

BUG BOUNTY

Work Smarter, Not Harder

WHOAMI?

Kamil Vavra - Ethical hacker, penetration tester, bug bounty hunter

Ways to Contact Me



@vavkamil



vavkamil.cz



vavkamil@protonmail.com

Contact Me Through Social Media



[@vavkamil](https://twitter.com/vavkamil)

[reddit.com/u/_vavkamil_](https://www.reddit.com/u/_vavkamil_)

github.com/vavkamil

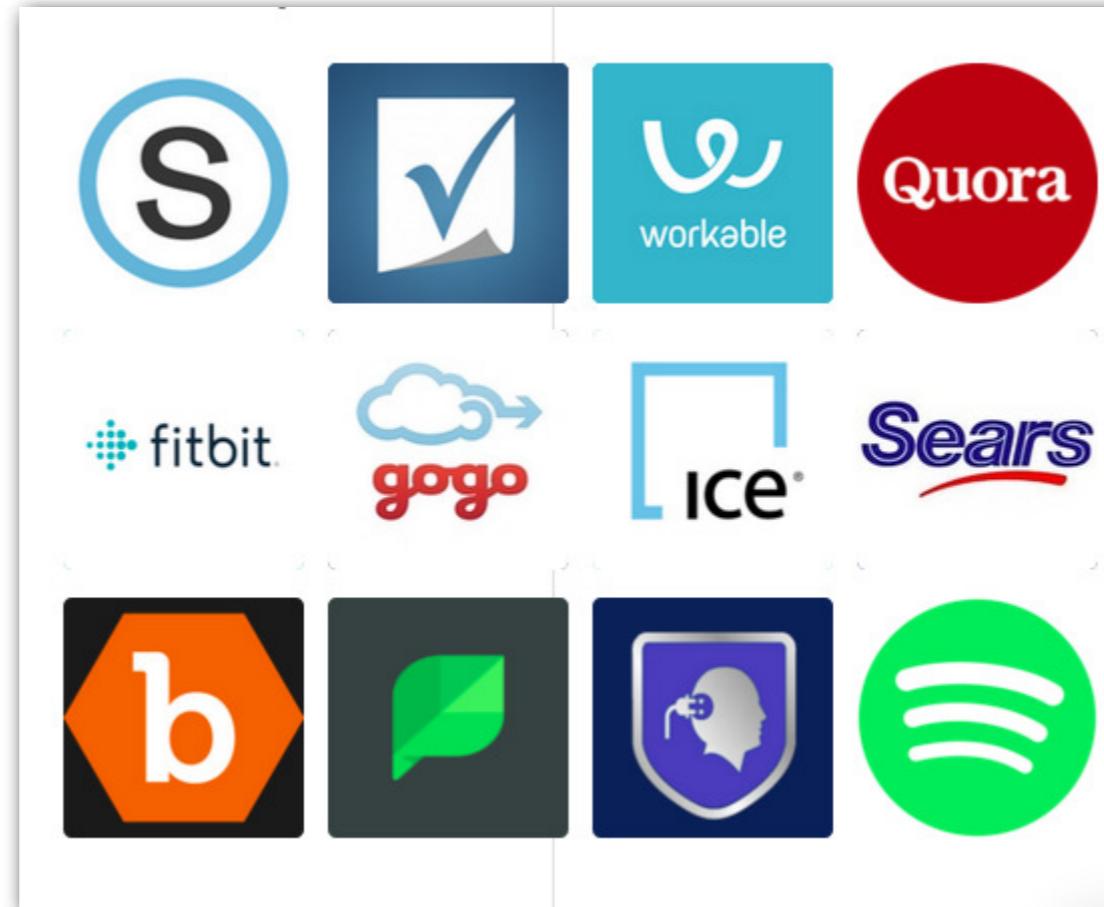
WHOAMI?

<https://vavkamil.cz/whoami/bug-bounty>



WHOAMI?

<https://vavkamil.cz/whoami/bug-bounty>



01

What is bug bounty & main platforms

Quick recap for beginners



02

Knowledge sharing & free resources

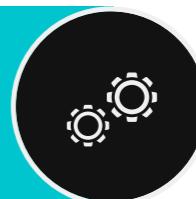
How to gain skill and learn faster



03

Useful open-source tools & scripts

What is everybody using for automation



AGENDA

WTF is this talk about?!

04

Methodology, know-how, tips & tricks

How to catch 'em all

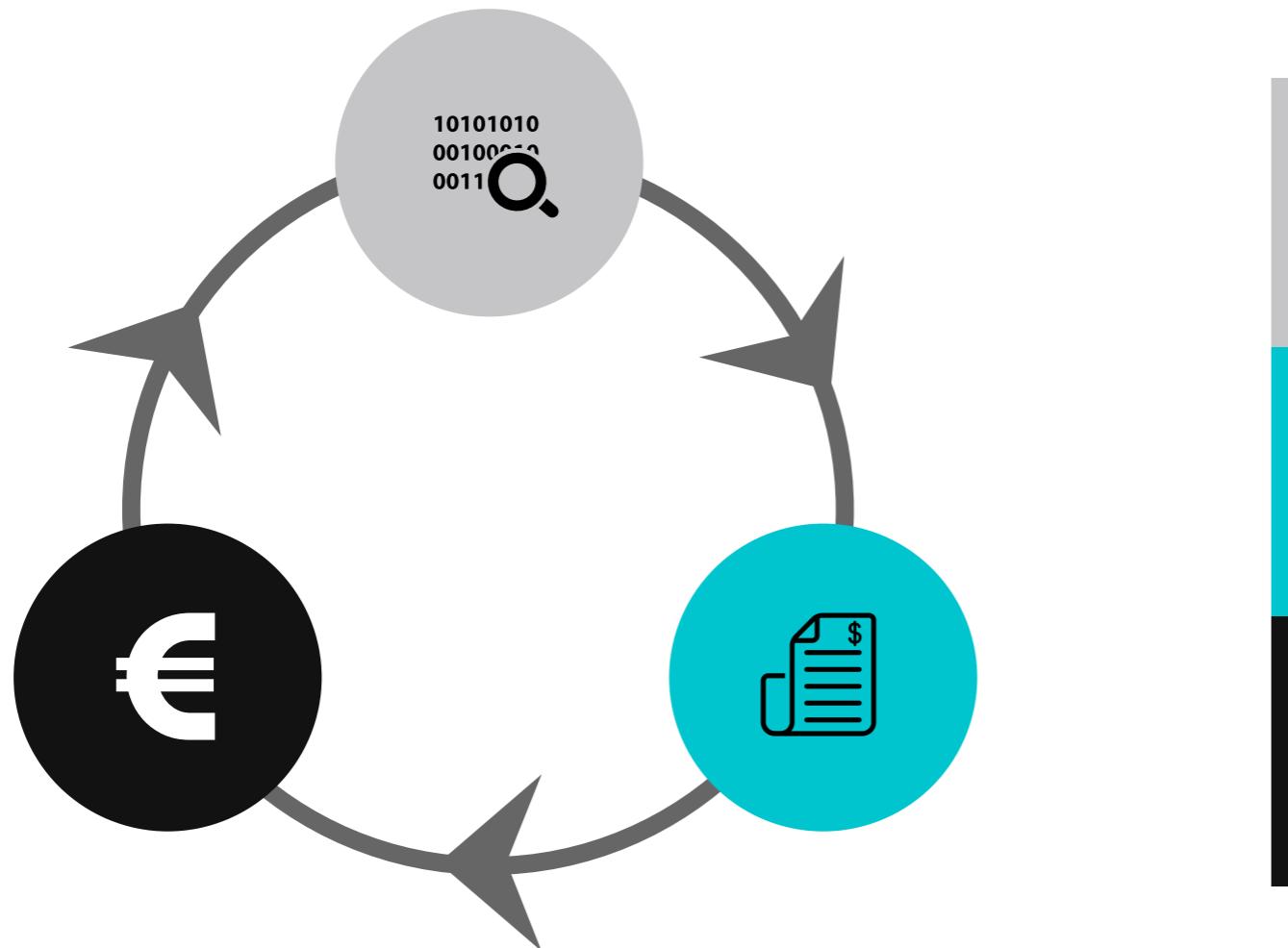


What is bug bounty & main platforms

Quick recap for beginners

3-STEPS BUG BOUNTY MODEL

How does a bug bounty program work?



Find a Bug

Learn to hack, hack to learn

Report a Bug

Don't underestimate quality of report

Get a Bounty

Be kind and respect the amount

MAIN PLATFORMS

Crowdsourced security & vulnerability disclosure platforms

Bugcrowd Inc.

Website	www.bugcrowd.com
Founded	2012
Funding raised	\$51.7M
Estimated Employees	111
Estimated Annual Revenue	\$3.8M
Twitter	@Bugcrowd

HackerOne, Inc.

Website	www.hackerone.com
Founded	2012
Funding raised	\$74M
Estimated Employees	366
Estimated Annual Revenue	\$4.9M
Twitter	@Hacker0x01

Should I start?

Is it worth it?

...it is worth a try!

A major chunk of the hacker's mindset consists of wanting to learn more.

While bug bounty hunting, you will learn a lot; will practice on real world targets, build your reputation and get paid for it ...





Pros

You will learn a lot

Knowledge never ends, sharing is caring, and bug bounty community is awesome

You will earn \$\$

Money shouldn't be the main reason, but it feels nice to be rewarded and recognized



Cons

It takes a lot of time

If you get lucky, you can score your first bounty quite fast. But as every hobby, it takes time to master

There is a lots of competition

You can expect skilled rivals, duplicate reports, boring targets, delayed triagings and payouts



HOW TO BECOME A HACKER



Learn to make it; then break it!

Read blogs, articles, books; lots of content!

Join community; ask questions!

Participate in open-source projects; learn to code!

Smile when you get feedback; don't be a jerk!

Learn to approach targets; reconnaissance is a must!

Knowledge sharing & free resources

How to gain skill and learn faster

WHAT TO READ?

Web Hacking 101

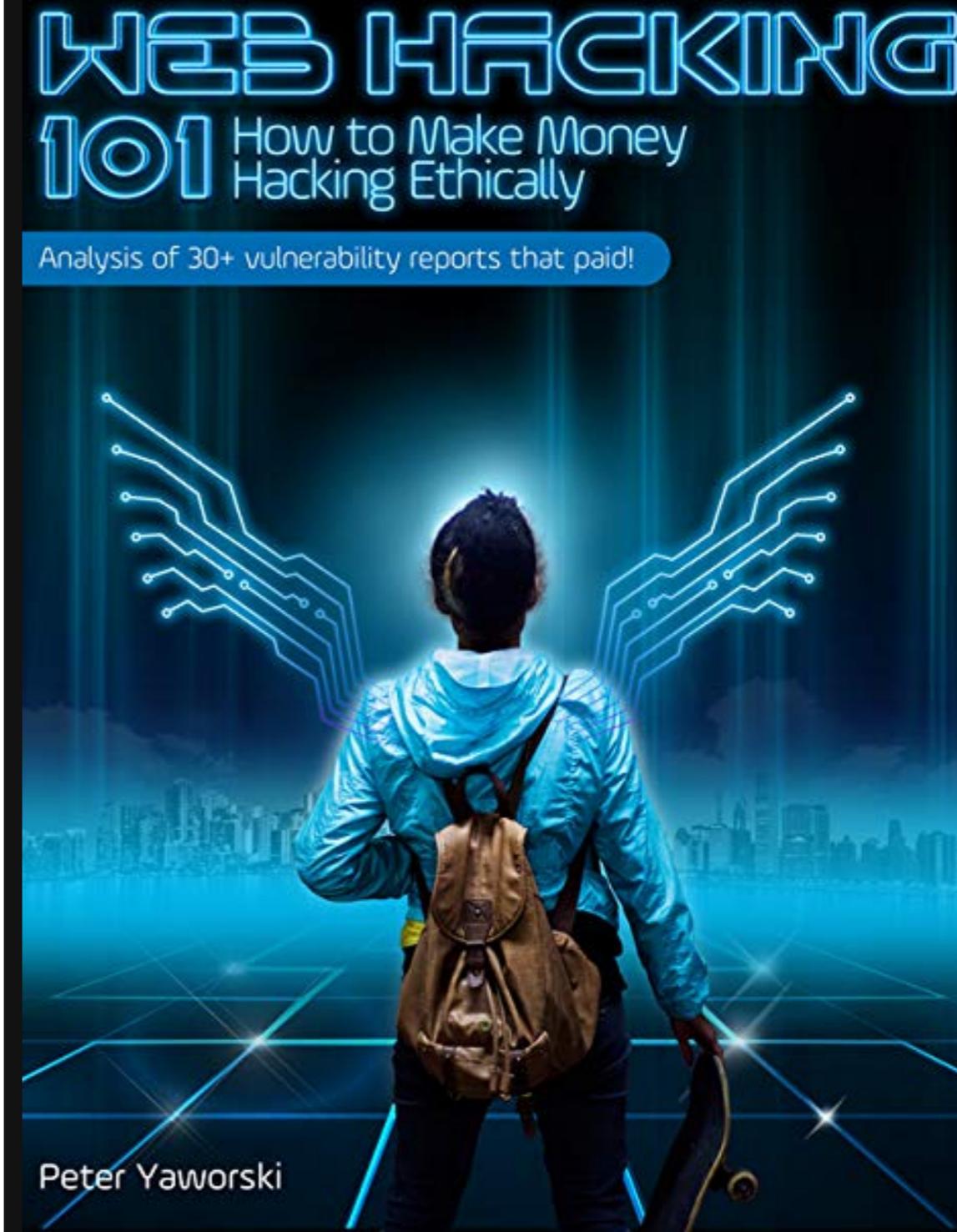
Peter Yaworski

Using publicly disclosed vulnerabilities, Web Hacking 101 explains common web vulnerabilities and will show you how to start finding vulnerabilities and collecting bounties.

After reading this book, your eyes will be opened to the wide array of vulnerabilities that exist and you'll likely never look at a website or API the same way.

<https://leanpub.com/web-hacking-101>

<https://www.hackerone.com/blog/Hack-Learn-Earn-with-a-Free-E-Book>

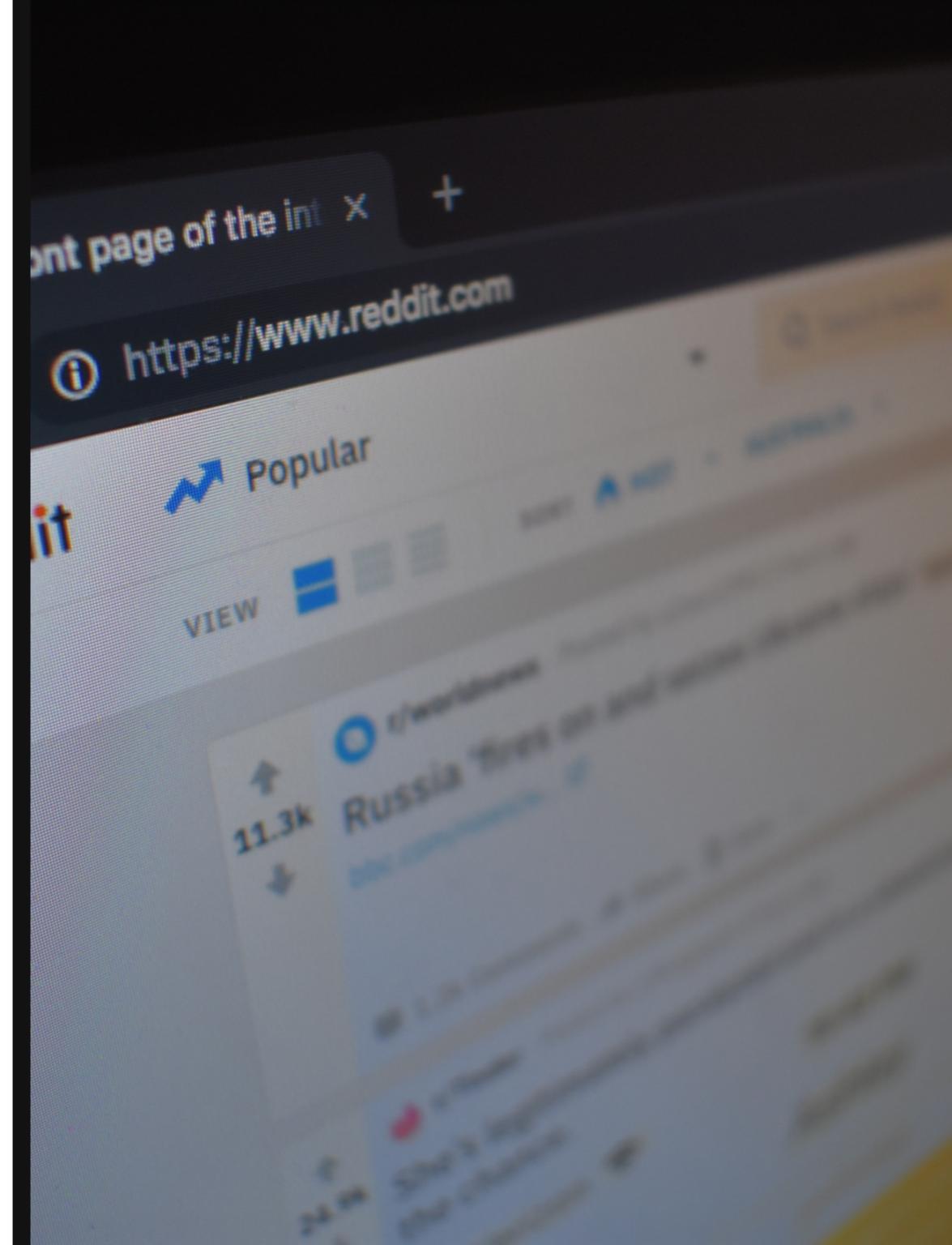


REDDIT

[/r/bugbounty](https://www.reddit.com/r/bugbounty)

3k+ subscribers

Moderator; sharing interesting bug bounty
write-ups almost every day



WHO TO FOLLOW ON TWITTER



@Bugcrowd

<https://twitter.com/bugcrowd/lists/security-researchers>



@PentesterLand

<https://twitter.com/pentesterland>
and



@intigriti

<https://twitter.com/intigriti>



@Hacker0x01

<https://twitter.com/Hacker0x01>



@BugBountyHQ

<https://twitter.com/bugbountyhq>



@disclosedh1

<https://twitter.com/disclosedh1>

GitHub

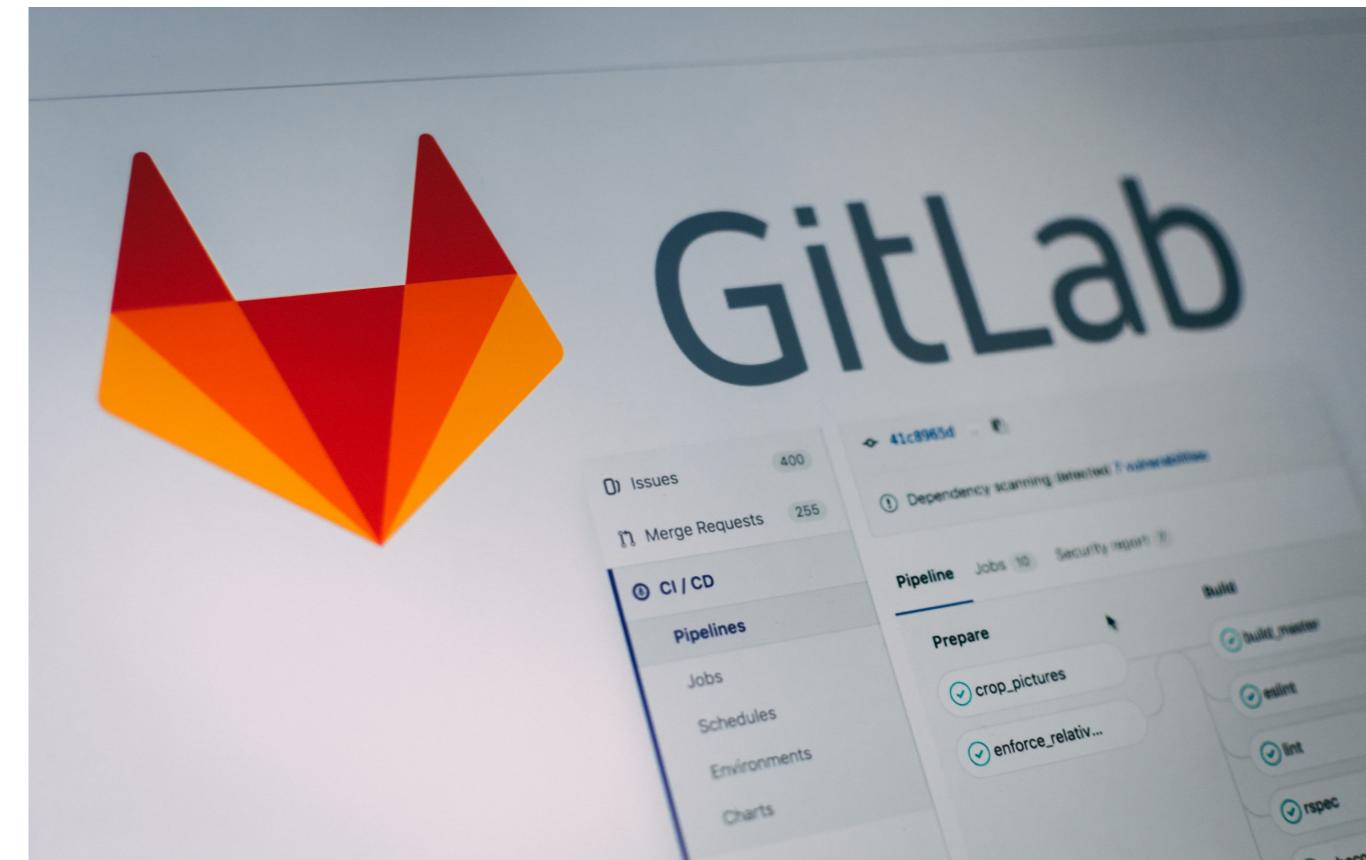
List of bug bounty write-ups

awesome-bug-bounty

<https://github.com/djadmin/awesome-bug-bounty>

bug-bounty-reference

<https://github.com/ngalongc/bug-bounty-reference>



Pentester Land

<https://pentester.land/>

List of bug bounty writeups

<https://pentester.land/list-of-bug-bounty-writeups.html>

The 5 Hacking NewsLetter

<https://pentester.land/newsletter>

The Bug Hunter Podcast

<https://pentester.land/podcast>



PENTESTER LAND

OFFENSIVE INFOSEC



6,000+
HackerOne

Disclosed Reports

<http://sec.eddyproject.com/6000-hackerone-disclosed-reports/>

Useful open-source tools & scripts

What is everybody using for automation

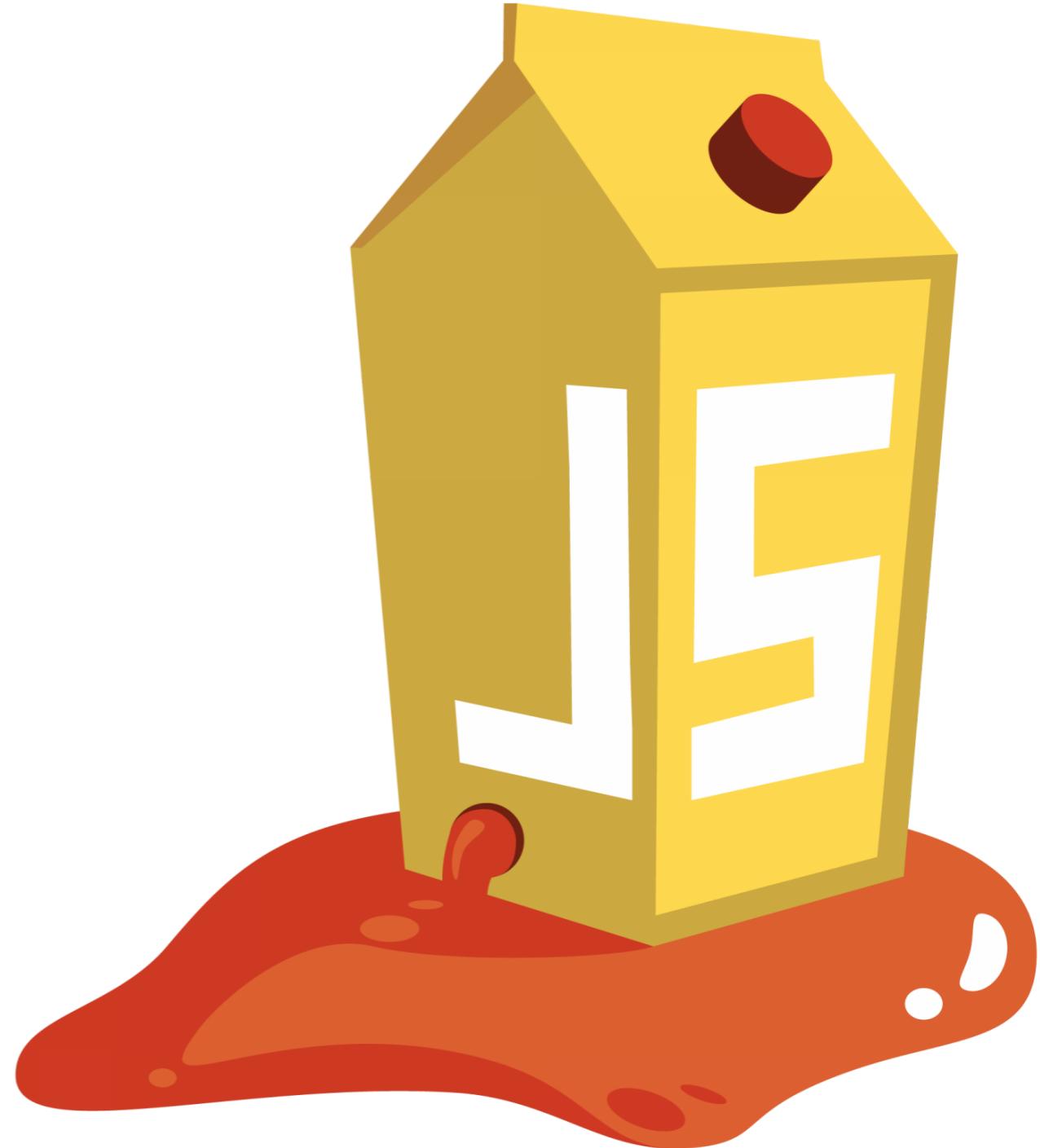
**OWASP Juice Shop is probably the most modern
and sophisticated insecure web application!**

Written in Node.js, Express and Angular.

<https://github.com/bkimminich/juice-shop>

https://www.owasp.org/index.php/OWASP_Juice_Shop_Project

OWASP
JUICE SHOP



XSS IS EVERYWHERE

XSS Polyglot

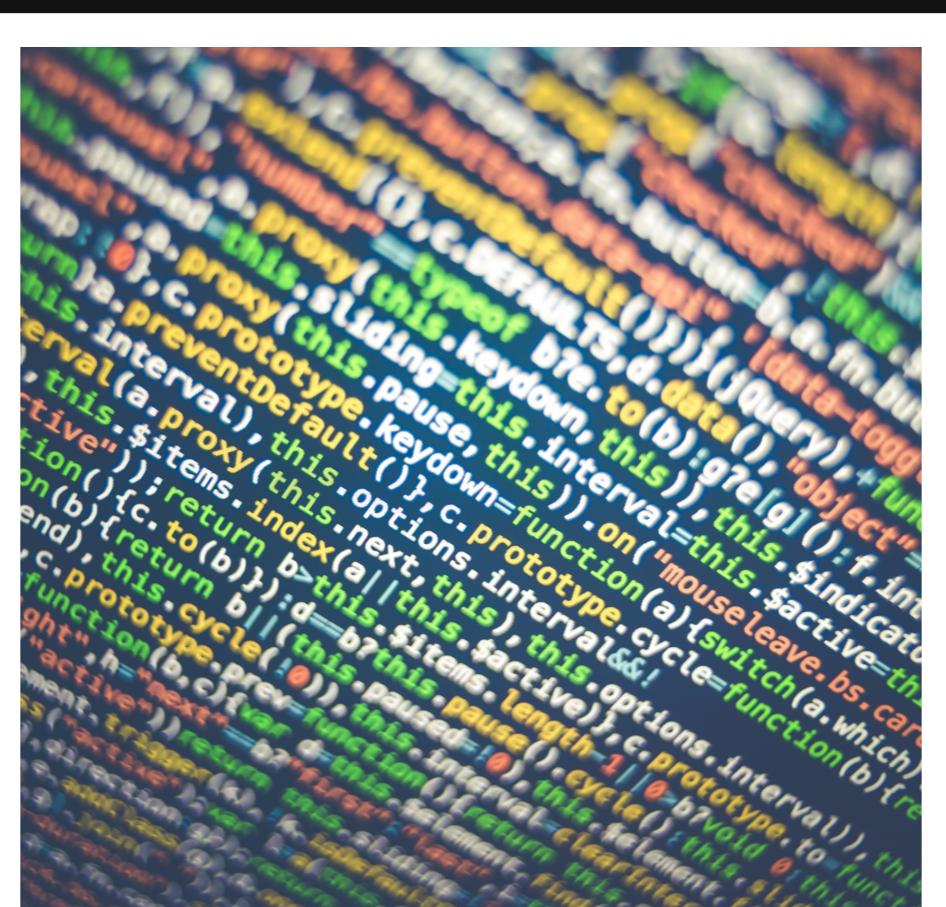
A XSS payload which runs in multiple contexts. Useful in testing XSS because it minimizes manual efforts and increases the success rate of blind XSS.

<https://polyglot.innerht.ml>

KNOXSS

KNOXSS is an online XSS tool with demonstration of vulnerability (PoC - Proof of Concept).

<https://knoxss.me/>



XSStrike

Cross Site Scripting detection suite equipped with four hand written parsers, an intelligent payload generator, a powerful fuzzing engine and an incredibly fast crawler.

<https://github.com/s0md3v/XSStrike>

LinkFinder

Python script written to discover endpoints and their parameters in JavaScript files.

<https://github.com/GerbenJavado/LinkFinder>

RECOMMENDED TOOLS

Open-source tools for target/scope recon & enumeration

<https://blog.appsecco.com/a-penetration-testers-guide-to-sub-domain-enumeration-7d842d5570f6>

Amass

Obtains subdomain by scraping data sources, recursive brute forcing, crawling web archives, permuting/altering names and reverse DNS.

<https://github.com/caffix/amass>

Sublist3r

Python tool that enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu, and Ask, VirusTotal.

<https://github.com/aboul3la/Sublist3r>

DNSdumpster

FREE domain research tool that can discover hosts related to a domain.

<https://dnsdumpster.com/>

Masscan

Internet-scale port scanner. It can scan the entire Internet in under 6 minutes, transmitting 10 million packets per second, from a single machine.

<https://github.com/robertdavidgraham/masscan>

RECOMMENDED TOOLS

Open-source tools for subdomain take-overs

<https://www.hackerone.com/blog/Guide-Subdomain-Takeovers>

<https://github.com/EdOverflow/can-i-take-over-xyz>

subjack

Tool written in Go designed to scan a list of subdomains concurrently and identify ones that are able to be hijacked.

<https://github.com/hacker/subjack>

SubOver

Tool originally written in python but rewritten from scratch in Golang. Since it's redesign, it has been aimed with speed and efficiency in mind.

<https://github.com/Ice3man543/SubOver>

<https://0xpatrik.com/>

aquatone

Tool for visual inspection of websites across a large amount of hosts and is convenient for quickly gaining an overview of HTTP-based attack surface.

<https://github.com/michenriksen/aquatone>

Subdomain takeover detection with AQUATONE

A new addition to the AQUATONE toolset is aquatone-takeover which can detect potential subdomain takeover issues across a bunch of popular external services.

<https://michenriksen.com/blog/subdomain-takeover-detection-with-aquatone/>

RECOMMENDED TOOLS

Open-source tools for AWS buckets take-overs

<https://github.com/toniblyx/my-arsenal-of-aws-security-tools>

S3Scanner

Tool to find open S3 buckets and dump their contents

<https://github.com/sa7mon/S3Scanner>

cloudfrunt

Tool for identifying misconfigured CloudFront domains. CloudFront is a Content Delivery Network (CDN) provided by Amazon Web Services (AWS).

<https://github.com/MindPointGroup/cloudfrunt>

CloudScraper

Tool to enumerate targets in search of cloud resources. S3 Buckets, Azure Blobs, Digital Ocean Storage Space.

<https://github.com/jordanpotti/CloudScraper>

pacu

AWS exploitation framework, designed for offensive security testing against cloud environments.

<https://github.com/RhinoSecurityLabs/pacu>

dkimsc4n

Asynchronous wordlist based DKIM scanner

Useful during bug bounty hunting or red teaming to find insufficient DKIM records with RSA 512-bit keys

CWE-326: Inadequate Encryption Strength

Insufficient DKIM record with RSA 512-bit key used

<https://github.com/vavkamil/dkimsc4n>

<https://asciinema.org/a/243588>

```
vavkamil@desktop:~/Documents/Python/dkimsc4n$ python3 dkimsc4n.py -D domains.txt
[!] v0.1
[i] Using wordlist: dkim.lst
[i] DKIM selectors in a wordlist: 47
[i] Scanning multiple domains: domains.txt
[i] Domains in a list: 6
[i] Domain: facebook.com
      [?] DKIM selector: default           RSA key size: 768
[i] Domain: google.com
      [+]
      [+] DKIM selector: 20161025          RSA key size: 2048
      [i] DKIM selector: delta            RSA key size: 1024
[i] Domain: youtube.com
      [+]
      [+] DKIM selector: 20161025          RSA key size: 2048
      [i] DKIM selector: beta             RSA key size: 1024
      [i] DKIM selector: selector1        RSA key size: 1024
[i] Domain: instagram.com
      [?]
      [?] DKIM selector: pm              RSA key size: 768
      [i] DKIM selector: smtpapi         RSA key size: 1024
[i] Domain: 360.cn
      [!]
      [!] DKIM selector: mail            RSA key size: 512
[i] Domain: wordpress.com
      [i] DKIM selector: k1              RSA key size: 1024
      [i] DKIM selector: m1              RSA key size: 1024
      [i] DKIM selector: mandrill        RSA key size: 1024
      [i] DKIM selector: my5             RSA key size: 1024
      [i] DKIM selector: zendesk1        RSA key size: 1024
[!] Have a nice day ;)
```

Methodology, know-how, tips & tricks

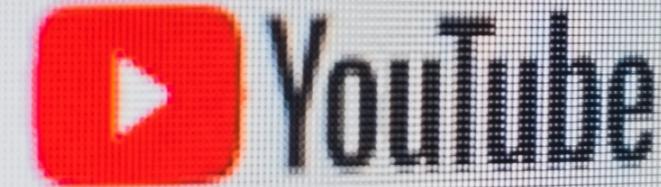
How to catch 'em all

YOUTUBE

Bug Bounty Hunter Methodology v3

Jason Haddix (Bugcrowd)

https://www.youtube.com/watch?v=Qw1nNPiH_Go



Home

Trending

tions

KNOW-HOW, TIPS & TRICKS

bounty-targets-data

This repo contains data dumps of Hackerone and Bugcrowd scopes (i.e. the domains that are eligible for bug bounty reports).

<https://github.com/arkadiyt/bounty-targets-data>

PayloadsAllTheThings

A list of useful payloads and bypass for Web Application Security and Pentest/CTF

<https://github.com/swisskyrepo/PayloadsAllTheThings>

SecLists

Collection of lists include usernames, passwords, URLs, sensitive data patterns, fuzzing payloads, web shells, and many more.

<https://github.com/danielmiessler/SecLists>

EyeWitness

Designed to take screenshots of websites, provide some server header info, and identify default credentials if possible.

<https://github.com/FortyNorthSecurity/EyeWitness>

bugbounty-cheatsheet

A list of interesting payloads, tips and tricks for bug bounty hunters.

<https://github.com/EdOverflow/bugbounty-cheatsheet>

gobuster

Directory/file & DNS busting tool written in Go.

<https://github.com/OJ/gobuster>

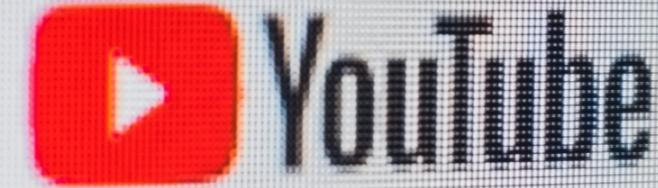
YOUTUBE

Bug Bounty Hunting on Steroids

DEF CON 26 RECON VILLAGE

- Anshuman Bhartiya, Glenn Grant

<https://www.youtube.com/watch?v=7WYjSDZxFYc&index=21&list=PL9fPq3eQfaaCk1MUOZD4Tnvr8T9bFgjH>



Home

Trending

tions



DON'T BE EVIL

Google Hacking Database

<https://www.exploit-db.com/google-hacking-database>

Open Bug Bounty Community

<https://www.openbugbounty.org/>

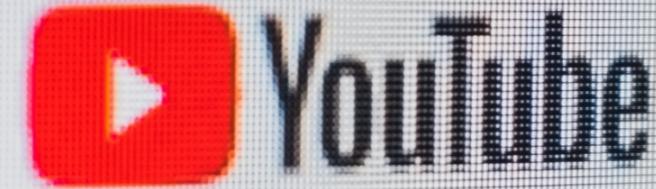
YOUTUBE

Offensive JavaScript Techniques for Red Teamers

BSidesSF 2019

(Dylan Ayrey • Christian Frichot)

<https://www.youtube.com/watch?v=HfpnloZM61I>



Home

Trending

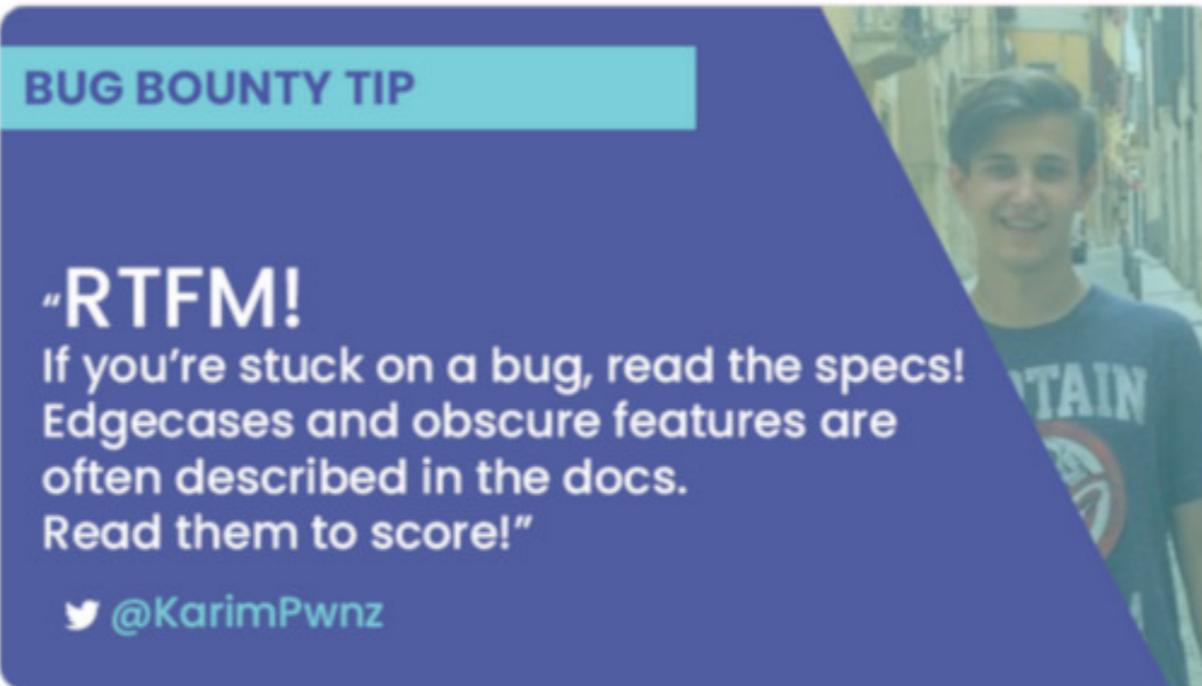
tions

#bugbountytip

<https://twitter.com/search?q=%23bugbountytip>

Ed and 6 others liked

 intigriti @intigriti · Apr 18
.@KarimPwnz bug bounty tip for today: RTFM! 🤓💻#BugBountyTip
#HackWithIntigriti


BUG BOUNTY TIP
"RTFM!
If you're stuck on a bug, read the specs!
Edgecases and obscure features are
often described in the docs.
Read them to score!"

@KarimPwnz

3 16 85

#bugbountytip

<https://twitter.com/search?q=%23bugbountytip>

1 heart Rakesh Mane and 1 other liked



Guilherme Keerok @k33r0k · Jan 5

in some cases you can have an Open Redirect using %0d%0a and two "/" directly on the main url:

<http://victim//%0d%0ahttp://google.com/>

#bugbountytip #openredirect #BugBounty

```
1. bash
bash-3.2$ curl "https://████████████████████████████████.com//%0d%0ahttp://google.com/"
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
<script src="/cdn-cgi/apps/head/i0r06iabdPGeXE7JxTeeSlvonIA.js"></script></head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://google.com">here</a>.</p>
</body></html>
bash-3.2$
```

#bugbountytip

<https://twitter.com/search?q=%23bugbountytip>



AppSec-Academy @_AppSecAcademy · Apr 23

#BugBounty #bugbounties #bugbountytip #infosec

Bypass #SSRF filters by using http://127.1 instead of http://127.0.0.1

It resolves to the same but confuses filters blocking localhost/127.0.0.1 specifically!



#bugbountytip

Sharing is caring, follow the tips on Twitter



<https://bugbountytip.com>

<https://github.com/vavkamil/bugbountytip.com>



THANK YOU!

DO YOU HAVE ANY BITCOINS?

`1Hx7eLzzUyAqM6k8d8AVffCVYeFv7b2sw7`

<https://vavkamil.cz/whoami/public-talks>

https://vavkamil.cz/wp-content/uploads/2019/05/ctjb_2019_bugbounty.pdf