ROADMAP TO WEB APPLICATION SECURITY

By Bikram Kharal

ABOUT ME

Bikram Kharal

Cyber Security Enthusiast
Engineering Student
Part-Time Bug Bounty Hunter
CRTP,eWPTXv2, BSCP

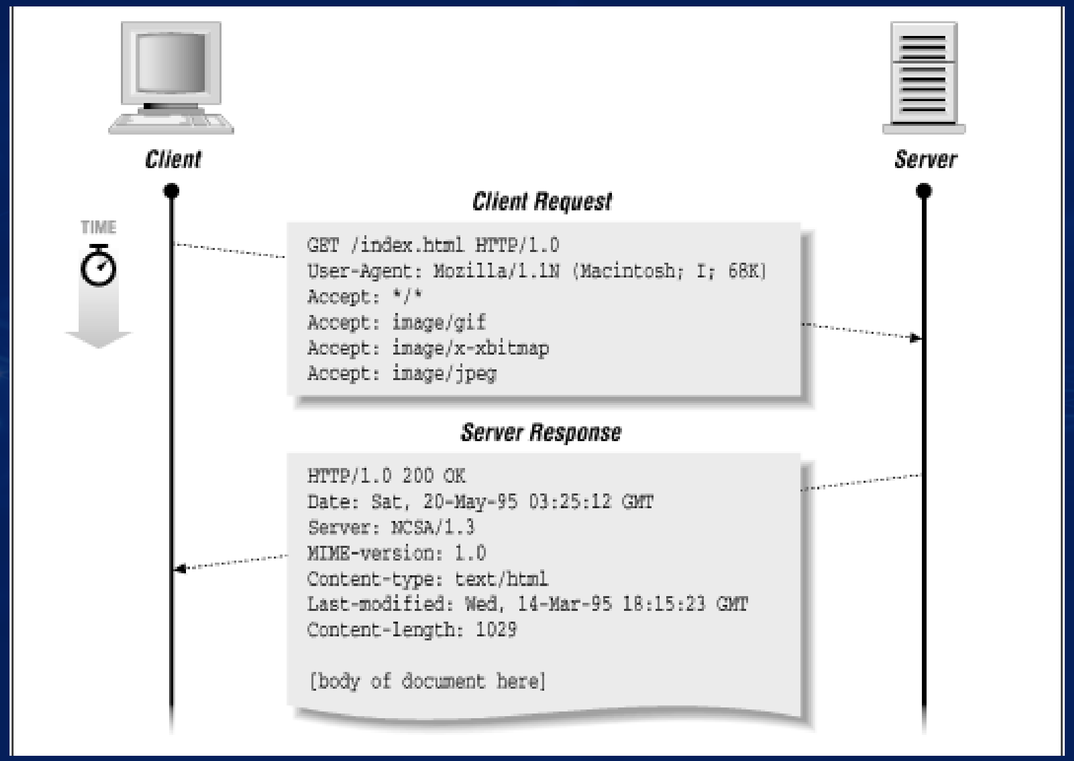
INTRODUCTION

- Web application security is the practice of detecting and preventing cyber attacks on websites.

- Vulnerability is the flaw or weakness in the system

How the Web Works?

- HTTP Headers
- Request and Response
- Status Codes



LEARN THE FUNDAMENTALS

LEARN THE FUNDAMENTALS

CIA TRIAD

- Confidentiality
- Integrity
- Availability

Servers

PROGRAMMING

- PHP, Javascript
- Python, Bash

TYPES OF WEB APPLICATION TESTING

Static Application Security Testing (SAST)

SAST is a white-box testing method that analyzes the source code, bytecode, or binary of an application without executing it.

Dynamic Application Security Testing (DAST)

DAST is a black-box testing technique that involves executing an application and analyzing its behavior to identify potential security vulnerabilities

SECURITY CONCEPTS

OWASP TOP 10

- Broken Access Control
- Cryptographic failures
- Injection
- Insecure design
- Security misconfiguration
- Vulnerable and outdated component
- Identification and authentication failures
- Software and data integrity failures
- Security logging and monitoring failures
- Server-side request forgery

Common Web Attacks

- Cross-Site Scripting
- SQL Injection
- Indirect Object Reference
- Cross Site Request Forgery

Tools

- Wappalyzer
- Nmap
- BurpSuite

LABS

- DVWA
- Portswigger
- Tryhackme

IMPLEMENTATION

- CTFs
- Bug Bounty Platforms
- Development
- Certifications
  - CEH
  - eWPTX

STAY UPDATED

Security Newsletters

- Intigriti Bug Bytes
- Hive Five Newsletter
- Pentesterland

Social Media

- Twitter
- Youtube
- Medium

Follow

- Pentester Nepal
- Nahamsec
- Jhaddix
- Thecybermentor
- JohnHammond
- Critical Thinking - BBP

ANY QUESTIONS?

Get In Touch

themarkib

themarkib

https://bikramkharal.com.np