

Security Playbook



K. Scott Allen

@OdeToCode

Cookies and Tokens

Cookies



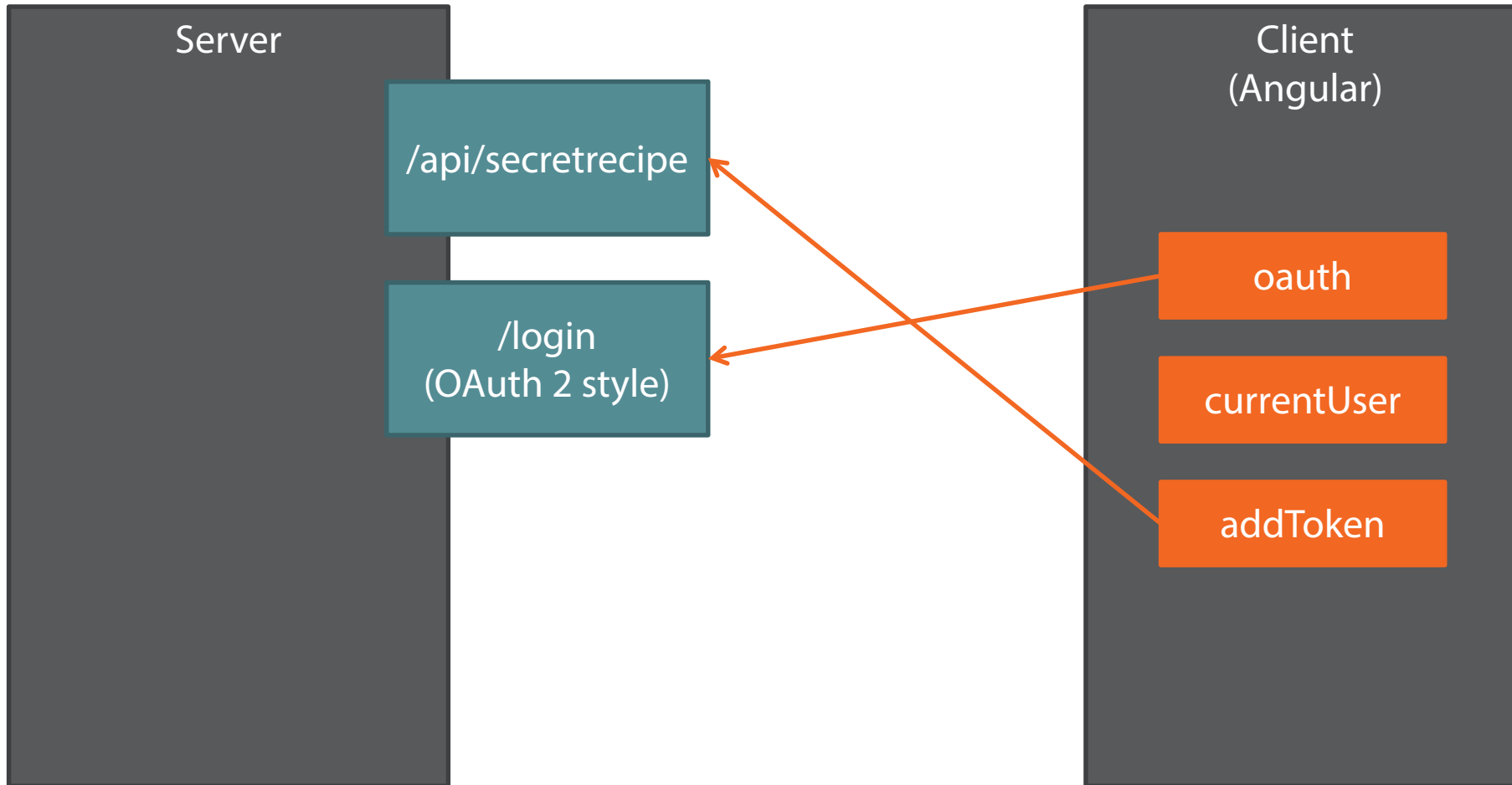
- Sent with every request
- Susceptible to CSRF
- Difficult to use across domains

Tokens

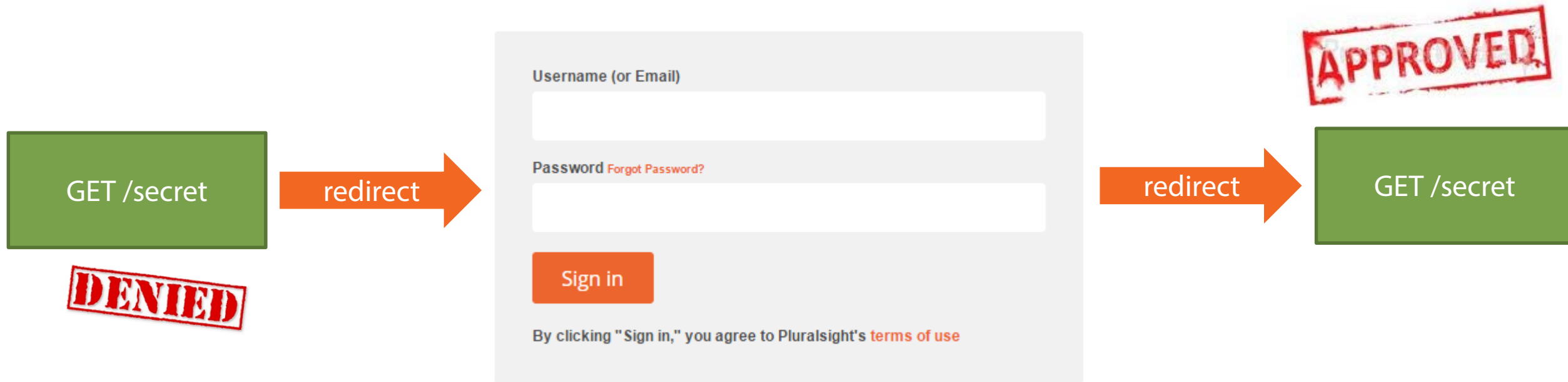


- Offer more control, no forgeries
- Work across domains
- Require more code

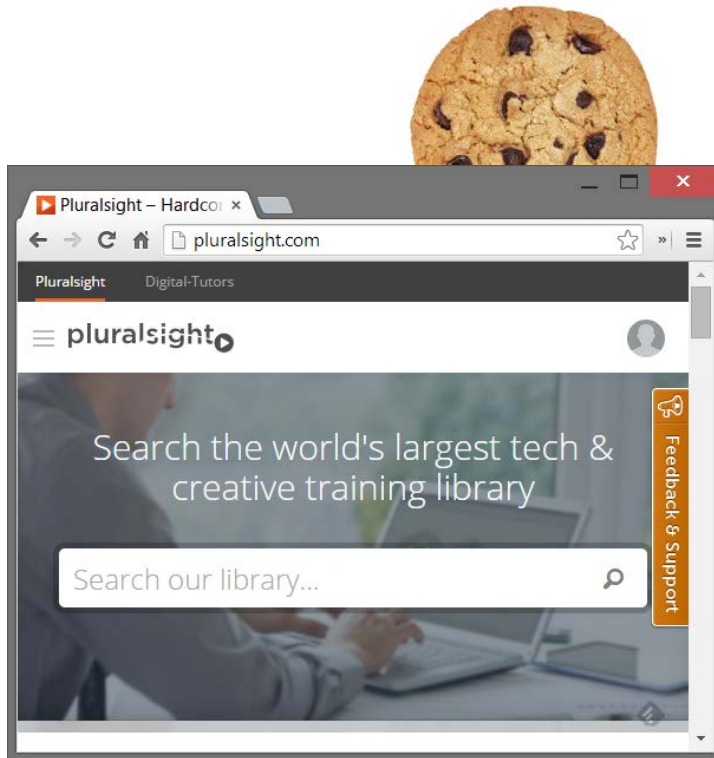
Overview



Logins and Redirects



Managing Tokens



Angular and XSS

Discussion

195 comments

livefyre 🔥



scott-allen ▾

49 people listening



`<b onmouseover=alert('hack!!')>click me!`|



- Unfollow

Share ▾

Post comment

Sanitization



\$sce

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

A yellow rectangular sign with a black border and rounded corners. The word "CAUTION" is written in bold, black, uppercase letters in the center.

CAUTION

A light gray rectangular area with the word "TRUST" in the center. The word is in a bold, green, sans-serif font and has a reflection effect below it.

TRUST

To Summarize ...

