Secure HTTP Headers

Akash Mahajan

c0c0n 2011

Agenda

- Programmers should know about the new HTTP response headers
- Web security testers should be testing for these response headers as defenses
- All you Facebook/Google+ users should be aware of these as well

Overview of the Talk

- Cover ~~all~~ some of the new HTTP response headers
- Cover which attacks are mitigated by using these headers
- Build an case for upgrading to IE8/9, Firefox 5+ or Chrome if that is your type

HTTP Response Headers

- X-Frame-Options
- X-XSS-Protection
- X-Content-Type-Options
- X-Content-Security-Policy
- Set-Cookie
  - Secure
  - HttpOnly

X-Frame-Options

- Used to prevent Clickjacking
- Doesn’t allow page to be rendered in a frame
- DENY : Don’t render at all if inside a frame, SAMEORIGIN : Only if being served from the origin
- IE8+, FF4+, Chrome5+

X-XSS-Protection

- Used to prevent reflected XSS
- Doesn’t allow the page to be rendered if a reflected XSS attack is detected
- 0 is off, 1 is on, Additional mode = block
- IE8+, Chrome, No FF (use noscript)

X-Content-Type-Options

- Used to prevent mime based attacks.
- Browser will not try to figure out content type if not sent to it in the response header
  - An image uploading site with script code is bad
- X-Content-Type-Options: nosniff
- IE8+

X-Content-Security-Policy: policy

- Used to define a whitelist of domains and actions which are allowed.
- Example usage
  - ***X-Content-Security-Policy:***
    allow 'self';
    img-src *;
    object-src media1.com media2.com;
    script-src userscripts.example.com;
    allow https://payments.example.com
- FF4+

Set-Cookie with Secure and HTTPOnly

- With Secure keyword
  - Only allow cookie to travel with a secure connection
  - An attack where HTTP and HTTPs is mixed
- With HTTPOnly keyword
  - Scripts can't read the cookie
  - Any attack where session cookie is stolen
- IE7+, Chrome12+, FF3+

Compatibility with browsers

Headers / Browsers	MS Internet Explorer	Google Chrome	Mozilla Firefox
X-Frame-Options	YES	YES	YES
X-XSS-Protection	YES	YES	NO
X-Content-Type-Options	YES	NO	NO
X-Content-Security-Policy	NO	NO	YES
Set-Cookie Secure HttpOnly	YES	YES	YES

This slide needs a lot more work. Specific versions, more browsers.

A logical argument for upgrading IE

- A ten year old browser (IE6) just can't keep up with the advanced web application attacks against users. The new crop of browsers are proactively adding support to stop the attacks at the browser level itself.

- Microsoft runs a http://ie6countdown.com with a mission of *moving the world off Internet Explorer 6*

Revisiting the attacks and headers

- X-Frame-Options
  - Especially useful against clickjacking
- X-XSS-Protection
  - Refelected XSS
- X-Content-Type-Options
  - Mime attacks for executing malicious scripts

Revisiting the attacks and headers

- Set-Cookie
  - Secure
    - No sniffing of user session cookie
  - HttpOnly
    - Not allowing javascript to read the session cookie
- X-Content-Security-Policy
  - Whitelisting of content domains for including in the page

My info while I answer your questions

Akash Mahajan

That Web Application Security Guy

–Web Application Security Consultant

–null Co-Founder, Bangalore Chapter Lead

–Certified Ethical Hacker

@makash | http://akashm.com | akashmahajan@gmail.com | 9980527182