Bug Bytes #40 – Third Level Domains, LevelUp 0x05 & Authorization Token Manipulation

BY INTIGRITI · OCTOBER 15, 2019 · LAST UPDATED ON JULY 30, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-40-third-level-domains-levelup-0x05-authorization-token-manipulation

Bug Bytes is a weekly newsletter curated by members of the bug bounty community. The first series are curated by Mariem, better known as **PentesterLand**. Every week, she keeps us updated with a comprehensive list of all write-ups, tools, tutorials and resources we should not have missed.

This issue covers the week from 04 to 11 of October.

Intigriti news

- Colruyt just changed their framework and is looking for fresh bugs!

Our favorite 5 hacking items

1. Video of the week

> Bug Bounty – Hunting Third Level Domains

If you have heard of recursive subdomain enumeration and wished to see practical examples, this is a video for you.
@thecybermentor shows how to enumerate subdomains, spot interesting ones, and iterate enumeration to get third level domains. He also shows how to organize findings, automate the whole process, and go further by using Nmap and Eyewitness. Really helpful for beginners to automation and recon!

2. Slides of the week

> Entrepreneurship for hackers: "A thing or two I learnt while building PentesterLab"

As a hacker and entrepreneur, I'm very interested in what @snyff has to say. He built Pentester Lab by himself, without investors and has been living from it since 2018, while providing real value to clients.
If you too are interested in entrepreneurship, you might want to read about his advice on what a good idea is, why external funding is not necessarily an advantage, why starting a business with a free product is a bad idea, how to price your product, etc.

3. Tools of the week

> – Dr. Watson
> – GitHub tools collection

Dr. Watson is a Burp Suite extension that passively detects secrets in domains in scope based on a Regex. To try it, I have added Github to Burp's scope and navigated a repository that I knew contained a lot of sensitive information. Immediately, new issues appeared for github.com: "Asset discovered: S3 bucket", "Asset discovered: IP"...
The tool can find keys, S3 buckets, DigitalOcean Space, Azure blobs, IP addresses, domains and subdomains. But since regexes are defined in a file (issues_library.json), it is possible to extend its capabilities by adding new regexes.
The second set of tools are scripts for finding sensitive information on Github. I love that they are lighweight, each do one specific thing, and are great examples to study for anyone who wants to learn programming for hacking purposes.

4. Conference of the week

- LevelUp 0x05

It's always a joy to watch LevelUp. I think it is one of the best conferences for bug hunters and Web app pentesters.
In this edition, there are four talks on car hacking, Android app vulnerabilities, GSuite security, and GraphQL hacking.

5. Tutorial of the week

- Authorization Token manipulation using Burp Suite extender & BearerAuthToken

This tutorial and tool might be handy if you have to test an application that requires an authorization token for each request, with a short session timeout.
Once a token expires, you have to manually re-authenticate on the app to get a new one. But this breaks Burp's scanner automation.
The solution offered, BearerAuthToken, is a Burp Suite extension that automatically generates a new token for each request to make sure that it will be valid and that the authenticated state will be maintained. So useful and easy to use!

Other amazing things we stumbled upon this week

Videos

- 09/15/2019 – Live Bug Bounty Recon Session on Yahoo (meg, assetfinder, etc) w/ @Tomnomnom
- Top 3 Certifications for Landing an Ethical Hacking Job
- Automating Recon with Bash Scripting
- Finding Your First Bug: Business Logic Errors
- 6 Things No One Tells You About Getting A Good Job
- Nmap Primer (Part 1) & Part 2
- Python For Penetration Testing – Developing A Banner Grabber

Podcasts

- That Security Podcast S01 Episode 03 – Bug Bounties
- 7MS #384: Creating Kick-Butt Credential-Capturing Phishing Campaigns
- Security Now 735 – Makes Ya WannaCry
- Hackable? 32 – Keyless Ignition
- Coalcast Episode S1E7 – Hiring A Pentester
- Security In Five Podcast Episode 597 – The Internet Gets A Little More Secure At HTTP v3 Rolls Out
- Security In Five Podcast Episode 595 – Tools, Tips and Tricks – Facebook Container By Mozilla
- Hack Naked News #237
- Application Security Weekly #79

Webinars & Webcasts

- InfosecGirls + WoSec session with Liran Tal on Node.js Security
- Webcast: Open Source Exploits in the Cloud's Big Data Services – Cloud TradeCraft
- Webcast: In-Depth SILENTTRINITY Demo, Explanation & Walkthrough
- InfoSecGirls September 2019 Tech talk – Why Report Writing is important in Infosec
- SANS Webcast: Kerberos & Attacks 101
- When Hacking Becomes Deadly – InfoSec in the Age of Connected Medical Devices (Free registration required)

Conferences

- BSides Augusta 2019
- OWASP Bay Area
  - Protecting your web-application from Magecart
  - The Pulse of AppSec: 2019 Trends and Insights
  - Practical Approach to Automate the Discovery and Eradication of Open-Source Software Vulnerabilities

Slides only

- XXSS – Exotic Cross-Site-Scripting Vectors
- The significance of mobile exploit applications
- Step by step AWS Cloud Hacking

- Mobile Pentesting with Frida
- Mining for gold: A framework for accessing Pastebin's hidden treasures
- SSRF – Make the Cloud Rain

Tutorials

Medium to advanced

- Authorization Token manipulation using Burp Suite extender & BearerAuthToken
- Abusing PHP strip tags to bypass modern WAF to exploit XSS
- Mettle your ios with frida
- Automated Frida hook generation with JEB & Sample JEB script
- Understanding insecure implementation of Jackson Deserialization
- An Indirect Way to Change cPanel Passwords
- Proxy-Aware Payload Testing
- How to Exfiltrate AWS EC2 Data
- Internal domain name collision
- Delegating like a boss: Abusing Kerberos Delegation in Active Directory
- Persistence – New Service, Screensaver & Shortcut Modification

Beginners corner

- How to use HTTP Request Smuggler
- Subdomains Enumeration: what is, how to do it, monitoring automation using webhooks and centralizing your findings
- Bypass NAC (Network Access Control)
- XSS SVG
- A run-time approach for penetration testing of iOS apps Part-I & Part-II (Objection in Action)
- (Almost) All The Ways to File Transfer

Writeups

Challenge writeups

- Intigriti XSS challenge writeup & Winner
- XSS challenge: Theory of Browser Evolution

Pentest writeups

- Chaining Low/Info Level Vulnerabilities for Pwnage
- Remote Desktop tunneling tips & tricks

Responsible(ish) disclosure writeups

- WooCommerce 3.6.4 – CSRF Bypass to Stored XSS #Web #CodeReview
- HackMD Stored XSS and HackMD Desktop RCE #Web
- Bludit Brute Force Mitigation Bypass #Web #CodeReview
- Multiple D-Link Routers Found Vulnerable To Unauthenticated Remote Code Execution #RCE #CodeReview
- Rusty Joomla RCE #RCE #CodeReview
- Security Advisory: Active Directory Open to More NTLM Attacks #NTLM

Bug bounty writeups

- XSS escalated to RCE on Valve ($9,000)
- Rate-limiting bypass on Shopify ($500)
- Authorization flaw on Shopify ($1,000)
- Information disclosure on Shopify ($1,500)
- Information disclosure on Samsung
- IDOR & RCE
- XSS ($1,000)
  - https://twitter.com/MasterSEC_AR/status/1182791786051317761
- XSS on Google

See more writeups on The list of bug bounty writeups.

Tools

If you don't have time

- DomainDog: A cli tool to perform reverse whois lookups through viewdns.info
- StatusParser: Retrieve the status codes from a list of URLs

More tools, if you have time

- Snapback: HTTP(s) Screenshots for Pen Testers Who Value Their Time
- Pivoting into VPC networks: Pivot into private VPC networks using a VPN connection

- PHP Object Injection Slinger: Burp Suite extension to automatically identify serialization issues in PHP Frameworks
- Traxss: Automated XSS Vulnerability Scanner
- Entrust-identityguard-tools: Tools for playing with Entrust IdentityGuard soft tokens, such as decrypting QR codes and deriving OTP secrets
- Callback Catcher: A multi-socket control tool designed to aid in pentest activities, like the love child of Burp Collaborator & Responder

Misc. pentest & bug bounty resources

- [A]ndroid [A]pplication [P]entest [G]uide
- Whitepaper: The Definitive Guide to Same-origin Policy
- Bug Bounty Methodology (TTP- Tactics, Techniques, and Procedures) V 2.0
- APIsecurity.io Issue 52: NIST Zero Trust Architecture Guidelines
- World's Biggest Data Breaches & Hacks
- Network pentest tutorials
- Resources Discord Server

Challenges

- Websocket security challenge by Mikhail Egorov
- XSS challenge by Orange Tsai & filedescriptor
- 3 JS/CSS & client-side attacks challenges & Solutions
- 2 challenges by m0z

Articles

- XS-Leak: Leaking IDs using focus
- Understanding the full potential of sqlmap during bug bounty hunting
- Recon Everything
- Super Magic Hashes
- Windows Credential Theft: RDP & Internet Explorer 11
- All your creds are belong to us!
- FIDO2: Solving the Password Problem
- Intelligence Gathering on U.S. Critical Infrastructure

News

Bug bounty & Pentest news

- @daeken AMA
- Update on the arrested and charged Coalfire Pentesters
- The Python 2 branch of EyeWitness is no longer supported. The Python 3 version of EyeWitness has just been merged in
- DNS Bruteforce Injection Point Definition: Pull request to Gobuster to expand its subdomain enumeration capabilities
- Better Bug Bounties & Hacking for Good: Leveraging HackerOne Data to Develop an Economic Model of Bug Bounties
- AWS Cloudfront protects against http desync / request smuggling attacks, but ALB is still vulnerable

Reports

- Rapid7 Introduces Industry Cyber-Exposure Report: Deutsche Börse Prime Standard 320
- The Price of Influence: Disinformation in the Private Sector
- Most Americans don't have a clue what https:// means

Vulnerabilities

- Microsoft NTLM vulnerabilities could lead to full domain compromise & TL;DR
- Signal immediately fixed FaceTime-style eavesdropping bug
- WhatsApp Flaw Opens Android Devices to Remote Code Execution
- Android devices hit by zero-day exploit Google thought it had patched
- Apple iTunes Bug Actively Exploited in BitPaymer/iEncrypt Campaign
- Vulnerable Twitter API Leaves Tens of Thousands of iOS Apps Open to Attacks
- October Patch Tuesday: Microsoft fixes critical remote desktop bug
- D-Link router remote code execution vulnerability will not be patched

Breaches & Attacks

- Reductor malware bundles tricks to compromise TLS traffic
- Hackers bypassing some types of 2FA security FBI warns
- Activists' phones targeted by one of the world's most advanced spyware apps

Other news

- Microsoft Improves Azure Active Directory Security with New Roles
- No More Mixed Messages About HTTPS: Chrome plans on blocking mixed content
- Copy-and-paste sharing on Stack Overflow spreads insecure code
- Twitter Apologizes for Using Your Phone Number for Advertising
- Researchers Say They Uncovered Uzbekistan Hacking Operations Due to Spectacularly Bad OPSEC
- Referring researchers following terms of your bug bounty to the FBI isn't cool
- These are the 29 countries vulnerable to Simjacker attacks

Non technical

- The Next-Gen Attackers (and What Attacks Will Look Like in Future)
- How to Scope a Network Pentest: Tips from a Pentester
- OPSEC in The After Life
- Bugs Wanted Dead or Alive — A New Approach to Responsible Disclosure for All
- Nemesis Contreras
- Real-life social engineering. Another two days in tweets

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 10/04/2019 to 10/11/2019.

Curated by Pentester Land & Sponsored by Intigriti

Disclaimer:The views and opinions expressed in this article are those of the curators and do not necessarily reflect the position of intigriti.