



Hardening of SAP[®] HTTP- and Webservices

Frederik Weidemann

Virtual Forge GmbH

frederik.weidemann (at) virtualforge.de

OWASP

Nürnberg 20.10.2010

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation

<http://www.owasp.org>

About me

■ Frederik Weidemann

- ▶ Senior IT-Security Consultant
- ▶ Trainer for Software Security
- ▶ Auditor and Pentester
- ▶ Co-Author of „Sichere ABAP-Programmierung“, SAP Press

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

A1	Injection
A2	Cross-Site Scripting (XSS)
A3	Broken Authentication and Session Management
A4	Insecure Direct Object References
A5	Cross-Site Request Forgery (CSRF)
A6	Security Misconfiguration
A7	Insecure Cryptographic Storage
A8	Failure to Restrict URL Access
A9	Insufficient Transport Layer Protection
A10	Unvalidated Redirects and Forwards

History of SAP Web App Technology

ITS

- Release R/3, 4.6b+

SAP Web AS

- ICM
- Release 6.10

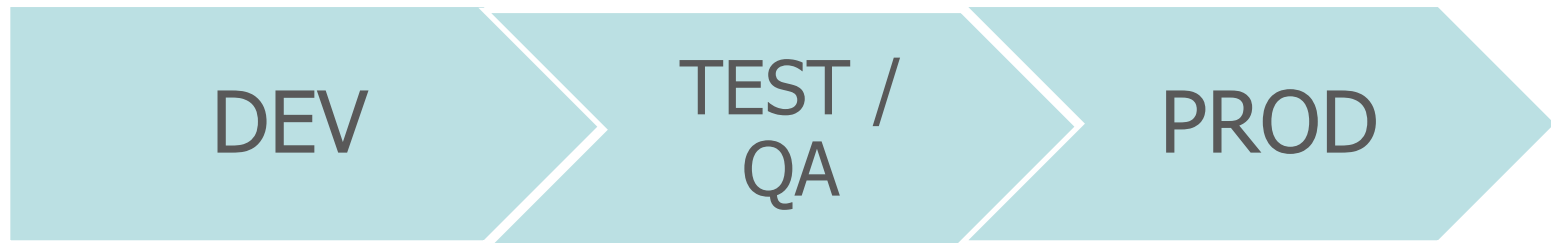
SAP NW AS ABAP

- Replaces Web AS



Introduction SAP Landscape Setup

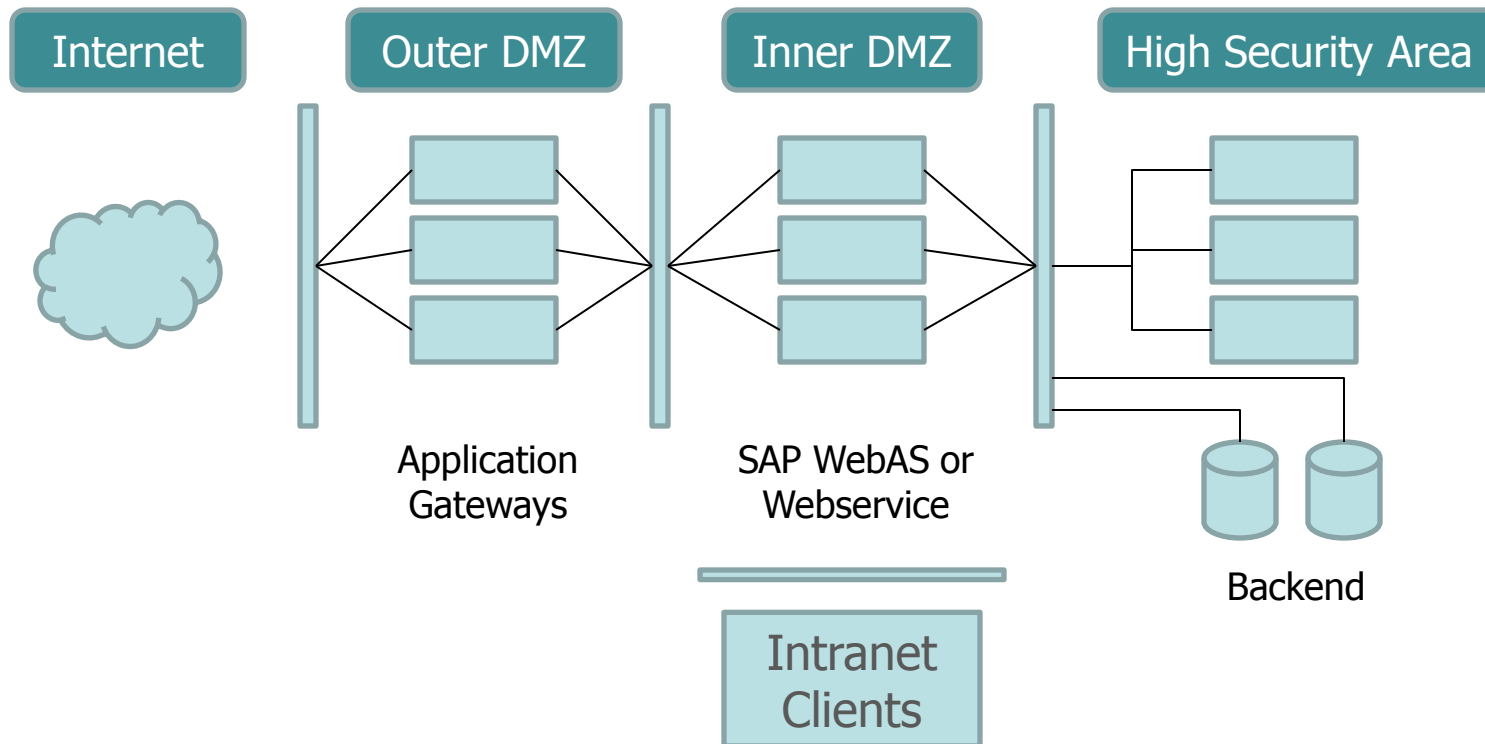
- Landscape should consist of at least 3 systems



- 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



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/permited_uri_char_range`)

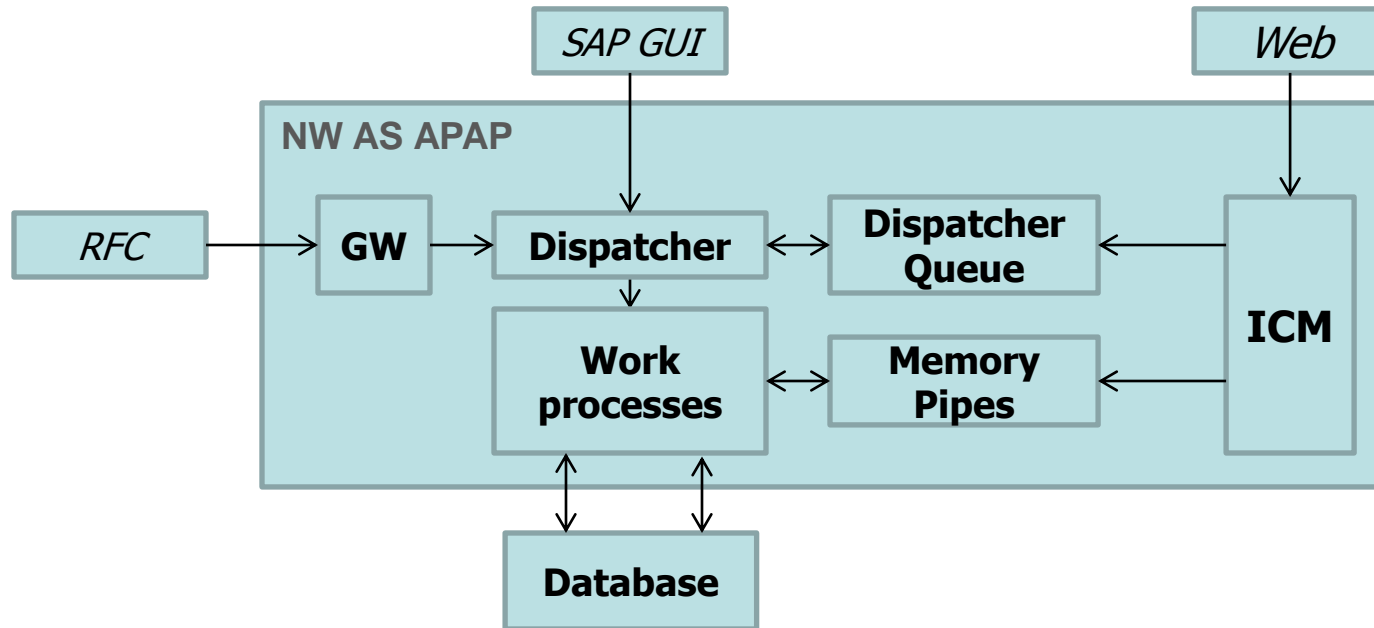
```
# Permissions
P    /sap/bc/
P    /sap/owasp/
D    *
```

■ Other Reverse Proxies

- ▶ Often seen: Apache `mod_security`, `mod_proxy`
- ▶ Other commercial vendors ...

■ Recommendation: Reverse proxy is a must have

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

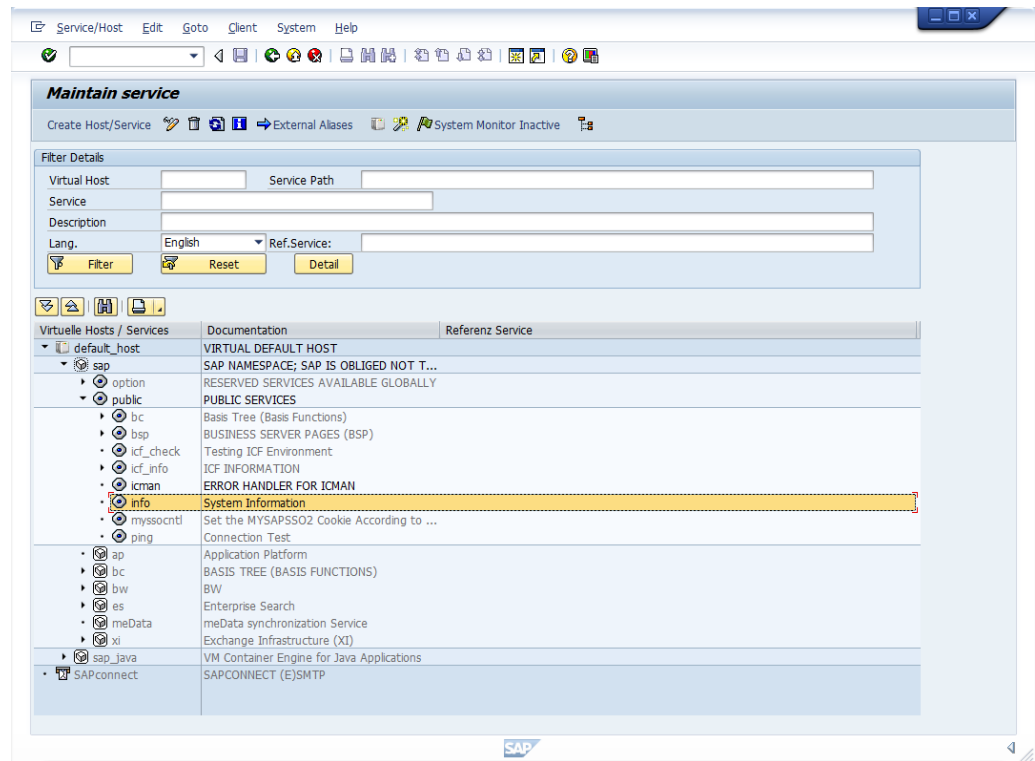
■ Overview

- ▶ 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 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 Authentication Methods

■ Admin overview ICF node

Path

Service Name System Service (Active)

Lang. [Other Languages](#)

Description

Description 1

Description 2

Description 3

Service Data Logon Data Handler List Error Pages Administration

Procedure

Use All Logon Procedures

Logon Data

Client

User

Password

Language

Password Status

Security Requirement

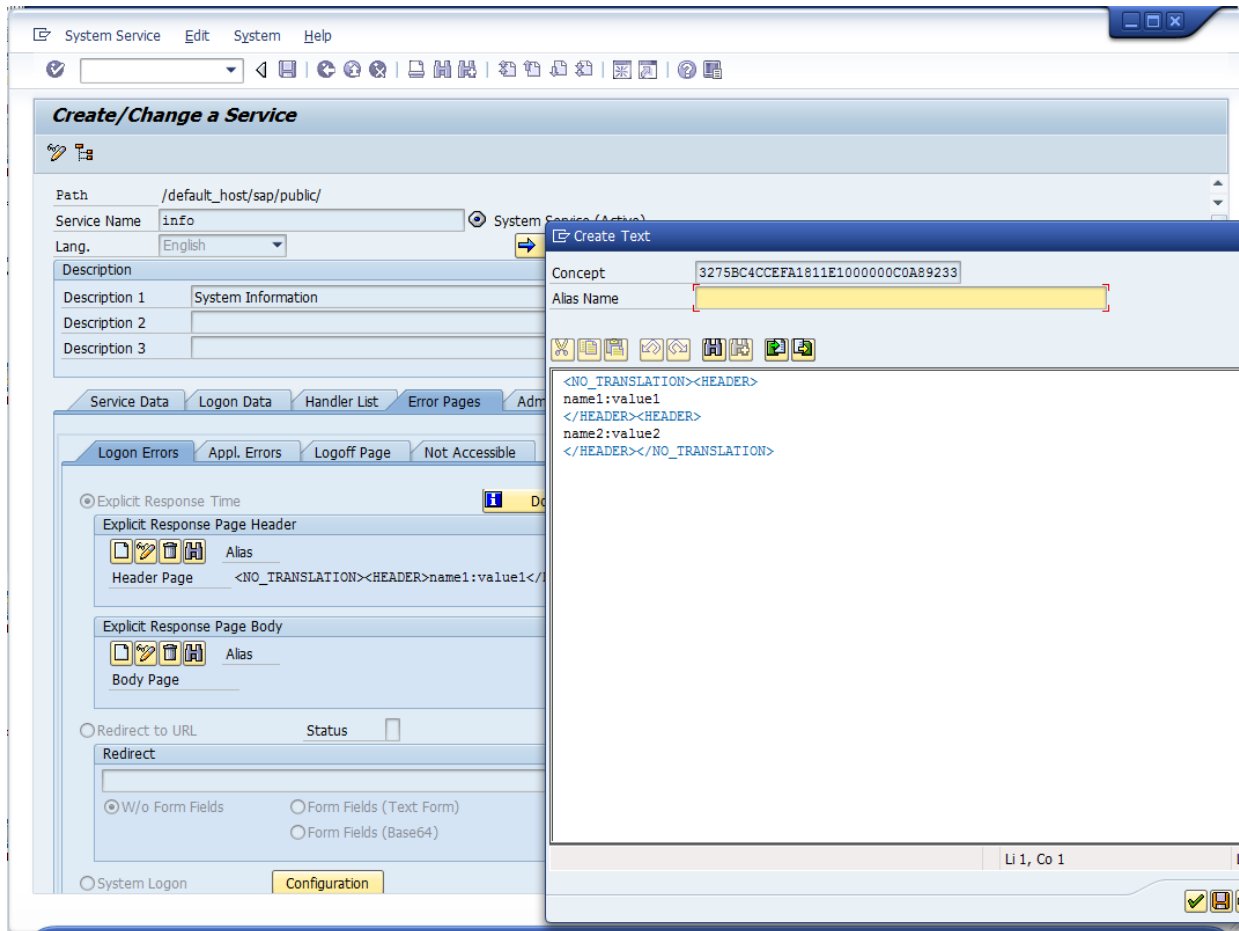
Standard SSL

Authentication

Standard SAP User Internet User

Secure Configuration SAP NW ABAP Error Handling

- Can be configured, must not be programmed



The screenshot displays the SAP System Service configuration interface. The main window is titled "Create/Change a Service" and shows the configuration for a service named "info" at the path "/default_host/sap/public/". The service is currently active. The configuration is divided into several tabs: "Service Data", "Logon Data", "Handler List", "Error Pages", and "Admin". The "Error Pages" tab is selected, and the "Logon Errors" sub-tab is active. Under "Logon Errors", the "Explicit Response Time" option is selected. The "Explicit Response Page Header" section shows a header page configuration with the text: `<NO_TRANSLATION><HEADER>name1:value1</HEADER><HEADER>`. The "Explicit Response Page Body" section shows a body page configuration with the text: `name2:value2</HEADER></NO_TRANSLATION>`. The "Redirect to URL" section is also visible, with a "Redirect" field and options for "W/o Form Fields", "Form Fields (Text Form)", and "Form Fields (Base64)". The "System Logon" section is at the bottom, with a "Configuration" button. A "Create Text" dialog box is open over the configuration, showing a "Concept" field with the value "3275BC4CCEFA1811E100000C0A89233" and an "Alias Name" field. The dialog also contains the same XML-like text seen in the configuration fields.

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
- ▶ ...

■ Others

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

■ Logon

- ▶ login/fails_to_session_end
- ▶ login/fails_to_user_lock
- ▶ login/failed_user_auto_unlock
- ▶ ...

■ Validity

- ▶ login/min_password_digits
- ▶ login/password_max_new_valid
- ▶ login/password_max_reset_valid

■ 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)

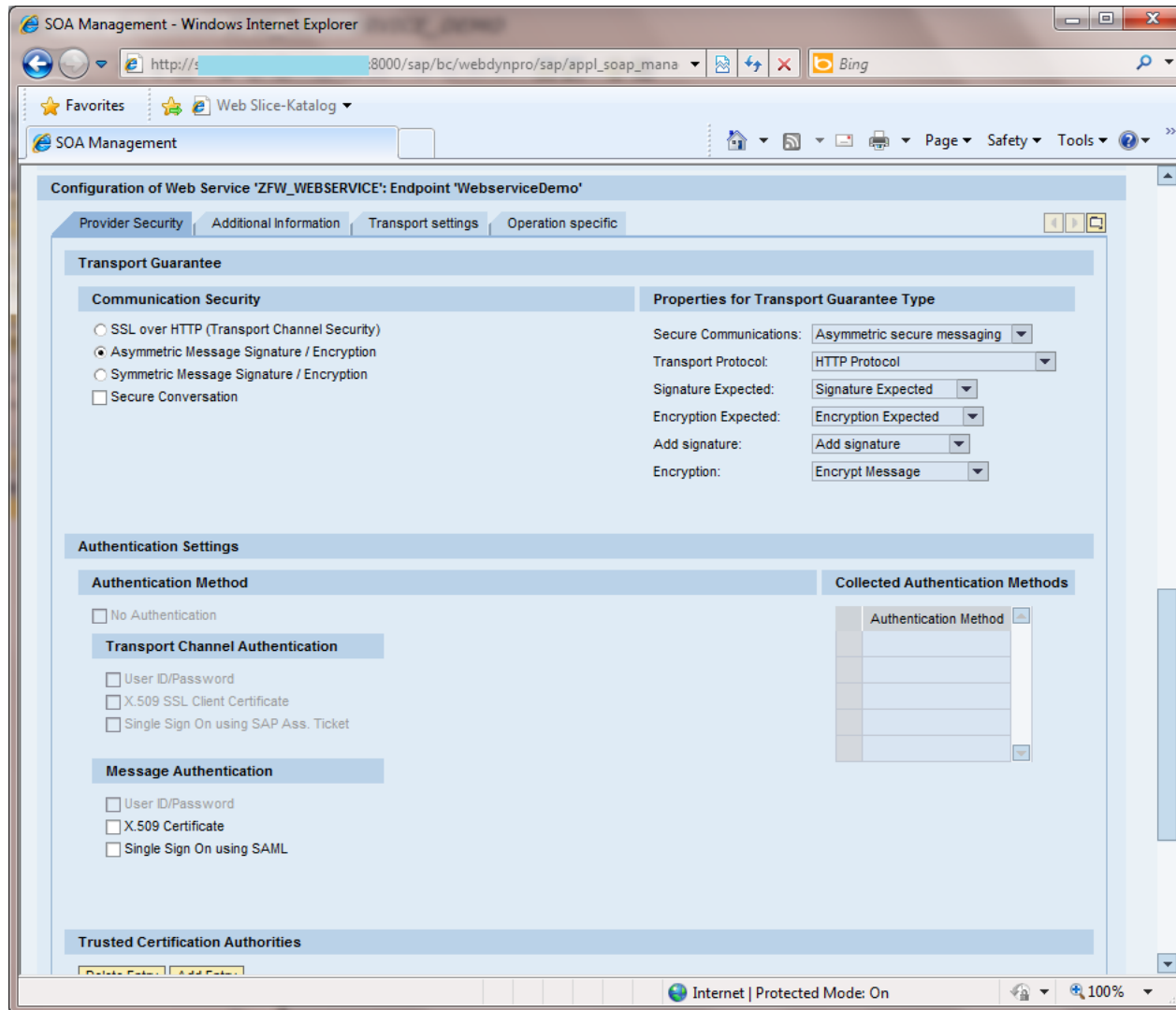
■ Maintenance:

formerly Tr. WSCONFIG + WSADMIN

since NW 2004s SP14 Tr. SOAMANAGER

- ▶ Redirects to WebDynpro ABAP App → Must be enabled previously

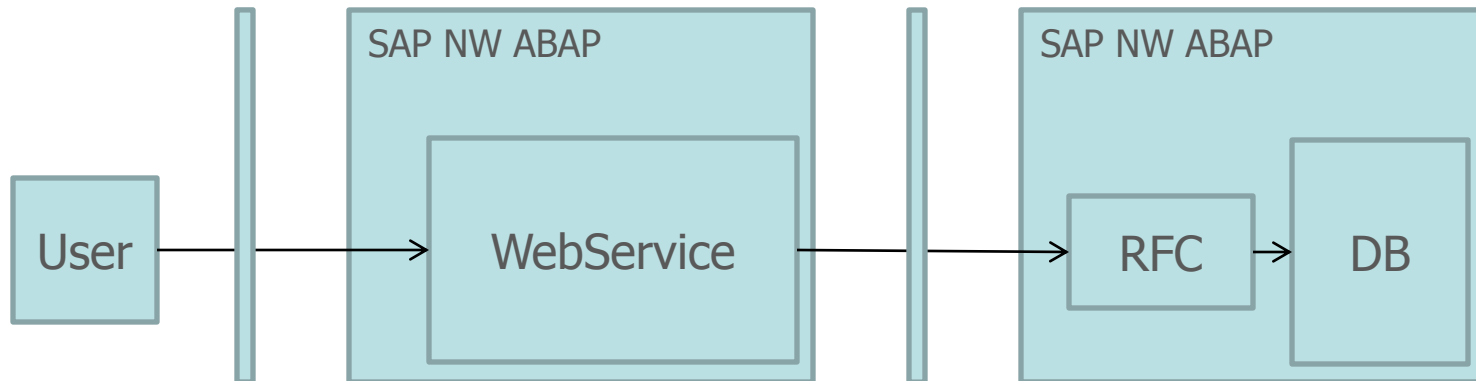
SAP Web Services with ABAP - SOAMANAGER



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

A1	Injection
A2	Cross-Site Scripting (XSS)
A3	Broken Authentication and Session Management
A4	Insecure Direct Object References
A5	Cross-Site Request Forgery (CSRF)
A6	Security Misconfiguration
A7	Insecure Cryptographic Storage
A8	Failure to Restrict URL Access
A9	Insufficient Transport Layer Protection
A10	Unvalidated Redirects and Forwards

OWASP Top 10 – 2010

A1	Injection	
A2	Cross-Site Scripting (XSS)	
A3	Broken Authentication and Session Management	<input checked="" type="checkbox"/>
A4	Insecure Direct Object References	<input checked="" type="checkbox"/>
A5	Cross-Site Request Forgery (CSRF)	
A6	Security Misconfiguration	<input checked="" type="checkbox"/>
A7	Insecure Cryptographic Storage	
A8	Failure to Restrict URL Access	<input checked="" type="checkbox"/> (<i>partly</i>)
A9	Insufficient Transport Layer Protection	<input checked="" type="checkbox"/>
A10	Unvalidated Redirects and Forwards	<input checked="" type="checkbox"/>

Questions ...

- Thank you for your attention

... ????

Literature

- SAP NetWeaver Security Guide ([click](#))
- Sichere ABAP Programmierung,
Wiegenstein, Schumacher, Schinzel, Weidemann, Galileo Press
<http://www.sap-press.de/2037>
- The Developer's Guide to SAP NetWeaver Security,
Martin Raeppe, 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.