Web Security

Selection from OWASP App Sec EU 2013

What You Get

- A few personal highlights from App Sec EU 2013
  - key notes, hackpra, …
- Application independent security
  - HTTP Header
  - Short rating pros & cons
- Links to further information

OWASP.org

Open Web Application Security Project

Personal Highlights

- Angela Sasse :: Busting The Myth of Dancing Pigs: Angela's Top 10 list of reasons why users bypass security measures
- Michele Orrù :: HackPra Allstars -- Rooting Your Internals
- Paul Stone :: HackPra Allstars -- Browser Timing Attacks
- Thomas Roessler :: Secure all the things: fiction from the Web's immediate future
- David Ross :: Insane in the IFRAME
- Sebastian Lekies, Martin Johns :: Clickjacking Protection Under Non-trivial Circumstances

Application Independent Security
What works?

add protection within the infrastructure

HOW & WHERE

- Pinning (Meta) Information
  - Time, Location & Scope
  - Errors within spec & implementation
- HTTP Header
  - Can be manipulated too
    - Header Injection, etc.
  - First Contact Issues

HTTP Header

- Content Security Policy (CSP/CSP1.1)
- X-XSS-Protection
- HTTP Strict Transport Security (HSTS)
- X-Frame-Options
- X-Content-Type-Options
- Public-Key-Pins (Draft)
- (Access-Control-Allow-Origin)

CSP

- Content-Security-Policy
- Heavy Impact
- Spec Issues in 1.0 -> 1.1 in pipeline
- start with: Content-Security-Policy-Report-Only

X-XSS-Protection

- All modern browsers / releases support it
- raises the bar
- even if far from perfect yet

HSTS

- Protocol layer, RFC 6797
- Only for https based sites / subdomains
  - everything is https - isn’t it?
- Current Support: FF + Chrome + Andriod 4.4+
- First Contact
  - Prefetchlist: http://dev.chromium.org/sts

HSTS Prefetch

```
467     // Force HTTPS for sites that have requested it.
468     { "name": "www.paypal.com", "mode": "force-https" },
469     { "name": "paypal.com", "mode": "force-https" },
470     { "name": "www.elanex.biz", "mode": "force-https" },
471     { "name": "jottit.com", "include_subdomains": true, "mode": "force-https" },
472     { "name": "sunshinepress.org", "include_subdomains": true, "mode": "force-https" },
473     { "name": "www.noisebridge.net", "mode": "force-https" },
474     { "name": "neg9.org", "mode": "force-https" },
475     { "name": "riseup.net", "include_subdomains": true, "mode": "force-https" },
476     { "name": "factor.cc", "mode": "force-https" },
477     { "name": "members.mayfirst.org", "include_subdomains": true, "mode": "force-https" },
478     { "name": "support.mayfirst.org", "include_subdomains": true, "mode": "force-https" },
479     { "name": "id.mayfirst.org", "include_subdomains": true, "mode": "force-https" },
480     { "name": "lists.mayfirst.org", "include_subdomains": true, "mode": "force-https" },
481     { "name": "webmail.mayfirst.org", "include_subdomains": true, "mode": "force-https" },
482     { "name": "roundcube.mayfirst.org", "include_subdomains": true, "mode": "force-https" },
483     { "name": "aladdinschools.appspot.com", "mode": "force-https" },
484     { "name": "ottospora.nl", "include_subdomains": true, "mode": "force-https" },
485     { "name": "www.paycheckrecords.com", "mode": "force-https" },
486     { "name": "lastpass.com", "mode": "force-https" },
487     { "name": "www.lastpass.com", "mode": "force-https" },
488     { "name": "keyerror.com", "include_subdomains": true, "mode": "force-https" },
489     { "name": "entropia.de", "mode": "force-https" },
490     { "name": "www.entropia.de", "mode": "force-https" },
491     { "name": "romab.com", "include_subdomains": true, "mode": "force-https" },
```

X-Frame-Options

- No JavaScript required
- Framebusting JS isn’t easy
- Will be included within CSP 1.1

X-Content-Type-Options

- protects agains some drive by issues
- reduces cross site scripting issues
- don’t guess ‘my’ content

Public Key Pins

- Cache hashed public key information
- Reporting Options
- Limit CA issues
- First Contact (HSTS)

Don’t become lazy!

Stay Tuned!

References

- App Sec EU 2013
  - https://www.owasp.org/index.php/AppSecEU2013
- HTTP security related header
  - https://www.owasp.org/index.php/List_of_useful_HTTP_headers
  - http://www.ibuildings.com/blog/2013/03/4-http-security-headers-you-should-always-be-using
  - http://recxltd.blogspot.com/2012/03/seven-web-server-http-headers-that.html
  - http://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
  - http://caniuse.com/#feat=contentsecuritypolicy
  - http://lzone.de/How-Common-Are-HTTP-Security-Headers

Contact

- twitter :: @ektoplant
- e-mail :: dalini@entropia.de
-