HORIZONSHIELD ORIGINALS · BOOK 21

Bug Bounty Methodology

From Recon to Report — Earning from Ethical Hacking

End-to-end bug bounty hunting methodology covering program selection, reconnaissance automation, vulnerability discovery, exploitation techniques, report writing, and maximizing bounty earnings.

HORIZONSHIELD

PRACTICAL

Contents

CHAPTER 01

Bug Bounty Program Strategy

Bug bounty success is as much strategy as technical skill. Choosing the right programs, scoping correctly, and prioritizing high-value targets determines your earnings more than raw hacking ability.

Bug Bounty Platform Comparison

Platform	Programs	Average Payout	Best For
HackerOne	3,000+	$500–$10K critical	Large programs, established hunters
Bugcrowd	800+	$300–$5K critical	Beginners, diverse program types
Intigriti	500+	€500–€20K critical	European companies, GDPR-focused
Synack	Invite-only	$1K–$50K+	Elite hunters, private programs
YesWeHack	300+	€200–€15K critical	European hunters, government programs
Direct programs	Google, Apple, Microsoft	$5K–$1M+	High-skill hunters, product-specific expertise

Program Selection Criteria

- **Scope size:** Broad scope (*.company.com) = more attack surface = more opportunities
- **Response time:** Check Disclosure reports — slow response = frustration
- **Payout history:** Look for actual paid reports on Hacktivity/disclosed reports
- **Age of program:** New programs have more low-hanging fruit
- **Competition level:** Private programs have fewer hunters; higher success rate

>
>
> **Start Private:** Many platforms invite new hunters to private programs with less competition. Focus on building reputation on public programs first (even small findings), then receive private invitations. Private programs typically pay 2-3x more than equivalent public programs.

CHAPTER 02

Recon Automation for Bug Bounty

Reconnaissance is where bounties are won or lost. Automated recon pipelines find assets that other hunters miss — subdomains, forgotten endpoints, and newly deployed services that haven't been hardened yet.

Automated Recon Pipeline

```
# Subfinder — passive subdomain enumeration
subfinder -d target.com -o subs.txt -all

# Amass — active + passive enumeration
amass enum -d target.com -o amass_subs.txt

# Combine and deduplicate
cat subs.txt amass_subs.txt | sort -u > all_subs.txt

# Check which subdomains are alive
cat all_subs.txt | httpx -silent -status-code   -title -tech-detect -o live_subs.txt

# Nuclei — scan all live assets for known vulnerabilities
nuclei -list live_subs.txt   -t ~/nuclei-templates/   -severity critical,high,medium   -o nuclei_findings.txt

# Waybackurls — find historical endpoints
cat all_subs.txt | waybackurls | sort -u > urls.txt
# Find juicy endpoints
grep -E "(api|admin|auth|login|token|secret)" urls.txt
```

High-Value Recon Targets

Target Type	Why It's Valuable	Finding Method
Forgotten staging/dev environments	Weaker security, exposed internals	Subdomain brute-force + httpx
Newly launched features	Less security testing	Monitor company changelog, job postings
Acquired company assets	Security posture varies widely	Track acquisitions via Crunchbase
API endpoints	Often have BOLA, auth issues	JS file parsing, Wayback Machine
Mobile app backends	Less scrutinized than web	APK/IPA decompilation + traffic proxy

CHAPTER 03

Vulnerability Classes with High Bounty Value

Not all vulnerabilities pay equally. Understanding which vulnerability classes command the highest bounties — and how to find them — maximizes your return on time invested.

High-Value Bug Classes

Vulnerability Class	Typical Bounty Range	Difficulty to Find
Remote Code Execution (RCE)	$10K–$200K+	Very High
Authentication bypass	$5K–$50K	High
SQL Injection (data exfil)	$3K–$30K	Medium-High
SSRF to internal network	$2K–$20K	Medium
IDOR (account takeover)	$2K–$15K	Medium
XXE (file read or SSRF)	$1K–$10K	Medium
Business logic flaw	$1K–$25K	High (context-dependent)
Stored XSS (high-impact)	$500–$5K	Low-Medium
Subdomain takeover	$200–$2K	Low (via automation)

Vulnerability Chaining: A medium-severity finding chained with another medium = critical payout. Example: SSRF (medium) + internal metadata access (medium) + cloud credentials in metadata (medium) = RCE equivalent = critical bounty. Always ask "what can I do with this?" before reporting a medium-severity finding.

CHAPTER 04

Writing High-Quality Bug Reports

A mediocre report of a critical bug earns less than an excellent report of the same bug. Triage teams are busy — reports that clearly demonstrate impact and provide perfect reproduction steps get paid faster and rated higher.

Bug Report Structure

```
## Summary
One-sentence description of the vulnerability and its impact.
Example: "Unauthenticated IDOR in /api/v2/users/{id} allows
any user to view and modify any other user's profile data."

## Severity
Critical/High/Medium/Low — justify with CVSS v3.1 score if possible

## Impact
What can an attacker actually do with this?
Be specific: "An attacker can access all user PII including email,
phone, and payment method last 4 digits for all 2.3M users."

## Steps to Reproduce
1. Create two accounts: attacker@test.com and victim@test.com
2. Login as attacker, capture request to GET /api/v2/users/12345
3. Change user ID from 12345 (attacker) to 12346 (victim)
4. Observe victim's full profile data returned in response

## Proof of Concept
[Screenshots / video / curl command demonstrating the issue]
curl -H "Authorization: Bearer ATTACKER_TOKEN"   https://api.target.com/v2/users/VICTIM_ID

## Suggested Remediation
Validate that the requesting user's ID matches the requested
resource ID server-side. Do not rely on client-supplied IDs.
```

HS

HORIZONSHIELD ORIGINALS

Complete Security Library

HorizonShield Originals are practitioner-written guides designed for real-world implementation — from SMB security foundations to advanced threat hunting, cloud architecture, and regulatory compliance.

AVAILABLE IN THIS SERIES

01 SMB Cybersecurity Guide 2026
02 Penetration Testing Checklist
03 Incident Response Playbook
04 DORA Compliance Guide
05 Cloud Security Hardening
06 Zero Trust Architecture
07 Threat Hunting SOC Operations
08 DevSecOps Implementation
09 Web Application Security
10 Network Security Fundamentals
11 Linux & Systems Security
12 Social Engineering & Human Hacking
13 Malware Analysis & Reverse Engineering
14 Digital Forensics & Incident Response
15 Applied Cryptography
16 Compliance Audit & Risk Management
17 AI & LLM Security Guide
18 OT & ICS Security
19 Mobile Security
20 Kubernetes Security
21 Bug Bounty Methodology
22 Security Architecture for Startups

horizonshield.net/library

Download all 16 books · Access labs · Track your progress

horizonshield.net