Bug Bytes #55 – Frans Rosen's keynote, 2nd order IDOR & Bug Bounty Checklist

BY INTIGRITI · JANUARY 28, 2020 · LAST UPDATED ON AUGUST 8, 2026

Want to read the latest version? Visit the link below:
https://www.intigriti.com/researchers/blog/bug-bytes/bug-bytes-55-frans-rosens-keynote-2nd-order-idor-bug-bounty-checklist

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 17 to 24 of January.

Our favorite 5 hacking items

1. Conference of the week

Frans Rosén Keynote at BSides Ahmedabad

This is a talk I've been impatiently waiting for since it was announced. @fransrosen shares his methodology for breaking Web apps/APIs by using fuzzing and information disclosure.
He uses an imaginary app to show practical examples of building custom API wordlists, finding hidden endpoints, etc. An absolute must watch if you've ever come accross tips on Web app fuzzing and did not know how to apply them in practice.

2. Writeup of the week

A Less Known Attack Vector, Second Order IDOR Attacks

This writeup shows two instances where an app seemed safe but was actually vulnerable to IDOR.
In one case, trying to access another account's info returned an error but the information was displayed in a different location.
The second example seems weird. It involves many steps, so I am not going to try to sum it up in a sentence. But it is definitely something I will start testing for.

3. Video of the week

@Jhaddix Talks About Defcon, Burp Suite, Hacking, Bug Bounties and How He Does Recon!

This is a cool interview with @Jhaddix. Watch if you want to know how he increased his bug bounty payouts and how he deals with companies that silently fix bugs as soon as they detect that he found them. He transformed an N/A report into a 15K bounty using reporting wizardry

4. Tools of the week

> – Sourcemapper
> – Recon-pipeline & How to Build an Automated Recon Pipeline with Python and Luigi – Part VI (Wrapping Up)

Sourcemapper is a Bash script that reconstructs JavaScript from a sourcemap. It is a reliable and fast way to retrieve JS files for further analysis (using tools like LinkFinder).
The recon pipeline is an awesome example of recon automation using Python. The tutorials are fantastic for anyone who want not only a recon tool, but mostly how to build your own.

5. Resources of the week

> – Bug Bounty Checklist for Web App
> – Rewrote my recon bot to output to markdown and upload to a git server

These are cool examples of leveraging markdown to save recon results in a Git repository and to create a testing checklist (in any Markdown note-taking app like Joplin).
It seems so obvious now but when I started using Markdown, I did not think that it could help with these two situations.
In both cases, markdown allows you to take notes that are easy to backup and are displayed in a human-friendly format.

Other amazing things we stumbled upon this week

Videos

- NahamSec Kicks off the New Year With an AMA!
- WHAT? HOW? 28 questions about BUG BOUNTY answered!
- How to check account type using Burp Suite?
- How to make $100,000 a month in Cybersecurity – Informal Chat w. @The Cyber Mentor
- Messing with web attackers with SpiderTrap – John Strand
- Google Hacking For Penetration Testing & Article
- PWNED – SE1 EP1
- IoT Security: Backdooring a smart camera by creating a malicious firmware upgrade
- CVE-2020-0601 aka Curveball: A technical look inside the critical Microsoft CryptoAPI vulnerability

Podcasts

- Darknet Diaries EP 57: MS08-067
- Security Now 750 – The Crypto CurveBall
- Undetected 01 Johan Edholm – Evolution of hacking; Web Security to companies of all sizes

- 7MS #397: OPSEC Tips for Security Consultants
- Risky Business #569 — Bezos' Saudi hack claims, Glenn Greenwald facing cybercrime charges
- The Privacy, Security, & OSINT Show – 153-Privacy News, Travel Routers, & OSINT Updates
- Telnet, ADP, Clearview, VPNs, and How The FBI Handles Hacking Attempts In The Election – SWN #5
- [CPRadio] UltraHack: The Security Risks of Medical IoT

Webinars & Webcasts

- Kerberos Pass-The-Ticket Basics
- 2020 Security Trends from TrustedSec—What's Happening Today, Tomorrow and Far Out

Conferences

- Sector 2019
- Cyber Defense Summit 2019 | Technical Track
- Cyber Defense Summit 2019 | Executive Track
- 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System

Slides only

- API Security Testing – null Bangalore January 2020
- Expose Yourself: Without Insecurity
- Attacking Active Directory for fun and profit

Tutorials

Medium to advanced

- How to Build an Automated Recon Pipeline with Python and Luigi – Part VI (Wrapping Up) & recon-pipeline repo
- Discovering the IP address of a WordPress site hidden behind Cloudflare
- SQL Injection WAF bypass techniques
- [1/3] Cloud-ready Burp Suite on Docker & [2/3] Cloud-ready SSH on Docker
- Analyzing Kony Mobile Applications & Konyutils
- Decrypting values from the Citrix Netscaler config
- CVE-2020-0601 – A curveball breaking the trust

- Revisiting Remote Desktop Lateral Movement
- Get Process List with Command Line Arguments
- PowerShell Obfuscation using SecureString
- Persistence – WMI Event Subscription
- Persistence – Modify Existing Service
- Targeted Active Directory Host Enumeration

Beginners corner

- How to use Arachni to scan Web APIs
- Files on web servers Part I: History Files
- Build a 10 USD Raspberry Pi Tunnel Gateway
- How to Snoop on Bluetooth Devices Using Kali Linux
- Hiding Your Tracks: Bash History
- Exif Data Exposure

Writeups

Challenge writeups

- SQL Murder Mystery

Pentest writeups

- How i got domain admin ?
- Zero to Domain Admin: Bypassing NAC and getting the goods

Responsible(ish) disclosure writeups

- Android (AOSP) Download Provider SQL Injection in Query Selection Parameter (CVE-2019-2198) & PoC #Android
- WordPress <= 5.2.3: Hardening Bypass #Web
- Rate Limit issues that can lead to disclosing some of Spreaker user's data & PoC #Web
- ConnectWise Control 19.3.25270.7185 – Eight Vulnerabilities, Including Critical #Web
- Missing Authorization Check In wpCentral Plugin Leads To Multiple Vulnerabilities #Web #CodeReview
- Juicy Infos hidden in js scripts leads to RCE #Web
- Netgear Signed TLS Cert Private Key Disclosure #InfoDisclosure #Firmware

- CVE-2020-2655 JSSE Client Authentication Bypass #TLS/DTLS
- Finding a Privilege Escalation in the Intel Trusted Connect Service Client #Windows

Bug bounty writeups

- Creating malformed URLs via new line character in-between two URLs leads to misrepresented hyperlinks in Tweets/DMs on Twitter ($560)
- Arbitrary local system file read on open-xchange server on Open-Xchange ($2,000)
- Ubuntu/Debian installation method allows key poisoning and code execution for network attacker on MariaDB #Crypto
- GGvulnz — How I hacked hundreds of companies through Google Groups & How to check your domain and groups settings
- User Account Takeover via Signup Feature | Bug Bounty POC
- Cross-Site Websocket Hijacking bug in Facebook that leads to account takeover ($12,500)
- Password Reset Token Leak Via Referrer

Tools

If you don't have time

- ccrawlen: Python script that uses the CommonCrawl dataset API (petabytes of data!) to extrat subdomains and crawl the data to get interesting endpoints and js files
- Top-Port-Slicer: Python script to give you subsets of the nmap "top-ports". For example, I want the 10th to 100th most common TCP ports. Spits out a comma separated list you can copy into -p arg for nmap or masscan
- Playwright: Node library to automate Chromium, Firefox and WebKit browsers
- Rusty Hogs: A suite of secret scanners built in Rust for performance. Based on TruffleHog (https://github.com/dxa4481/truffleHog) which is written in Python

More tools, if you have time

- Scanner/Poc for CVE-2020-0609 & CVE-2020-0610 (BlueGate): by @MalwareTechBlog & by @ollypwn
- Naabu: A fast port scanner written in go with focus on reliability and simplicity. Designed to be used in combination with other tools for attack surface discovery in bug bounties and pentests
- Peirates: Kubernetes Penetration Testing tool
- S3 Bucket Scraper: A tool for scraping S3 buckets on AWS
- Blinder: A python library to automate time-based blind SQL injection
- Pullit: Find leaked credentials on Github
- ApplicationInspector: A source code analyzer by Microsoft for almost any modern language

- Satellite & Introduction: A Payload and Proxy Service for Red Team Operations
- SharpCookieMonster & Introduction: C# tool that dumps cookies from Chrome for all sites, even those with httpOnly/secure/session flags
- Pcapinator: A tool for processing a lot of pcaps using tshark
- TAS: Framework for easily manipulating the tty and creating fake binaries. Useful as a post-exploitation technique to perform privilege escalation and information gathering
- Grouper2: Find vulnerabilities in AD Group Policy
- Red_Team: Some scripts useful for red team activities
- Zipper: A CobaltStrike file and folder compression utility

Misc. pentest & bug bounty resources

- A simple list with jira, zabbix, kibana and other popular domains in companies
- Chrome-CORS: A demo vulnerable application for stealing sensitive information by abusing Google Chrome cache
- Hacking on a budget
- Java-Deserialization-Cheat-Sheet
- Penetration testing ultimate collection of Cheat sheets
- AwesomeSearch
- Curl HTTP cheat sheet
- thc-1001-tips-and-tricks
- Adversary Tactics: PowerShell: Free SpecterOps PowerShell training
- Windows Red Team Cheat Sheet

Challenges

Articles & Papers

- The Fall Of Mighty Django, Exploiting Unicode Case Transformations
- Unauthorized Google Maps API Key Usage Cases, and Why You Need to Care & Google Maps API Scanner
- Analysis of a Fake Threema App
- Trending Client-Side Innovations In Malvertising Payloads
- ShadowMove: A Stealthy Lateral Movement Strategy & Demo
- Information Leaks via Safari's Intelligent Tracking Prevention

- Defending Infrastructure as Code in GitHub Enterprise
- VirusTotal is not an Incident Responder
- Red Team: Use Case of Open Source Weaponization
- BMW Connected Apps Protocol #CarHacking
- Anatomy of a Facebook-Hosted Phishing Attack

News

Bug bounty & Pentest news

- The owasp membership price changes depending on the country you live in. Makeing it more inclusive!
- @InsiderPhD AMA
- Windows test images before Win10 not on Microsoft site anymore, but can be found on the Wayback Machine
- OAuth 2.0 Token Exchange is now RFC 8693. This specification standardizes an already widely-deployed pattern in production use by Box, Microsoft, RedHat, Salesforce, and many others
- testssl.sh 3.0 released with many improvements
- YesWeHack VDP Finder extension
- InnoGames Models Avatar After Top Ethical Hacker
- Pwn2Own Miami: Hackers scoop $250,000 in prizes during inaugural ICS security contest

Reports

- Crowdstrike Services Cyber Front Lines Report
- Double Dutch: Netherlands tops GDPR breach report index for second year running
- Check Point's 2020 Cyber Security Report
- Malware attacks cost Vietnam $900m in 2019, report claims

Vulnerabilities

- Internet Explorer zero-day surfaces in 'limited targeted attacks'
- Did you really 'like' that? How Chameleon attacks spring in Facebook, Twitter, LinkedIn
- Google to Apple: Safari's privacy feature actually opens iPhone users to tracking
- 'BlackVue' offers an internet dashcam. It's like Amazon's Ring, but for cars. Users can tune into others' feeds. But we found a way to scrape and store the real-time location of drivers across the US. BlackVue said this was not supposed to be possible
- Windows EFS Feature May Help Ransomware Attackers

- Citrix Releases Final Patch as Ransomware Attacks Ramp Up
- Critical, Unpatched 'MDhex' Bugs Threaten Hospital Devices

Breaches & Attacks

- Here Is the Technical Report Suggesting Saudi Arabia's Prince Hacked Jeff Bezos' Phone & Key Technical Elements
- Vivin Nets Thousands of Dollars Using Cryptomining Malware
- Hacker leaks passwords for more than 500,000 servers, routers, and IoT devices
- Trend Micro antivirus zero-day used in Mitsubishi Electric hack
- URL redirect malware infects thousands of WordPress sites
- Betting companies given access to UK gov't information on millions of children
- Microsoft Exposes 250M Customer Support Records on Leaky Servers
- This Citibank Phishing Scam Could Trick Many People

Other news

- ProtonVPN apps handed to open source community in transparency push: contains links to audit reports of the Windows/MasOS, iOS & Android apps
- NIST's new privacy rules – what you need to know
- Clearview app lets strangers find your name, info with snap of a photo, report says
- Want your photo removed from our facial recognition database? Just send us your photo and government-issued ID...
- LastPass Mistakenly Removes Extension from Chrome Store, Causes Outage
- Exclusive: Apple dropped plan for encrypting backups after FBI complained – sources
- The novel way police in Italy hacked suspects' phones
- This Is The Surprising Truth About SMS Security

Non technical

- 5 things to do before running your first bug bounty program
- 6 Habits to save your valuable hours
- Cybersecurity Careers: Your Options
- What's in a name? Thoughts on Red Team nomenclature
- Case Closed: Work-From-Home Is the World's Smartest Management Strategy
- How To Recover From These Three Unavoidable Job Search Setbacks

- 2020 ShmooCon Hiring List

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 01/17/2020 to 01/24/2020.

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