iGNITE Technologies

Web Application

Penetration Testing Training

www.ignitetechnologies.in

ABOUT

Well-Known Entity for Offensive Security

{Training and Services}

About us

With an outreach to over a million students
and over thousand colleges, Ignite Technologies stood out to be
a trusted brand in cyber security training and services

WHO CAN ?

- College Students
- IS/IT specialist, analyst, or manager
- IS/IT auditor or consultant
- IT operations manager
- Network security officers and
- Practitioners
- Site administrators
- Technical support engineer
- Senior systems engineer
- Systems analyst or administrator
- IT security specialist, analyst, manager,
- Architect, or administrator
- IT security officer, auditor, or engineer
- Network specialist, analyst, manager,
- Architect, consultant, or administrator

WHY US ?

- Level up each candidate by providing the fundamental knowledge required to begin the Sessions.
- Hands-on Experience for all Practical Sessions.
- Get Course PDF and famous website links for content and Tools
- Customized and flexible training schedule.
- Get recorded videos after the session for each participant.
- Get post-training assistance and backup sessions.
- Common Platform for Group discussion along with the trainer.
- Work-in Professional Trainer to provide realtime exposure.
- Get a training certificate of participation.

Web Pentest

Web Pentest program, also known as the Bug Bounty program, is a crowdsourcing initiative hosted by organizations to give a platform to security researchers and white hat hackers from across the globe to showcase their skills and discover any security holes in their infrastructure. Depending upon the severity level of the bug report and the details presented within the Proof of Concept (POC), they are either rewarded with remuneration or recognition as a token of appreciation.

While a large majority of the bug bounty programs are public, certain are private events and are strictly invite-based. Such programs have stringent terms and conditions that the invitees must always abide by

During this course, you will acquire knowledge in the fundamentals of application security vulnerabilities and penetration testing.

Prerequisites

In order to initiate the Bug Bounty Training, you should be aware of the basic concepts of the development web applications; frontend and backend.

iGNITE Technologies

COURSE DURATION: 25 to 30 HOURS

How We Function Training Type

Type 1

A GROUP SESSION will have a maximum of 10 candidates.

Pros:

- Less Expensive than Type2 & Type3.
- Get a chance to build connections across the world.

Type 2

A PERSONALIZED SESSIONS will be a one-on-one session.

Pros: Flexible slot as per candidate availability.

Type 2

A CUSTOMIZED PERSONALIZED session will be a one-on-one session that can be fine-tuned as per the Candidate's requirement.

Pros:

- Flexible slot as per candidate availabilities
- Including Live Website Testing

iGNITE Technologies

What You Will Achieve?

OUR FOCUS

- Level up all candidates from the various domains to make the curriculum cohesive.

- Gained an in-depth knowledge of web application concepts.

- Give hands-on experience

- Maintain the security posture by adhering to industry best practices.

- Work-in Professionals Red Teamers and Pentesters around the world will be conducting all sessions live. Follow OWASP and NIST standards for how to respond to the attack.

iGNITE Technologies

Course Overview

Introduction

- Introduction Web Servers & Web Applications
- The Bug Bounty Program
- Web Application Penetration Testing & its Methodologies
- Introduction to HTTP Protocol
- OWASP & its Top 10
- Introduction to Burp Suite

Pentest Lab Setup

- Web Server Lab Setup
- Web Application Lab Setup
- Configuring Burp Suite Pro

Information Gathering & Reconnaissance

- What Is Information Gathering?
- Information Gathering Cheat Sheet
- DNS Enumeration
- Perform Web Application Fingerprinting
- Spider/Crawl For Missed or Hidden Content Directory Brute Forcing
- Google Advanced Search

Netcat for Pentester

- Introduction to Netcat
- Netcat as Banner Grabber
- Netcat File Transfer
- Netcat Reverse Shell
- Netcat Shells Over Payload

iGNITE Technologies

Configuration Management Testing

- Enumerate Infrastructure and Application Admin Interfaces
- Check For Backup and Unreferenced Files for Sensitive Information
- Check HTTP Methods Supported And Cross Site Tracing (XST)
- Test File Extensions Handling
- HTTP Strict Transport Security
- Test Network/Infrastructure Configuration

Cryptography

- Check SSL Version, Algorithms, Key Length
- Check For Digital Certificate Validity (Duration, Signature And Cn)
- Check Credentials Only Delivered Over Https
- Check That The Login Form Is Delivered Over Https
- Check Session Tokens Only Delivered Over Https
- Check If Http Strict Transport Security (HSTS) In Use

Authentication

- What is Authentication?
- HTTP Authentication Exploitation
- Introduction to Broken Authentication
- Broken Authentication Exploitation.
- Test For User Enumeration
- Test For Brute force Protection
- Test For Default Logins
- Test Password Reset and/or Recovery
- Test Password Change Process
- Test CAPTCHA
- Test Password Quality Rules
- Test For Autocomplete on Password Forms/Input
- Mitigation Steps

iGNITE Technologies

Session Management

- What are Sessions and Cookies?
- Introduction to Session Management
- Check session tokens for cookie flags
- Check session cookie duration
- Test session cookies for randomness
- Insecure Session Exploitation
- Mitigation Steps

Local File Inclusion

- Introduction to Local File Inclusion
- Basic LFI Technique
- Null byte Technique
- Base64 Technique
- Fuzzing Technique
- LFI Suite
- LFI over File Upload
- LFI Log Poisoning
- Mitigation Steps

Remote File Inclusion

- Introduction to RFI
- Why Remote File Inclusion Occurs?
- Remote File Inclusion Exploitation
- Basic Remote File Inclusion
- Reverse Shell through Netcat
- RFI over Metasploit
- Bypass a Blacklist Implemented
- Null Byte Attack
- Exploitation through SMB Server
- Mitigation Steps

iGNITE Technologies

Path Traversal

- Linux Server Path Traversal Exploitation
- Basic Path Traversal
- Blocked Traversal Sequence
- Validated Path Traversal
- Path Disclosure in URL
- Null Byte Bypass
- Windows Server Path Traversal Exploitation
- Basic Path Traversal
- Double dots with Forward-Backward Slashes
- Blocked Traversal Sequences

SQL Injection

- What are Databases?
- Introduction to SQL Injection
- SQL Injection Error Based
- SQL Injection via SQLmap
- Manual SQL Exploitation
- Boolean Based Exploitation
- SQL Injection Form Based Exploitation
- Authentication Bypass
- Remote Code Execution with SQLmap
- Mitigation Steps

XXE Injection

- Introduction to XML
- Introduction to XXE Injection
- XXE for SSRF
- XXE Billion Laugh Attack
- XXE Exploitation
- Blind XXE
- Mitigation Steps

Bonus Section

- Automated Vulnerability Scanner
- Firefox Add-ons
- Encoding Methods
- Reporting

iGNITE Technologies

CONTACT US

Phone No.

+91 9599 387 41 | +91 1145 1031 30

WhatsApp

https://wa.me/message/HIOPPNENLOX6F1

EMAIL ADDRESS

info@ignitetechnologies.in

WEBSITE

www.ignitetechnologies.in

BLOG

www.hackingarticles.in

LINKEDIN

https://www.linkedin.com/company/hackingarticles/

TWITTER

https://twitter.com/hackinarticles

GITHUB

https://github.com/ignitetechnologies

iGNITE Technologies