser

Ex: Content-Security-Policy: script-src ‘none’
disable scripts

CSRF motivating example:

```
<form method="GET">
  <input name="stock" />
  <input name="amount" />
  <input type="submit" value="buy!" />
</form>
```

When pressing button, browser does GET request

GET /buy-stock?stock=GOOG&amount=10000

Server should:
sanitize input before including in output
test for legit values
authenticate user (via session cookies)
Did user intend to make this GET request?

Ways in which user may not have intended this req.
- redirect from bad guy’s website
- include `<img src="../buy-stock?....."/>

makes browser send GET request
(result is not image, so [?I displayed)
cookies for this domain will be sent!

**CSRF attack:** (cwe 352)

**Countermeasures:**
- use POST instead of GET
  - won't fix everything!