

No. 127

CYBERSECURITY

Bug Bounty Hunting

Finding and reporting security bugs legally, for rewards and recognition

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 127

Bug Bounty Hunting

Finding and reporting security bugs legally, for rewards and recognition

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Bug Bounty Hunting
Finding and reporting security bugs legally, for rewards and recognition

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Platform, product and company names mentioned in this book are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 What bug bounties are 5
2 Disclosure programmes 6
3 Who is involved 7
4 Why organizations run programmes 8
5 The law and safe harbour 9
6 Programme policies 10
7 Scope 11
8 Programme rules 12
9 Ethics 13
10 Platforms 14

PART II · HUNTING

11 Skills 16
12 Practising safely 17
13 Choosing programmes 18
14 Understanding the target 19
15 Common findings 20
16 AI applications 21
17 Tools 22
18 Keeping notes 23
19 Avoiding harm 24
20 Handling personal data 25

PART III · REPORTING

21 Writing the report 27
22 Explaining impact 28
23 Severity 29

FREE SAMPLE · ojayo.com

24 Report quality 30
25 Triage 31
26 Duplicates 32
27 Rewards 33
28 Disclosure 6
29 Handling disagreements 35

PART IV · THE BIGGER PICTURE

30 AI and hackbots 37
31 Running a programme 38
32 security.txt 39
33 Careers 41
34 Money and taxes 42
35 Wellbeing 43
36 Common mistakes 44
37 A worked example 45
38 A learning path 46
Checklists 47
Glossary 48
Further reading 49

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

A **bug bounty** programme invites independent security researchers to find and report vulnerabilities in an organization's systems, and rewards valid reports, usually with money. Thousands of organizations, from tech giants to governments, run such programmes, and many researchers learn their craft through them.

This beginner's book explains how bug bounties and vulnerability disclosure work, how to read a programme policy, the rules and ethics that keep you legal, how to practise, how to write a report that gets accepted, and how organizations can run their own programmes. It focuses on process and judgement rather than attack techniques.

What this book covers

- Vulnerability disclosure programmes and bug bounties.
- Programme policies, scope, safe harbour and the law.
- Platforms, common findings and how hunters work.
- Writing reports, triage, rewards and disclosure.
- AI in bug bounty, careers and running your own programme.

Who this book is for

- **Beginners** wanting to start bug hunting legally.
- **Developers** who receive bug reports.
- **Security teams** considering a programme.

FREE SAMPLE · ojayo.com

How the book is organized

- **Part I — Foundations** (Chapters 1–10): what bug bounties are, disclosure programmes, who is involved, why organizations run them, the law and safe harbour, policies, scope, rules, ethics and platforms.
- **Part II — Hunting** (Chapters 11–20): skills, practice, choosing programmes, understanding targets, common findings, AI applications, tools, notes, avoiding harm and handling personal data.
- **Part III — Reporting** (Chapters 21–29): the report, impact, severity, quality, triage, duplicates, rewards, disclosure and disputes.
- **Part IV — The bigger picture** (Chapters 30–38): AI and hackbots, running a programme, security.txt, careers, money and taxes, wellbeing, mistakes, a worked example and a learning path.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP

Practical advice you can use straight away.

IN PRACTICE

How an idea looks in real programmes.

WATCH OUT

Common mistakes and risks.

KEY IDEA

The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on the law

A programme's policy is your permission. Testing anything outside it can be illegal. Screens are **simplified illustrations**.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain how bug bounties and disclosure programmes work, and the rules that keep researchers on the right side of the law.

FREE SAMPLE · ojayo.com

CHAPTER 1

What bug bounties are

Bug bounties reward researchers for finding bugs.

A definition

A **bug bounty programme** is a public or private offer by an organization: if you find a security vulnerability within the published scope and follow the rules, you can report it and receive a reward.

The scale

According to HackerOne's 2025 Hacker-Powered Security Report, programmes on its platform paid researchers about **$81 million** over the year to June 2025, with an average bounty of about $1,090.

KEY IDEA

Bug bounties turn independent security research into a legal, structured and rewarded activity.

FREE SAMPLE · ojayo.com

CHAPTER 2

Disclosure programmes

Not every programme pays.

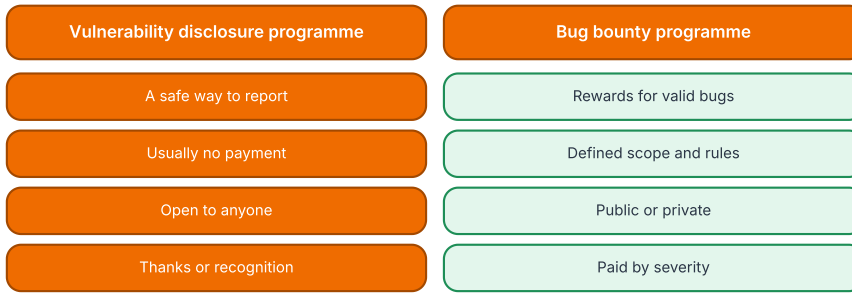


Figure 2.1 Disclosure programmes and bug bounties

Why VDPs matter

A **vulnerability disclosure programme** (VDP) gives anyone a safe, published way to report a security problem. In the US, federal civilian agencies have been required to publish VDPs since a 2020 CISA directive. International standards ISO/IEC 29147 and 30111 describe how organizations should receive and handle reports.

FREE SAMPLE · ojayo.com

CHAPTER 3

Who is involved

Several parties take part.

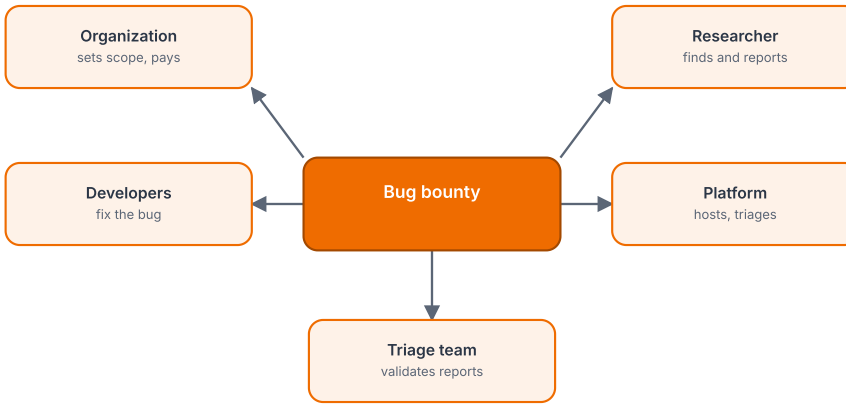


Figure 3.1 Who is involved

Triage

Large programmes receive many reports. Triage teams, often provided by the platform, check each report, reproduce it, remove duplicates and pass valid issues to the organization.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting (you are reading this)
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Bug Bounty Hunting

Enjoyed it? The full book has 54 pages and 38 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.