Security Playbook

K. Scott Allen

@OdeToCode

Cookies and Tokens

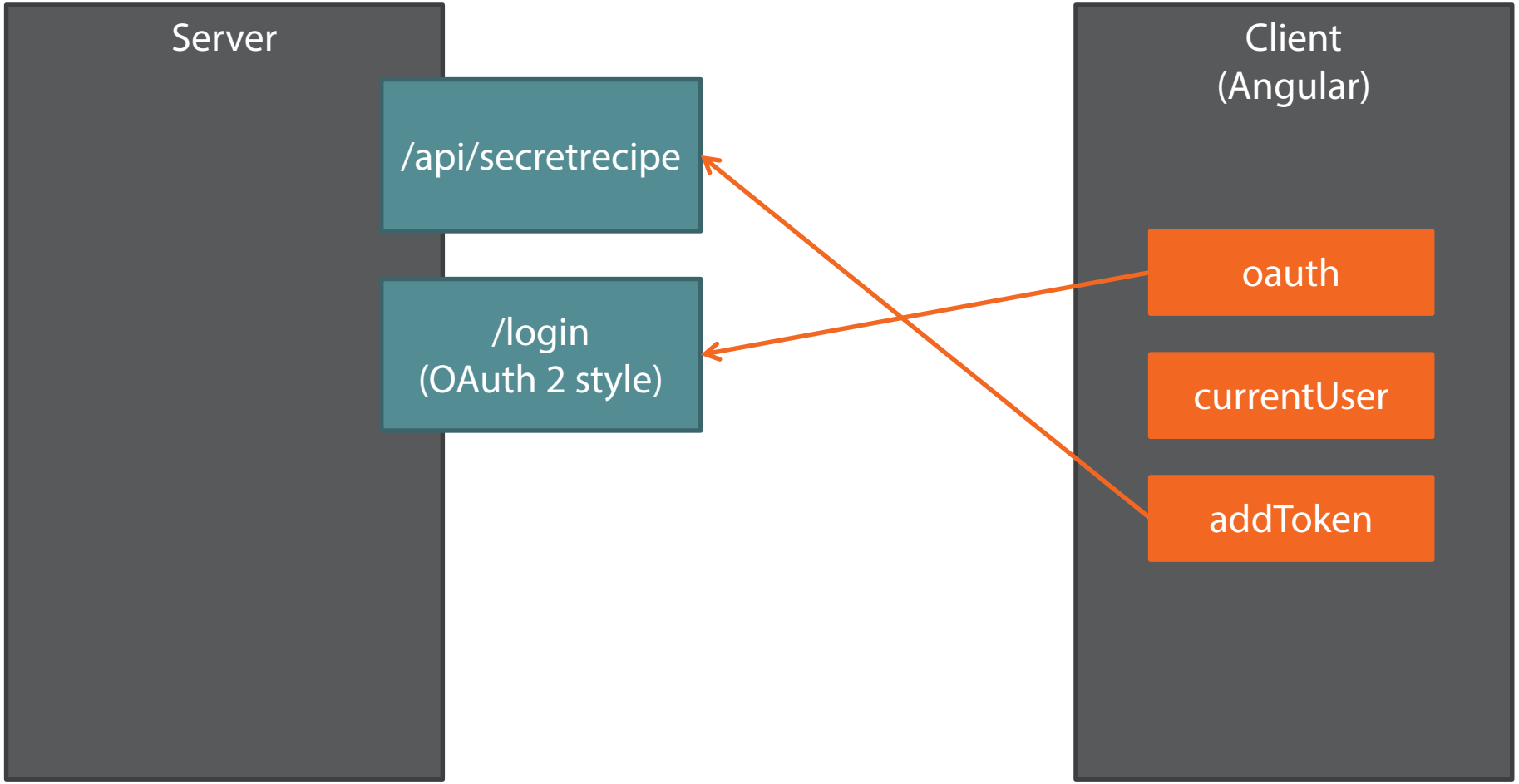
Cookies

- Sent with every request
- Susceptible to CSRF
- Difficult to use across domains

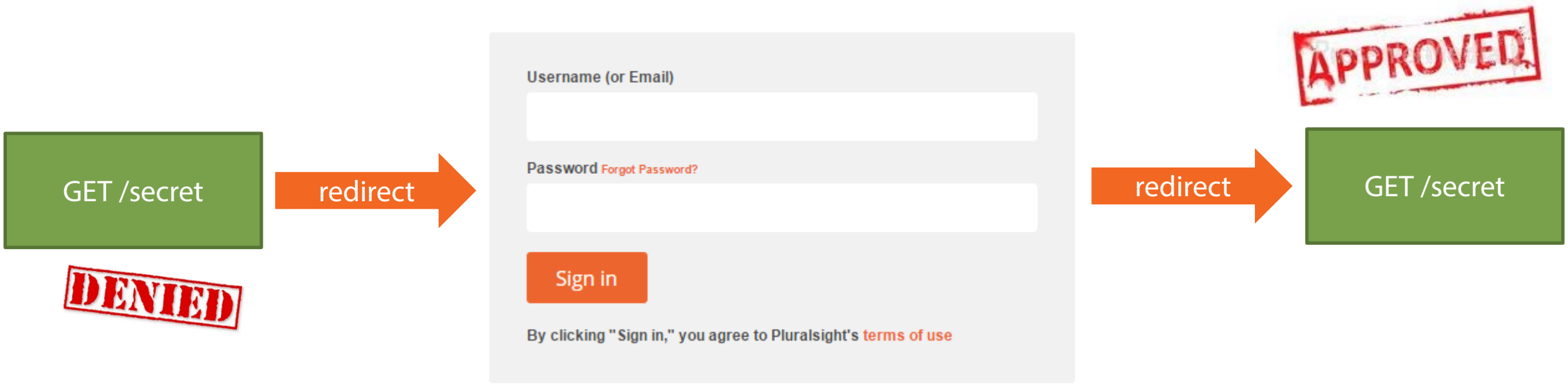
Tokens

- Offer more control, no forgeries
- Work across domains
- Require more code

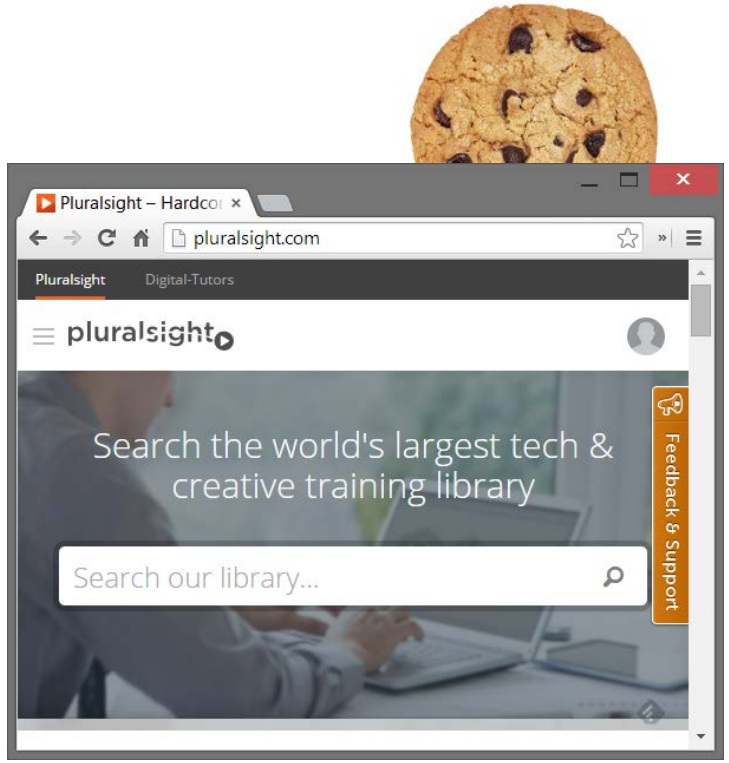
Overview



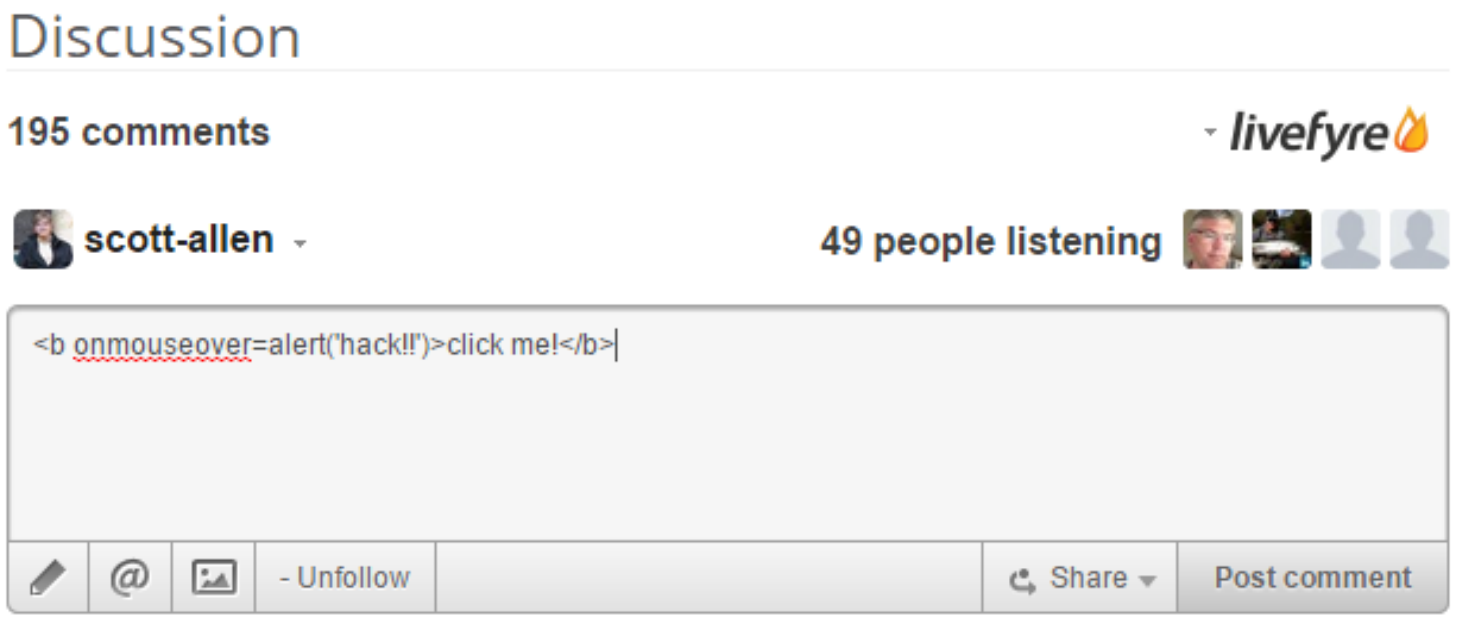
Logins and Redirects



Managing Tokens



Angular and XSS



Sanitization

$sce

- Strict Contextual Escaping
  - Secures ng-bind-html, ng-href, ng-include
  - Use to create trusted objects

To Summarize …