onapsis
Securing Business Essentials

ATTACKS TO SAP WEB APPLICATIONS

by Mariano Nuñez Di Croce
mnunez@onapsis.com

BlackHat DC 2011 Briefings

Abstract

"SAP platforms are only accessible internally". While that was true in many organizations more than a decade ago, the current situation is completely different: driven by modern business requirements, SAP systems are getting more and more connected to the Internet. This scenario drastically increases the universe of possible attackers, as remote malicious parties can try to compromise the organization's SAP platform in order to perform espionage, sabotage and fraud attacks.

SAP provides different Web interfaces, such as the Enterprise Portal, the Internet Communication Manager (ICM) and the Internet Transaction Server (ITS). These components feature their own security models and technical infrastructures, which may be prone to specific security vulnerabilities. If exploited, the business crown jewels can end up in the hands of cyber criminals.

This whitepaper demonstrates possible attacks to the SAP Web application components and the necessary measures that need to be applied in order to prevent them. This information will enable organizations to better protect their business-critical systems from cyber-attacks performed over Web scenarios.

Onapsis offers no specific guarantee regarding the accuracy or completeness of the information presented, but the professional staff of Onapsis makes every reasonable effort to present the most reliable information available to it and to meet or exceed any applicable industry standards.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.

TABLE OF CONTENTS

Note:

In order to find the latest version of this white-paper, please check the Onapsis Research Labs website at http://www.onapsis.com/research.html

1. INTRODUCTION

SAP applications are used to run the world's more important businesses. Key processes such as sales, invoicing, manufacturing, procurement, human resources management and financial planning are managed and processed by systems running SAP software.

This critical nature is what makes them highly attractive for cyber-criminals and cyber-terrorists. If a malicious party is able to compromise the organization's SAP platform, he would be able to engage in espionage, sabotage and fraud attacks to the business, leading to severe economic damage.

Several years ago, the use of these integrated business systems was only available to internal employees, working behind corporations' firewalls. Nowadays, driven by modern business requirements, these firewalls had to be opened and SAP platforms made available to external, untrusted networks such as the Internet. Under this new paradigm, the choice for the technological platform for this new interconnectivity was obvious: the Web.

SAP has developed several proprietary Web Application components through its history: the Internet Transaction Server (ITS), the Internet Communication Manager (ICM) and the Enterprise Portal (EP). These components feature their own security models and thus require specialized knowledge to understand current and future threats to the business information processed by them.

This white-paper describes some threats affecting the security of standard applications and configurations of these components, in order to understand the possible workarounds and solutions to mitigate them. This information will enable organizations to better protect their business-critical systems from cyber-attacks performed over Web scenarios.

The security of *custom* SAP Web applications, protecting against attacks such as SQL Injection, Cross-Site Scripting (XSS) and Path Traversals generally falls under the domain of Secure Development practices and will be covered in a future work.

2. SAP WEB APPLICATIONS

Along its history, SAP developed different technologies in order to provide Web access to the core backend systems. This section provides a quick introduction into these components.

The SAP Internet Transaction Server (ITS)

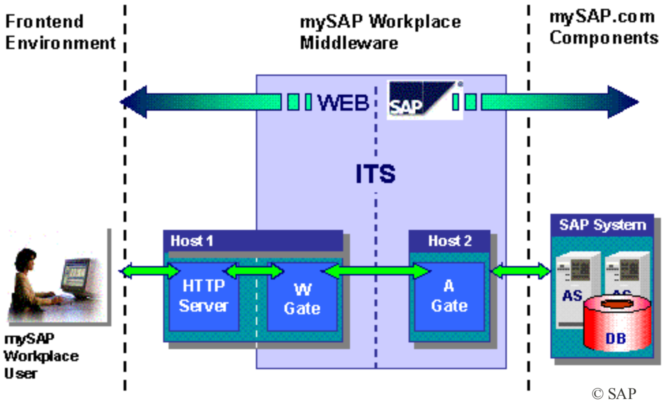
The ITS was released in 1996, being SAP's first approach to enable Internet access to the SAP systems.

This component acts as a middleware which works mainly by translating SAP Dynpros (dynamic programs) into HTML pages.

The ITS is built upon two sub-components:

- **Wgate:** Web filter (CGI/ISAPI) that receives HTTP requests for the ITS system. Forwards the requests to the Agate.
- **Agate:** Receives requests from Wgate and translates them to RFC/DIAG calls to the backend SAP Application Server. Receives results, translates them to HTML and forwards them to the Wgate.

The following figure presents the architecture of a standalone ITS deployment:



© SAP

ITS functionality is delivered in the form of *services*. These services are represented by operating system files (.*srvc)*, located in the Agate server. Each service contains the necessary information to connect to the backend SAP system and perform the required operation.

End users access these services by requesting URLs with a specific format:

http://<server>:<port>/<path_to_wgate>/<service_name>/!?<optional_params>

By default, the *path_to_wgate* is configured as “*/scripts/wgate/*”.

Since release 6.40, the ITS has been integrated into the Web Application Server and is offered as a service within the ICF (Internet Communication Framework).

More information about the ITS can be obtained at [1].

The SAP Internet Communication Manager (ICM)

The ICM is the evolution of the ITS component. In this new scenario, there is no need to deploy an intermediate, middleware component to process HTTP requests, as the SAP kernel itself has been enhanced to support the processing of the HTTP(S) and SMTP protocols.

Specifically, the component in charge of processing requests is the Internet Communication Framework (ICF). This framework provides access to *ICF services*.

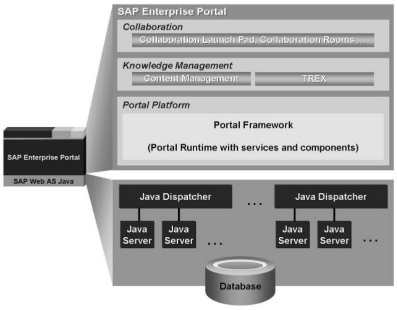
More information about the ICM can be obtained at [2].

The SAP Enterprise Portal (EP)

The SAP Enterprise Portal is SAP's solution to provide an unique access point to the organization's SAP (an non-SAP) systems through the Web.

According to SAP, the EP “provides employees, partners, customers, and other workers with immediate, secure, and role-based access to key information and applications”.

Technically, the Enterprise Portal is an J2EE application running on top of the SAP J2EE Engine (renamed to SAP AS Java since 7.1). This application is composed of three main components: the Portal Platform, Knowledge Management and Collaboration.



More information about the EP can be obtained at [3].

3. ATTACKS TO SAP WEB APPLICATIONS

This section analyzes some of the current security threats to the components detailed in the previous chapter and the possible countermeasures to mitigate them.

3.1. Identification of SAP Web Servers through Banners

Just as any regular Web server, SAP Web servers return an HTTP Server header describing the underlying technology. Attackers can use this information in order to discover these systems in the wild and obtain their version information.

ITS

As the Web-facing component of the ITS is a regular Web server (such as Microsoft IIS, Apache, etc), identifying ITS components through this technique is not feasible.

ICM

The ICM can return the following *Server* headers:

server: SAP Web Application Server (1.0;<VERSION>)

server: SAP NetWeaver Application Server (1.0;<VERSION>)

server: SAP NetWeaver Application Server / ABAP <VERSION>

server: SAP NetWeaver Application Server <VERSION> / ICM <VERSION>

For example:

- server: SAP Web Application Server (1.0;640)
- server: SAP NetWeaver Application Server (1.0;700)
- server: SAP NetWeaver Application Server / ABAP 701

J2EE Engine (SAP EP)

The J2EE Engine can return the following *Server* headers:

Server: SAP J2EE Engine/<VERSION>

Server: SAP NetWeaver Application Server <VERSION> / AS Java <VERSION>

For example:

- Server: SAP J2EE Engine/7.00
- Server: SAP NetWeaver Application Server 7.10 / AS Java 7.10

Protection / Countermeasures

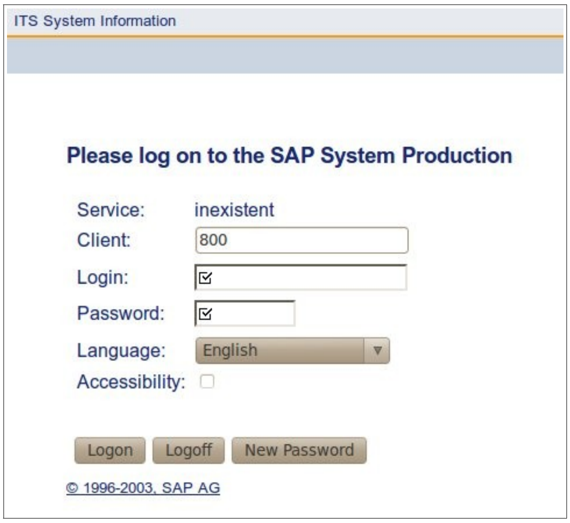
- Disable or configure a customized HTTP Server header for the ICM server. Check SAP Note 1329326.
- For the J2EE Engine, disable the server banner through property *UseServerHeader.* Check [12] for more information.

3.2. Exploration of SAP Web Servers through Error Messages

By requesting specific URLs and triggering error conditions, an attacker would be able to identify the underlying software component and obtain information that could be used in the next phases of the attack.

ITS

Requesting a non-existent ITS service (such as */scripts/wgate/inexistent/!)* will trigger an error message where the use of this component can be confirmed. The screen returned depends on the ITS version in use. In some cases it will return a login screen, such as the following:



ITS System Information

Please log on to the SAP System Production

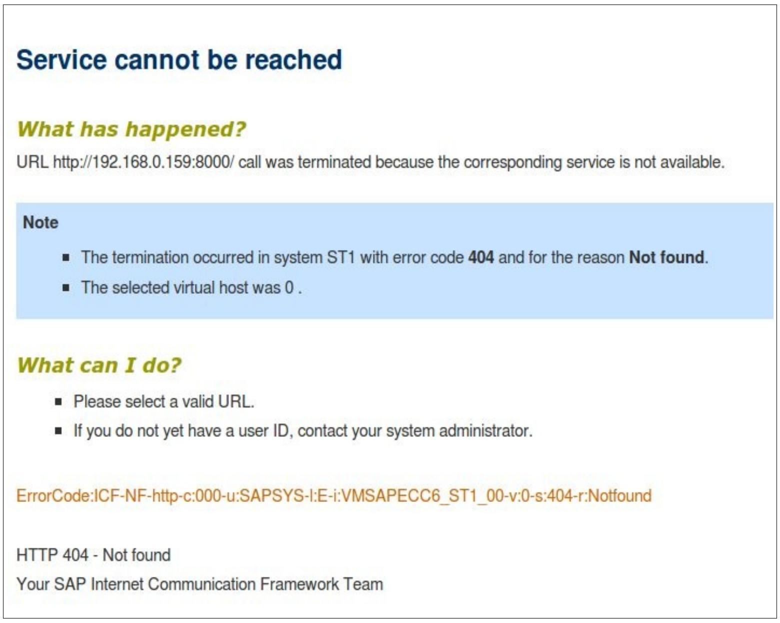
Service: inexistent
Client: 800
Login: ☑
Password: ☑
Language: English
Accessibility: □

Furthermore, by analyzing the source code of this Web page, the attacker will be able to obtain sensitive information from the ITS infrastructure:

```
<!--
 This page was created by the
 SAP Internet Transaction Server (ITS, Version 6200.1004.33246.0,
Build 587598, Virtual Server PROD, Add. service info none, WGate-AGate
Host abtrwu, WGate-Instance PROD)
 All rights reserved.
 Creation time:  Mon Jan 03 02:36:27 2011
 Charset:        utf-8
 Template:       zwebfal98/99/login
-->
```

ICM

The ICM returns a descriptive error message in HTTP 404 and 403 responses:



Service cannot be reached

What has happened?

URL http://192.168.0.159:8000/ call was terminated because the corresponding service is not available.

Note

- The termination occurred in system ST1 with error code **404** and for the reason **Not found**.
- The selected virtual host was 0 .

What can I do?

- Please select a valid URL.
- If you do not yet have a user ID, contact your system administrator.

ErrorCode:ICF-NF-http-c:000-u:SAPSYS-l:E-i:VMSAPECC6_ST1_00-v:0-s:404-r:Notfound

HTTP 404 - Not found
Your SAP Internet Communication Framework Team

From this message, it is possible to obtain:

- SAP server hostname.
- SAP System ID (SAPSID).
- SAP system number.

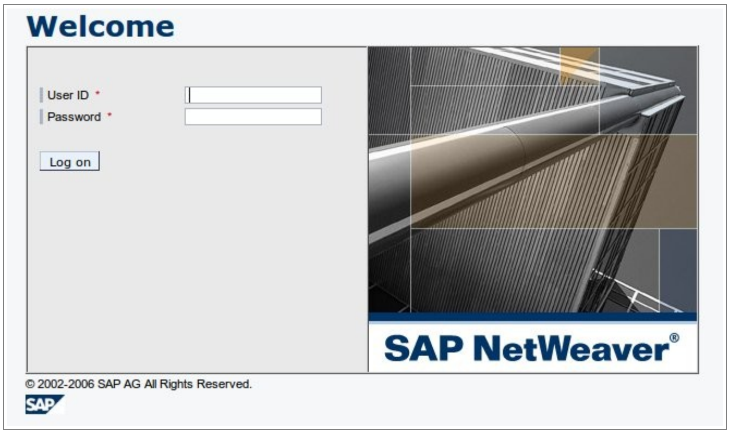
By accessing a protected service, it is also possible to retrieve the SAPSID of the target SAP system.

Hint

You can use **Onapsis Bizploit's** **icmErrorInfodisc** plugin in order to verify if your SAP platform is affected by this issue.

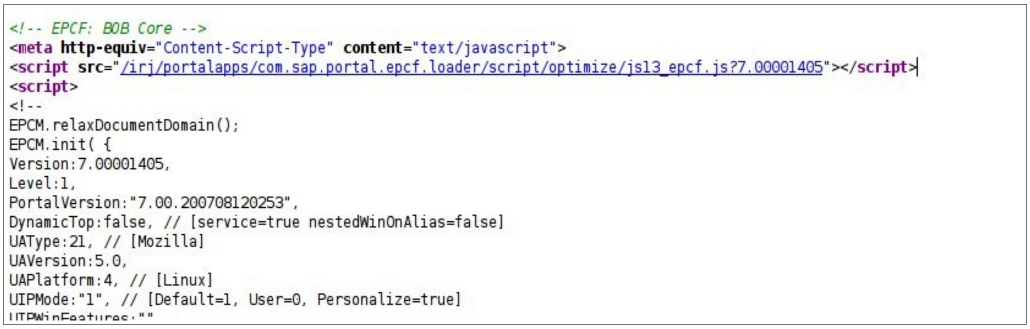
J2EE Engine (SAP EP)

The presence of the SAP Enterprise Portal can be checked by trying to access the default path for the application (*/irj/portal*). If available (and anonymous access is restricted), a logon screen will be presented:



Furthermore, by requesting a non-existent resource, it is also possible to obtain the SAP J2EE Engine version presented in the top of the resulting page.

The SAP EP also provides version information in the source code of the generated pages:



```
<!-- EPCF: BOB Core -->
<meta http-equiv="Content-Script-Type" content="text/javascript">
<script src="/irj/portalapps/com.sap.portal.epcf.loader/script/optimize/js13_epcf.js?7.00001405"></script>
<script>
<!--
EPCM.relaxDocumentDomain();
EPCM.init( {
Version:7.00001405,
Level:1,
PortalVersion:"7.00.200708120253",
DynamicTop:false, // [service=true nestedWinOnAlias=false]
UAType:21, // [Mozilla]
UAVersion:5.0,
UAPlatform:4, // [Linux]
UIPMode:"1", // [Default=1, User=0, Personalize=true]
UIPWinFeatures:""
```

Protection / Countermeasures

- For the ITS, check SAP Note 747818 to disable the disclosure of hidden version information.
- For the ICM, customize generated error pages to avoid disclosing infrastructure information. Check [6] and [7].

3.3. Unrestricted Access to ICF Services

When a request for an ICF service is received, the SAP system will first verify whether the service is *public* or not. If it is public, no authentication credentials are required. If not, the currently defined authentication procedure takes place.

After the user has been successfully authenticated, the SAP kernel will check that it has has the following authorization object:

- S_ICF
  - ICF_FIELD = 'SERVICE'
  - ICF_VALUE = '<authorization_value>'

where *authorization_value* is the value assigned in the "Authorization" field of the requested service's configuration.

While this situation may seem secure in the first place, a major security threat arises: ***the lack of default authorization checks.***

By default, ICF services do not have an *Authorization* value configured. This means that **any authenticated user can execute any ICF service.** The user will only be restricted by the authority checks defined in the code of the specific service he is accessing.

Furthermore, standard users, such as SAP*, DDIC, EARLYWATCH, SAPCPIC and TMSADM have widely known default passwords. **If these users have not been secured, a malicious attacker will be able to use them to access sensitive ICF services and possibly take complete control of the SAP server.**

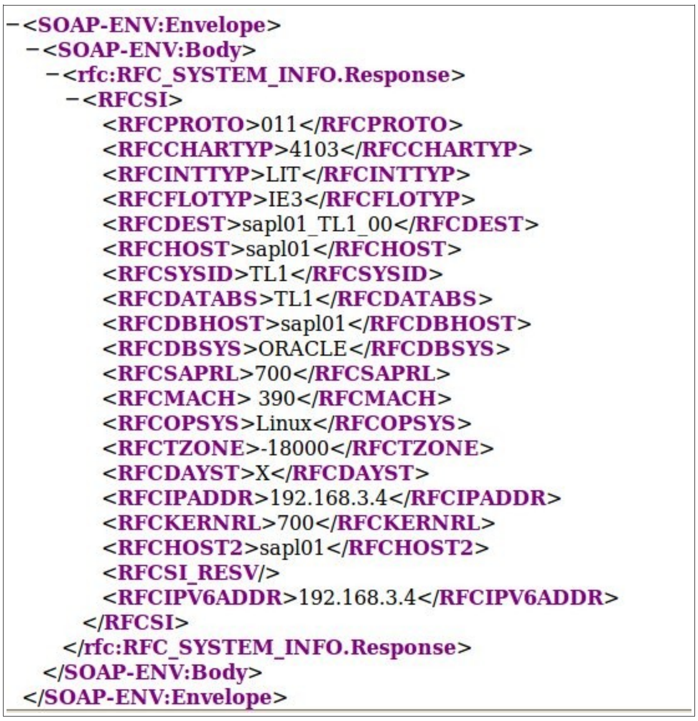
The following sections describe some dangerous ICF services that can be abused by attackers.

Protection / Countermeasures ⛔

- Make sure that standard users don't have default passwords. You can use report RSUSR003.
- Disable any ICF service that is not enabled due to business requirements. Check SAP Note 1498575 and [8].
- Maintain ICF Authorization Data as described in [9] and [10].

3.3.1. The Info Service

This service can be accessed anonymously through the */sap/public/info* URL and discloses sensitive information about the SAP platform:



```
−<SOAP-ENV:Envelope>
  −<SOAP-ENV:Body>
    −<rfc:RFC_SYSTEM_INFO.Response>
      −<RFCSI>
          <RFCPROTO>011</RFCPROTO>
          <RFCCHARTYP>4103</RFCCHARTYP>
          <RFCINTTYP>LIT</RFCINTTYP>
          <RFCFLOTYP>IE3</RFCFLOTYP>
          <RFCDEST>sapl01_TL1_00</RFCDEST>
          <RFCHOST>sapl01</RFCHOST>
          <RFCSYSID>TL1</RFCSYSID>
          <RFCDATABS>TL1</RFCDATABS>
          <RFCDBHOST>sapl01</RFCDBHOST>
          <RFCDBSYS>ORACLE</RFCDBSYS>
          <RFCSAPRL>700</RFCSAPRL>
          <RFCMACH> 390</RFCMACH>
          <RFCOPSYS>Linux</RFCOPSYS>
          <RFCTZONE>-18000</RFCTZONE>
          <RFCDAYST>X</RFCDAYST>
          <RFCIPADDR>192.168.3.4</RFCIPADDR>
          <RFCKERNRL>700</RFCKERNRL>
          <RFCHOST2>sapl01</RFCHOST2>
          <RFCSI_RESV/>
          <RFCIPV6ADDR>192.168.3.4</RFCIPV6ADDR>
        </RFCSI>
      </rfc:RFC_SYSTEM_INFO.Response>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

Protection / Countermeasures

The usage of the Info service should be analyzed. If this service is not in use following business requirements, it must be deactivated through transaction SICF.

Hint

You can use **Onapsis Bizploit**'s **icmInfo** plugin in order to verify if your SAP platform is affected by this issue.

3.3.2. The SOAP RFC Service

This service is used to execute SAP RFC function calls over the HTTP protocol. The RFC protocol is used to execute ABAP Function Modules on remote SAP servers, and represent a critical aspect of the system's security.

If this service is available, a remote attacker has access to perform sensitive operations over the system, which could result in the compromise of the target SAP server.

Protection / Countermeasures ⛔

The SOAP RFC service has been marked as *dangerous* by SAP and should be deactivated. Please see [4] for more information.

3.3.3. The WEBGUI Service

The WEBGUI service is part of the Integrated ITS of the ICM, and can be accessed through the */sap/bc/gui/sap/its/webgui* URL.

This service provides a complete SAPGUI interface through a Web browser.

If this service is available, a remote attacker would be able to login to the server and perform sensitive operations over the business information, given that he has valid user credentials in the system.

Protection / Countermeasures ⛔

The usage of the WEBGUI service should be analyzed. If this service is not in use following business requirements, it must be deactivated through transaction SICF.

Hint 💡

You can use **Onapsis Bizploit**'s **icmWebgui** plugin in order to verify if your SAP platform is affected by this issue.

3.4. SAP J2EE Engine HTTP Header Variables Authentication

The SAP J2EE Engine allows the configuration of different standard (and customized) logon modules to provide flexible authentication procedures.
One of these methods is the *HTTP Header Variables* authentication, which is used in the following scenarios:

- Integrated Windows Authentication (now replaced by Kerberos)
- Authentication by third parties tools (EAM/WAM solutions)

Under these scenarios, the user is authenticated against the intermediate server (for instance an IIS Server or a third party solution such as RSA ClearTrust). If the authentication procedure is successful, this server communicates with the SAP J2EE Engine and instructs it to authenticate the user. This information is sent in HTTP header variables. When the SAP server receives the request, it checks whether the user exists and, if so, a new Single Sign-On ticket is generated and forwarded to the user.

Protection / Countermeasures ⛔

The entire security of this method relies in the fact that the user should never be able to connect directly to the SAP server, as otherwise he will be able to impersonate the intermediate server and obtain a SSO ticket without providing access credentials.

This can be enforced by configuring trust relationships and mutual authentication between the SAP server and the intermediate authentication server.

Direct requests to the SAP server from end-users must be prohibited.

For more information check [11].

3.5. Exploitation of Vulnerable ICF Services

As described before, an attacker would be able to abuse of dangerous ICF services to perform sensitive operations over the SAP system. Among them, the SOAP RFC service represent one of the most serious threats, as it can be used to perform remote RFC calls to the system. This can lead to different attacks such as:

- Obtain the currently logged on users

  The attacker can call the TH_USER_LIST function module and obtain a list of the currently logged on users.

- Take full control of the target SAP system

  Exploiting a shell character injection vulnerability in the TH_GREP function on Unix platforms (can be protected through [5]), discovered by Joris van de Vis, the attacker is able to execute operating system commands over the SAP application server and obtain full control of the system's database. These privileges are equivalent as having the SAP_ALL profile over the system.

  This situation is highly dangerous as this function module can be executed by the EARLYWATCH standard user.

Please note that the above mentioned cases are just two examples of attack vectors. However, the attacker can execute any RFC function module (according to the authorizations of the user used for the attack).

If an attacker is able to obtain valid credentials for a high-privileged user (like SAP*), he would be able to perform even more sensitive operations (create SAP_ALL users directly, access SAP tables, modify business information, etc).

3.6. Internal Port-scanning through SAP wsNavigator

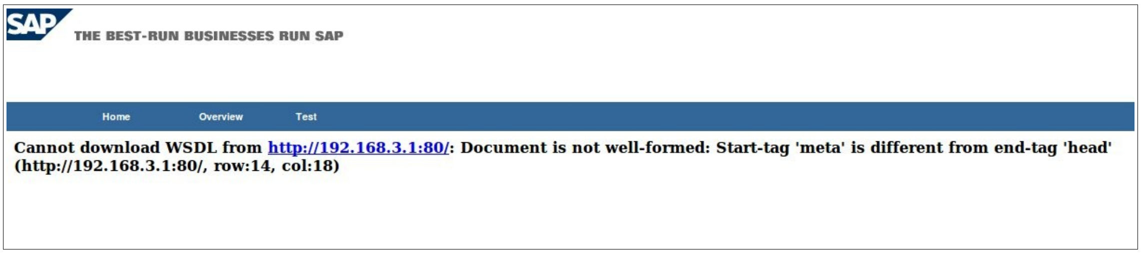
The SAP J2EE Engine has an application named *wsnavigator*, which is used to analyze the available Web Services in the SAP J2EE cluster.
Beyond interacting with these services, this application allows users to retrieve the WSDL from an URL.

When a URL is provided, the application dispatches an HTTP request to the specified server. If the request is not successful, a descriptive error message is presented.

Therefore, analyzing the generated responses, the attacker will be able to perform a discovery/portscanning of systems located in the internal network through this web interface.

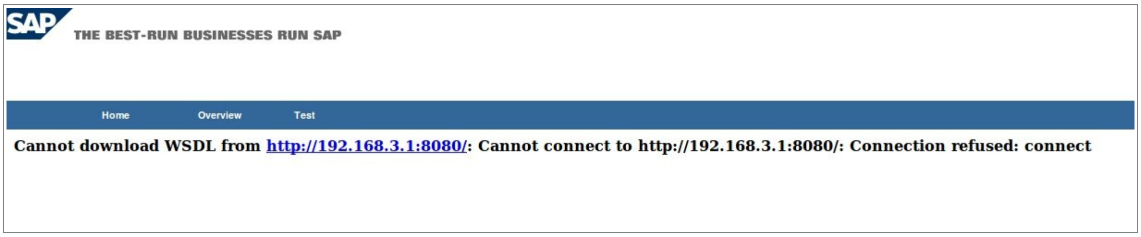
Following some examples are presented:

Connection to a live host with an open TCP port



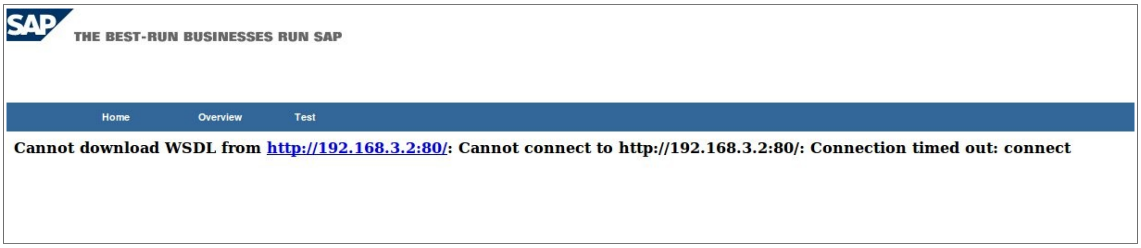
Cannot download WSDL from http://192.168.3.1:80/: Document is not well-formed: Start-tag 'meta' is different from end-tag 'head' (http://192.168.3.1:80/, row:14, col:18)

Connection to a live host with a closed TCP port



Cannot download WSDL from http://192.168.3.1:8080/: Cannot connect to http://192.168.3.1:8080/: Connection refused: connect

Connection to an unavailable or filtered host/port



Cannot download WSDL from http://192.168.3.2:80/: Cannot connect to http://192.168.3.2:80/: Connection timed out: connect

Protection / Countermeasures

The wsNavigator application should not be used in productive environments. In order to prevent this (and other) issues, this application should be disabled.

Check SAP Note 1461268 and 1394544, which contain specific protections for this vulnerability.

Also check SAP Note 781882 and 871394, which lists mandatory and optional services on the J2EE Engine

3.7. Bypass of “secured” SAP Portal Authentication

SAP J2EE Engine HTTP Header Variables Authentication was designed to increase the security level of the entire SAP platform. By implementing a two-factor authentication scheme, it is supposed that the probability of successful attacks to the authentication mechanisms will be drastically reduced.

Several industry's recognized EAM/WAM solutions are integrated to SAP environments through this mechanism. Some examples include:

- RSA ClearTrust
- CA SiteMinder
- Oracle Oblix
- Entrust GetAccess
- Microsoft Integrated Windows Authentication

However, if these components are not implemented correctly, the cure turns worse than the disease: ***a remote anonymous attacker would be able to access the SAP J2EE Engine applications (such as the Enterprise Portal), impersonating any user in the system.***

The attacker will only need to impersonate the third-party tool, by sending the following HTTP request to the SAP server:

```
GET /irj/portal HTTP/1.1
Host: <server>:<port>
<additional_headers>
<AUTH_HEADER>: <user_to_impersonate>
```

The HTTP header *AUTH_HEADER* is dependent on the third-party solution in use. For instance, in the case of Integrated Windows Authentication, the header name is *REMOTE_USER*.

If successful, the SAP server will return a valid logon cookie and the attacker would be able to access the business content with the privileges of the impersonated user.

4. CONCLUSIONS

SAP features a broad range of technologies to provide Web access to the organizations' core business information. Each of these technologies involves its own proprietary security models and therefore is exposed to specific threats that need to be understood and mitigated as soon as possible.

Contrary to many popular beliefs, **many SAP systems are currently connected to the Internet** and other untrusted networks, which drastically **increases the universe of possible attackers.**

By exploiting vulnerabilities in SAP web components, it would be possible for remote attackers to perform espionage, sabotage and fraud attacks to the organization's business-critical information.

It is important to stress the fact that **these attacks will be possible only if organizations are not following SAP's security recommendations and applying the appropriate settings.**

SAP is moving quickly to increase the security of its systems. The SAP Security Guides, newly released white-papers and regular patching days are some examples of this long-term policy. **Now customers need to catch-up and protect their core business information as soon as possible.**

This whitepaper has outlined only some of the existing risks and their impact. Other research lines are already in place and will be presented in a future work.

It is expected that, by understanding the presented threats and following the detailed recommendations, **SAP customers can increase the security level of their ERP systems and business-critical platforms** and protect themselves against the rising threat of cyber-attacks to corporate applications.

For further information into this subject or to request specialized assistance, feel free to contact Onapsis at info@onapsis.com

5. REFERENCES

[1] http://www.sdn.sap.com/irj/sdn/sap-its

[2] http://help.sap.com/saphelp_nw04/helpdata/en/0a/a7903febb15a7be10000000a11405a/frameset.htm

[3] http://help.sap.com/saphelp_ep60sp0/helpdata/en/index.htm

[4] https://service.sap.com/sap/support/notes/1394100

[5] https://service.sap.com/sap/support/notes/1433101

[6] http://help.sap.com/saphelp_nw73/helpdata/en/48/69efc9e8a607d6e10000000a42189c/frameset.htm

[7] http://help.sap.com/saphelp_nw73/helpdata/en/48/45acaf43a64bb8e10000000a42189b/frameset.htm

[8] http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/f0d2445f-509d-2d10-6fa7-9d3608950fee

[9] http://help.sap.com/saphelp_nw70ehp2/helpdata/en/39/e11482b2d23a428e583a59bef07515/frameset.htm

[10] http://help.sap.com/saphelp_nw70ehp2/helpdata/en/9f/fc5e900b62d94e8878eb94db5b986f/frameset.htm

[11] http://help.sap.com/saphelp_nw70ehp2/helpdata/en/d0/a3d940c2653126e10000000a1550b0/frameset.htm

[12] http://help.sap.com/saphelp_nw73/helpdata/en/55/4202bc3067492aa6887bcd97ed76a6/frameset.htm

ABOUT ONAPSIS

Onapsis is the leading provider of solutions for the **security of ERP systems and business-critical applications.** Through different innovative products and services, Onapsis helps its global customers to effectively increase the security level of their core business platforms, protecting their information and decreasing financial fraud risks.

Onapsis is built upon a team of world-renowned experts in the SAP security field, with several years of experience in the assessment and protection of critical platforms in world-wide customers, such as Fortune-500 companies and governmental entities.

Our star product, Onapsis X1, enables our customers to perform automated Security & Compliance Audits, Vulnerability Assessments and Penetration Tests over their SAP platform, helping them enforce compliance requirements, decrease financial fraud risks an reduce audit costs drastically.

Some of our featured services include SAP Penetration Testing, SAP Gateway & RFC security, SAP Enterprise Portal security assessment, Security Support for SAP Implementations and Upgrades, SAP System Hardening and SAP Technical Security Audits.

For further information about our solutions, please contact us at info@onapsis.com and visit our website at www.onapsis.com.