WMF Application Security Training
Fall 2018 - Fundraising Tech

Who am I?

Scott Bassett - new Application Security Engineer

security@ is your friend!

WIKIMEDIA
FOUNDATION

“Security is a process not a destination.”

—csteipp
(and probably many others)

<https://commons.wikimedia.org/wiki/File:MediaWiki_Security.ogv>

The Basics

1. OWASP Top 10
   a. <https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project>
   b. Still updated every 3 years or so - current version: 2017.
   c. Also: controversy (rc1 A7: Insufficient Attack Prevention, WAF) <http://phpa.me/owasp-list-1456>
2. CWE/SANS Top 25
   a. <https://cwe.mitre.org/top25/> (though ~700 CWEs total)
   b. Not updated since 2011, full db still updated, ver 3.1 3/2018: <https://cwe.mitre.org/data/>
   c. Broader list than OWASP Top 10, content still relevant.
   d. Mapping to OWASP Top 10: <https://cwe.mitre.org/data/definitions/1026.html>
   e. Also: CAPEC <http://capec.mitre.org/data/definitions/1000.html>
3. Martinfowler.com
   a. <https://martinfowler.com/articles/web-security-basics.html>

Tools

1. FLOSS-y
    a. DAST: Burp CE, Zap, Arachni, Wapiti, Nikto, Gauntlt, SQLMap, Browser Plugins
    b. SAST: <https://github.com/mre/awesome-static-analysis>
    c. WMF CI: Security-Check, Phan, Phan-Taint-Check-Plugin
    d. Online: <ssllabs.com/ssltest/>, <securityheaders.net>
    e. Caveats: maintenance and code quality.

2. Not-so-FLOSS
    a. <https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools>
    b. Most commercial black-box scanning tools tend to just be giant, expensive filters.

The Security Team's View

1. Our Security Review Process
    a. CSP update - report-only every wiki, logged-in users. More to come.
    b. We are always open to questions - email security@ or find us on IRC.
    c. We have documentation!
    d. <https://www.mediawiki.org/wiki/Wikimedia_Security_Team/Security_reviews>
    e. <https://www.mediawiki.org/wiki/Security_checklist_for_developers>
    f. <https://www.mediawiki.org/wiki/Wikimedia_Security_Team/Security_reviews/What_we_are_looking_for>
    g. <https://www.mediawiki.org/wiki/Manual:MediaWiki_Security_Guide>
    h. <https://www.mediawiki.org/wiki/Phan-taint-check-plugin>
        i. Older version for CentralNotice?
    i. <https://www.mediawiki.org/wiki/Wikimedia_Security_Team/Prioritization_of_bugs>
        i. In process of updating under Risk Management.

WIKIMEDIA
FOUNDATION

Spot the Vulnerability!

1. Demo 1!
2. Demo 2!
3. Demo 3!

<https://github.com/sbassett29/Application-Security-Training>

WIKIMEDIA
FOUNDATION

Thanks - Questions?