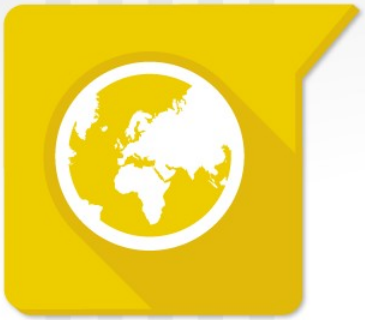

Portal Security: Guidelines to Ensure Corporate Safety

Tomáš Polešovský

Software Engineer

Agenda

- Product security
- Corporate safety
- Typical web application security issues
- Secure your Liferay deployment

Product security

Product Security

- Security is important for us
  - Standard procedures as other vendors
    - 3rd party audits of a build
    - Announcements and Hot fixes
    - How to report an issue
  - We believe in Responsible Disclosure
    - Notify the vendor before public release

Product Security

- Development process
  - Tools
  - Internal security training
  - Guidelines
  - Long term process

Corporate Safety

Corporate safety

- How to do it - apply a standard
  - Wikipedia: Cyber_Security_Standards
  - ISO/IEC 27k - Information Security Management System
  - People, systems, processes
  - Attackers, suppliers & infrastructure
  - Expensive for one portal deployment

Corporate safety

- How to start and make it in my budget?
  - Simplify and focus on important
    - Plan, Do, Check, Act (PDCA)
    - Think of people, processes, infrastructure, attackers, failures
  - Verizon's 2012 Data Breach Report (3)

    “96% of attacks were not highly difficult”

    “97% of data breaches were avoidable through simple or intermediate controls”

Typical Web Application Security Issues

Typical Web App Security Issues

- OWASP Top 10 (2010)
  - Open Web Application Security Project
  - Most frequent security issues
- CWE/SANS Top 25 (2011)
  - Common Weakness Enumeration
  - Top 25 Most Dangerous Software Errors

OWASP Top 10

- A1: Injection
  - Manipulation of input parameters
  - SQL Injection, Command Injection
  - Serving files from disk, network, etc.
- Validate and sanitize input

OWASP Top 10

- A2: Cross Site Scripting (XSS)
  - Attacker triggers action in your browser
  - Typical: attacker can steal cookies
  - Browser can be turned into weapon
- Validate output
  - Use portal HtmlUtil.escape* methods

OWASP Top 10

- A3: Broken Authentication / Session
  - User can create account, use different authentication method, etc.
  - Session is good for small things, do not use session for guest
- Turn off everything you don't need

OWASP Top 10

- A5: Cross Site Request Forgery (CSRF)
  - Calling portal URLs from untrusted site
  - Triggering actions user is not aware of

```
<img src="http://example.com/c/portal/logout"
width="0" height="0" />
```

  - Abuse user cookies
- Use Portlet Action phase for changing state
- Render phase should not change session

OWASP Top 10

- A6: Security misconfiguration
  - Have up-to-date Java frameworks
  - Do not expose sensitive information
    - Using errors in your portlets
    - Using 404/503 App. Server pages

OWASP Top 10

- A7: Insecure Cryptographic Storage
  - Encrypt passwords in DB
  - Hash with different salts
  - Don't put user credentials into log files
  - Make sure all sensitive information are safe

OWASP Top 10

- A8: Failure to restrict URL Access
  - “Security by obscurity”
  - Restrict sensitive URLs if you don't need them
    - Control Panel
    - Hidden administrative pages

OWASP Top 10

- A9: Insufficient Transport Layer Protection
  - Turn on HTTPS, always
  - Use TLS >= 1.1
  - Make your cookies secureOnly
  - Don't allow mixed content

OWASP Top 10

- A10: Unvalidated Redirects and Forwards
  - Attacker can redirect user to a malicious site (response.sendRedirect)
  - Attacker can load different JSP with your initialized context (RequestDispatcher.include/forward)
  - In some cases attacker can steal jsessionid from Referer header

CWE/SANS Top 25

- CWE-306: Missing Authentication for Critical Function
  - Make sure you secured all ways to your data
  - Leverage portal to secure your portlets, don't use Servlets in your plugins for accessing any data

CWE/SANS Top 25

- CWE-862: Missing Authorization
  - Make difference between
    - System calls – use *LocalService
    - User calls – use *Service
  - Check whether PermissionThreadLocal is initialized, otherwise assume Guest

CWE/SANS Top 25

- CWE-798: Use of Hard-coded Credentials
  - What to say – seriously, don't do it :)
  - Encrypt sensitive data
    - Use portal Encryptor class
    - Save in DB (e.g. PortalPreferences)

CWE/SANS Top 25

- CWE-250: Execution with Unnecessary Privileges
  - Configure your portal roles properly
  - Don't rely on the built-in roles unless you know what permission they have
  - Start with no permissions and iteratively add new permissions to your roles

CWE/SANS Top 25

- CWE-863: Incorrect Authorization
  - Take care when initializing PermissionThreadLocal
  - Use *LocalService only for system calls
  - Check the right permissions
    - Even for relations

Other

- Denial Of Service (DOS) leaks
  - CPU - blocking a thread on the server
  - Memory – static variables, HTTP session
  - Disk – big log files
  - DB – tons of rows in one table
- Arbitrary Code Execution
  - ScriptingUtil

Secure your Liferay

Secure your Liferay deployment

- Change the default configuration
  - Deploy only portal (no 7Cogs)
  - Change default admin login/password
  - Don't allow remote access to your production from outside

Secure your Liferay deployment

- Turn off everything you don't use
  - It's only a portal configuration
  - Remote API (servlets, JSONAction)
  - Login portlet methods & options
  - Minimize potential vulnerabilities

Secure your Liferay deployment

- Secure your URLs for public (private?) webs
  - Disable access to Control panel
  - Deny access on the web server or use a Web Application Firewall
  - Use always HTTPS (with TLS >= 1.1)

Secure your Liferay deployment

- Protect your custom plugins
  - Lessons from Liferay (I)
    - Check & sanitize input
    - Escape output – use HtmlUtil.escape*, <aui-input>, <search-container-row escapeModel=true>
    - Careful with static variables, session
    - Use AutoResetThreadLocal

Secure your Liferay deployment

- Protect your custom plugins
  - Lessons from Liferay (II)
    - Watch what you load in your RequestDispatcher, URL, File and HttpClient
    - Don't change session in render phase
    - Perform application “write action” only in portlet action phase

Secure your Liferay deployment

- Protect your custom plugins
  - Lessons from Liferay (III)
    - Don't use unauthenticated Servlets
    - *LocalService only for system calls
    - Encrypt sensitive data - Encryptor

Summary To Remember

- Simple protection is better than nothing
  - Don't use default configuration
  - Turn off everything you don't need
  - Protect your plugins

Thank you!

- Refrences

http://en.wikipedia.org/wiki/Cyber_security_standards

http://en.wikipedia.org/wiki/ISO/IEC_27000-series

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.0.pdf

https://www.owasp.org/index.php/Top_10_2010

http://cwe.mitre.org/top25/