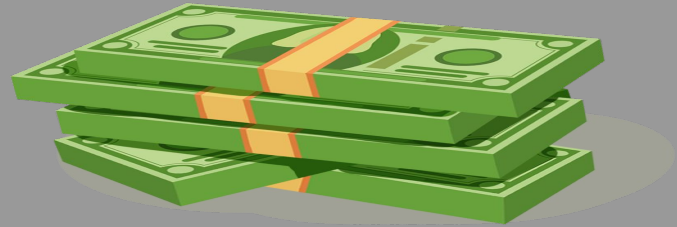




Bug

Bounty Hunting



Mahmoud M. Awali

 **@0xAwali**

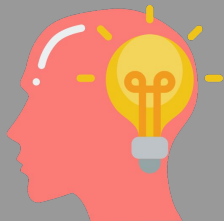
Prerequisites

- English Language
- How to Study

Marty Lobdell - Study Less Study Smart

<https://www.youtube.com/watch?v=IIU-zDU6aQ0>

- Your Mind



Methodology

Bug Bounty Hunting

**Target
Reconnaissance
Scanning
Exploitation
Reporting**

Web Apps Pen Testing

**Pre-engagement
Reconnaissance
Scanning
Exploitation
Post Exploitation
Covering Tracks
Reporting**

More Information !

- **Web Apps Pen Testing**

Course eLearnSecurity Web Application Pen Testing Module 1

<https://www.elearnsecurity.com/certification/ewpt/>

- **Bug Bounty Hunting**

DEF CON 22 - Nir Valtman - Bug Bounty Programs Evolution

<https://www.youtube.com/watch?v=l1GHeebvqPw>

Networks

- **CCNA Routing and Switching**

CCNA Routing and Switching OR N+ ?

Do Not Study Both

Course INE CCNA Routing and Switching

<https://my.ine.com/course/ccna-routing-switching-technologies/8536ecd3-4010-11e4-a79f-22000b3582a3>

Networks

- **Domain Name Server Protocol**

Managing Mission - Critical Domains and DNS:

Demystifying nameservers, DNS, and domain names

<https://www.amazon.com/Managing-Mission-Critical-Demystifying-nameservers/dp/1789135079>

Networks

- **HyperText Transfer Protocol**

HTTP: The Definitive Guide

<https://www.amazon.com/HTTP-Definitive-Guide-Guides/dp/1565925092>

Networks

- **HyperText Transfer Protocol**

HTTP/2 in Action

[https://www.amazon.com/HTTP-2-Action-Barry-Pollard/
dp/1617295167](https://www.amazon.com/HTTP-2-Action-Barry-Pollard/dp/1617295167)

Operating System

- **Your Main Distribution**

Kali Linux with XFCE Desktop Environment

Why Kali Linux ?

**Kali Linux Revealed: Mastering the Penetration Testing
Distribution**

<https://www.amazon.com/Kali-Linux-Revealed-Penetration-Distribution/dp/0997615605>

Operating System

- **Commands**

Linux® Notes for Professionals book

<https://goalkicker.com/LinuxBook/>

Operating System

- **Tmux Terminal**

Tmux OR Terminator

Getting Started with tmux

<https://www.packtpub.com/hardware-and-creative/getting-started-tmux>

Operating System

- **HTTP Command Line**

Curl AND HTTPie

Everything curl - the book

<https://curl.haxx.se/book.html>

HTTPie: a CLI , cURL-like Tool For Humans

<https://httpie.io/static/docs/httpie-0.9.8.pdf>

Operating System

- **Regular Expression**

Why Regular Expression ?

Mastering Regular Expressions

<https://www.amazon.com/Mastering-Regular-Expressions-Jeffrey-Friedl/dp/0596528124>

Operating System

- **Bash Scripting**

Bash Notes for Professionals book
<https://goalkicker.com/BashBook/>

Operating System

- Sed And Awk

sed & awk: UNIX Power Tools

<https://www.amazon.com/sed-awk-Power-Nutshell-Handbooks-ebook/dp/B004D4Y302>

Web Server

- **Nginx Web Server**

Nginx Fundamentals

High Performance Servers from Scratch

<https://www.udemy.com/course/nginx-fundamentals/>

Web Server

- **HTTP Secure**

How to Configure ?

SSL Complete Guide: HTTP to HTTPS

<https://www.udemy.com/course/ssl-complete-guide/>

Web Server

Reference

**You Want To Learn Nginx AND Apache
Servers for Hackers**

<https://leanpub.com/serversforhackers>

Web Apps Pen Testing

Prerequisite

CS50

Web Apps Pen Testing

CS50 Lectures 2018

<https://www.youtube.com/playlist?list=PLhQjrBD2T382eX9-tF75Wa4ImIC7sxNDH>

CS50's Web Programming with Python and JavaScript

<https://www.youtube.com/playlist?list=PLhQjrBD2T382hIW-lsOVuXP1uMzEvmcE5>

Web Apps Pen Testing

- **Web App Hacker's Handbook**

The Web Application Hacker's Handbook

<https://www.amazon.com/Web-Application-Hackers-Handbook-Exploiting/dp/1118026470>

Web Apps Pen Testing

- **Web Security Testing Guide**

Web Security Testing Guide v4.2

<https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf>

Reconnaissance

- **Bugcrowd University**

Sajeed Lohani OR Jason Haddix

Recon & Discovery

<https://www.youtube.com/watch?v=La3iWKRX-tE>

Bug Bounty Hunter Methodology v3

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

Reconnaissance

- Nahamsec

Ben Sadeghipour - It's the Little Things - BSides Portland
2018

<https://www.youtube.com/watch?v=YT5Zl2jW3wg&t=1s>

Reconnaissance

Nahamsec Live Bug Bounty Recon

Live

<https://www.twitch.tv/nahamsec/>

Youtube Channel

<https://www.youtube.com/channel/UCCZDt7MuC3Hzs6lH4xODLBw>

Reconnaissance

- NahamCon2020-2021

The Bug Hunter's Methodology v4.0

<https://www.youtube.com/watch?v=p4Jglu1mcel>

How to Use Amass Efficiently

<https://www.youtube.com/watch?v=H1wdBgY1rtg>

Amassive Leap in Host Discovery

<https://www.youtube.com/watch?v=yCZqggg-GNx8>

Distributed Recon Automation Using Axiom

<https://www.youtube.com/watch?v=tWml8Dy5RyM>

Reconnaissance

- Dirty Coder

Recon Like A Boss

<https://bugbountytuts.files.wordpress.com/2019/01/dirty-recon-1.pdf>

Reconnaissance

- Prateek Tiwari

BUG BOUNTY FUNSHOP

https://docs.google.com/presentation/d/1cpcxEbEb0dyXwRqSWQ6bknJS-PQO_e242Dioy9SU2lo/edit#slide=id.p

p

Reconnaissance

- Sam Erb

Hunting Certificates And Servers

<https://github.com/erbbysam/Hunting-Certificates-And-Servers/blob/master/Hunting%20Certificates%20%26%20Servers.pdf>

Reconnaissance

- **Sergey Bobrov**

BUG BOUNTY AUTOMATION

<https://2018.zeronights.ru/wp-content/uploads/materials/4%20ZN2018%20WV%20-%20BugBounty%20automation.pdf>

Reconnaissance

- Google Search

Google Hacking for Penetration Testers

<https://www.amazon.com/Google-Hacking-Penetration-Testers-Johnny/dp/0128029641>

Reconnaissance

- Alexey Morozov

Misconfiguration in development infrastructure

<https://2018.zeronights.ru/wp-content/uploads/materials/6%20ZN2018%20WV%20-%20Misconfiguration%20in%20development%20infrastructure.pdf>

Reconnaissance

- **Bugcrowd University**

Majd Aldeen Atiyat

GitHub Recon and Sensitive Data Exposure

https://www.youtube.com/watch?v=l0YsEk_59fQ&t=3s

Reconnaissance

Twitter Hashtag

#OSINT

#Recon

Services Scanning

- **NMAP**

Nmap OR Masscan

Nmap Network Scanning

<https://www.amazon.com/Nmap-Network-Scanning-Official-Discovery/dp/0979958717>

Services Scanning

CVE

<https://cve.mitre.org/>

Exploit-DB

<https://www.exploit-db.com/>

Github

<https://github.com/>

Subdomains Takeover

DNS Hijacking

<https://www.youtube.com/watch?v=FXCzdWm2qDg>

Can I Takeover XYZ ?

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

Patrik Hudak

<https://0xpatrik.com/>

DNS Takeover

Can I Takeover DNS ?

<https://github.com/indianajson/can-i-take-over-dns>

Patrik Hudak

<https://0xpatrik.com/subdomain-takeover-ns/>

Dependency Confusion

Alex Birsan

<https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610?sk=991ef9a180558d25c5c6bc5081c99089>

Dhiyaneshwaran

<https://dhiyaneshgeek.github.io/web/security/2021/09/04/dependency-confusion/>

Content Discovery

- Assetnote



<https://www.youtube.com/watch?v=DEW5C9r3rc0>

<https://blog.assetnote.io/2021/04/05/contextual-content-discovery/>

<https://www.youtube.com/watch?v=hNs8fpWfcyU>

Content Discovery

- Turbo Intruder



Abusing HTTP Misfeatures To Accelerate Attacks

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

<https://portswigger.net/research/turbo-intruder-embracing-the-billion-request-attack>

Content Discovery

- **FFUF**

How to Master FFUF For Bug Bounties

<https://www.youtube.com/watch?v=iLFkxAmwXF0&t=1s>

Content Discovery

- **Wordlist**

Who , What , Where , When , Wordlist

https://www.youtube.com/watch?v=W4_QCSlujQ4

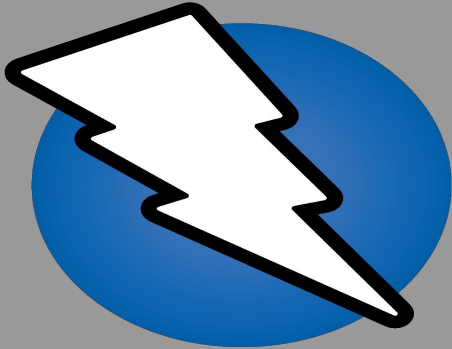
Creating Wordlists For Hacking

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

PROXY

ZAP

BURP SUITE



0\$

 **BURP**SUITE

PROFESSIONAL

400\$

PROXY

Burp Suite Cookbook

<https://www.amazon.com/Burp-Suite-Cookbook-Practical-penetration/dp/178953173X>

Mastering Burp Suite

<https://hakin9.org/course/mastering-burp-suite-professional/>

PROXY

Getting Started with ZAP

<https://www.pluralsight.com/courses/owasp-zap-web-app-pentesting-getting-started>

ZAP Deep Dive

https://www.youtube.com/playlist?list=PLz_NN8o2uh8AQ7VyUEN1GCCnpzl5_FaJA

Broken Link Hijacking

Broken Link Hijacking

<https://edoverflow.com/2017/broken-link-hijacking/>

More Than Subdomain Takeover

<https://sec.okta.com/articles/2020/12/more-subdomain-takeover-ways-takeover-hijack-and-impersonate-your>

Takeover Company's LinkedIn Page

<https://medium.com/@bathinivijaysimhareddy/how-i-takeover-the-companys-linkedin-page-790c9ed2b04d>

HTTP Methods

GET , POST , OPTIONS ,
PUT , DELETE , CONNECT ,
HEAD , TRACE , **FAKE**

Host Header Injection

Cracking The Lens

<https://www.youtube.com/watch?v=zP4b3pw94s0>

Practical Host Header Attacks

<https://www.skeletonscribe.net/2013/05/practical-http-host-header-attacks.html>

Host Header Injection

Multiple Host Ambiguities in
HTTP Implementations

<https://www.youtube.com/watch?v=V8f6gqrCbZU>

Host Header Injection

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

Web Cache Attacks

- Web Cache Deception

Web Cache Deception Attack

<https://www.youtube.com/watch?v=mroq9eHFOIU>

Cached and Confused

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

Web Cache Attacks

- Web Cache Poisoning

Practical Web Cache Poisoning: Redefining
'Unexploitable'

<https://www.youtube.com/watch?v=j2RrmNxJZ5c>

Web Cache Entanglement

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

Web Cache Attacks

- Web Cache Poisoning DOS

CPDoS: Cache Poisoned Denial of Service

<https://cpdos.org/>

Responsible denial of service with web cache poisoning

<https://portswigger.net/research/responsible-denial-of-service-with-web-cache-poisoning>

Web Cache Attacks

- **Edge Side Include Injection**

DEF CON 26 Edge Side Include Injection Abusing Caching
Servers into SSRF

<https://www.youtube.com/watch?v=VUZGZnpSg8I>

Web Cache Attacks

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

Path Normalization

Breaking Parser Logic

<https://www.youtube.com/watch?v=28xWcRegncw&t=2s>

Reverse Proxies

<https://2018.zeronights.ru/wp-content/uploads/materials/20-Reverse-proxies-Inconsistency.pdf>

<https://speakerdeck.com/greendog/2-and-a-bit-of-magic>

Open Redirection

PwnFunction

https://www.youtube.com/watch?v=4Jk_I-cw4WE&t=2s

Cheat Sheet

<https://pentester.land/cheatsheets/2018/11/02/open-redirect-cheatsheet.html>

CRLF

CRLF and Open Redirection

https://2017.zeronights.org/wp-content/uploads/materials/ZN17_Karbutov_CRLF_PDF.pdf

CRLF Reports

[site:hackerone.com](https://hackerone.com) CRLF

Client Side Technologies

Front-End Roadmap

<https://github.com/kamranahmedse/developer-roadmap#frontend-roadmap>

Client Side Technologies

HTML5 Notes for Professionals

<https://goalkicker.com/HTML5Book/>

Client Side Technologies

CSS Notes for Professionals

<https://goalkicker.com/CSSBook/>

Client Side Technologies

JavaScript Notes for Professionals

<https://goalkicker.com/JavaScriptBook/>

The Modern JavaScript Bootcamp

<https://www.udemy.com/course/modern-javascript/>

The Complete JavaScript Course

<https://www.udemy.com/course/the-complete-javascript-course/>

Client Side Technologies

jQuery Notes for Professionals

<https://goalkicker.com/jQueryBook/>

Client Side Technologies

How Browsers Work

<https://www.html5rocks.com/en/tutorials/internals/howbrowserswork/>

Client Side Technologies

Third-Party JavaScript

<https://www.amazon.com/Third-Party-JavaScript-Ben-Vinegar/dp/1617290548>

Client Side Technologies

Complete JSON AJAX API

<https://www.udemy.com/course/complete-json-ajax-course/>

Cross site Scripting

Reflected
Persistent
DOM-based
Blind

Cross site Scripting

XSS Attacks

<https://www.amazon.com/XSS-Attacks-Scripting-Exploits-Defense/dp/1597491543>

XSS Magic Tricks

<https://www.slideshare.net/GarethHeyes/xss-magic-tricks>

Cross site Scripting

BLIND XSS

<https://2018.zeronights.ru/wp-content/uploads/materials/2020ZN2018%20WV%20-%20Blind%20Xss%20%28femida%20plogin%29.pdf>

Cross site Scripting

XSS Cheat Sheet

<https://portswigger.net/web-security/cross-site-scripting/cheat-sheet>

Cross site Scripting

XSS Reports

[site:hackerone.com xss](#)

Twitter Hashtag

[#Bugbountytip xss](#)

[#bugbounty blind xss](#)

[#xss](#)

[#bxss](#)

Content Security Policy

CSP

<https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>

Bypassing CSP

<https://www.youtube.com/watch?v=eewyLp9QLEs>

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

https://www.youtube.com/watch?v=RR_EqKsYb9o

https://www.youtube.com/watch?v=_L06HetskC4

Cross site Scripting

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

Cross site Scripting



Get Invitation

HackerOne CTF

<https://ctf.hacker101.com/>

CSRF

Cross-Site Request Forgery

<https://www.pluralsight.com/courses/cross-site-forgery-request-web-app>

CSRF-protection Bypassing

<https://www.slideshare.net/0ang3el/neat-tricks-to-bypass-csrf-protection>

CSRF

CSRF Reports

[site:hackerone.com csrf](#)

Twitter Hashtag

[#Bugbountytip csrf](#)

[#bugbounty csrf](#)

[#csrf](#)

CSRF

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

CORS Misconfiguration

CORS in Action

[https://www.amazon.com/CORS-Action-Creating-consumin
g-cross-origin/dp/161729182X](https://www.amazon.com/CORS-Action-Creating-consumin-g-cross-origin/dp/161729182X)

Exploiting CORS

<https://www.youtube.com/watch?v=wgkj4Zgxl4c>

CORS Misconfiguration

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

WebSocket Hijacking

Guide to HTML5 WebSocket

<https://www.amazon.com/Definitive-Guide-HTML5-WebSocket/dp/1430247401>

Security Testing of WebSockets

<https://www.theseus.fi/bitstream/handle/10024/113390/Harri+Kuosmanen+-+Masters+thesis+-+Security+Testing+of+WebSockets+-+Final.pdf?sequence=1>

WebSocket Hijacking

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

postMessage

Hunting postMessage Vulnerabilities

<https://www.sec-1.com/blog/wp-content/uploads/2016/08/Hunting-postMessage-Vulnerabilities.pdf>

postMessage Reports

[site:hackerone.com postmessage](https://www.hackerone.com/search?query=postmessage)

Clickjacking

All about Clickjacking

<https://cure53.de/xfo-clickjacking.pdf>

clickjacking Reports

site:hackerone.com clickjacking

Clickjacking

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

More Client-side Bugs

Learning and Reports

T o o l s - P a y l o a d s

<https://appsecwiki.com/#/frontend>

Client-side Books

The Tangled Web

<https://www.amazon.com/Tangled-Web-Securing-Modern-Applications/dp/1593273886>

The Browser Hacker's Handbook

<https://www.amazon.com/Browser-Hackers-Handbook-Wade-Alcorn/dp/1118662091>

Browser security whitepaper

<https://github.com/cure53/browser-sec-whitepaper/blob/master/browser-security-whitepaper.pdf>

Server Side Technologies

Back-End Roadmap

<https://github.com/kamranahmedse/developer-roadmap#back-end-roadmap>

Server Side Technologies

Great Course

Node.js , SQL , NOSQL , REST API , GraphQL and More

NodeJS - The Complete Guide

<https://www.udemy.com/course/nodejs-the-complete-guide/>

E-mail Injection

Exploiting E-Mail Systems

https://www.youtube.com/watch?v=cThFNXrBYQU&feature=emb_logo

SMTP Injection Via Recipient Email Addresses

<https://www.mbsd.jp/Whitepaper/smtpi.pdf>

SQL Injection

ERROR-Based

UNION-Based

BOOLEAN-Based

TIME-Based

SQL Injection

SQL Notes for Professionals

<https://books.goalkicker.com/SQLBook/>

SQL Injection Strategies

[https://www.packtpub.com/product/sql-injection-strategies/
9781839215643](https://www.packtpub.com/product/sql-injection-strategies/9781839215643)

SQL Injection Attacks and Defense

[https://www.amazon.com/Injection-Attacks-Defense-Justin-
Clarke/dp/1597499633](https://www.amazon.com/Injection-Attacks-Defense-Justin-Clarke/dp/1597499633)

SQL Injection

SQLi Reports

[site:hackerone.com sqli](#)

Twitter Hashtag

[#Bugbountytip sqli](#)

[#bugbounty sqli](#)

SQL Injection

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

NOSQL Injection

MongoDB Notes for Professionals

<https://books.goalkicker.com/MongoDBBook/>

Investigation and Validation of NoSQL Injection

<https://patrick-spiegel.de/MasterThesis.pdf>

NOSQL INJECTION

<https://www.owasp.org/images/e/ed/GOD16-NOSQL.pdf>

NOSQL Injection

NOSQL Reports

Use Google

Twitter Hashtag

#Bugbounty nosql

Local File Inclusion

Local file inclusion

<https://appsecwiki.com/#/serversidesecurity?id=local-file-inclusion>

Local File Inclusion

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

Remote Code Execution

Remote Code Execution

<https://appsecwiki.com/#/serversidesecurity?id=remote-code-execution>

Remote Code Execution

Commix

<https://www.youtube.com/watch?v=8U88YvLMYQo>

Remote Code Execution

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

Template Injection

Server-side Template Injection

<https://www.youtube.com/watch?v=3cT0uE7Y87s&t=4s>

Client-side Template Injection

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

Template Injection

SPEL INJECTION

<https://2018.zeronights.ru/wp-content/uploads/materials/10%20ZN2018%20WV%20-%20Spel%20injection%20.pdf>

Template Injection

SSTI Reports

[site:hackerone.com ssti](https://hackerone.com/ssti)

Template Injection

Client-Side Template Injection

https://2017.zeronights.org/wp-content/uploads/materials/ZN17_Karbutov_CSTI_PDF.pdf

Template Injection

AngularJS Security

https://www.youtube.com/watch?v=67Yc8_Bszlk&list=PLhixgUqwRTjwJTlkNopKuGLk3Pm9Ri1sF

Template Injection

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

Broken Authentication

Advanced REST API Course

F l a s k a n d P y t h o n

E-mail Confirmation , Image upload , OAuth 2.0 and Payment

<https://www.udemy.com/course/advanced-rest-apis-flask-python/>

Broken Authentication

- Login Page

Hacking Authentication

<https://www.pluralsight.com/courses/hacking-authentication-web-app>

Cookie Attacks

<https://www.pluralsight.com/courses/cookie-attacks-web-app-hacking>

Broken Authentication

- OAuth 2.0

OAuth 2 in Action

<https://www.amazon.com/OAuth-2-Action-Justin-Richer/dp/161729327X>

Oauth security

<https://appsecwiki.com/#/serversidesecurity?id=oauth-security>

Broken Authentication

- OAuth 2.0

Hacking OAuth 2.0 For Fun And Profit

<https://www.youtube.com/watch?v=X0mV9HXbKHY>

Broken Authentication

- Password Reset

Hacking Password Reset Functionality

<https://www.pluralsight.com/courses/web-app-hacking-password-reset-functionality>

D o y o u R e m e m b e r

Host Header Injection

Broken Authentication

Hack Your API First

<https://www.pluralsight.com/courses/hack-your-api-first>

API Security: Offence and Defence

<https://hakin9.org/course/api-security-offence-and-defence/>

Broken Authentication

- Bugcrowd LevelUP 0x03

Bad API , hAPI Hackers

<https://www.youtube.com/watch?v=UT7-ZVawdzA>

API Security 101

<https://appsecwiki.com/#/serversidesecurity?id=oauth-security>

Broken Authentication

- **Attacking JSON WEB TOKENS**

JSON WEB TOKENS

<https://appsecwiki.com/#/serversidesecurity?id=json-web-tokenjwt>

JWT Parkour

<https://2019.pass-the-salt.org/files/slides/09-JWAT.pdf>

Broken Authentication

Security Assertion Markup Language

<https://appsecwiki.com/#/serversidesecurity?id=saml>

SSO Wars

<https://www.youtube.com/watch?v=ObxxXU8GRMI>

Identity Theft: Attacks on SSO Systems

<https://www.youtube.com/watch?v=Zjrty05REoc>

Broken Authentication

Insecure Direct Object Reference

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

IDOR Vulnerability Automation

<https://www.youtube.com/watch?v=3K1-a7dnA60>

Broken Authentication

Advanced API Security

<https://www.amazon.com/Advanced-API-Security-Securing-Connect/dp/1430268182>

OWASP API Security TOP 10

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

Broken Authentication

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

Cryptography

Crypto 101

<https://www.crypto101.io/Crypto101.pdf>

Hash Crack

<https://www.amazon.com/Hash-Crack-Password-Cracking-Manual-ebook/dp/B075QWTYPM>

Cryptography



Get Invitation

HackerOne CTF

<https://ctf.hacker101.com/>

GraphQL

The Modern GraphQL

<https://www.udemy.com/course/graphql-bootcamp/>

Abusing GraphQL to Attack

https://www.youtube.com/watch?v=NPDp7GHmMa0&feature=emb_logo

GraphQL

GraphQL Apps Security Testing Automation

https://zeronights.ru/wp-content/themes/zeronights-2019/public/materials/2_ZN2019_sorokinpf_graphql.pdf

GraphQL



Get Invitation
HackerOne CTF

<https://ctf.hacker101.com/>

DevOps Technologies

DevOps Roadmap

<https://github.com/kamranahmedse/developer-roadmap#devops-roadmap>

Amazon Web Services

AWS Certified Solutions Architect

<https://www.udemy.com/course/aws-certified-solutions-architect-associate/>

AWS Serverless APIs

<https://www.udemy.com/course/aws-serverless-a-complete-introduction/>

Amazon Web Services

Hands-On AWS Penetration Testing

<https://www.amazon.com/Hands-Penetration-Testing-Kali-Linux/dp/1789136725>

Deep dive into AWS S3

https://labs.detectify.com/2017/07/13/a-deep-dive-into-aws-s3-access-controls-taking-full-control-over-your-assets/?utm_source=blog&utm_campaign=s3_buckets

SSRF

Server Side Request Forgery

<https://www.youtube.com/watch?v=4kLcblAuQlw>

Server side browsing

<https://www.youtube.com/watch?v=oxpbmUYCS4g>

SSRF

BLIND SSRF Morozov Alexey

https://zeronights.ru/wp-content/themes/zeronights-2019/public/materials/4_ZN2019_Morozov_SSRF.pdf

A Glossary of Blind SSRF Chains

<https://blog.assetnote.io/2021/01/13/blind-ssrf-chains/>

SSRF

New Era of SSRF Exploiting

<https://www.youtube.com/watch?v=ds4Gp4xoaeA>

SSRF AND PDF GENERATOR

<https://www.youtube.com/watch?v=o-tL9ULF0KI>

SSRF

SSRF bible. Cheatsheet

<https://docs.google.com/document/d/1v1TkWZtrhzRLy0bYXBcdLUedXGb9njTNIJXa3u9akHM/edit>

SSRF

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

Microservices

Microservices Web App

React AND Django AND Flask

<https://www.youtube.com/watch?v=0iB5IPoTDts&t=1117s>

Microservices

Attacking Secondary Contexts

<https://www.youtube.com/watch?v=hWmXEAi9z5w>

Traversing My Way In The Internal Network

<https://www.youtube.com/watch?v=f5lEe5r9to8>

Microservices

Middleware , Middleware Everywhere

<https://labs.detectify.com/2021/02/18/middleware-middleware-everywhere-and-lots-of-misconfigurations-to-fix/>

Methodology Using Fuzzing AND Info Disclosure

<https://www.slideshare.net/bsidesahmedabad/frans-rosn-key-note-at-bsides-ahmedabad>

XML Schema

XML Schema and XSLT

<https://www.udemy.com/course/xml-novice-to-ninja/>

XML External Entity

XML External Entity Injection

<https://www.youtube.com/watch?v=9ZokuRHo-eY>

XXE: How to become a Jedi

<https://www.slideshare.net/ssuserf09cba/xxe-how-to-become-a-jedi>

XML External Entity

Attacking xml processing

<https://www.youtube.com/watch?v=2ufnBHXx3cU&t=2465s>

XML Out-Of-Band Exploitation

http://www.nosuchcon.org/talks/2013/D3_03_Alex&Timur_XML_Out_Of_Band.pdf

XML External Entity

DTD Attacks

Against a XML Parsers

https://www.nds.ruhr-uni-bochum.de/media/nds/arbeiten/2015/11/04/spaeth-dtd_attacks.pdf

XML External Entity

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

HTTP Parameter Pollution

PwnFunction

<https://www.youtube.com/watch?v=QVZBI8yxVX0>

Marco Balduzzi

<https://www.blackhat.com/docs/webcast/bhwebcast28-balduzzi.pdf>

File Uploading

File Uploading Vulnerabilities

<https://www.sans.org/reading-room/whitepapers/testing/web-application-file-upload-vulnerabilities-36487>

File Uploading

FFmpeg Video Converters

<https://www.youtube.com/watch?v=tZil9j7TTps>

Attacks on Video Converters

https://docs.google.com/presentation/d/1yqWy_aE3dQNXAhW8kxMxRqtP7qMHalfMzUDpEqFneos/edit#slide=id.p

File Uploading

FFmpeg and Imagemagick

https://2017.zeronights.org/wp-content/uploads/materials/ZN17_yngwie_ffmpeg.pdf

PostScript and ghostScript

<https://ruxcon.org.au/assets/2017/slides/hong-ps-and-gs-ruxcon2017.pdf>

File Uploading

Killing with Filedescriptor

<https://speakerdeck.com/filedescriptor/killing-with>

File Uploading

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

HTTP Smuggling

Hiding Wookiees in HTTP

<https://www.youtube.com/watch?v=dVU9i5PsMPY>

HTTP Desync Attacks

<https://www.youtube.com/watch?v=w-eJM2Pc0KI>

HTTP Smuggling

Practical Attacks Using HTTP Request Smuggling

<https://www.youtube.com/watch?v=3tpnuzFLU8g>

HTTP Request Smuggling in 2020

<https://i.blackhat.com/USA-20/Wednesday/us-20-Klein-HTTP-Request-Smuggling-In-2020-New-Variants-New-Defenses-And-New-Challenges.pdf>

Response Smuggling: Pwning HTTP 1 1 Connections

<https://www.youtube.com/watch?v=suxDcYViwao&list=PL9fPq3eQfaaBUD1zVxJWJmX86A6d0isBI&index=48>

HTTP Smuggling

What's Wrong With WebSocket APIs

Smuggling Through Websocket

<https://www.youtube.com/watch?v=gANzRo7UHt8>

HTTP Smuggling

HTTP Request Smuggling Via Higher HTTP Versions

<https://standoff365.com/phdays10/schedule/tech/http-request-smuggling-via-higher-http-versions/>

HTTP2: The Sequel is Always Worse

<https://www.youtube.com/watch?v=rHxVVeM9R-M>

HTTP Smuggling

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

DNS Rebinding

There's no place like 127.0.0.1

https://www.youtube.com/watch?v=Q0JG_eKLcws

State of DNS Rebinding

<https://www.youtube.com/watch?v=y9-0lICNjOQ&t=1116s>

More Server-side Bugs

Learning and Reports

T o o l s - P a y l o a d s

<https://appsecwiki.com/#/serversidesecurity>

More Server-side Bugs

WebSecurity
Academy Materials



<https://portswigger.net/web-security/all-materials>

More Server-side Bugs

- HOP BY HOP Request Header

Hop-by-Hop Request Headers

<https://nathandavison.com/blog/abusing-http-hop-by-hop-request-headers>

More Server-side Bugs

- **Shellshock Vulnerability**

Shellshock Vulnerability

https://owasp.org/www-pdf-archive/Shellshock_-_Tudor_Enache.pdf

More Server-side Bugs

- **Sensitive Files**

**Small Files And Big Bounties,
Exploiting Sensitive Files**

<https://www.youtube.com/watch?v=pzH-gytUWWI>

More Server-side Bugs

WebSecurity
Academy Labs



<https://portswigger.net/web-security/all-labs>

More Server-side Bugs



Get Invitation

HackerOne CTF

<https://ctf.hacker101.com/>

Source Code Review

OWASP Code Review

https://www.owasp.org/images/5/53/OWASP_Code_Review_Guide_v2.pdf

Source Code Review

Finding 0days in Enterprise Web Applications

<https://www.youtube.com/watch?v=1UWtlgDA3HA&t=1309s>

Source Code Review

- **Reading Javascript Files**

**Let's be a Dork and Read
javascript files with zseano**

<https://www.youtube.com/watch?v=0jM8dDVifal>

Web App Firewall

Web Application Defender

<https://www.amazon.com/Web-Application-Defenders-Cookbook-Protecting/dp/1118362187>

Web Application Obfuscation

<https://www.amazon.com/Web-Application-Obfuscation-Evasion-Filters/dp/1597496049>

Automation

Write Your Tools

Language is Up To You

Awesome Talks

- **Asynchronous Vulnerabilities**

Hunting Asynchronous Vulnerabilities

<https://www.youtube.com/watch?v=ha6LD1-RiJU>

Awesome Talks

- **AEM Hacking**

**Approaching Adobe Experience Manager
Webapps by Mikhail Egorov**

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

Awesome Talks

- Hacking Jenkins

Hacking Jenkins - Orange Tsai

https://www.youtube.com/watch?v=_x8BsBnQPmU

Awesome Talks

- Infiltrating Corporate Internet

Orange Tsai - Infiltrating Corporate
Intranet Like NSA Preauth RCE

https://www.youtube.com/watch?v=1loythC_pLY

Awesome Talks

- **Apache Solr Injection**

Apache Solr Injection

<https://www.youtube.com/watch?v=xf2E64o4hWc>

Awesome Talks

- Hunting For Top Bounties

Nicolas Grégoire

Hunting For Top Bounties

<https://www.youtube.com/watch?v=mQjTgDuLsp4>

Awesome Talks

- Demystifying The Server Side

SSRF - XXE - RCE

Reverse Proxy

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

Awesome Talks

- **Backslash Powered Scanning**

**Backslash Powered Scanning: Hunting
Unknown Vulnerability Classes**

<https://www.youtube.com/watch?v=apOLZ67TZd0>

Awesome Talks

- NahamCon2021

Hacking IIS

<https://www.youtube.com/watch?v=cqM-MdPkaWo>

Awesome Talks

- Red Team Village

**Knock knock , Who's There?
Identifying Assets in the Cloud**

<https://www.youtube.com/watch?v=W5htGHdlc-M>

Awesome Talks

- Zseano's Thoughts

A Look Into Zseano's Thoughts
When Testing a Target

<https://www.youtube.com/watch?v=T6BROEozJOk>

https://www.youtube.com/watch?v=8Sqp_kryB4E

Bug Bounty Hunting Books

Bug Bounty Playbook v1

<https://payhip.com/b/wAoh>

Bug Bounty Playbook v2

<https://payhip.com/b/nRia>

Bug Bounty Hunting Books

Web Hacking 101

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

Real-World Bug Hunting

<https://nostarch.com/bughunting>

Bug Bounty Hunting Books

Bug Bounty Bootcamp

<https://nostarch.com/bug-bounty-bootcamp>

Hacking APIs

<https://nostarch.com/hacking-apis>

Certifications

Web Hacking

<https://notsosecure.com/hacking-training/web-hacking/>

Advanced Web Hacking

<https://notsosecure.com/hacking-training/advanced-web-hacking/>

Certifications

Advanced Web Attacks and Exploitation

<https://www.offensive-security.com/awae-oswe/>

Keep Learning

Twitter

Following List is Up To You

Blogs

Security Researchers !

Conferences

ZeroNights - Defconf - Blackhat - etc

Keep Learning

Google



Depending On Yourself , It Will Be Better

Google Search

I'm Feeling Lucky

Thank You

Mahmoud M. Awali

 **@0xAwali**