



Bug Bounty for SAP Applications

Aditi Kulkarni, SAP Global Security
2022

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.

Agenda

What is bug bounty?

Bug bounty at SAP

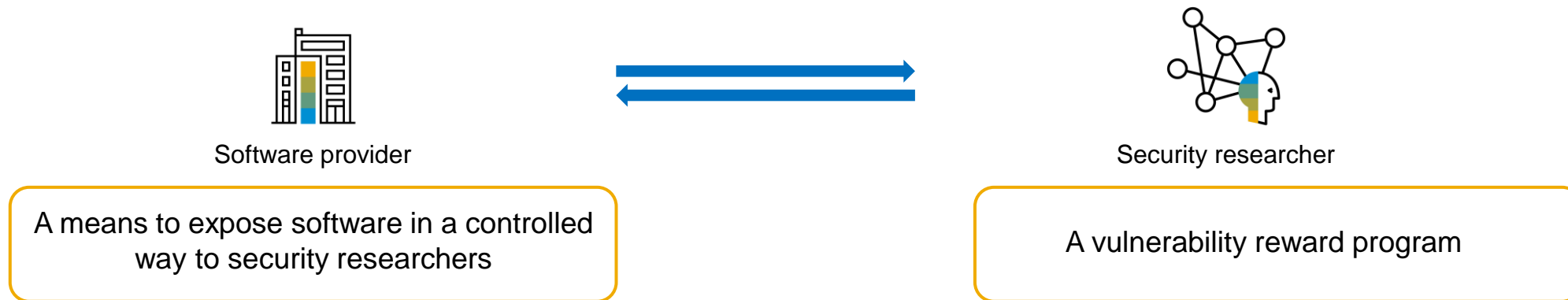
Where to report security issues to SAP?

SAP's Secure Software Development and Operations Lifecycle

What is bug bounty?

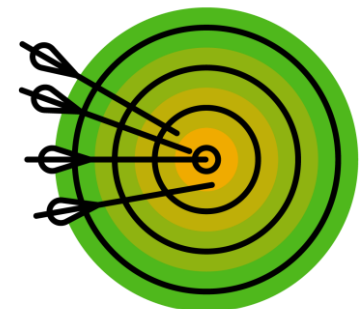


What is bug bounty?



Bug bounty goals

- **Improve software security** by leveraging the knowledge and experience of the worldwide hacker community
- Improve **relationship** between hackers and software vendors
- **Compensate** hackers for their continuous effort to improve software security
- **Learn** about new attack vectors, scenarios, impact of combination of vulnerabilities
- Add **new defensive measure** and mitigate entire classes of bugs



Bug bounty history and basics



Bug bounty history and basics

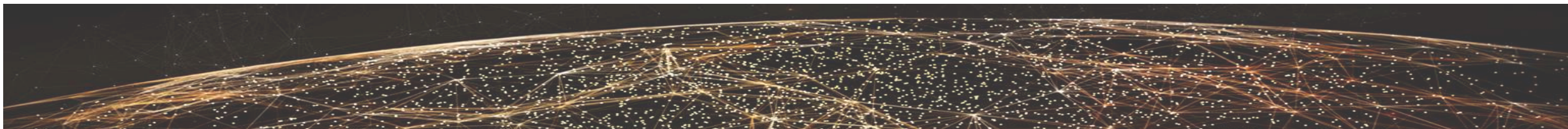
Netscape (1995), Mozilla (2004), subsequently Google, Facebook, PayPal, Microsoft, SAP

Ethical hackers are rewarded for finding vulnerabilities

- Strict rules for what is in scope and what is out
- Responsible disclosure of findings
- Rewards (bounties) are paid according to criticality of the finding based on CVSS ([Common Vulnerability Scoring System](#))

Bug bounty platform provider

- Registered hackers are under NDA and vetted according to specific criteria
- Manage relationship with ethical hacker community
- Manage communication between business and hackers
- Do first triage to eliminate false positives



Bug bounty at SAP



SAP's journey to bug bounty program

2016

Public "Hall of Fame" for security researchers submitting vulnerabilities to SAP Secure Inbox

2017 - 2021

Set up and continuous evolution of bug bounty programs at SAP

2022 onwards

General availability of bug bounty programs for all interested applications at SAP



SAP bug bounty program today

SAP Global Security provides

- **Central budget** for bug bounty platform service
- **Support** for setting up and running the bug bounties
 - Checklists
 - Legal and regulatory compliance
 - Compliance with internal security standards
 - Risk management
 - Coordinators that interface between bug bounty platform and development, create security incident tickets, consult on CVSS, and reward payouts

Findings are subject to SAP **SLAs** for fixing security vulnerabilities

Test systems are **isolated systems** with test data

Voluntary

Development provides

- Necessary staff
- Reward pool



SAP bug bounty program statistics

One of the main sources for vulnerability findings beside general vulnerability reports and customer disclosures

75% true positive rate

17% of disclosures rated with CVSS higher than 7.0

Reward range between \$100 and \$4000 to submissions with CVSS scores between 2.9 and 9.6

Average payout **\$983** per vulnerability

Findings range from simple vulnerabilities to design flaws



Bug Bounty vs Conventional Security Testing

Bug Bounty

- After product release
 - Defined scope (in / out of scope definition)
 - Ongoing
 - As many testers as you like
 - Regular scope extensions
 - Private and public programs
- Private:** Invited hackers only
- Public:** All hackers who are registered with the bug bounty platform service provider

Conventional security testing

- During the development lifecycle of a product
- Narrow scope
- One time activity at a set point in time with limited pen testers

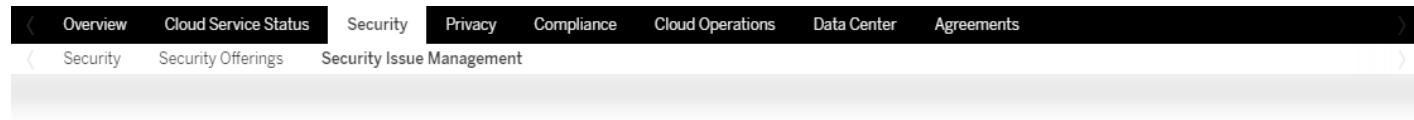
Bug Bounty in the Secure Software Development and Operations Lifecycle



Where to Report Security Issues to SAP?



Product Security Findings



Report a Security Issue

SAP is committed to identifying and addressing security issues that affect our software and cloud solutions. We are continuously working on improving our security processes. To report a potential security issue, choose from the options below.



SAP customers

Report a customer security issue by using the SAP ONE Support Launchpad to find a solution and get real-time support from an expert.

[View the launchpad >](#)



Security researchers

Inform the SAP Security Response Team of a security issue by completing and submitting the security vulnerability form.

[Access the form >](#)

Note: Include the following details in the report, as applicable, so that we can better analyze the nature and scope of the security issue: issue category, affected product version with support package and patch level, necessary pre/post-conditions for the exploit to work, description with proof of concept or exploit code, and impact of the issue if exploited.

<https://www.sap.com/about/trust-center/security/incident-management.html>

[Get the public PGP key >](#)

[Learn more about disclosure guidelines >](#)

SAP Security Patch Day and Researcher Acknowledgement

SAP Security Patch Day



Fix vulnerabilities discovered in SAP products

Review notes from our monthly SAP Security Patch Day to learn about vulnerabilities discovered in SAP products and apply patches to protect your SAP landscape.

[Read the SAP Security Patch Day blog >](#)



Join us in acknowledging our security researchers

Learn about the security researchers who help us identify and solve security vulnerabilities, so we can help maintain the security and safety of our customers and partners.

[See the list of security researchers >](#)



SAP Trust Center – Security – Security Issue Management

Aditi Kulkarni
SAP Global Security

Follow us



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 for additional trademark information and notices.