Bug Bytes #48 – 20 char XSS, HackerOne accidental account takeover & one-time

BY INTIGRITI · DECEMBER 10, 2019 · LAST UPDATED ON MARCH 6, 2025

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series is curated by Mariem, better known as **PentesterLand.** Every week, she keeps us up to date with a comprehensive list of write-ups, tools, tutorials and resources.

This issue covers the week from 29 of November to 06 of December.

Our favorite 5 hacking items

1. Tutorial of the week

> "Exploiting XSS with 20 characters limitation"

This tutorial solves a specific problem: bypassing character limitation to exploit XSS. To do that, the idea is to load a remote JavaScript file hosted on a very short domain.
What I love about this tutorial is that it goes further than theory: in practice most short domains are taken or very expensive. Using Unicode, it is possible to redirect to domains like .pw (5 characters) which expands to telsr.pw (8 characters).
Two excellent resources for working with Unicode are also shared.

2. Writeup of the week

> "– Account takeover via leaked session cookie on HackerOne ($20,000)
> – HTTP Request Smuggling + IDOR"

These writeups are both worth reading for different reasons. The HackerOne account takeover was the most shared/debated this week. @haxta4ok reported a false positive, but the triager's response included their valid session cookie. $20,000 for human error (and an initial false positive)! HackerOne have added mitigations to prevent this happening again, but it could happen to employees that don't use HackerOne's triage or triagers from other companies.
The second writeup shows how you can chain HTTP Request Smuggling with IDOR for increased impact.

3. Resource of the week

> "One-time Mobile Numbers Thread"

This is a collection of websites for receiving SMS online for free. I haven't had the occasion to test them yet, but I'm bookmarking this for future pentest engagements and bug bounty. They will be handy for SMS verification and 2FA.

4. Conference of the week

> "Wild West Hackin' fest (WWHF) 2019"

This looks like a fun conference to attend. Topics range from Burp Suite collaboration to hacking your career, Google Calendar attack surface, social engineering, building an escape room, Kerberos, etc. There is probably something that woud interest you whether you're into pentest, red team, bug bounty, physical security, social engineering or incident response.

5. Article of the week

> "Server Side Request Forgery (SSRF) and AWS EC2 instances after Instance Meta Data Service version 2(IMDSv2)"

Following the Capital One breach, AWS EC2 recently introduced new changes to the way metadata information is retrieved. This prevents SSRF exloitation and may leave you wondering whether you should stop looking for SSRF on EC2.
This article is a nice summary of the new changes and what they mean for hackers/bug hunters.

Other amazing things we stumbled upon this week

Videos

- @erbbysam talks about defcon, scanning the entire internet for certs, and becoming a HackerOne MVH!
- Best Operating Systems for Hacking?!
- Setting Up Your Ubuntu Box for Pentest and Bug Bounty Automation
- Ted Demopoulos: How To Be A Cyber Security Consultant | DailyCyber 207
- Cybertalk – EP3 – Cybersecurity Certifications & Learning Resources

Podcasts

- Security Now 743 – Android "StrandHogg"
- Risky Business #565 — Crypto bro takes Jong turn
- Hackable? 36 – Gone Phishin'
- Application Security Weekly #87 – Facebook, Twitter, & Firefox
- Hack Naked News #244

Webinars & Webcasts

- Knock knock, who's there? Authenticating your single page apps using JSON Web Tokens

- Webcast: Group Policies That Kill Kill Chains

Conferences

- Reverse Engineering WhatsApp Encryption for Chat Manipulation and More
- Authentication fundamentals: The basics | Azure Active Directory

Slides only

- @PhilippeDeRyck's Talks and slide decks

Tutorials

Medium to advanced

- Developing and Debugging Java Burp Extensions with Visual Studio Code
- Attacking FreeIPA — Part II Enumeration
- Linux Privilege Escalation using Capabilities
- Automation Testing With Ansible, Molecule, and Vagrant
- The Difference Between System V and SystemD
- Android SSL Pinning Bypass Using Objection and Frida Scripts
- Using SerializationDumper for Java Deserialization and CTFs

Beginners corner

- Authenticated Scan using OWASP-ZAP
- XXE Attacks — Part 2: XML DTD related Attacks
- Hacking XML Data
- Getting a Grasp on GoogleID's & TL;DR
- Windows for Pentester: Certutil
- Understanding Reverse Shells
- Commands and Tools for Embedded Reverse Engineering

Writeups

Pentest writeups

- How I was able to uniquely bypass authentication while web pentesting?

Responsible(ish) disclosure writeups

- BlackDirect: Microsoft Azure Account Takeover #Web
- Shopping for an admin account via path traversal #Web
- Strapi Framework Vulnerable to Remote Code Execution (CVE-2019-19609) #Web #RCE
- Flaws vs bugs (CVE-2019-9745) #Windows
- Rendering McAfee web protection ineffective #Antivirus #Web

Bug bounty writeups

- Web cache deception attack on Vanilla ($150)
- Information disclosure via GraphQL on Hackerone ($2,500)
- Privilege escalation on Rockstar Games ($750)
- Information disclosure via GraphQL on GitLab ($1,000)
- Stored XSS via cookie on Grammarly ($2,000)

Tools

If you don't have time

- Automatic API Attack Tool & Introduction: Imperva's customizable API attack tool takes an API specification as an input, generates and runs attacks that are based on it as an output
- Barq & Introduction: AWS Cloud Post Exploitation framework. Useful for attacking EC2 instances without having the original instance SSH keypairs
- CodeCat: Tool to help in manual analysis in codereview
- Issue2report: Generate pentest reports based on github issues
- Crtsh: Go script that shows the result of crt.sh with different optional filters
- Subdomain Extractor: Burp extension for extracting subdomains. Usage: Go to your Site Map -> Select All -> Right click -> Copy sub domains

More tools, if you have time

- Awspx & Introduction: A graph-based tool for visualizing effective access and resource relationships in AWS environments (meaning Bloodhound for AWS)
- Mitaka: A browser extension for OSINT search
- Zap-operator: ZAP plugin that helps to attack your Kubernetes applications in production
- bountyRecon: Just an initiative for automating bug bounty recon

- Bug-bounty-kit: Recon setup + automation
- Blue eye: A python Recon script
- Fetcher.sh: Oneliner to quickly check the status code of 1000 urls or more
- Chepy: A python library with a handy CLI that is aimed to mirror some of the capabilities of CyberChef
- NTLMRecon: A fast NTLM reconnaissance and information gathering tool without external dependencies
- Caligo & Introduction: A simple C2 for hostile "dropbox" devices management used in physical security assessments
- JA3Transport & Introduction: A Go library for impersonating JA3 signatures
- Lsassy & Introduction (in French): Remotely parse lsass dumps and extract credentials

Misc. pentest & bug bounty resources

- AWS Ramp-Up Guide: Security – For AWS Cloud Security, Governance & Compliance Professionals, especially AWS Well-Architected Security Labs
- Beginner's Ubuntu Handbook
- Bug Hunting 101 – Web Application Security Testing (Free ebook but in Bahasa)
- Security Tool List Update Dec 2020
- An Overview of Cryptography
- APIsecurity.io Issue 60: Microsoft Azure OAuth2 Vulnerability, 5G Threat Landscape, Webinars
- Find (almost) any GitHub user's email address!
- PEASS – Privilege Escalation Awesome Scripts SUITE (with colors): Privilege escalation tools for Windows and Linux/Unix

Challenges

- DOM XSS challenge by @PwnFunction

Articles

- Help Test Firefox's built-in HTML Sanitizer to protect against UXSS bugs
- Passwords: Our First Line of Defense
- Email authentication: SPF, DKIM and DMARC out in the wild
- Obtaining shells via Logitech Unifying Dongles

- Public SSH keys can leak your private infrastructure

News

Bug bounty & Pentest news

- When Santa invites you to a free hacking conference at the North Pole, you definitely want to be there.
- I want to be James Kettle @albinowax when I grow up...
- Interview with one of the world's best competitive bug hunters

Reports

- The New Norm: Trend Micro Security Predictions for 2020
- A Window into Malicious Advertising – 61% of malvertising targets Windows devices
- Malvertising is on the decline but serious security issues remain
- 44 million Microsoft users reused passwords in the first three months of 2019
- Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021

Vulnerabilities

- The best hacks from Black Hat Europe 2019
- Hack that lifts limits on contactless card payments debuts at Black Hat Europe 2019
- New vulnerability lets attackers sniff or hijack VPN connections
- SMS Replacement is Exposing Users to Text, Call Interception Thanks to Sloppy Telecos
- Some Hardware-based Password Managers Have Poor Security
- Critical DoS messaging flaw fixed in December Android update

Breaches & Attacks

- Android vulnerability StrandHogg shatters user privacy, impacts top 500 apps & interesting comments by @LukasStefanko & @fs0c131y
- Hackers Find Ways Around a Years-Old Microsoft Outlook Fix
- 'Ultimate' MiTM Attack Steals $1M from Israeli Startup
- iCloud-hacking politician to be sentenced on Christmas eve
- Clever Microsoft Phishing Scam Creates a Local Login Form
- Malicious Python Package Available in PyPI Repo for a Year

Malicious apps/sites

Other news

- UK Government Releases Photos of Russian Hackers, Whose Lives Look Awesome
- Top gadgets for the security and privacy conscious (or the super paranoid!)
- This cheap gadget can stop your smartphone or tablet being hacked at an airport, hotel or cafe
- You Can Still Upgrade to Windows 10 For Free, Here's How
- Protecting users from government-backed hacking and disinformation
- FBI Recommends Securing Your Smart TVs and IoT Devices
- 5G hackers: These eight groups will try to break into the networks of tomorrow
- These are the worst hacks, cyberattacks, and data breaches of 2019

Non technical

- The Motivation Secret: How to Maintain Intense Motivation as a Hacker (or Anything)
- Art as a Methodology for Security Research
- The snooping girl on a train, again. How to compromise a business
- Misconceptions: Unrestricted Release of Offensive Security Tools
- How Remote Workers Make Work Friends
- More Tips for Social Media and Presenting
- Red Team Engagement Guide: How an Organization Should React

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 11/29/2019 to 12/06/2019.

Disclaimer:

The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti. ***Curated by Pentester Land & Sponsored by Intigriti***