Hey Hackermans!

Here is where you'll learn how to become a 

yourself!!

What are we learning today?

While this is a beginner introduction to cybersec... we want to first inspire you by what you can do in the field of cybersecurity

Industry Roles	What can you do as a cybersec engineer?
Certifications and Resources	How you can learn/practice cybersecurity? (Certs, books, websites)
Web Vulnerabilities	OWASP Top 10 with examples
Hands-on Demo!	Exploit a command injection vulnerability (and win a $20 gift card 👀)

How do you make money though?

01

SOC Analyst

Detect attacks even before they happen...

02

Bug Bounty

Rewarding public to find bugs for you??

03

Penetration Tester

Break through defenses before the hackers do

04

Malware Analyst

Analyzing and reversing malware samples

05

Forensics

Recovery and investigation!

Which one's your favorite?

SOC Analyst

"an ounce of prevention is worth a pound of cure"

- Benjamin Franklin

SOC Analyst

Identify attack vectors

Potential places an attack can happen in your software?

Monitoring infrastructure

Anomalies/suspicious activity over the network

Response & Resolution

Oh! you found something sus... time to fix it :)

SOC Analyst - Skills

SIEM

- Security Information and Event Monitoring Systems
  - Splunk
  - IBM QRadar
  - ArcSight

Network Security

- Firewalls
- Monitoring traffic

Threat Hunting

- Vulnerability assessments
- Penetration testing

02

Bug Bounty

Bug Bounties

- Get PAID to discover and report security vulnerabilities
- Payment can range anywhere from $0 to thousands
- Some platforms:

hackerone

bugcrowd

See Security Differently™

U.S. Dept Of Defense

Vulnerability Disclosure Program

Access policy page for scope

No bounty reward
Response efficiency: 100%

See details

Yahoo!

Updated

Bug Bounty Program

Triaged by HackerOne, Retesting, Bounty splitting

Other 58 | Domain 6 | Source co... 3 | Android: ... 1 | +1

Gold Standard

$100 - $15k
Response efficiency: 95%

See details

AT&T

Bug Bounty Program

Triaged by HackerOne

Other 1

$50 - $2k
Response efficiency: 97%

See details

Adobe

Bug Bounty Program

Triaged by HackerOne

Domain 85 | Executable 32 | Android: ... 6 | Other 4 | +2

See policy page for bounty
Response efficiency: 100%

See details

MTN Group

Vulnerability Disclosure Program

Domain 293

No bounty reward
Response efficiency: 61%

See details

IBM

Vulnerability Disclosure Program

Triaged by HackerOne

Other 3

No bounty reward
Response efficiency: 98%

See details

Sony

Vulnerability Disclosure Program

Triaged by HackerOne

Other 1

No bounty reward
Response efficiency: 97%

See details

Ford

Vulnerability Disclosure Program

Triaged by HackerOne

iOS: App St... 12 | Android: Pl... 11 | Domain 5 | Hardware/IoT 1

No bounty reward
Response efficiency: 99%

See details

Uber

Bug Bounty Program

Triaged by HackerOne, Retesting, Bounty splitting

Other 1

$250 - $15k
Response efficiency: 99%

See details

Shopify

Bug Bounty Program

Retesting

Domain 12 | Other 5

$500 - $200k
Response efficiency: 96%

See details

IRL Examples!

Reddit Reflected XSS

132 #1051373 **XSS Reflected on reddit.com via url path**

Share:

TIMELINE

criptex submitted a report to Reddit. Dec 5th (2 years ago)

Hi I found a XSS-R

To reproduce the issue please click the poc link and then press the "verify email" button

PoC:

https://www.reddit.com/verification/asd',%20alert(document.location),%20%27

Impact

With the help of XSS an attacker can steal your cookies, in many cases steal sessions, download malware onto your system and send a custom request. Users can be socially engineered by the attacker by redirecting them from the real website to a fake one and there are many more attack scenarios that an expert attacker can perform with XSS.
It is also possible to inject html thus modifying the original page

1 attachment:
F1105408: PoC-Reddit.png

criptex posted a comment. Dec 5th (2 years ago)

please copy the poc link and paste it into your browser, for some reason it doesn't work from the hackerone links

gunther_reddit Reddit staff updated the severity to High. Dec 7th (2 years ago)

gunther_reddit Reddit staff changed the status to ● Triaged. Dec 7th (2 years ago)

Checked this out, looks like a new experiment for email verification and we forgot to sanitize the token string before generating the interstitial page (as this only pops when you click the "Verify Email" button. Working with devs to add in validations/sanitization. There are two other "hidden" request parameters that get included in the renderer as well, so going to take care of those too.

criptex posted a comment. Dec 8th (2 years ago)

Hi @gunther_reddit I re-analyzed the Issue and saw that it has been resolved, now I can't inject the xss.

kind regards

Reported December 5, 2020 4:47pm -0500

criptex

Participants

State ● Resolved ()

Reported to Reddit Managed

Disclosed September 27, 2022 12:04pm -0400

Severity High (7 ~ 8.9)

Weakness Cross-site Scripting (XSS) - Reflected

Bounty $5,000

Time spent *None*

CVE ID *None*

Account de... *None*

Snapchat IDOR

124 #1819832 **Delete anyone's content spotlight remotely.**

Share:

TIMELINE

prickn9 submitted a report to Snapchat. Jan 1st (2 months ago)

Hello Snapchat,
Snapchat has viral video feature callled spotlight which alone was the biggest trend and increase snapchat users and profit in millions.
I found a way to delete anyone's spotlight remotely.

Please see the below poc:-

1. First go to https://my.snapchat.com/myposts and log in there.
2. You will see your posts .
3. Now turn burp suite and intercept. 4.Select any of your posts and click delete option.
4. Now capture the delete request. In delete request there is parameter of id

{"operationName":"DeleteStorySnaps","variables":{"ids":["[redacted]"],"storyType":"SPOTLIGHT_STORY"},"query":"mutation DeleteStorySnaps($ids: [String!]!, $storyType: StoryType!) {\n deleteStorySnaps(ids: $ids, storyType: $storyType)\n}\n"}

6. You just have to change this id parameter. You can easily get the id parameter. Now forward the request after replacing id with someone's else video id.

And the video of other user will get delete.

HOW TO GET ID PARAMETER

1. Whenever you share spotlight you can see the parameter in the url as: https://story.snapchat.com/spotlight/[redacted]

I have attached a video POC please check it out

Impact

Delete anyone's Content Spotlight. Imagine deleting video biggest influencers and content creators.

prickn9 posted a comment. Updated Mar 6th (3 days ago)

I have further checked that spotlight once deleted are not eligible for crystal awards(mode of payment of snapchat). So people with large no. of views will not be eligible for payment.[redacted]

bugtriage-jack posted a comment. Jan 3rd (2 months ago)

Thank you for your report @prickn9,

Reported January 1, 2023 11:06am -0500

prickn9

Participants

State	Resolved ()
Reported to	Snapchat
Disclosed	March 6, 2023 4:32pm -0500
Severity	High (7 ~ 8.9)
Weakness	*None*
Bounty	$15,000
Time spent	*None*
CVE ID	*None*
Account de...	*None*

GitLab Command Execution

238 #1679624 **Remote Command Execution via Github import**

Share:

TIMELINE

vakzz submitted a report to GitLab. Aug 25th (7 months ago)

Summary

This is very similar to https://about.gitlab.com/releases/2022/08/22/critical-security-release-gitlab-15-3-1-released/#Remote%20Command%20Execution%20via%20Github%20import and allows arbitrary redis commands to be injected when imported a GitHub repository.

When importing a GitHub repo the api client uses `Sawyer` for handling the responses. This takes a json hash and converts it into a ruby class that has methods matching all of the keys:

https://github.com/lostisland/sawyer/blob/v0.9.2/lib/sawyer/resource.rb#L106-L110

Code 414 Bytes Wrap lines Copy Download

```
1   def self.attr_accessor(*attrs)
2     attrs.each do |attribute|
3       class_eval do
4         define_method attribute do
5           @attrs[attribute.to_sym]
6         end
7
8         define_method "#{attribute}=" do |value|
9           @attrs[attribute.to_sym] = value
10        end
11
12        define_method "#{attribute}?" do
13          !!@attrs[attribute.to_sym]
14        end
15      end
16    end
17  end
```

This happens recursively, and allows for any method to be overridden including built-in methods such as `to_s`.

The redis gem uses `to_s` and `bytesize` to generate the RESP command, so if a `Sawyer::Resource` is ever passed in that has a controllable hash it can allow arbitrary redis commands to be injected into the stream as the string will be shorter than the `$` size provided (see

Reported August 25, 2022 12:07am -0400

vakzz

Participants

State ● Resolved ()

Reported to GitLab Managed

Disclosed October 6, 2022 4:19pm -0400

Severity Critical (9.9)

Weakness Command Injection - Generic

Bounty $33,510

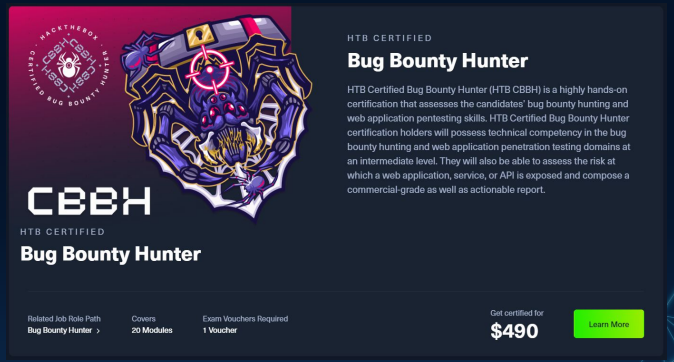
Time spent *None*

CVE ID CVE-2022-2884

Account de... *None*

How to Get Started: Certs

- HackTheBox Certified Bug Bounty Hunter (HTB CBBH)
  - $210 exam, $8 monthly student subscription



- OffSec Web Assessor (OSWA)
  - $1599 Course + Exam

Penetration Tester

Penetration Tester/Ethical Hacker

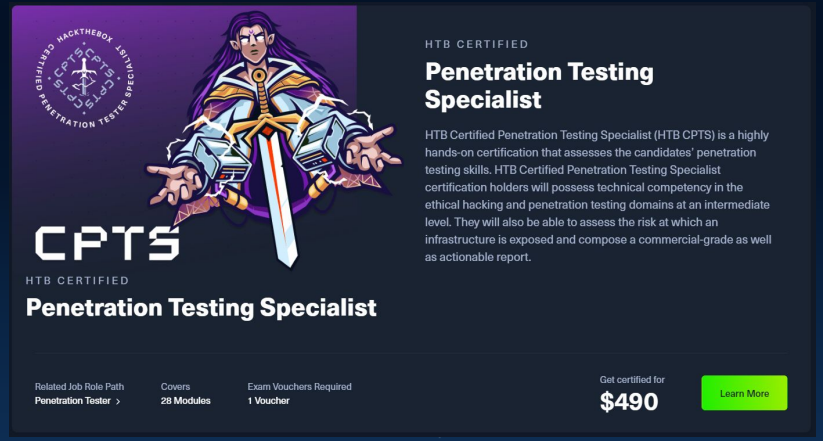
- Employed by a company to hack them

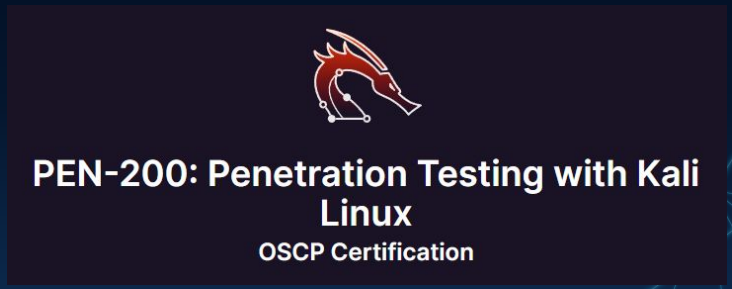
- Responsibilities:
  - Simulating cyber attacks for the purpose of identifying vulnerabilities
  - Produces reports with findings and any recommendations
  - May assist during remediation process

Bug bounty = freelance pentesting

How to become a pentester

- Get certified!
  - OffSec Certified Professional
  - HTB Certified Penetration Testing Specialist





04

Malware Analyst

Malware Analyst

- Takes apart malware to determine how the attack was deployed
- Determines what the attacker was trying to gain from the malware
- Dissect the exploit and identify the key vulnerability that was exploited which is then fixed by the developers

Malware Analyst - Skills

- Understanding of:
  - Operating Systems
  - Networking
  - Memory analysis

- Reverse Engineering
  - Assembly, Debugging, Analyzing code

- Malware analysis tools
  - Volatility, IDA, Ghidra

05

Forensics

Analyze

Conduct analysis of log files, evidence, and other information

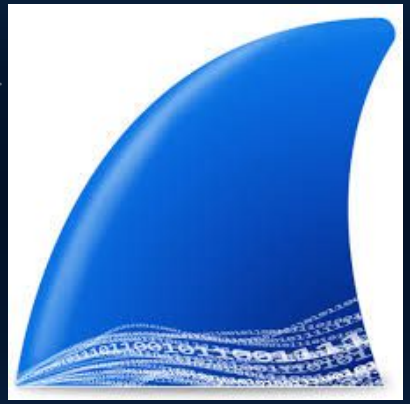
Identify

Confirm what is known about an intrusion and discover new information

Report

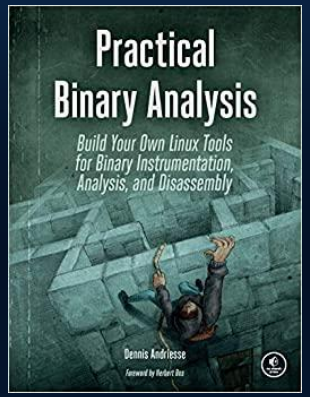
Report any detected and identified details about the intrusions

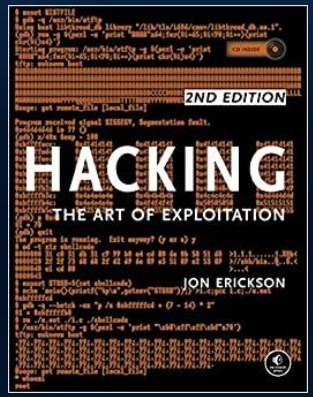
Tools used



Learning Resources

- Multiple Websites:
  - Hackthebox.eu
  - tryhackme.com
  - picoCTF
  - pwn.college
- Textbooks --
  - Practical Malware Analysis
  - Practical Binary Analysis
  - Hacking: The Art of Exploitation!!
- Infosec course -- CSC347 and CSC427 at UTM





Certifications

Offensive Security

Industry standard

Penetration Testing

- PEN-200: Penetration Testing with Kali Linux (OSCP)
- PEN-210: Foundational Wireless Network Attacks (OSWP)
- PEN-300: Advanced Evasion Techniques and Breaching Defenses (OSEP)

Web Application

- WEB-200: Foundational Web Application Assessments with Kali Linux (OSWA)
- WEB-300: Advanced Web Attacks and Exploitation (OSWE)

HackTheBox Academy

Affordable

Prelude: OWASP Top 10

Open Web Application Security Project

OWASP Top 10 2021

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable & Outdated Components
7. Identification & Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging & Monitoring Failures
10. Server-Side Request Forgery

Hands-on Demo!

EZ Linux Reference

- pwd - print working directory
- ls - list files in current directory
- cd [path]- change current directory
  - cd .. - go up one level
  - cd / - go to root directory
  - cd - go to home directory
- cat [filename] - print contents of file

Connecting to the Demo

- Visit your assigned http://34.130.93.18:port/ site (make sure you're using http, not https)
- If you find the flag hosted on the server, enter it in the discord server stage chat so we know who won, we'll contact you with your prize!

Thanks!

Do you have any questions?

@gdscutm
@utmmcss

Please keep this slide for attribution

CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon** and infographics & images by **Freepik**