The Need For a Coherent Web Security Policy Framework

Or

Why Frankenstein's Monster Can't Rule The Wild West

Jeff Hodges
Andy Steingruebl
The Current State of the Web

- Current system has evolved rather than been designed
Web Apps' vulnerabilities / attacks

- Cross-Site-Request Forgery (CSRF)
- Content-sniffing cross-site-scripting (XSS)
- Attacks against browsers supporting anti-XSS policies
- Clickjacking
- Malvertising
- man-in-the-middle (MITM) attacks against “secure” sites
Current Security Policies Sprinkled All Over the Web

- **HTTP Headers**
  - Strict-Transport-Security
  - No-Sniff
  - X-Frame-Options

- **Cookies**
  - Secure, HTTPOnly

- **Meta Tags**
  - Content-Type
We’d Rather Have This

http://upload.wikimedia.org/wikipedia/commons/3/33/Golden_gate2-2.jpg
We Need A Policy Framework

• The right way to set policy is via *configurable* declaration, **not** (hard) code

• Current policy mechanisms require every developer to do the right thing every time. *(This is the wrong way to do it)*
  – Set Secure and HTTPOnly Flag on Cookies
  – Set Content-Encoding
  – Set Scheme to HTTPS for all links
We aren't Innocent

The authors of this preso helped create
Strict-Transport-Security

.... *Behind our shining armour of righteous indignation lurks a convicted and only half-repentant sinner ....*

- Jane Harrison
Individual I-Ds in IETF – hasmat wg?

- HSTS – HTTP Strict Transport Security
  - draft-hodges-strict-transport-sec

- Origin definition and explicit header
  - draft-abarth-origin

- Content sniffing rules
  - draft-abarth-mime-sniff
Work in W3C

• Creation of “Web Application Security WG” is proposed
  • Draft Charter circulating
  • Sent to hasmat@ list by Thomas Roessler

• CORS and UMP
  • Cross Origin Resource Sharing
  • Unified Messaging

• CSP – Content Security Policy
  • Developed by Mozilla folk
  • In Firefox 4
Questions?

Jeff.Hodges@paypal.com
asteingruenbl@paypal.com