Bug Bytes #15 – New Content Discovery Wordlist, IDOR on Shopify & #askstok Bug Bounty live stream by @stokfredrik

BY INTIGRITI · APRIL 23, 2019 · LAST UPDATED ON MARCH 6, 2025

Hey hackers! These are our favorite resources shared by pentesters and bug hunters last week.
This issue covers the week from 05 to 12 of April.

Our favorite 5 hacking items

1. Resource of the week

> "Content_discovery_nullenc0de.txt"

This is a new content discovery wordlist by @nullenc0de, to use for file & directory bruteforce with tools like dirsearch, dirb, etc.
It's based on @JHaddix's content_discovery_all.txt dictionary but has 300k more directories/files.
As a comparison, here is the exact number of entries in these two and in *dirsearch*'s default dictionary:

```
# wc -l content_discovery_all.txt
373535 content_discovery_all.txt
# wc -l /root/tools/dirsearch/db/dicc.txt
6087 /root/tools/dirsearch/db/dicc.txt
# wc -l content_discovery_nullenc0de.txt
623103 content_discovery_nullenc0de.txt
```

2. Writeup of the week

> "IDOR on Shopify"

This writeup is a gem for so many reasons! I highly recommend reading it and paying attention to all the details:

- How @_ayoubfathi_ used automation to get notifications of new API endpoints (and not only new subdomains!)
- How he created script on-the-fly to during bug hunting to solve specific issues (like building a list of valid Shopify stores)
- How he leveraged a passive DNS database to get a bigger list of Shopify stores
- How he kept trying new approaches over weeks and solving one issue after the other until he confirmed the bug
- How he adapted a BASH script to bypass rate-limiting (WAF) even if it meants that the script would take days to run

- The mistake he made that rendered this awesome finding not eligible for a bounty

3. Non technical item of the week

> "Want to learn a new skill? Take some short breaks"

Taking breaks from the computer is something at which I'm so bad! I get kind of obsessive when working on anything security related.
But this study really motivates me to start taking more breaks. Researchers found that taking a short rest helps our brains retain more information learned a few seconds earlier.
So instead of thinking that rest is a waste of time, it's better to think that it plays a critical role in learning.
More rest = More productity.

4. Video of the week

> "I accidentally started a live stream and it turned into #askstok"

I love this live stream by @stokfredrik! Being relatively new to bug bounty and already getting good results (at least financially), he has a unique perspective. I think that's why newcomers can easily relate to his advice/experience.
So if you're learning bug hunting, and want to get practical advice in an entertaining format (he started live-streaming by accident!), this is the right video to watch. He answers questions like: Can you live out of bug bounty? Do you need to know programming? Is 2019 too late to start bug hunting?...
Let's hope he makes other Q&As. I love peeking at what other hunters are doing and the live interaction is a great opportunity to get instant feedback/answers.

5. Slides of the week

> "H"

Last tuesday, I was thinking about critical server-side issues and decided to switch my focus to SSRF for the next weeks. The day after that, @Alyssa_Herrera_ tweeted about this presentation!
It's a great introduction to this vulnerability class, including both theory and an example of SSRF found on a DoD site.
Just make sure to check out the comments below each slide (they won't appear if you download the file as PDF).

Other amazing things we stumbled upon this week

Videos

- Fuzzing Browsers for weird XSS Vectors
- I accidentally started a live stream and it turned into #askstok
- Can you detect hidden cameras in hotel rooms?

- Clickjacking: how to delete someone else's account?
- Live coding #1: Fixing website security vulnerabilities
- Bug Bounty Hunting – Tools I Use
- Zero to Hero Pentesting: Episode 5 – Scanning Tools (Nmap, Nessus, BurpSuite, etc.) & Tactics
- Intro to WebApp Security Testing – Session 01 – The Basics

Podcasts

- Security Now 710 – DragonBlood
- Darknet Diaries Ep 36: Jeremy from Marketing
- Risky Business #537 — Assange arrested, WordPress ecosystem on fire
- Smashing Security 124: Poisoned porn ads, the A word, and why why why Wipro?
- Sophos podcast Ep. 028 – SPEWS, Android security and scary Facebook messages
- 7MS #358: 4 Ways to Write a Better Pentest Report
- 7MS #359: Windows 10 Security Baselining
- We need to talk about InfoSec – Burning Out

Webinars & Webcasts

- April 2019 Pwn School – What's zDeal with zBang?! Discover Hidden Risks in AD with zBang.

Conferences

- Jessica Payne – Building Security People – BSides Portland 2018 Keynote
- Move Fast and Secure Things (with Static Analysis) & Slides
- B-Sides Orlando 2019
  - Weaponizing Corporate Intel
  - I got loyalty, got royalty inside my DNA

Slides only

- Piercing the Veil: Server Side Request Forgery to NIPRNet access
- CSP: A successful mess between hardening and mitigation
- Trusted Types and the end of DOM XSS
- Active Directory Security – AD Attacks & Mitigation

Tutorials

Medium to advanced

- Separating Subdomains From Third-Party Hosted WWW Domains
- BloodHound and CypherDog Cheatsheet
- Simple AV Evasion Symantec and P4wnP1 USB
- AV WARS: Fighting fire with fire [AV Bypass Technique]
- The "-" impact of Network Level Authentication on failed logon events – 4625
- Antimalware Scan Interface (AMSI) — A Red Team Analysis on Evasion

Beginners corner

- Cobalt Strike. Walkthrough for Red Teamers
- Security Headers
- OWASP Top 10 – What are Different Types of XSS ?
- Additional Book Exercises: Apache Tomcat Guessable Credentials

Writeups

Challenge writeups

- Securinets Final 2019 / Woow
- PlaidCTF 2019: Potent Quotables
- BreizhCTF 2019 – Primera sangra

Pentest writeups

- My Personal OSINT Techniques, Part 1 of 2: Key & Layer, Contingency Seeding
- Drop-by-Drop: Bleeding through libvips & Automatic detection of image processing memory disclosure added to the upload-scanner Burp extension
- Being Stubborn Pays Off pt. 1 – CVE-2018-19204
- Exploiting Apache Solr through OpenCMS
- Drop-by-Drop: Bleeding through libvips
- How NOT to use the PAM trust – Leveraging Shadow Principals for Cross Forest Attacks

Responsible disclosure writeups

- Tic Toc Pwned

- [Special Case] HerkoKuDns is Still vulnerable to Subdomain Takeovers (Live PoC)
- Tchap: The super (not) secure app of the French government
- CSTI & RCE on EA's Origin desktop client
- OE Classic <= 2.8.0 RCE via stored XSS
- CareMonkey SaaS BB #1 – Token Reset Vulnerability
- _CVE-2019-3799_ :Directory Traversal with spring-cloud-config-server
- Technical Advisory: Multiple Vulnerabilities in SmarterMail
- Unsafe Object Deserialization in Sitecore <= 9.1.0
- Microsoft Edge Uses a Secret Trick And Breaks Internet Explorer's Security: 0day in Internet Explorer that allows stealing users' files

Bug bounty writeups

- DOM XSS on Shopify ($5,000)
- XS-Search / Information disclosure on Twitter ($560)
- Domain & Twitter account hijacking on @EdOverflow's BBP (0.00579259 BTC)
- Homograph attack on HackerOne ($500)
- Authorization/Logic flaw on HackerOne ($500)
- IDOR on private program ($5,000)
- Authorization flaw on GitLab ($2,000)
- Ticket trick / Authorization flaw on private program ($9,500)
- File disclosure on private program: Steps for exploiting Dump.rdb files
- SSRF on PDFReacter parser used by private program

See more writeups on The list of bug bounty writeups.

Tools

- Brute53: A tool to bruteforce nameservers when working with subdomain delegations to AWS
- PyWhatCMS: Unofficial WhatCMS API package
- Web-cve-tests & Introduction: A simple framework for sending test payloads for known web CVEs
- w12scan: An asset discovery engine for cybersecurity. Seems interesting but it's in Chinese :/
- SharpGPO-RemoteAccessPolicies: A C# tool for enumerating remote access policies through group policy. Useful for targeted lateral movement

- Vampire: Vampire is an aggressor script which adds a “Mark Owned” right click option to beacons. For better Cobalt Strike organization during pentests/red teams

Misc. pentest & bug bounty resources

- Pwny Racing: Live streamed pwnable challenge competitions
- Book of BugBounty Tips
- Content_discovery_nullenc0de.txt: 300k more dirs/files added to @Jhaddix’s content_discovery_all.txt
- XSS Tricks
- Top 13 Online Vulnerability Scanning Tools
- OSCP repo
- PenTestTools.xlsx
- APIsecurity.io Issue 27: MyCar vulnerability, serverless, IoT API security

Challenges

- Blaklis’ CTF challenges
- Hacker Test

Articles

- Unmasked: What 10 million passwords reveal about the people who choose them
- My Fight for the OSCP
- Yet Another OSCP Exam Blog Post
- Password Spraying- Common mistakes and how to avoid them
- Setting Up a Home Lab
- Cybersecurity: “Information Security has always had a tie to protecting data as a core part of its identity. CyberSecurity, on the other hand, includes more connotations around protecting anything and everything we depend on—including things like critical infrastructure.”
- Analysis of UXSS exploits and mitigations in Chromium
- Serious Security: Ransomware you’ll never find – and how to stop it
- Four tools to consider if you’re adopting ATT&CK
- DNS Hijacking Abuses Trust In Core Internet Service: “Technical details of a state-sponsored attack manipulating DNS systems”

News

Bug bounty news

- Two new Google operators for date filters: before & after
- Announcing rescope v1.0 – Scoping for Bug-Bounty Hunters Made Easy: “No longer do you have to copy/paste the scope section to a file and set excludes manually. Just tell rescope which program you’d like to scope and it’ll take care of the rest.”
- Announcing the Community T-shirt Winner(s)

Reports

- Shifting Docker security left

Vulnerabilities

- Broadcom WiFi Driver Flaws Expose Computers, Phones, IoT to RCE Attacks

Breaches & Attacks

- State-Sponsored DNS Hijacking Infiltrates 40 Firms Globally
- Hackers could read non-corporate Outlook.com, Hotmail for six months
- Facebook admits “supply chain data leak” in new Oculus headsets
- Dead Windows Live tiles regain new life in subdomain takeover
- Chrome flaw on iOS leads to 500 million unwanted pop-up ads
- WiPro vs Brian Krebs
- A security researcher with a grudge is dropping Web 0days on innocent users
- Matrix.org got hacked and the attacker posted GitHub issues with description how they did it: “Complete compromise could have been avoided if developers were prohibited from using ForwardAgent yes or not using -A in their SSH commands.”

Other news

- Facebook user data used as bargaining chip, according to leaked docs
- Facebook harvested 1.5 million people’s email contacts without their consent. It says it “unintentionally uploaded” them after asking users for their email passwords.
- Amazon staff listen to customers’ Alexa recordings, report says
- Article 13: EU countries approve copyright directive
- Former Mozilla exec: Google has sabotaged Firefox for years

- Security researcher MalwareTech pleads guilty

Non technical

- Want to learn a new skill? Take some short breaks
- Hacker Spotlight: Ambassador Arne Swinnen
- Meet our hackers – MPGN
- Q&A: What Is It Like to Be a Mobile App Pen Tester?
- From beginner to submitting 5 reports to HackerOne
- Know your attacker: Speaking with Josh Kamdjou from Sublime Security
- VAs, Scans and PenTests; not the same thing

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 04/05/2019 to 04/12/2019.

*Curated by Pentester Land & Sponsored by Intigriti*Subscribe to the newsletter here!