

Web 2.0 Security

Scott MacVicar

Who am I?

- Employed by Jelsoft (vBulletin)
- LibGD
- PHP Developer

Web 2.0

- Non Static
- User Orientated
- Buzzwords?

Vulnerabilities

- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- SQL Injection
- Remote Code Execution

XSS

- Insert HTML on page
- Bypass Browser Same Origin Policy
- Types
 - Non Persistent
 - Persistent

XSS Goals

- Embarrassment
- Site Defacement
- Cache Poisoning
- Session Takeover
- Password Theft

XSS Attack Vectors

- Unverified / Unexpected Input
- UTF-7 Encoding
- RSS Feed Injection
- Data URI Scheme (*Protocol*)
- File Upload and IE

Cross Site Request Forgery

- Similar to XSS
- Exploits user / site trust
- Unauthenticated Commands

SQL Injection

- Arbitrary Data Retrieval
- Data Manipulation
- Denial of Service

SQL Injection Solutions

- Escaping
 - `escape_string / DBL::quote`
 - unquoted integers can't be escaped
 - character set escaping
- Prepared Statements
- Stored Procedures

Remote Code Execution

- Unescaped Shell Commands
- Calls to `eval()`
- Library loading

Sessions

- HTTP lacks state
- Potential Exploits
 - Session Hijacking
 - Session Fixation

Miscellaneous

- Sensitive Data Storage
- Brute Force Attacks
- Information Disclosure
- Denial of Service / Unoptimised Code

High Profile Attacks

- GMail Contact List Hijack
- Flickr Cross-domain API
- MySpace Worm

Preventing Attacks

- XSS
 - Python - `cgi.escape`
 - PHP - Filter Extension
- SQL Injection - Native Escape String
- Remote Code Execution - Avoid Eval
- Update Software
- Install Suhosin if you use PHP

Input Validation

- User Input is unreliable and under no circumstances can it be trusted
 - Corrupted en route
 - Modified by user in an unintended manner
 - Intentional attempt to gain access

Testing

- Code Audit
- Cheat Sheets
- Automated Scanners

Resources

- XSS Cheat Sheet - <http://ha.ckers.org/xss.html>
- XSS Scanner - <http://springenwerk.org>
- LiveHTTP Header Viewer + Firebug
<https://addons.mozilla.org>
- Talk - <http://macvicar.net/talks/>

Questions

- Web Application Security
- PHP
- Experience with vBulletin