Bug Bytes #75 – NahamCon, ServiceNow misconfigurations & Creating your own Alfred

BY ANNA HAMMOND · JUNE 17, 2020 · LAST UPDATED ON MARCH 6, 2025

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-75-nahamcon-servicenow-misconfigurations-creating-your-own-alfred

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 05 to 12 of June.

Our favorite 5 hacking items

1. Conference & Videos of the week

NahamCon day 1, Day 2, Schedule & Slides

How To Do Recon: API Enumeration & Live API Hacking Demo

NahamCon is a bug hunter's paradise. One place where you could hear from top bug hunters about amazing practical hacking techniques, new research, online and for free!

To give you a taste: @defparam dropped some pretty serious HTTP request smuggling stories. @securinti shared some of his mindblowing email hacking kung fu. @Jhaddix published his long awaited Bug Hunter's Methodology v4. @tomnomnom demystified the art of creating custom wordlists. Plus a lot more hacking goodness!

@InsiderPhD's video series on API recon is also a valuable resource. She does a great job of breaking it down into actionable steps, with lots of demos.

2. Writeups of the week

Multiple Information exposed due to misconfigured Service-now ITSM instances ($30,000)

This is yet another example of a bug that seems so simple... after you hear about it! The difficulty is knowing what to focus on. So, kuddos to @Th3G3nt3lman! He analyzed ServiceNow products and found that the Knowledge Management app has some endpoints that are accessible without authentication. He was able to access sensitive data of several companies.

This is a cool example of new research. It is similar to techniques previously seen like exposed Atlassian pages, but applied to different products.

3. Tool of the week

Infosec-Alfred & The Art of automation, creating your own Alfred

This tool is an awesome effort to solve a common problem: information overload, and information being scattered across so many different sites that don't always have an RSS feed.

@0xsha uses Web scraping to monitor sites (e.g. Github Advisory, Exploit DB, Pentester Land, HackerOne Hacktivity) for new content. New links are added to an SQLite3 database. This kind of scraping and gathering news at the same place is such a time saver!

4. Tutorials of the week

Editing Files on your VPS with sublime on local machine.

Save and Search Your Web Traffic Forever with elasticArchive for Mitmproxy

I know, VIM, Burp and love are all you need... Why would anyone want to edit files on a VPS with a GUI editor? Or use a Web proxy in addition to Burp?

Using an editor like Sublime Text over your VPS is really convenient. It allows for running a headless distribution on the server, and still browsing remote files as if they were on your local system, without having to deal with the "How to exit VIM?" riddle.

The ElasticArchive setup is also handy, especially for bug hunters who want to be able to save and later analyze all traffic, all targets combined. It makes it easier to revisit historical data.

5. Non technical item of the week

How a Lazy Bitch like me learned to be Productive

This is a good read for anyone who feels like there is so much to do, not enough time, and everything is a priority. So, what ends up happening? Nothing! Trying to do everything at once generally doesn't work long term.

This blog is about 3 rules that help deal with this feeling of overwhelm and improve productivity. The tone is fun and there is comfort in knowing other people are struggling with this too!

Other amazing things we stumbled upon this week

Videos

- Bounty Thursdays – URLPROBE, GITSCRAPER, NAHAMCON, SSHGIT and much more!
- @LiveOverflow Talks About the Importance of CTFs, Hacking, Creating Content for Hackers, and more!
- Bug Bounties with InsiderPhD (not PHP)
- Hacking Sunday ep. 1
- Learn Git
- Approaching an e-commerce target!

- Interview with a hacker: John hammond
- Cracking RAR Password (The smart way) w/Hashcat & John The Ripper
- Cybertalk – EP6 – Don't Dual Boot

Podcasts

- Security Now 770 – Zoom's E2EE Debacle
- Darknet Diaries Ep 67: The Big House
- Risky Business #587 — Full scale of Indian hacking-for-hire revealed
- Cybersecurity careers: How to stand out, get hired and make more money
- PSW #653 – "Burn-In: A Novel of the Real Robotic Revolution" – Peter Singer
- PSW #655 – New Web Technology & Impact on Automated Security Testing – Benjamin Daniel Mussler
- PSW #655 – OSS Vulnerabilities, UPnP Flaws, & 0-Days for Bad People
- ASW #110 – Zoom Vulns, Apple 0-Days, & Abandoned Domains

Webinars & Webcasts

- DLL Hijacking with Invoke-PrintDemon
- Modern Web Application Penetration Testing Part 3, NoSQL injection with MongoDB
- SANS @MIC Talk – Introduction to Docker for security work

Conferences

- WomenHackerz, Track 2, Schedule & @InsiderPhd's slides
- Hacker Rights – Chloe Messdaghi

Tutorials

Medium to advanced

- Creating an Internal Pen Test VM with Ngrok
- Content Security Policy Bypass
- Protect your resources from web attacks with Fetch Metadata
- Malicious AzureAD Application Registrations
- Red Team: How to embed Golang tools in C#
- Abusing Windows Telemetry for Persistence

- Red Team: Using SharpChisel to exfil internal network
- How to get a reverse shell from Golden/Silver Ticket without Metasploit?

Beginners corner

- Intercepting Flutter traffic on iOS & Intercepting Flutter traffic on Android x64
- Compromising Android Applications with Intent Manipulation
- Smali: Assembler for Android's VM
- Hacking Android Application: Secret Diary
- Real-time third-party code injection
- Subdomain Takeover via Intercom with steps (Video)
- Active Directory: My Way (Part 1) & Part 2
- Beyond the Edge: How to Secure SMB Traffic in Windows #BlueTeam
- Email to Flickr-account #1 & #2

Writeups

Challenge writeups

- Writeup of @terjanq's Scriptless Pwn2Win 2020 CTF
- OSINT geolocation challenge or else "How to stalk with Google"

Pentest writeups

- How to hack a company by circumventing its WAF for fun and profit – part 3
- SAP PENTEST: Metasploit Writeup

Responsible(ish) disclosure writeups

- Apache Kylin 3.0.1 Command Injection Vulnerability #Java #RCE #CodeReview
- CallStranger #UPnP
- CVE-2020-13777: TLS 1.3 session resumption works without master key, allowing MITM & CVE-2020-13777 GnuTLS audit: be scared #GnuTLS
- A Trio of Bugs Used to Exploit Inductive Automation at Pwn2Own Miami #Java #SCADA
- SMBleedingGhost Writeup: Chaining SMBleed (CVE-2020-1206) with SMBGhost #SMB
- Diving into the SMBLost vulnerability (CVE-2020-1301) #SMB
- Legacy LVFS S3 bucket takeover and CVE-2020-10759 fwupd signature verification bypass #Web
- Analysis of CVE 2020 7350 #RCE

- System Takeover Through New SAP ASE Vulnerabilities #SAP

Bug bounty writeups

- SSRF on project import via the remote_attachment_url on a Note (GitLab, $10,000)
- gitlab-workhorse bypass in Gitlab::Middleware::Multipart allowing files in `allowed_paths` to be read (GitLab, $10,000)
- Docker Registry HTTP API v2 exposed in HTTP without authentication leads to docker images dumping and poisoning (Semmle, $2,000)
- RCE as Admin defeats WordPress hardening and file permissions (WordPress, $800)
- This is fine 🔥 (Microsoft)
- DoS and BugBounties :A series of DoS attacks on HackerOne
- Local file read via XSS using PDF generate functionality
- From 3,99 to 1,650 USD (Part I) – Simple Vertical Privilege Escalation by Changing HTTP Response ($1,000)
- My First Bug Bounty – Gitter $1,000 one-click DoS (Video)
- Making further registrations difficult on Vanilla forum (Vanilla, $150)

See more writeups on The list of bug bounty writeups.

Tools

- URL Tracker: Change monitoring app that checks the content of web pages in different periods. It can be used to monitor S3, Azure, JS files...
- Penglab: Free hash cracking with hashcat on Google Collab
- SecretFinder: A python script for find sensitive data (apikeys, accesstoken,jwt,..) and search anything on javascript files
- Recox: Master script for web reconnaissance
- Ayfabtu & Intro: Scripts to extract files from SCM directories left on web servers
- TarlogicSecurity/kerbrute: An script to perform kerberos bruteforcing by using impacket
- ntlm_theft & Intro: A tool for generating multiple types of NTLMv2 hash theft files
- Shad0w & Introduction: A post exploitation framework designed to operate covertly on heavily monitored enviroments
- Linuxprivcheck: Python script for privilege escalation for Python
- Unicorn: Unicorn is a simple tool for using a PowerShell downgrade attack and inject shellcode straight into memory. Based on Matthew Graeber's powershell attacks and the powershell bypass technique presented by David Kennedy (TrustedSec) and Josh Kelly at Defcon 18
- Boko: Application Hijack Scanner for macOS

- Minimalistic TCP / UDP Port Scanner: Minimalistic TCP & UDP port scanners for avoiding EDR detection
- NTLMRawUnhide.py
- Chisel: A fast TCP tunnel over HTTP (basically SSH over websockets)
- Reg1c1de: Registry permission scanner written in C# for finding potential privesc avenues within registry

Misc. pentest & bug bounty resources

- Q&A session with @Agarri_FR
- Bash alias to send Slack notifications
- CORS one liner command exploiter: A one liner Bash command which finds CORS in every possible endpoint
- Hacker Container: Container with all the list of useful tools/commands while hacking Kubernetes Clusters
- SecGen: Create randomly insecure VMs
- The Hacker Book Club
- Phishing Toolkit: Top 20 Best Phishing Tools
- Awesome automotive
- How to get started in Industrial Control Systems (ICS) cyber security
- Adaz: Active Directory Hunting Lab in Azure: Automatically deploy customizable Active Directory labs in Azure
- GitHub Dorks for Penetration Testing

Challenges

- Intigriti's June XSS Challenge: Winner gets a Burp license!
- @kinugawamasato's XSS Challenge 2020-06
- Mortal Kombat Mini XSS Challenge

Articles

- Cmd Hijack – a command/argument confusion with path traversal in cmd.exe
- U2F with Duo Web Phishable by default
- Searching Facebook Fans... IS BACK!
- Security Analysis of the Democracy Live Online Voting System & Election security: Democracy Live's online voting system 'open to manipulation'

- Explaining how a wallpaper can break a phone and why it happened(summed up)
- Blue teams helping red teams: A tale of a process crash, PowerShell, and the MITRE ATT&CK evaluation

News

Bug bounty & Pentest news

- h@ctivitycon Call for Speakers
- Bugcrowd Releases Vulnerability Rating Taxonomy 1.9 with More Classifications for Credential Exposure
- Burp Suite Pro/Community 2020.5 released
- Empire 3.2.3 is out!
- Terms of engagement: US computer crime laws out of step with changing attitudes to pen tests, ethical hacking

Reports

- (How) Do People Change Their Passwords & TL;DR
- Cybercrime report: Malware slingers riding the crest of the coronavirus pandemic

Vulnerabilities

- GnuTLS fixes 'encryption interruptus' security flaw
- CallStranger UPnP bug allows data theft, DDoS attacks, LAN scans
- Microsoft June Patch Tuesday Fixes 129 Flaws in Largest-Ever Update
- Expiring SSL certs expected to break smart TVs, fridges, and IoTs
- Firefox and Chrome yet to fix privacy issue that leaks user searches to ISPs
- Intel, ARM Hit By Side-Channel Attack Disclosures
- Thought you'd addressed those data-leaking Spectre holes on Linux? Guess again. The patches aren't perfect
- Critical traffic light system vulnerability could cause 'chaos' on the roads
- Windows Group Policy flaw lets attackers gain admin privileges

Breaches & Attacks

- Thanos Ransomware First to Weaponize RIPlace Tactic
- Kingminer patches vulnerable servers to lock out competitors
- Fake ransomware decryptor double-encrypts desperate victims' files

- Researchers unmask Indian ‘infosec’ firm to reveal hacker-for-hire op that targeted pretty much anyone clients wanted
- Microsoft discovers cryptomining gang hijacking ML-focused Kubernetes clusters
- Why would someone want to hack Germany’s PPE supply chain? We’re glad you masked
- Fake SpaceX YouTube channels scam viewers out of $150K in bitcoin
- Gamaredon hackers use Outlook macros to spread malware to contacts
- Encryption Utility Firm Accused of Bundling Malware Functions in Product
- Nation-state actors deploy multi-stage ransomware on critical infrastructure honeypot
- Snake Ransomware Delivers Double-Strike on Honda, Energy Co.

Other news

- Facebook paid for a 0-day to help FBI unmask child predator
- Whatsapp blamed own users for failure to keep phone number repo off Google searches
- G Suite Marketplace primed for a privacy scandal, researchers warn
- Keepnet kerfuffle: Firing legal threats at bloggers did infosec biz more damage than its exposed database
- Microsoft Joins Ban on Sale of Facial Recognition Tech to Police
- FBI warns of increased hacking risk if using mobile banking apps
- Jenkins team avoids security disaster after partial user database loss

Non technical

- What Happened When I Leaked My Server Password on GitHub.com
- Unsecured databases attacked 18 times per day by hackers
- Offensive OSINT: Emulating an advanced attacker
- Vicarious trauma and OSINT – a practical guide
- How to write a Bug Bounty report
- Game Security

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 06/05/2020 to 05/12/2020.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com