

TRENDING VULNERABILITIES WITH INSIGHTS TO OWASP TOP 10

By - Harsh Bothra

WHO-AM-I?

Cyber Security Consultant @RedHuntLabs

Core Pentester @Cobalt.io

Lazy Bug Bounty Hunter - Bugcrowd | Synack | Private

Author | Blogger | Speaker

Creator @ProjectBheem

Going through #Learn365

AGENDA



INTRODUCTION TO APPLICATION
SECURITY



OWASP TOP 10



TRENDING VULNERABILITIES



HUNTING : MY WAY

$$a^0 = 1 [a^0]$$

$$\tan h$$

$$\cos(-x) = \cos(x)$$

$$\arcsin(z)$$

INTRODUCTION TO APPLICATION SECURITY

$$x_{n+1} =$$

APPLICATION SECURITY - TECH CLASSIFICATION



Web Application



Mobile Application



APIs



Thick Clients

OWASP TOP 10

Injection

Broken Authentication

Sensitive Data Exposure

XML External Entities

Broken Access Control

Security
Misconfiguration

Cross-Site Scripting

Insecure Deserialization

Using Component with
Known Vulnerabilities

Insufficient Logging
and Monitoring

COMMONLY IDENTIFIED VULNERABILITIES

Sensitive Information in JS & Public Resources

Broken Access Controls

Authorization Check Bypass & Privilege Escalations

Server-Side Request Forgery

Cross-Site Scripting

Business Logic Abuse

TRENDING VULNERABILITIES

GraphQL
Vulnerabilities

WebSocket
Vulnerabilities

OAuth
Vulnerabilities

SAML
Vulnerabilities

NoSQL Injection

Cache Based
Vulnerabilities

Bypasses

JWT

APPROACHING TRENDING VULNERABILITIES

Hunting - My Way!

TIPS & TRICKS!

GET IN TOUCH AT

Twitter: @harshbothra_

LinkedIn: /in/harshbothra

Instagram: @harshbothra_

SpeakerDeck: /harshbothra

Email: hbothra22@gmail.com

THANK YOU!
