Top 10 Defenses for Website Security

August 2012
Jim Manico  @manicode

- VP of Security Architecture, WhiteHat Security
- 15 years of web-based, database-driven software development and analysis experience
- Over 7 years as a provider of secure developer training courses for SANS, Aspect Security and others
- Running for the OWASP Board 2013
- OWASP Connections Committee Chair
  - OWASP Podcast Series Producer/Host
  - OWASP Cheat-Sheet Series Manager
$stmt = $dbh->prepare("INSERT INTO REGISTRY (name, value) VALUES (:name, :value)");

$stmt->bindParam(':name', $name);
$stmt->bindParam(':value', $value);
SqlConnection objConnection = new SqlConnection(_ConnectionString);

objConnection.Open();
SqlCommand objCommand = new SqlCommand(
    "SELECT * FROM User WHERE Name = @Name AND Password = @Password",
    objConnection);

objCommand.Parameters.Add("@Name", NameTextBox.Text);
objCommand.Parameters.Add("@Password", PassTextBox.Text);

SqlDataReader objReader = objCommand.ExecuteReader();
String newName = request.getParameter("newName") ;
String id = request.getParameter("id");

//SQL
PreparedStatement pstmt = con.prepareStatement("UPDATE
EMPLOYEES SET NAME = ? WHERE ID = ?");
pstmt.setString(1, newName);
pstmt.setString(2, id);

//HQL
Query safeHQLQuery = session.createQuery("from Employees
where id=:empId");
safeHQLQuery.setParameter("empId", id);
# Create
Project.create!(:name => 'owasp')

# Read
Project.all(:conditions => "name = ?", name)
Project.all(:conditions => { :name => name })
Project.where("name = :name", :name => name)
Project.where(:id=> params[:id]).all

# Update
project.update_attributes(:name => 'owasp')
Query Parameterization *Fail* (Ruby)

# Create
Project.create!(:name => 'owasp')

# Read
Project.all(:conditions => "name = ?", name)
Project.all(:conditions => { :name => name })
Project.where("name = :name", :name => name)
**Project.where(:id=> params[:id]).all**

# Update
project.update_attributes(:name => 'owasp')
<cfquery name="getFirst" dataSource="cfsnippets">

    SELECT * FROM #strDatabasePrefix#_courses WHERE intCourseID = <cfqueryparam value=#intCourseID# CFSQLType="CF_SQL_INTEGER">

</cfquery>
my $sql = "INSERT INTO foo (bar, baz) VALUES (?, ?)";

my $sth = $dbh->prepare( $sql );

$sth->execute( $bar, $baz );
public bool login(string loginId, string shrPass) {
    DataClassesDataContext db = new DataClassesDataContext();
    var validUsers = from user in db.USER_PROFILE
                     where user.LOGIN_ID == loginId
                           && user.PASSWORDH == shrPass
                     select user;
    if (validUsers.Count() > 0) return true;
    return false;
}
public String hash(String password, String userSalt, int iterations)
        throws EncryptionException {
    byte[] bytes = null;
    try {
        MessageDigest digest = MessageDigest.getInstance(hashAlgorithm);
        digest.reset();
        digest.update(ESAPI.securityConfiguration().getMasterSalt());
        digest.update(userSalt.getBytes(encoding));
        digest.update(password.getBytes(encoding));

        // rehash a number of times to help strengthen weak passwords
        bytes = digest.digest();
        for (int i = 0; i < iterations; i++) {
            digest.reset();
            bytes = digest.digest(bytes);
        }
        String encoded = ESAPI.encoder().encodeForBase64(bytes,false);
        return encoded;
    } catch (Exception ex) {
        throw new EncryptionException("Internal error", "Error");
    }
}
public String hash(String password, String userSalt, int iterations)
        throws EncryptionException {
    byte[] bytes = null;
    try {
        MessageDigest digest = MessageDigest.getInstance(hashAlgorithm);
        digest.reset();
        digest.update(ESAPI.securityConfiguration().getMasterSalt());
        digest.update(userSalt.getBytes(encoding));
        digest.update(password.getBytes(encoding));

        // rehash a number of times to help strengthen weak passwords
        bytes = digest.digest();
        for (int i = 0; i < iterations; i++) {
            digest.reset();
            bytes = digest.digest(bytes);
        }

        String encoded = ESAPI.encoder().encodeForBase64(bytes, false);
        return encoded;
    } catch (Exception ex) {
        throw new EncryptionException("Internal error", "Error");
    }
}
public String hash(String password, String userSalt, int iterations) throws EncryptionException {
    byte[] bytes = null;
    try {
        MessageDigest digest = MessageDigest.getInstance(hashAlgorithm);
        digest.reset();
        digest.update(ESAPI.securityConfiguration().getMasterSalt());
        digest.update(userSalt.getBytes(encoding));
        digest.update(password.getBytes(encoding));

        // rehash a number of times to help strengthen weak passwords
        bytes = digest.digest();
        for (int i = 0; i < iterations; i++) {
            digest.reset();
            bytes = digest.digest(salts + bytes + hash(i));
        }
        String encoded = ESAPI.encoder().encodeForBase64(bytes, false);
        return encoded;
    } catch (Exception ex) {
        throw new EncryptionException("Internal error", "Error");
    }
}
Secure Password Storage

• BCRYPT
  - Really slow on purpose
  - Blowfish derived
  - Suppose you are supporting millions on concurrent logins…
  - Takes about 10 concurrent runs of BCRYPT to pin a high performance laptop CPU

• PBKDF2
  - Takes up a lot of memory
  - Suppose you are supporting millions on concurrent logins…
OWASP Password Storage Cheat Sheet
Contextual Output Encoding (XSS Defense)

- Session Hijacking
- Site Defacement
- Network Scanning
- Undermining CSRF Defenses
- Site Redirection/Phishing
- Load of Remotely Hosted Scripts
- Data Theft
- Keystroke Logging
- Attackers using XSS more frequently
## XSS Defense by Data Type and Context

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Context</th>
<th>Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>HTML Body</td>
<td>HTML Entity Encode</td>
</tr>
<tr>
<td>String</td>
<td>HTML Attribute</td>
<td>Minimal Attribute Encoding</td>
</tr>
<tr>
<td>String</td>
<td>GET Parameter</td>
<td>URL Encoding</td>
</tr>
<tr>
<td>String</td>
<td>Untrusted URL</td>
<td>URL Validation, avoid javascript: URLs, Attribute encoding, safe URL verification</td>
</tr>
<tr>
<td>String</td>
<td>CSS</td>
<td>Strict structural validation, CSS Hex encoding, good design</td>
</tr>
<tr>
<td>HTML</td>
<td>HTML Body</td>
<td>HTML Validation (JSoup, AntiSamy, HTML Sanitizer)</td>
</tr>
<tr>
<td>Any</td>
<td>DOM</td>
<td>DOM XSS Cheat Sheet</td>
</tr>
<tr>
<td>Untrusted JavaScript</td>
<td>Any</td>
<td>Sandboxing</td>
</tr>
<tr>
<td>JSON</td>
<td>Client Parse Time</td>
<td>JSON.parse() or json2.js</td>
</tr>
</tbody>
</table>

**Safe HTML Attributes include:**
align, alink, alt, bgcolor, border, cellpadding, cellspacing, class, color, cols, colspan, coords, dir, face, height, hspace, ismap, lang, marginheight, marginwidth, multiple, nohref, noresize, noshade, nowrap, ref, rel, rev, rows, rowspan, scrolling, shape, span, summary, tabindex, title, usemap, valign, value, vlink, vspace, width
HTML Attribute Context

<input type="text" name="fname" value="UNTRUSTED DATA">
HTTP GET Parameter Context

<a href="/site/search?value=UNTRUSTED%20DATA">clickme</a>
URL Context

<a href="UNTRUSTED URL">clickme</a>
<iframe src="UNTRUSTED URL"/>
<div style="width: UNTRUSTED DATA;">Selection</div>
JavaScript Variable Context

```
<script>
var currentValue='UNTRUSTED DATA';
</script>

<script>
someFunction('UNTRUSTED DATA');
</script>
```
JSON Parsing Context

`JSON.parse(UNTRUSTED JSON DATA)`
• SAFE use of JQuery
  • $('#element').text(UNTRUSTED DATA);

• UNSAFE use of JQuery
  • $('#element').html(UNTRUSTED DATA);
### Dangerous jQuery 1.7.2 Data Types

<table>
<thead>
<tr>
<th>CSS</th>
<th>Some Attribute Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTML</td>
<td>URL (Potential Redirect)</td>
</tr>
</tbody>
</table>

#### jQuery methods that directly update DOM or can execute JavaScript

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(() or jQuery())</td>
<td>.attr()</td>
</tr>
<tr>
<td>.add()</td>
<td>.css()</td>
</tr>
<tr>
<td>.after()</td>
<td>.html()</td>
</tr>
<tr>
<td>.animate()</td>
<td>.insertAfter()</td>
</tr>
<tr>
<td>.append()</td>
<td>.insertBefore()</td>
</tr>
<tr>
<td>.appendTo()</td>
<td>Note: .text() updates DOM, but is safe.</td>
</tr>
</tbody>
</table>

#### jQuery methods that accept URLs to potentially unsafe content

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>jQuery.ajax()</td>
<td>jQuery.post()</td>
</tr>
<tr>
<td>jQuery.get()</td>
<td>load()</td>
</tr>
<tr>
<td>jQuery.getScript()</td>
<td></td>
</tr>
</tbody>
</table>
JQuery Encoding with JQencoder

- Contextual encoding is a crucial technique needed to stop all types of XSS

- jncoder is a jQuery plugin that allows developers to do contextual encoding in JavaScript to stop DOM-based XSS
  

  ➔ `$('#element').encode('html', cdata);`
Best Practice: DOM-Based XSS Defense

• Untrusted data should only be treated as displayable text

• JavaScript encode and delimit untrusted data as quoted strings

• Use `document.createElement("...")`, `element.setAttribute("...","value")`, `element.appendChild(…)` etc. to build dynamic interfaces (safe attributes only)

• Avoid use of HTML rendering methods

• Make sure that any untrusted data passed to `eval()` methods is delimited with string delimiters and enclosed within a closure such as `eval(someFunction('UNTRUSTED DATA'))`;
Content Security Policy

- Anti-XSS W3C standard
- CSP 1.1 Draft 19 published August 2012
  - [https://dvcs.w3.org/hg/content-security-policy/raw-file/tip/csp-specification.dev.html](https://dvcs.w3.org/hg/content-security-policy/raw-file/tip/csp-specification.dev.html)
- Must move all inline script and style into external scripts
- Add the X-Content-Security-Policy response header to instruct the browser that CSP is in use
  - Firefox/IE10PR: X-Content-Security-Policy
  - Chrome Experimental: X-WebKit-CSP
  - Content-Security-Policy-Report-Only
- Define a policy for the site regarding loading of content
CSP By Example 1


Content may only come from its own domain:

X-Content-Security-Policy: allow 'self'
CSP By Example 2


Site allows images from anywhere, plugin content from a list of trusted media providers, and scripts only from its server:

X-Content-Security-Policy: allow 'self'; img-src *; object-src media1.com media2.com; script-src scripts.example.com
CSP By Example 3


Force HTTPS

X-Content-Security-Policy: allow https://www.site.com
CSP By Example 4


Site that loads resources from a content delivery network and does not need framed content or any plugins

**X-Content-Security-Policy:** default-src https://cdn.example.net; frame-src 'none'; object-src 'none'
OWASP Content Security Policy
Cheat Sheet
(in progress)
Cross-Site Request Forgery Tokens and Re-authentication

- **Cryptographic Tokens**
  - *Primary and most powerful defense. Randomness is your friend*

- **Require users to re-authenticate**
  - *Amazon.com does this *really* well*

- **Double-cookie submit defense**
  - *Decent defense, but not based on randomness; based on SOP*
Multi Factor Authentication

• Passwords as a single AuthN factor are DEAD!

• Mobile devices are quickly becoming the “what you have” factor

• SMS and native apps for MFA are not perfect but heavily reduce risk vs. passwords only

• Password strength and password policy can be MUCH WEAKER in the face of MFA

• If you are protecting your magic user and fireball wand with MFA (Blizzard.net) you may also wish to consider protecting your multi-billion dollar enterprise with MFA
Forgot Password Secure Design

- Require identity and security questions
  - Last name, account number, email, DOB
  - Enforce lockout policy
  - Ask one or more good security questions
    - http://www.goodsecurityquestions.com/
- Send the user a randomly generated token via out-of-band method
  - email, SMS or token
- Verify code in same Web session
  - Enforce lockout policy
- Change password
  - Enforce password policy
OWASP Forgot Password Cheat Sheet
Session Defenses

• Ensure secure session IDs
  - 20+ bytes, cryptographically random
  - Stored in HTTP Cookies
  - Cookies: Secure, HTTP Only, limited path
  - No Wildcard Domains

• Generate new session ID at login time
  - To avoid session fixation

• Session Timeout
  - Idle Timeout
  - Absolute Timeout
  - Logout Functionality
OWASP Session Management Cheat Sheet
// to prevent all framing of this content
response.addHeader("X-FRAME-OPTIONS", "DENY");

// to allow framing of this content only by this site
response.addHeader("X-FRAME-OPTIONS", "SAMEORIGIN");

// to allow framing from a specific domain
response.addHeader("X-FRAME-OPTIONS", "ALLOW-FROM X");
 Encryption in Transit (HTTPS/TLS)

- Authentication credentials and session identifiers must be encrypted in transit via HTTPS/SSL
  - Starting when the login form is rendered
  - Until logout is complete
  - CSP and HSTS can help here

- [https://www.ssllabs.com](https://www.ssllabs.com) free online assessment of public-facing server HTTPS configuration

OWASP Transport Layer Protection Cheat Sheet
Thank You

jim@owasp.org
jim.manico@whitehatsec.com