Disclosed.

The bug bounty world, curated.

THE BEST BUG BOUNTY RESOURCES FOR 2026

Every resource here survived a three-stage filter: automated discovery, AI scoring for actionability and depth, and human editorial review.

Curated by @infinitelogins | February 2026

[BUG BOUNTY PLATFORMS]

MAJOR PROGRAMS

- HackerOne (@Hacker0x01)

  Hacktivity feed provides disclosed vulnerability reports showing detailed exploitation paths across major programs. Leading platform for enterprise bug bounty programs and live hacking events.

- Bugcrowd (@Bugcrowd)

  Methodology-focused education teaching systematic vulnerability discovery and repeatable attack pathways. Features researcher spotlight series and tool recommendations.

- Intigriti (@intigriti)

  Highest volume of educational content with Advanced Exploitation Guide series (JWT, XSS, SSRF, logic flaws), monthly CTF challenges, and Bug Bytes weekly newsletter.

- YesWeHack (@yeswehack)

  Highest quality technical guides with Ultimate Guide series covering HTTP smuggling, GraphQL, and Android recon. Mobile security specialist with Dojo lab environments and monthly challenges.

[TOOLS]

CORE TOOLKIT

- Burp Suite (@portswigger)

  Industry-standard proxy for intercepting and modifying HTTP traffic. Extension ecosystem integrates third-party recon tools, scanners, and specialized analyzers (Community Edition free).

- Caido (@caidoio)

  Lighter proxy alternative with desktop and CLI clients, optimized for bug bounty.

- ProjectDiscovery Suite (@pdiscoveryio)

  Open-source scanning and enumeration toolkit. Detects known vulnerabilities, maps application surfaces through recon and crawling, with tools that work together for complete workflows.

- XNL-H4CK3R Suite (@xnl_h4ck3r)

  Recon automation for mining archived web data and more.

[TRAINING PLATFORMS]

Free Training - Start Here

ESSENTIAL

- PortSwigger Web Security Academy (portswigger.net)
  200+ interactive labs and free certification make it the gold standard for learning fundamentals and new attack classes.
- Hacker101 (hacker101.com)
  CTF challenges earn invitations to private HackerOne programs.
- YesWeHack Dojo (dojo-yeswehack.com)
  Monthly CTF challenges with published solutions covering OS command injection, JSON to RCE, and API vulnerabilities.
- Wiz Bug Bounty Masterclass (wiz.io)
  Cloud security platform teaching hunting vulnerabilities in modern applications (launched January 2026).

Paid Training - Invest in Skills

FROM $20

MONTHLY SUBSCRIPTIONS:

- PentesterLab (pentesterlab.com)
  ($20/mo) 15+ certificates specializing in application testing and bypass techniques for intermediate to advanced researchers.
- TCM Security - Practical Bug Bounty (academy.tcm-sec.com)
  ($30/mo) Practical Bug Bounty course with Intigriti partnership, OWASP Top 10 deep dive, Burp Suite mastery, and WAF bypass techniques.

SELF-PACED COURSES ($50-200):

- HackingHub (app.hackinghub.io)
  by Ben Sadeghipour - Scenario-based courses covering recon methodology, target approach, and program understanding. Paid courses run $50-199 with 100+ hands-on labs, plus free resources available in the webapp.
- From Zero to [BAC] Hero (arcanum-sec.com)
  by the_IDORminator - Broken Access Control course covering IDOR, authentication bypasses, business logic flaws, and platform-specific vulnerabilities.

LIVE COURSES ($149-2,000):

- Arcanum (arcanum-sec.com)
  by Jason Haddix - Live courses including The Bug Hunter's Methodology and Attacking AI teaching systematic hunting frameworks.
- Ars0n Bug Bounty Course (ars0nsecurity.com)
  by Harrison Richardson - Bug Bounty Launch Pad workshop February 21, 2026 with free ars0n-framework-v2 automation tool.

[PEOPLE TO FOLLOW]

SIGNAL SOURCES

DISCLOSED AUTHOR

- Harley Kimball (@infinitelogins)

  Runs Disclosed newsletter curating weekly bug bounty intelligence and co-founded Bug Bounty Village at DEF CON. Shares writeups, tools, research, and techniques from the bug bounty community.

- Bug Bounty Village (@BugBountyDEFCON)

  DEF CON village for bug bounty community. Hosts talks, CTF competitions, and networking events with all content published on YouTube.

PODCAST HOSTS

- Critical Thinking Hosts (@ctbbpodcast)

  (@rhynorater / @rez0__ / @gr3pme) Only active bug bounty podcast featuring technical deep dives with top researchers on advanced vulnerability classes, novel attack techniques, and hunting methodologies.

EDUCATORS

- NahamSec (@nahamsec)

  NahamCon and Hacking Hub founder focusing on recon methodology, multi-step vulnerability chaining, tool automation, and practical hunting workflows.

- Jason Haddix (@Jhaddix)

  Created The Bug Hunter's Methodology (TBHM) and Attacking AI course, defining industry standards for reconnaissance and systematic vulnerability discovery.

TOOL BUILDERS

- XNL-H4CK3R (@xnl_h4ck3r)

  Tool suite author specializing in recon automation (endpoint discovery, parameter extraction, dorking, etc.).

- z0idsec (@z0idsec)

  Tool suite author creating recon automation (path normalization, DNS resolution, attack surface discovery).

RESEARCHERS

- André Baptista (@0xacb)

  Ethiack co-founder sharing WAF bypass techniques, fuzzing approaches, and curated resources.

- James Kettle (@albinowax)

  Director of Research at PortSwigger and a leading web security researcher known for pioneering modern research into HTTP request smuggling and web cache poisoning.

- Gareth Heyes (@garethheyes)

  PortSwigger researcher focused on client-side security. Shares research on DOM-based vulnerabilities, JavaScript exploitation techniques, and encoding transformations.

- Sam Curry (@samwcyo)

  Coordinated disclosure researcher known for enterprise-scale security research. Shares findings on API vulnerabilities and systematic approaches to mapping corporate attack surfaces.

- Shubs (@infosec_au)

  Assetnote co-founder creating attack surface management tools and sharing research on SSRF, API testing, and more.

- Youssef Sammouda (@samm0uda)

  Meta BBP researcher focused on chaining vulnerabilities into account takeovers.

- Slonser (@slonser_)

  Security researcher at Solidlab covering XSS exploitation, DOMPurify bypasses, protocol vulnerabilities, and AI agent security.

- Jorian Woltjer (@J0R1AN)

  CTF writeups and XSS exploitation covering client-side vulnerabilities and browser behavior.

- payloadartist (@payloadartist)

  Shares working PoCs, security testing guides, and bypass techniques for common protections.

- Behi (@Behi_Sec)

  Curator of bug bounty tools and learning resources maintaining roadmaps and practical vulnerability tips.

- Jenish Sojitra (@_jensec)

  HackerOne elite hacker with seven-figure earnings sharing practical tooling and candid insights on bug bounty hunting.

[YOUTUBE CHANNELS]

BEST CHANNELS

- NahamSec (@NahamSec)
  Recon methodology tutorials, multi-step vulnerability chaining, tool walkthroughs, and practical hunting techniques.
- Medusa (@Medusa0xf)
  Practical exploitation demos covering major vulnerability classes with hands-on tool usage and PortSwigger lab walkthroughs.
- Lostsec (@lostsec_vip)
  Practical recon workflows, bypass techniques, and efficient vulnerability discovery methods.
- rs0n_live (@rs0n_live)
  Methodology walkthroughs with disclosed HackerOne reports, recon automation, and hypothesis-driven testing.
- DeadOverflow (@deadoverflow)
  AI-assisted workflows, bounty case studies with payout context, and responsible disclosure practices.

[PODCAST]

- Critical Thinking - Bug Bounty Podcast (@ctbbpodcast)
  Covers technical deep dives on advanced vulnerability classes, researcher interviews on full-time hunting strategies, and exploration of novel attack techniques.

[COMMUNITY]

- BugBounty.Forum (bugbounty.forum)
  Anonymous bug bounty discussions with validated earnings proof and peer networking.

[ABOUT DISCLOSED]

Disclosed (getdisclosed.com) is a weekly newsletter delivering curated bug bounty intelligence to security researchers. Every resource in this guide appeared in published Disclosed issues between October 2025 and February 2026.

The pipeline starts with automated discovery (monitoring X accounts, YouTube channels, personal blogs, newsletter sources, and manual submissions), moves to AI scoring for actionability and technical depth, and ends with human editorial review. Everything featured here passed that filter.

Curated by Harley Kimball (@infinitelogins), who leads researcher strategy at HackerOne, co-founded Bug Bounty Village at DEF CON, and runs Disclosed.

Want weekly curated bug bounty intelligence?

→ getdisclosed.com

Follow @infinitelogins for daily insights

#BugBounty