

ABOUT THE TRAINING



ONLINE ETHICAL HACKING TRAINING

Learn to hack and secure web applications

The Ethical Hacking Training by Internshala is a 6-week online training program in the field of web application security. In this training program, you will learn how to perform vulnerability assessment and penetration testing on a web application in a virtual lab environment.

This training program is created by Internshala's team of experts. You will learn through video tutorials. For a great hands-on learning experience, this training program is packed with assignments, assessment tests, quizzes, and practice exercises.

At the end of this training program, you will be hacking a web application and generating an industry standard report. For doubt clearing, you can post your queries on the forum and get answers within 24 hours.

TABLE OF CONTENTS



■ Introduction to Information Security and Basics of Computer Networking

- 1.1 Introduction to Information Security
- 1.2 Hacking Methodologies and Types of Security Testing
- 1.3 Computer Networking
- 1.4 IP Addressing and NAT
- 1.5 DNS- The Google Maps of the Internet
- 1.6 Ports and Services
- 1.7 Protocols, TCP/IP and OSI Model
- 1.8 Proxy and VPN
- 1.9 Module Test

■ Information Gathering and Basics of Web Development:

- 2.1 Digital Footprints and Information Gathering
- 2.2 Advanced Information Gathering about People and Websites
- 2.3 Google Dorking- Hacking using Google
- 2.4 Introduction to Web Architecture and Understanding Common Security Misconceptions
- 2.5 HTML Basics
- 2.6 HTML and Introduction to Javascript
- 2.7 Introduction to PHP and Setting up XAMPP
- 2.8 Putting Brains into Beauty- Working with PHP
- 2.9 Handling User Input and Building Basic Applications using PHP
- 2.10 Module Test

TABLE OF CONTENTS



■ Introduction to Web VAPT, OWASP and SQL Injections

- 3.1 Introduction to VAPT and OWASP
- 3.2 Basics of Databases and SQL
- 3.3 Authentication Bypass using SQL Injection
- 3.4 GET based SQL Injection- Part 1
- 3.5 GET based SQL Injection- Part 2
- 3.6 POST based SQL Injection- Part 1
- 3.7 POST based SQL Injection- Part 2
- 3.8 Advanced SQL Injections
- 3.9 Automating SQL Injections- SQL Map
- 3.10 Module Test

■ Advanced Web Application Attacks

- 4.1 Bypassing Client Side Filters using Burp
- 4.2 Suite
- 4.3 IDOR and Rate-limiting issues
- 4.4 Arbitrary File Upload Vulnerabilities
- 4.5 Module Test

■ Client Side Attacks

- 5.1 Understanding Important Response Headers, DOM, and Event Listeners
- 5.2 Fundamentals of Cross Site Scripting (XSS)
- 5.3 Understanding Forced Browsing and Session-Cookie Flaws
- 5.4 Cross Site Request Forgery (CSRF) and Open Redirections
- 5.5 Brute Force Attacks using Burp Suite
- 5.6 Personally Identifiable Information (PII) Leakage and Sensitive Information Disclosure
- 5.7 Module Test

TABLE OF CONTENTS



■ Identifying Security Misconfigurations and Exploiting Outdated Web Applications

- 6.1 Common Security Misconfigurations
- 6.2 Default/Weak Password Vulnerabilities
- 6.3 Fingerprinting Components with Known Vulnerabilities
- 6.4 Scanning for Bugs in Wordpress and Drupal
- 6.5 Using Public Exploits and Looking at Live Case Studies
- 6.6 Module Test

■ Automating VAPT and Secure Code Development

- 7.1 Information Gathering for Endpoints
- 7.2 Application Assessment using Nmap
- 7.3 Automating VAPT with Nikto and Burp Suite Pro
- 7.4 Concepts of Code Security and Patching
- 7.5 Module Test

■ Documenting and Reporting Vulnerabilities

- 8.1 Documenting Stages of Vulnerabilities using Tools
- 8.2 VAPT Reports: Developer Report v/s Higher Management Report
- 8.3 Parts of a VAPT Report
- 8.4 Common Good Practices and Bad Practices
- 8.5 Module Test

Excited to learn Ethical Hacking? Click [here](#) to sign-up for the training.

FREQUENTLY ASKED QUESTIONS



How will the training be imparted?

The Ethical Hacking Training will be delivered using video tutorials and interactive exercises.

What is the duration of this training?

This is a 6 weeks training program.

What are the timings of this training program?

As this is a purely online training program, students can choose to learn at any time of the day. The students can decide the timing according to their convenience.

Who can join? I am a beginner/advanced user, is this training program for me?

This training would be better suited to beginners who have no prior knowledge of Ethical Hacking. Anyone who is willing to learn and has interest in Ethical Hacking can opt for this training program.

Are there any prerequisites for joining this program?

This program is for beginners. There are no prerequisites for the training

What hardware/software are required for doing this training?

No hardware is required for doing this training. All the necessary software is uploaded online which can be downloaded during training

FREQUENTLY ASKED QUESTIONS



Will there be a certificate provided at the end of the training?

Yes, a certificate will be provided by Internshala upon completion of the training. Students may download a soft copy of the certificate through our portal.

What hardware/software are required for doing this training?

You will be required to have a computer/laptop (minimum 4GB RAM) for this training. All the necessary software is present online which can be downloaded for free during the training.

Can the material be used by a group of students?

No. These training programs are meant for individual users. Multiple users will not be allowed to access the portal using the same account.

If you have any queries or any doubts regarding the training, please write to us at trainings@internshala.com or call us on +91 844 8444 853.

REGISTER NOW