Introducing Bug Bytes, a newsletter curated by the community

BY INTIGRITI · JANUARY 17, 2019 · LAST UPDATED ON MARCH 6, 2025

The world of information security changes every day. As tools come out, write-ups are published and zero-days fly by, it can be a challenge to keep up with everything. That is why we are launching **Bug Bytes**, a newsletter curated by members of the bug bounty community. The first series will be curated by Mariem, better known as **PentesterLand.** Every week, she will keep you updated with a comprehensive list of all write-ups, tools, tutorials and resources you should not have missed.

You can receive every issue straight in your inbox by signing up here:

SIGN UP FOR THE NEWSLETTER

Without further ado, here are our favorite resources shared by pentesters and bug hunters last week. This issue covers the week from 04 to 11 of January.

Our favorite 5 hacking items

1. Article of the week

> "Avoid rookie mistakes and progress positively in bug bounty"

This is simple but to the point advice. Sometimes, as bug hunters, we may let ourselves be transported by exciting tests and forget the obvious: more emphasis should be put on the report, on trying to escalate/chain bugs, avoiding known invalid bugs, having a business mindset when writing impacts, etc.

These are some of the things mentioned in this article. Read it and keep them in mind when you're hunting for bugs, they could help you perform better and have a smoother experience.

2. Writeup of the week

> "Stored XSS & SQL injection on YNAB ($1,500)"

I hesitated between this writeup and the "XSS in steam react chat client" (see the Bug bounty writeups section below). The latter is an amazing account of how to find XSS on a React app and escalate it to RCE. But it's advanced stuff.

If you're at a beginner level, I recommend this writeup of a stored XSS & SQL injection. I love how it is written and includes the detailed methodology, what worked and what didn't work, and lessons learned.

3. Slides of the week

> "Recon like a boss"

This is a great guide on recon. It's a lot of techniques on the following topics: subdomain enumeration, finding new endpoints from JS files, AWS hacking, Github recon & content discovery.

Attention, must read!

4. Tool of the week

> "Bypass-firewalls-by-DNS-history"

One known technique for bypassing firewalls (like CloudFlare) is checking DNS history records. If you find the real IP address of your target, you'll be able to attack it directly and completely circumvent firewalls.

Many databases record DNS history. This tool is a great way to query many of them programmatically including: SecurityTrails, CrimeFlare, certspotter, DNSDumpster & IPinfo.

Unless you already have an alternative DNS history checker script, I recommend adding this one to your arsenal.

5. Non technical item of the week

> "How to Build a Successful Career in Information Security"

Daniel Miessler's blog in one that I follow very closely because of the quality of his writing. He write about a variety of topics from analysis of situations in America, to technical tutorials, or artifical intelligence, book reviews, etc.

I'm not interested in everything but many of his posts are gems. This particular one might answer a lot of your questions if you're starting out in information security. Even if you're already in this field, it might give you ideas or motivation for new things to try.

Other amazing things we stumbled upon this week

Videos

- Hacker101 – XML External Entities
- Hacker101 – Cookie Tampering Techniques

Podcasts

- Getting Into Infosec podcast: Jack Rhysider – From Odd-jobs to Network Analyst to SOC Architect to... Darknet Diaries!

Conference slides

- Threat modelling

Tutorials

Medium to advanced

- Virus Total: The best way to disclose your company secrets
- Accessing cross-site data using JSONP
- Two Interesting Session-Related Vulnerabilities
- UPNP Attacks : Hello Old Friend
- iOS Pentesting Tools Part 4: Binary Analysis and Debugging
- Kubernetes: Master Post
- Kubernetes: Kubernetes Dashboard
- Kubernetes: Kubelet API containerLogs endpoint
- 0x02 Learning Frida by Failing: Playing with Password Fields on Android
- Leveraging WSUS – Part One

Beginners corner

- SSRF – Server Side Request Forgery (Types and ways to exploit it) Part-1
- What is server side request forgery (SSRF)
- XXE Attacks— Part 1: XML Basics
- Clickjacking Attack on Facebook: How a Tiny Attribute Can Save the Corporation
- Cross site request forgery (CSRF)
- HTTP Security Headers Detailed Explanation
- SMB Penetration Testing (Port 445)
- SMTP Log Poisoning through LFI to Remote Code Execution
- Requests and Responses of an iOS Application & many other new tutorials on iOS hacking by Lucideus
- Install wfuzz in Termux & Removing Pycurl error

Writeups

Challenge writeups

- Hacken Cup 2018 CTF Walkthrough
- Express yourself – 35C3 CTF

Pentest & Responsible disclosure writeups

- From basic User to full right Admin access on the server (via XSS, LFI, WebShell)
- Reporting CSRF via Openbugbounty
- Abusing access control on a large online e-commerce site to register as supplier
- SSD Advisory – SME Server Unauthenticated XSS To Privileged Remote Code Execution
- Gradle Plugin Portal: Clickjacking & mCross-Site Request Forgery enabling Account Takeover
- Hackers in Hot Water. Pwning smart hot tubs, yes really

Bug bounty writeups

- XSS in steam react chat client ($7,500)
- Z-WASP Vulnerability Used to Phish Office 365 and ATP
- CSRF on Valve ($500)
- Cookie Hijacking & HTML Injection on private program
- CSRF & Account takeover on Pinterest ($2,400)
- Caching of sensitive information on Chaturbate ($300)

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- XSSOauthPersistence: Maintaining account persistence via XSS and Oauth
- JSON Web Token: Encode or Decode JWTs
- https://encoder.secapps.com: Online data encoder/decoder. Useful for quickly encoding payloads in various formats.
- Modlishka: Reverse Proxy for phishing campaigns & Explanation

More tools, if you have time

- Osmedeus: Automatic Reconnaisance and Scanning in Penetration Testing
- Stretcher: Tool designed to help identify open Elasticsearch servers that are exposing sensitive information
- SlackPirate: Slack Enumeration and Extraction Tool – extract sensitive information from a Slack Workspace

- KubiScan: A tool to scan Kubernetes cluster for risky permissions. Can be useful for configuration penetration tests if admin access is given.
- Kubelet Anonymous RCE: Executes commands on a kubelet endpoint that allows anonymous authentication (default)
- LeakLooker: Find open databases with Shodan & Description
- Nse-parse: Shell script for parsing vulnerable results from Nmap NSE scan output
- Hexyl: A command-line hex viewer
- Multitor: Tool that lets you create multiple TOR instances with a load-balancing
- Hediye: Hash Generator & Cracker Online Offline
- ServiceFu & Introduction
- WinPwn: Automation for internal Windows Penetration tests

Misc. pentest & bug bounty resources

- Comparing XSStrike with other XSS Scanners
- Learn Web Application Penetration Testing
- Cyber Security Resources: Resources related to ethical hacking / penetration testing, digital forensics and incident response (DFIR), vulnerability research, exploit development, reverse engineering & more
- Cheatsheet-God
- A guide for windows penetration testing
- 2019 OSINT Guide
- /r/netsec's Q1 2019 Information Security Hiring Thread
- 900 Startups Hiring Remotely in 2019

Challenges

- Intigriti challenge: Earn swag & one Burp Pro license (**before January 16th**)

Articles

- Why Framework Choice Matters in Web Application Security
- 2018's five easiest ways to break in
- The State of Web Application Vulnerabilities in 2018: Trend of increasing number of web application vulnerabilities particularly injections. WordPress vulnerabilities have tripled since last year. Drupal

vulnerabilities had a larger effect and were used in mass attacks. IoT, PHP & API vulnerabilities declined.

- OWASP Top 10: Real-World Examples (Part 1)
- Analysing Red Team Findings
- Why one of your favorite pen testing techniques doesn't work on AWS
- The Differences and Similarities Between IoT and ICS Security

News

- Facebook Bug Bounty: Introducing BountyCon
- New WhatsApp bug may have been discovered, exposes message history in plain text
- Zerodium Raises Zero-Day Payout Ceiling to $2M: "It's now paying $2 million for remote iOS jailbreaks, $1 million for WhatsApp/iMessage/SMS/MMS remote code-execution (RCE) and a half-million for Google Chrome RCEs."
- New year, new GitHub: Announcing unlimited free private repos and unified Enterprise offering (Finally!)
- Introducing Indian Rupee payments: Cheaper and faster bank transfers
- ICEPick-3PC: A Sophisticated Adware That Collects Data En Masse
- How Chinese hackers pulled off the Italian con job, a Rs 130-crore heist
- Millions of Android users tricked into downloading 85 adware apps from Google Play
- Google Public DNS now supports DNS-over-TLS
- Skype Glitch Allowed Android Authentication Bypass
- No more privacy: 202 Million private resumes exposed: An open and unprotected MongoDB instance was referenced on shodan.io & app.binaryedge.io
- Spoofing Google Search results

Non technical

- A chaotic mind leads to chaotic code
- Hacker Q&A with Yassine Aboukir
- Hacker Spotlight: Mikhail Egorov
- Meet the Hacker: europa: "I always trust my gut when I get the feeling that something is there"
- OSCP Insights: Busting Myths & Helpful Tips

- Tips for Getting the Right IT Job
- My Journey Into Infosec

Tweeted this week

We created a collection of our favorite pentest & bug bounty related tweets shared this past week. You're welcome to read them directly on Twitter: Tweets from 01/04/2019 to 01/11/2019.

Curated byPentester Land & Sponsored by Intigriti