



# Welcome to the jungle

## Navigating the complexity of security

Tobias Lejczyk, SAP

Public

# Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP's intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

## Organization

Awareness

Security Governance

Risk Management

## Process

Regulatory Process  
Compliance

Data Privacy &  
Protection

Audit &  
Fraud Management

## Application

User & Identity  
Management

Authentication  
& Single Sign-On

Roles &  
Authorizations

Custom Code  
Security

## System

### SAP Security Baseline Template

#### TABLE OF CONTENTS

1	Overview, Requirements and Guidelines	9
1.1	Purpose of this template	9
2	Regulations	10
2.1	Environment	11
2.1.1	Network Security	11
2.1.2	Operating System and Database Security	11
2.1.3	Client Security	11
2.2	System	11
2.2.1	Security Hardening	11
2.2.1.1	CHANGE: Protect Production System against changes	11
2.2.1.1.1	CHANGE-A: Protect Production System against changes – ABAP	11
2.2.1.2	DISCL: Information Disclosure	12
2.2.1.2.1	DISCL-A: Information Disclosure – ABAP	12
2.2.1.2.2	DISCL-J: Information Disclosure – Java	12
2.2.1.2.3	DISCL-O: Information Disclosure – Web Dispatcher	12
2.2.1.3	FILE: Directory Traversal Protection	13
2.2.1.3.1	FILE-A: Directory Traversal Protection – ABAP	13
2.2.1.4	MSGSRV: Message Server Security	13
2.2.1.4.1	MSGSRV-A: Message Server Security	13
2.2.1.4.2	MSGSRV-J: Message Server Security	14
2.2.1.5	NETCF: Secure Network Configuration	14
2.2.1.5.1	NETCF-A: Secure Network Configuration – ABAP	14
2.2.1.5.2	NETCF-H: Secure Network Configuration – HANA	15
2.2.1.5.3	NETCF-P: Secure Network Configuration – BTP	15
2.2.1.6	NOTEST: No Testing Functionality in Production	15
2.2.1.6.1	NOTEST-J: No Testing Functionality in Production – Java	15
2.2.1.7	OBSCNT: Obsolete Clients	15
2.2.1.7.1	OBSCNT-A: Obsolete Clients in ABAP	15
2.2.1.7.2	OBSCNT-H: Obsolete Tenants in HANA	15
2.2.1.8	SCRIPT: Scripting Protection	15
2.2.1.8.1	SCRIPT-A: Scripting Protection – ABAP	15
2.2.1.9	SESS: Session Protection	16
2.2.1.9.1	SESS-J: Session Protection – Java	16
2.2.1.10	TRACES: Critical Data in trace files	16
2.2.1.10.1	TRACES-H: Critical Data in trace files – HANA	16
2.2.1.11	USRCTR: User Control of Action	16
2.2.1.11.1	USRCTR-A: User Control of Action – ABAP	16

### SAP Security Baseline Template

2.2.1.11.2	USRCTR-Q: User Control of Action – Others	
2.2.2	Secure SAP Code	
2.2.2.1	SECUPD: Regular Security Updates	
2.2.2.1.1	SECUPD-J	
2.2.2.1.2	SECUPD-N	
2.2.2.1.3	SECUPD-I	
2.2.2.1.4	SECUPD-C	
2.2.2.1.5	SECUPD-F	
2.2.2.2	FEATAC: F	
2.2.2.2.1	FEATAC-P	
2.2.3	Security Mx	
2.3	Application	
2.3.1	User and Id	
2.3.1.1	SELFRO: I	
2.3.1.1.1	SELFRO-J	
2.3.1.2	STDUSR: I	
2.3.1.2.1	STDUSR-J	
2.3.1.2.2	STDUSR-I	
2.3.1.3	USRTYP: I	
2.3.1.3.1	USRTYP-F	
2.3.2	Authenticat	
2.3.2.1	NETENC: I	
2.3.2.1.1	NETENC-J	
2.3.2.1.2	NETENC-C	
2.3.2.2	PWDPOL: I	
2.3.2.2.1	PWDPOL-J	
2.3.2.2.2	PWDPOL-C	
2.3.2.2.3	PWDPOL-I	
2.3.2.3	RFCGW: F	
2.3.2.3.1	RFCGW-A	
2.3.2.3.2	RFCGW-J	
2.3.2.3.3	RFCGW-O	
2.3.2.4	SSO: Singl	
2.3.2.4.1	SSO-A: Sin	
2.3.2.4.2	SSO-J: Sin	
2.3.2.5	IDPROV: I	
2.3.2.5.1	IDPROV-P	
2.3.3	Roles and Authorizations	24
2.3.3.1	CRITAU: Critical Authorizations	24
2.3.3.1.1	CRITAU-A: Critical Authorizations – ABAP	24

## Environment

# CLOUD

366 document(s) found

Sort By: Relevance



[3129883 - CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 - AS Java Core Components' impact for Log4j vulnerability](#)



You are curious whether your SAP NetWeaver Application Server Java system is affected by ZeroDay security vulnerability in log4j library mentioned in the...blog.....Vulnerability CVE-2021-44228, CVE-2021-45046 & CVE-2021-45105 for log4j...How does t

BC-JAS-COR (Enterprise Runtime, Core J2EE Framework) 21.12.2021 SAP Knowledge Base Article (32 people found this document helpful)

[3131771 - Log4j Vulnerability on IDM System](#)



You are curious whether your SAP Identity Management system is affected by ZeroDay security vulnerability in Log4j Library. For more details, please refer to...Apache Log4j Security Vulnerabilities...Vulnerability CVE-2021-44228 and...CVE-2021-4104 for Lo

BC-IAM-IDM (Identity Management) 20.01.2022 SAP Knowledge Base Article (5 people found this document helpful)

[3129897 - CVE-2021-44228 - Log4j vulnerability - no impact on SAP Adaptive Server Enterprise \(ASE\)](#)



CVE-2021-44228 - Log4j vulnerability and SAP ASE...

BC-SYB-ASE (Sybase ASE Database Platform (non Business Suite)) 09.02.2022 SAP Knowledge Base Article (4 people found this document helpful)

[3131007 - CVE-2021-44228 - Log4j vulnerability - no impact on SAP Information Steward](#)



Log4j vulnerabilities, is there any impact on SAP Information Steward...CVE-2021-44228...CVE-2021-4104...CVE-2019-17571...CVE-2022-23302...CVE-2022-23305...CVE-2022-23307...

EIM-IS-SVR (Information Steward - Administration/Server) 07.02.2022 SAP Knowledge Base Article (4 people found this document helpful)

[3130943 - CVE-2021-44228 - AS Java Enterprise Portal Components' impact for Log4j vulnerability](#)



You are curious whether your SAP NetWeaver Enterprise Portal application is affected by ZeroDay security vulnerability in log4j library mentioned...here ...Vulnerability CVE-2021-44228 for log4j...How does this impact SAP Netweaver Application Server Ente





**Trust**

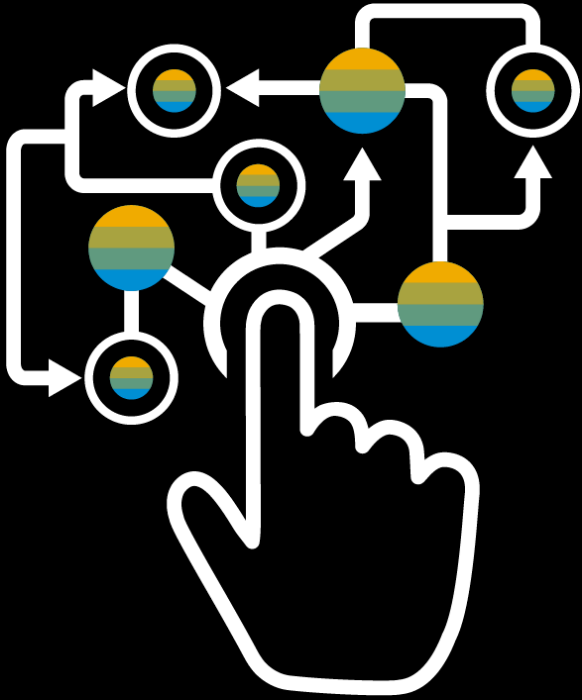
and

**Responsibility**



**Threat Modeling** is  
a **systematic approach**  
to perform **risk assessment**  
to uncover **security threats**  
at design time.

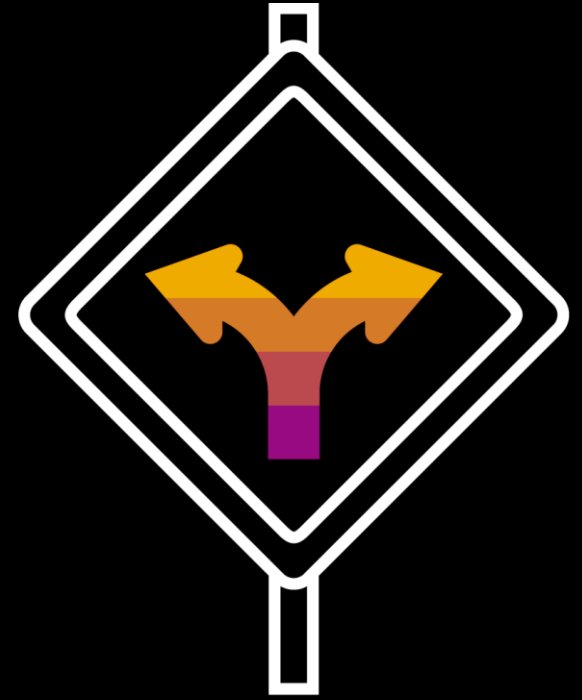
# Threat Modeling



Understand

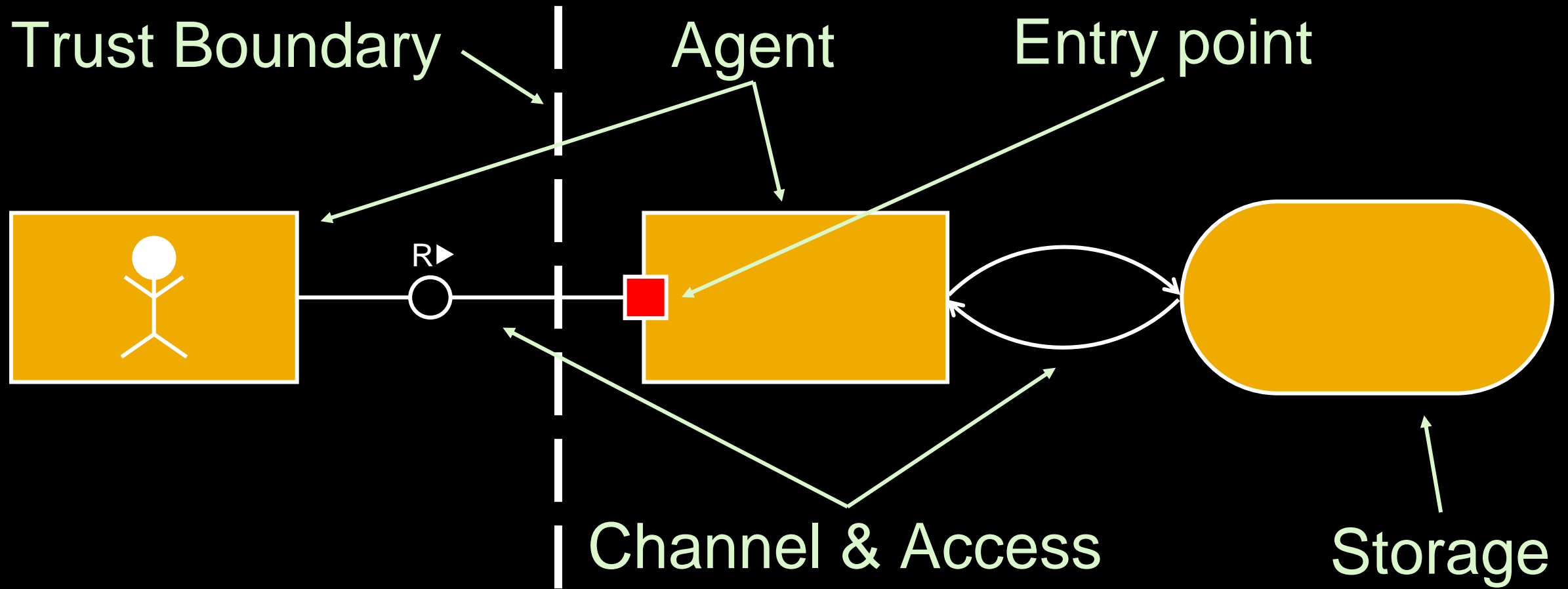


Analyze



Decide

# Understand





Analyze

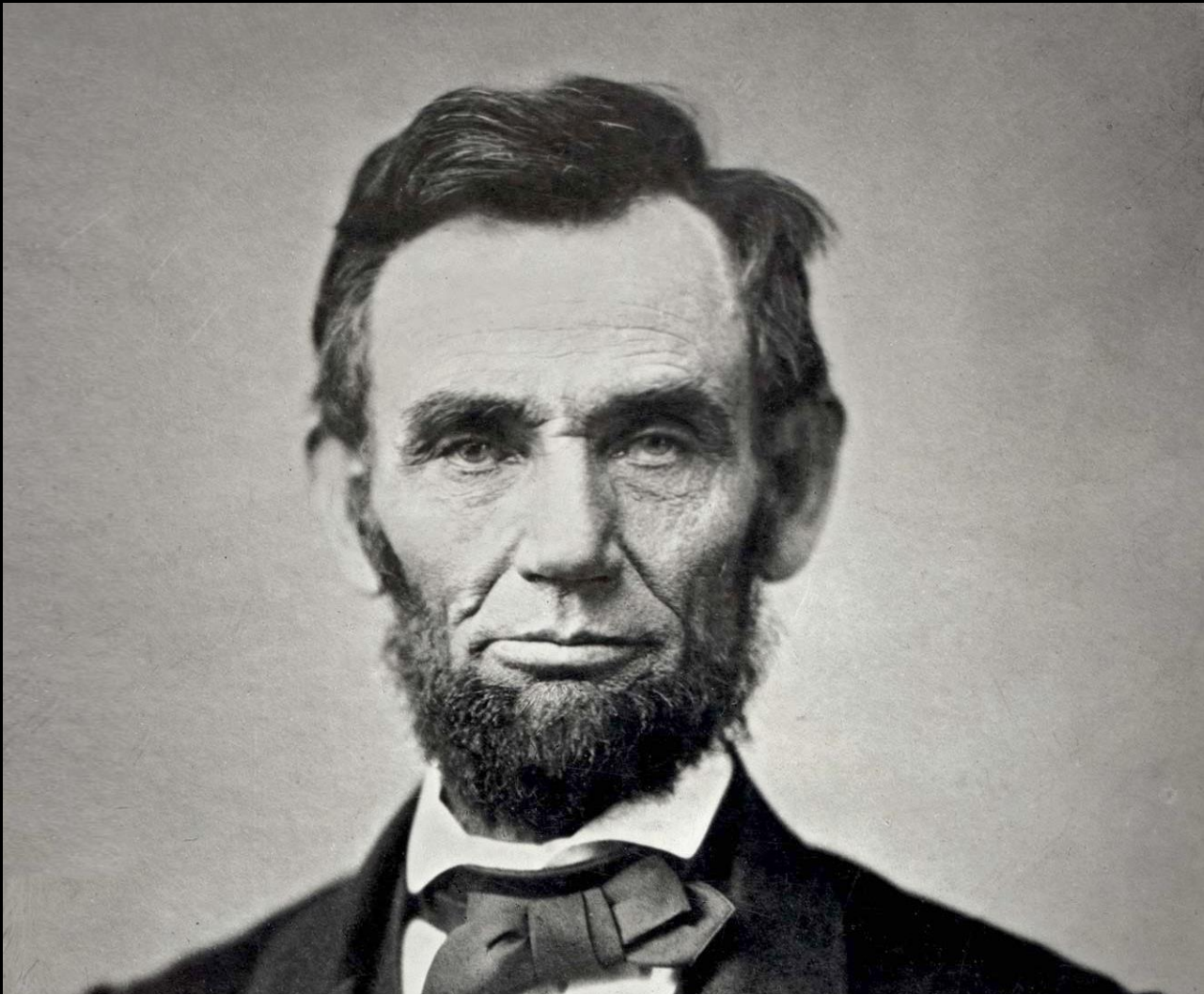
# S.T.R.I.D.E. Threat Classification





Don't believe  
everything you  
read on the  
internet.

*Abraham Lincoln*



**Spoofing**

# PC-Wahl 10



# Tampering

I didn't say that.

*Pete Hoekstra*



**Repudiation**





**Debit Card**  
@NeedADebitCard

Tweets  
**189**

Followers  
**18.8K**



**Debit Card**  
@NeedADebitCard

Please quit posting pictures of your debit cards, people.

 Debit Card Retweeted



**KD**  @prettyboy\_kd · 17 Aug 2016

My new debit card!! Blue looks good



 151

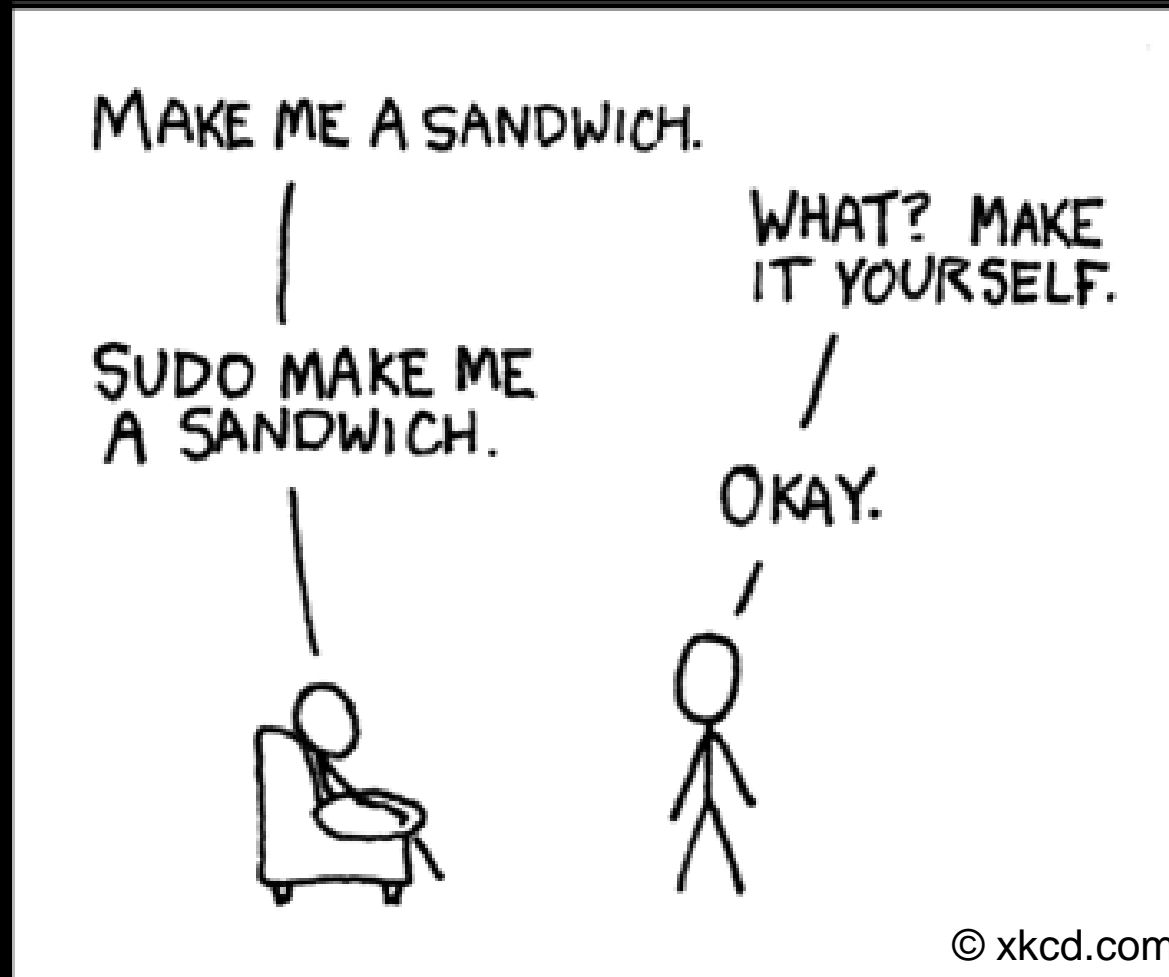
 1.0K

 833

# Information Disclosure



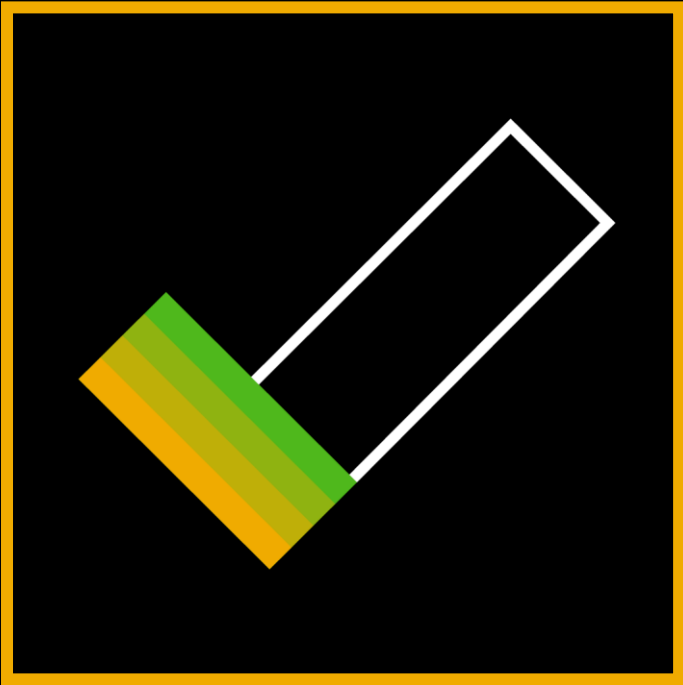
# Denial of service



# Elevation of privileges



# Decide





# Thank you.

Contact information:

Tobias Lejczyk  
tobias.lejczyk@sap.com



Follow us



[www.sap.com/contactsap](https://www.sap.com/contactsap)

© 2022 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See [www.sap.com/trademark](https://www.sap.com/trademark) for additional trademark information and notices.