Hardening of SAP® HTTP- and Webservices

Sebastian Schinzel
(Slides shamelessly stolen from by colleague Frederik Weidemann)
Virtual Forge GmbH
University of Mannheim
Hardening of SAP® HTTP- and Webservices

- Introduction
  - History
  - Network Landscape Overview

- Secure Configuration SAP NW ABAP
  - Services
  - What can be configured, what is programmed
  - Logging
  - Pitfalls

- SAP Web Services with ABAP
  - Overview
### OWASP Top 10 – 2010

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Injection</td>
</tr>
<tr>
<td>A2</td>
<td>Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>A3</td>
<td>Broken Authentication and Session Management</td>
</tr>
<tr>
<td>A4</td>
<td>Insecure Direct Object References</td>
</tr>
<tr>
<td>A5</td>
<td>Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>A6</td>
<td>Security Misconfiguration</td>
</tr>
<tr>
<td>A7</td>
<td>Insecure Cryptographic Storage</td>
</tr>
<tr>
<td>A8</td>
<td>Failure to Restrict URL Access</td>
</tr>
<tr>
<td>A9</td>
<td>Insufficient Transport Layer Protection</td>
</tr>
<tr>
<td>A10</td>
<td>Unvalidated Redirects and Forwards</td>
</tr>
</tbody>
</table>
## History of SAP Web App Technology

**ITS**
- Release R/3, 4.6b+

**SAP Web AS**
- ICM
- Release 6.10

**SAP NW AS ABAP**
- Replaces Web AS
Introduction SAP Landscape Setup

- Landscape should consist of at least 3 systems
  
  DEV ➔ TEST / QA ➔ PROD

- In the field: often only PROD or DEV+PROD
- But: sometimes also 4 systems (D➔T➔Q➔P)
Introduction - Network

Network Landscapes as described in the NW Security Guide

- Internet
- Outer DMZ
- Inner DMZ
- High Security Area

Application Gateways
SAP WebAS or Webservice
Backend

Intranet Clients
Protection on Network Layer (Web)

- **WebDispatcher**
  - Load Balancer
  - SSL Termination
  - URL Path whitelisting
  - Limit URL size (wdisp/max_permitted_uri_len)
  - Limit URL characters in range (wdisp/permitted_uri_char_range)

- **Other Reverse Proxies**
  - Often seen: Apache mod_security, mod_proxy
  - Other commercial vendors ...

- **Recommendation:** Reverse proxy is a must have

# Permissions

| P | /sap/bc/ |
| P | /sap/owasp/ |
| D | * |
Architecture SAP NetWeaver AS ABAP

- Architecture since release 6.10
- Integration of ICM (process) into the SAP Kernel
- ICM supports HTTP, HTTPS, SMTP, SOAP, WebDav
Secure Configuration SAP NW ABAP

■ Overview
  ‣ HTTP Standard Services
  ‣ Authentication Methods
  ‣ Protection by configuration

  ‣ Logging
  ‣ Security Audit Log
Secure Configuration SAP NW ABAP HTTP Standard Services

- Maintenance via Transaction (Tr.) SICF
- Release NW 7.01 EhP1 is delivered with deactivated services
- Older releases may need manual maintenance
  - Best practice: Deactivate ALL services and activate them individually as required
  - Avoid inherited activations
- (!) /sap/bc/soap/rfc
Secure Configuration SAP NW ABAP
HTTP Standard Services

Phishing:
Secure Configuration SAP NW ABAP
Authentication Methods

- Individual methods configurable for each ICF node
  - SSO
  - Basic Authentication
  - X.509 Client Certificates
  - Session based (only for stateful applications)
  - Anonymous logon via authentication on behalf of a hard coded user (configured by admin)

- Custom Development:
  - Use the secure standards provided by SAP

- Additional check configurable against authority object S_ICF
  (Tab Service Data → SAP Authoriz.)
Secure Configuration SAP NW ABAP
Profile Parameters

- ABAP Stack / profile parameter
- Accessed on OS level (/usr/sap/<SID>/SYS/profile) or via Transactions RZ10/RZ11
- Maintain password parameters
- Check SSL setup
- SSO Configuration
Secure Configuration SAP NW ABAP
Example Parameters

- **Password**
  - login/min_password_lng
  - login/min_password_digits
  - login/min_password_letters
  - login/min_password_specials
  - login/password_charset
  - login/min_password_diff
  - login/password_expiration_time
  - login/password_change_for_SSO
  - login/disable_password_logon
  - login/password_logon_usergroup
  - ...

- **Logon**
  - login/fails_to_session_end
  - login/fails_to_user_lock
  - login/failed_user_auto_unlock
  - login/no_automatic_user_sapstar
  - ...

- **Validity**
  - login/min_password_digits
  - login/password_max_new_valid
  - login/password_max_reset_valid

- **Others**
  - is/HTTP/show_detailed_errors
  - icm/HTTPS/verify_client
  - icm/security_log
  - ..., e.g. */HTTP/*/, icm/*

  - auth/rfc_authority_check

- **SSO**
  - login/accept_sso2_ticket
  - login/create_sso2_ticket
  - login/ticket_expiration_time
  - login/ticket_only_by_https
  - login/ticket_only_to_host
Secure Configuration SAP NW ABAP

Working with Redirects

- Example SAP URL Parameter: sap-exiturl
  Used upon exiting a stateful BSP

- Table `HTTP_WHITELIST` to maintain allowed redirect destinations (Maintenance via Tr. SE16)

- Empty table == no checks

- Example entry:
  protocol=https, host=mysite.owasp.org, port=23443, url=/sap/redirects/* (wildcard * is allowed)

- Development with ABAP:
  `CL_HTTP_UTILITY=>CHECK_HTTP_WHITELIST`
Secure Configuration SAP NW ABAP
Logging of ICM

- Tr. SMICM (Goto → HTTP Log → HTTP Server / Client)
- Deactivated by default
- Log format is equal to mod_log_config of Apache
- Log format can be customized
- Anonymizes certain parameters/header fields with dots:
  e.g. MYSAPSSO2 Cookie, jsessionid ...

Recommendation:
- Use reverse proxy logs → easier analysis
- If required, add SAPs ICM logging
  (Remember: x-forwarded-for header, parameter wdisp/
  add_xforwardedfor_header = TRUE for Web Dispatcher)
Secure Configuration SAP NW ABAP

Security Audit Log

- Inactive by default
- Enabled by rsau/enable = 1

- Maintained with Tr. SM20
- Logging of:
  - Dialog logon attempts
  - RFC logon attempts
  - RFC calls to function modules
  - Transaction starts
  - Report starts
  - Changes to the user master records
  - Changes to the audit configuration

- Caveat: Possible violation of data protection laws!
Secure Configuration SAP NW ABAP
Lessons Learned

Lessons learned:

- Log inactive by default
- Huge number of configuration possibilities
  → Complexity in Audits
  (Who maintains several hundred pages of documentation and who reads it???)
- SAP already offers a lot of functionality → Problem: you have to know about it
- SSL must be separately installed (SAPCRYPTOLIB) and activated
SAP Web Services with ABAP

- Server
  - Inside-Out
    (RFC-enabled function modules are used as a basis for generation)
  - Outside-In
    (Service Interface in ES Repository is used to generate the skeleton)

- Client

- UDDI compliant registry with NW 7.1
  (called ES Repository)

- Maintenance:
  formerly Tr. WSCONFIG + WSADMIN
  since NW 2004s SP14 Tr. SOAMANAGER
  - Redirects to WebDynpro ABAP App → Must be enabled previously
SAP Web Services with ABAP - SOAMANAGER
SAP Web Services with Custom ABAP Development - Top 3 problems

- **Typical Scenario**
  - User calls WebService
  - WebService calls a RFC in the backend
SAP Web Services with Custom ABAP Development - Top 3 problems

Most common problems

- Insufficient validation and authentication between frontend user and backend data
  - Usually backend calls are made with preconfigured high privilege accounts
  - Thus, iterating through parameters results in disclosure of data
  - → A4 - Insecure Direct Object References

- Missing encryption
  - → A6 - Security Misconfiguration
  - → A9 - Insufficient Transport Layer Protection

- Missing input validation in custom ABAP
  - → A1 - Injection
Results

- Network topology is complex
- Reverse Proxy required
- Configuration possibilities are great
- Configuration complexity is our enemy
  - Think about a lot of ICF nodes in combination with individual authority objects
  - Developers != Administrators
  - Administrators != Role Administrators
- Logging deactivated by default
- Custom Web Services are also affected by Owasp Top 10
# OWASP Top 10 – 2010

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Injection</td>
</tr>
<tr>
<td>A2</td>
<td>Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>A3</td>
<td>Broken Authentication and Session Management</td>
</tr>
<tr>
<td>A4</td>
<td>Insecure Direct Object References</td>
</tr>
<tr>
<td>A5</td>
<td>Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>A6</td>
<td>Security Misconfiguration</td>
</tr>
<tr>
<td>A7</td>
<td>Insecure Cryptographic Storage</td>
</tr>
<tr>
<td>A8</td>
<td>Failure to Restrict URL Access</td>
</tr>
<tr>
<td>A9</td>
<td>Insufficient Transport Layer Protection</td>
</tr>
<tr>
<td>A10</td>
<td>Unvalidated Redirects and Forwards</td>
</tr>
<tr>
<td>A1</td>
<td>Injection</td>
</tr>
<tr>
<td>A2</td>
<td>Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>A3</td>
<td><strong>Broken Authentication and Session Management</strong></td>
</tr>
<tr>
<td>A4</td>
<td>Insecure Direct Object References</td>
</tr>
<tr>
<td>A5</td>
<td>Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>A6</td>
<td><strong>Security Misconfiguration</strong></td>
</tr>
<tr>
<td>A7</td>
<td>Insecure Cryptographic Storage</td>
</tr>
<tr>
<td>A8</td>
<td><strong>Failure to Restrict URL Access</strong></td>
</tr>
<tr>
<td>A9</td>
<td>Insufficient Transport Layer Protection</td>
</tr>
<tr>
<td>A10</td>
<td>Unvalidated Redirects and Forwards</td>
</tr>
</tbody>
</table>
Questions ...

- Thank you for your attention

... ???
Literature

- SAP NetWeaver Security Guide (click)
- The Developer’s Guide to SAP NetWeaver Security, Martin Raepple, Galileo Press
- ABAP Cookbook, James Wood, Galileo Press
- SAP Security and Authorizations, Mario Linkies, Frank Off, Galileo Press
- ABAP Security Scanner http://www.codeprofilers.com
- DSAG ERP Security Guide
Trademarks

- SAP AG is the registered trademark holder of SAP, SAP R/3, mySAP, ABAP, NetWeaver, and other proprietary terms.