ASD ACADEMY

HACKER VLOG

DRONACHARYA BATCH WITH AI

2.5 MONTH ONLINE COURSE

15 DAYS INTERNSHIP

Introducing..

"CyberGuard AI Academy: Mastering Defense in the Age of Intelligence."

POWERED BY

REGISTERED BY

ETHICAL HACKING

Course Syllabus

S.No	Topic Name	Sub-Topics Covered
1	**Introduction to Ethical Hacking**	Learn The Fundamentals And Key Issues in Information Security, Including The Basics of Ethical Hacking, Information Security Controls, Relevant Laws, And Standard Procedures.
2	**Footprintingand Reconnaissance**	Learn How to Use The Latest Techniques And Tools For Footprinting And Reconnaissance, a Critical Pre-Attack Phase of Ethical Hacking.
3	**Scanning Networks**	Learn Different Network Scanning Techniques And Countermeasures.
4	**Enumeration**	Learn Various Enumeration Techniques, Including Border Gateway Protocol (BGP) and Network File Sharing (NFS) Exploits and Associated Countermeasures.
5	**Vulnerability Analysis**	Learn How to Identify Security Loopholes in a Target Organization's Network, Communication Infrastructure, and Systems. Diferent Types of Vulnerability Assessment and Vulnerability Assessment Tools are Also Included.
6	**System Hacking**	Learn About The Various System Hacking Methodologies Used to Discover System and Network Vulnerabilities, Including Steganography, Steganalysis Attacks, and How to Cover Tracks.
7	**Malware Threats**	Learn About Different Types of Malware (Trojan, Viruses, Worms, etc.), APT and Fileless Malware, Malware Analysis Procedures, And Malware Countermeasures.
8	**Sniffing**	Learn About Packet Sniffing Techniques And Their Uses For Discovering Network Vulnerabilities, Plus Countermeasures to Defend Against Snifing Attacks.
9	**Social Engineering**	Learn Social Engineering Concepts and Techniques, Including How to Identify The Attempts, Audit Human-Level Vulnerabilities, and Suggest Social Engineering Countermeasures.
10	**Denial-of-Service**	Learn about different Denial of Service (DoS) and Distributed Dos (DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.

S.No	Topic Name	Sub-Topics Covered
11	**Session Hijacking**	Learn the Various Session-Hijacking Techniques Used to Discover Network-Level Session Management, Authentication, Authorization, and Cryptographic Weaknesses and Associated Countermeasures.
12	**EvadingIDS, Firewalls, and Honeypots**	Learn About Firewalls, Intrusion Detection Systems (IDS), and Honeypot Evasion Techniques; The Tools Used to Audita Network Perimeter For Weaknesses; and Countermeasures.
13	**Hacking Web Servers**	Learn About Web Server Attacks, Including a Comprehensive Attack Methodology Used to Audit Vulnerabilities in Web Server Infrastructures and Countermeasures.
14	**Hacking Web Applications**	Learn About Web Application Attacks, Including a Comprehensive Hacking Methodology For Auditing Vulnerabilities in Web Applications and Countermeasures.
15	**SQL Injection**	Learn About SQL Injection Attack Techniques, Evasion,Techniques, and SQL Injection Counter Measures.
16	**Hacking Wireless Networks**	Learn About Different Types of Encryption, Threats, Hacking Methodologies, Hacking Tools, Security Tools, and Countermeasures For Wireless Networks.
17	**HackingMobile Platforms**	Learn Mobile Platform Attack Vectors, Android and ios Hacking, Mobile Device Management, Mobile Security Guidelines, and Security Tools.
18	**loT Hacking**	Learn Different Types of Internet of Things (IoT) and Operational Technology (OT) Attacks, Hacking Methodologies, Hacking Tools, and Countermeasures.
19	**Cloud Computing**	Learn Different Cloud Computing Concepts, Such as Container Technologies and Serverless Computing. Various Cloud Computing Threats, Attacks, Hacking Methodologies, and Cloud Security Techniques and Tools.
20	**Cryptography**	Learn About Encryption Algorithms, Cryptography Tools, Public Key Infrastructure (PKI), Email Encryption, Disk Encryption, Cryptography Attacks, and Cryptanalysis Tools.

WEB TESTING

Course Syllabus

S.No	Topic Name	Sub-Topics Covered
1	**Introduction to Web Application Testing**	Basics of testing web applications to identify security flaws and vulnerabilities.
2	**Burp Suite**	Learn to intercept, analyze, and modify HTTP requests using Burp Suite.
3	**ZAP Proxy & NetSparker**	Use automated tools to scan and detect web application vulnerabilities.
4	**Convert VA Report into PT**	Transform vulnerability assessment findings into a structured penetration testing report.
5	**Application Walkthrough, Identify Functionality & Report Writing**	Understand application flow, identify features, and document security findings.
6	**Security Headers**	Analyze HTTP security headers to enhance application protection.
7	**Cookies & SSL Vulnerabilities**	Identify risks related to cookies and SSL/TLS misconfigurations.
8	**SQL Injection & XSS**	Detect and exploit database injection and cross-site scripting flaws.
9	**CSRF & Clickjacking**	Understand attacks that trick users into performing unintended actions.
10	**DOM-Based Vulnerabilities & CORS**	Identify client-side vulnerabilities and misconfigured cross-origin policies.
11	**XXE & SSRF**	Exploit server-side request handling and XML parsing weaknesses.
12	**OS Command Injection & Path Traversal**	unauthorized access by executing system commands or accessing restricted files.
13	**Access Control Vulnerabilities & Authentication**	Find flaws in user permissions and authentication mechanisms.
14	**Insecure Deserialization & Information Disclosure**	Identify risks from unsafe data handling and leakage of sensitive information.
15	**Business Logic Vulnerabilities & HTTP Host Header Attacks**	Exploit application logic flaws and header manipulation issues.
16	**OAuth Authentication & File Upload Vulnerabilities**	Analyze weaknesses in third-party login systems and file upload features.
17	**JWT & Introduction to API Testing**	Understand token-based authentication and basics of testing APIs.

API TESTING

Course Syllabus

S.No	Topic Name	Sub-Topics Covered
1	**Broken Object Level Authorization**	APIs Tend to Expose Endpoints That Handle Object Identifiers, Creating a Wide Attack Surface of Object Level Access Control Issues.
2	**Broken Authentication**	Authentication Mechanisms are Often Implemented Incorrectly, Allowing Attackers to Compromise Authentication Tokens or to Exploit Implementation Flaws to Assume Other User's Identities Temporarily or Permanently.
3	**Broken Object Property Level Authorization**	Focusing on The Root Cause: The Lack of or Improper Authorization Validation at The Object Property Level.
4	**Unrestricted Resource Consumption**	Satisfying API Requests Requires Resources Such as Network Bandwidth, CPU, Memory, and Storage.
5	**Broken Function Level Authorization**	Complex Access Control Policies With Different Hierarchies, Groups, and Roles.
6	**Unrestricted Access to Sensitive Business Flows**	A Vulnerability Where an API Endpoint is Functionally Correct But Lacks Safeguards to Prevent Bots or Users From Excessively Exploiting The Business Logic.
7	**Server Side Request Forgery**	Server-Side Request Forgery (SSRF) Flaws can Occur When an API is Fetching a Remote Resource Without Validating The User-Supplied URI.
8	**Security Misconfiguration**	APIs and The Systems Supporting Them Typically Contain Complex Configurations, Meant to Make The APIs More Customizable. Software and DevOps Engineers Can Miss These Configurations.
9	**Improper Inventory Management**	APIs Tend to Expose More Endpoints Than Traditional Web Applications, Making Proper and Updated Documentation Highly Important.
10	**Unsafe Consumption of APIs**	Developers Tend to Trust Data Received From Third-Party APIs More Than User Input, and So Tend to Adopt Weaker Security Standards.

MOBILE APP TESTING

Course Syllabus

S.No	Topic Name	Sub-Topics Covered
1	**Improper Credential Usage**	The unauthorized or unintended use of login data—such as sharing, reusing, or stealing passwords—to gain access to systems and sensitive information.
2	**Inadequate Supply Chain Security**	Lack of security measures in third-party components or dependencies, leading to potential vulnerabilities.
3	**Insecure Authentication/Authorization**	Weak or flawed login and access control mechanisms allowing unauthorized access.
4	**Insufficient Input/Output Validation**	Failure to properly validate data inputs/outputs, leading to injection and other attacks.
5	**Insecure Communication**	Data transmitted without proper encryption, making it vulnerable to interception.
6	**Inadequate Privacy Controls**	Poor handling of user data, leading to unauthorized access or data exposure.
7	**Insufficient Binary Protections**	Lack of safeguards like obfuscation, making apps easier to reverse engineer.
8	**Security Misconfiguration**	Incorrect or default security settings exposing systems to attacks.
9	**Insecure Data Storage**	Sensitive data stored without proper protection, making it accessible to attackers.
10	**Insufficient Cryptography**	Weak or improper use of encryption techniques compromising data security.

Contact Us:

Website: www.asdacademy.in
Email: training@asdacademy.in
Phone: 8233150687 / 9680100687
Hacker Vlog
Hacker Vlog Podcast
@hackervlogofficial / @hackervlog / @cyberexpert.riddhisoral

Address:

AkanshaDeep Heights,18thFloor, No. 1841-1842, Kunadi, Kota (Rajasthan),
Pin Code - 324008

www.skilltrack.top

SCAN ME

ASD ACADEMY
India's Most Advanced
Hacking & Coding Academy

Thank You