

DURBHASI GURUKULAM

Cyber Security

DURBHASI GURUKULAM

- Advanced IT, Software Development & Cybersecurity services that transform and protect businesses through cutting-edge technology.
- Build, optimize, secure, and scale your digital solutions with Durbhasi Gurukulam.
- Durbhasi Gurukulam offers industry-relevant training in IT, Cyber Security, and Software Development, integrating traditional values with modern digital skills to empower the next generation of self-reliant professionals.

MENTOR INTRODUCTION

- Vikas Kumawat, a hands-on cybersecurity expert with 7+ years of experience in ethical hacking, red teaming, and exploit development. I mentor students and professionals in offensive security, CTFs, and real-world attack techniques, blending deep technical expertise with practical, field-tested training.

TRAINING CONTENTS

- Introduction
- Modules
- Examples
- Queries
- Summary

INTRODUCTION

This course provides a hands-on journey into the world of ethical hacking, network security, and real-world attack simulations. Learners will gain practical skills in web/app pentesting, system exploitation, red teaming, and cyber defense, making them job-ready cybersecurity professionals.

MODULE 1: ATTACK SURFACE MAPPING & INITIAL HARDENING

- Client-Server Web Protocols
- HTTP Transaction Cycle
- Web State Management & Session Control
- HTTP Metadata & Protocol Behavior
- Modern Web Authentication & Identity Protocols
- Difference: VA vs PT, Lifecycle, Scope, ROE
- Subdomain Discovery & Reconnaissance
- *Domain Infrastructure Analysis*
- Domain Registration & Ownership Intelligence
- Historical Web Footprint Analysis
- Technology Stack Profiling & Analysis

MODULE 2: APPLICATION VULNERABILITY MAPPING

Automated Reconnaissance & Scanning Tools

- OWASP ZAP
- Nikto
- Arachni
- Nuclei
- Burp Suite

Manual Web Application Analysis

- Application Behavior Mapping
- Parameter Enumeration
- Manual Fuzzing & Payload Injection
- Testing Authentication & Session Controls

MODULE 3: OWASP TOP 10 DEEP DIVE (EXPLOITATION)

- Access Control Vulnerabilities & Horizontal/Vertical Privilege Abuse
- Weak Encryption & Insecure Transport Layer Protocols
- Code Injection Techniques & Payload-Based Exploitation
- *Application Logic Vulnerabilities & Flow-Based Exploitation*
- Misconfigured Services & Default Insecure States
- Third-Party Component Exploitation & CVE Abuse
- Broken Authentication Mechanisms & Credential Exploits
- Supply Chain & Object Integrity Exploitation
- *Logging Blind Spots, Tampering & Detection Evasion*
- SSRF & File Injection Vulnerabilities

MODULE 4: ADVANCED WEB APPLICATION EXPLOITATION TECHNIQUES

- JWT Exploitation & Token Manipulation
- CORS Misconfigurations & Exploitation
- WebSocket-Based Vulnerabilities
- HTML Smuggling & Payload Delivery
- Content Security Policy (CSP) Bypass Techniques
- OAuth2 Misimplementation Exploits
- Host Header Injection & Exploitation
- HTTP Request Smuggling & CLTE Attacks
- Cache Poisoning & CDN-Based Attacks
- Clickjacking & UI Redress Attacks
- HTTP Parameter Pollution (HPP)
- Open Redirects & Post-Auth Redirect Exploits
- DOM-Based Attacks (XSS & Logic Abuse)
- WebSocket CSRF & WS Hijacking

MODULE 5: VULNERABILITY REPORTING & DOCUMENTATION

Technical Reporting & Communication in Security Assessments

Understanding Report Lifecycle

Severity & Risk Rating Frameworks

Report Delivery & Review

Writing Clear Vulnerability Reports

Best Practices in Pentest Reporting

:: QUERIES ::




- How would you exploit a JWT token with **alg: none** if the server accepts it? How can you forge your own token?
- Given a CORS policy that allows **Access-Control-Allow-Origin: *** with **credentials: true**, how can an attacker steal user data?
- What is Host Header Injection and how can it be used to poison password reset links?
- Intercept a login request using Burp Suite and attempt session fixation by injecting a known session ID before login. What behavior do you observe?
- You discover a file upload field. What techniques can you use to bypass extension-based filters to upload a web shell?
- How would you use tools like Nuclei and Wayback Machine together for discovering hidden attack surfaces?

SUMMARY

This syllabus provides a complete journey into advanced web security, covering automated and manual vulnerability assessment, OWASP Top 10 deep dive, real-world attack techniques (JWT, CORS, WebSockets, OAuth2, etc.), and advanced exploitation like HTTP smuggling and DOM attacks. It also includes professional reporting methods with CVSS/CWE, and 7 hands-on queries for practical learning — making it perfect for red teaming, bug bounty, and real-world appsec roles.

CONTACT US

Have questions about our courses, need guidance, or want to collaborate with us?
We're here to help you every step of the way in your cybersecurity journey.

 Email: info@durbhasigurukulam.in
 Phone/WhatsApp: +91-[7879054058](tel:7879054058)
 Website: www.durbhasigurukulam.in