mind Hacking Point

CHECK POINT

Basic Web Hacking

2 day class

Basic Track

This is an entry-level web application security testing course and also a recommended pre-requisite course before enrolling for our "Advanced Web Hacking" course. This foundation course of "Web Hacking" familiarises the attendees with the basics of web application and web application security concerns. A number of tools and techniques, backed up by a systematic approach on the various phases of hacking will be discussed during this 2-day course. If you would like to step into a career of Ethical Hacking / Pen Testing with the right amount of knowledge, this is the right course for you.

This course familiarizes the attendees with a wealth of tools and techniques required to breach and compromise the security of web applications.
The course starts by discussing the very basics of web application concepts, and gradually builds up to a level where attendees can not only use the tools andtechniques to hack various components involved in a web application, but also walk away with a solid understanding of the concepts on which these tools are based. The course will also talk about industry standards such as OWASP Top 10 and PCI DSS which form a critical part of web application security.
Numerous real life examples will be discussed during the course to help the attendees understand the true impact of these vulnerabilities.

- Intermediate knowledge of infrastructure application security (at least 2 years'experience)
- Common command line syntax competency
- Experience using virtual labs for pentesting and/or offensive research

Who it's for

- Security enthusiasts
- Anybody who wishes to make a career in this domain and gain some knowledge of networks and applications
- Web Developers
- System Administrators
- SOC Analysts
- Network Engineers
- Pen Testers who are wanting to level up their skills

This course is designed to help individuals bring their proficiency in web hacking and defense up to the industry baseline. It's a foundation course that can lead on to our Advanced courses after a year or more spent using your new skills out in the wild. Delegates should bring their laptop with windows operating system installed (either natively or running in a VM). Further, delegates must have administrative access to perform tasks such as installing software, disabling antivirus etc. Devices need to be connected to the internet in order to access the course environment.
Delegates should also have:

- Basic knowledge of web application security
- Basic familiarity with common command line syntax
- Basic knowledge of Burp Suite

Top 3 takeaways

- The ability to find and exploit web application vulnerabilities and other weaknesses
- Knowledge of how to apply the industry-recommended web security standards and approaches
- Time spent with experienced, practicing penetration testers who can answer your questions

NotSoSecure part of claranet cyber security

mind Hacking Point

CHECK POINT

What you'll learn

This course uses a Defense by Offense methodology based on real world offensive research (not theory). That means everything we teach has been tried and tested on live environments and in our labs and can be applied once the course is over. By the end, you'll know:

- Everything you need to about the risks associated with various web-based vulnerabilities
- How to think and behave like a real threat actor
- How to exploit vulnerabilities seen recently in the wild, as well as more archaic, but still prevalent vulns
- The fundamental principles of web application hacking

What you'll be doing

You'll be learning hands on:

- Spending most of the session (~80%) on lab-based exercises
- Using lab-based flows to explore and hack lifelike web application environments
- Trying out different hacking techniques to exploit the OWASP Top 10 and other vulns
- Discussing the real-world impact of the hacks covered with the course trainer

Why it's relevant

All modern organizations rely on web applications, making them the attack vector of choice for many threat actors. To protect these assets, security and software development teams need a thorough, contextual understanding of how and why they get targeted and what happens when those attacks succeed. Our Basic Web Hacking course provides delegates with this knowledge and more by schooling them in the latest and most useful offensive testing and remediation techniques.

Delegates with solid baseline knowledge and a consistent approach to ethical hacking tend to develop faster in the long-term, so we've curated a syllabus designed to comprehensively improve your subject matter understanding and practical methodology. It does this by analyzing both archaic and modern techniques, which once mastered, will help you progress into advanced topics.

What's in the syllabus

Note: our syllabuses are subject to change based on new vulnerabilities found and exploits released.

UNDERSTANDING THE HTTP PROTOCOL

- HTTP protocol basics
- Introduction to proxy tools

INFORMATION GATHERING

- Enumeration techniques
- Understanding web attack surface

ISSUES WITH SECURE SOCKETS LAYER (SSL) AND TRANSPORT LAYER SECURITY (TLS)

- SSL/TLS misconfiguration

USERNAME ENUMERATION AND FAULTY PASSWORD RESET

- Attacking authentication and faulty password mechanisms
- User enumeration
- Broken authentication
- Second factor authentication bypass

BROKEN ACCESS CONTROL – ROLE BASED AUTHORIZATION BYPASS

- Horizontal Privilege Escalation attack
- Vertical Privilege Escalation attack
- Insecure Direct Object Reference attack

SECURITY MISCONFIGURATION

- Business Logic attack

CROSS SITE SCRIPTING (XSS)

- Various types of XSS
- Session hijacking and other attacks

SERVER SITE REQUEST FORGERY (SSRF)

- Understanding SSRF attack
- Various impacts of SSRF attack

SQL INJECTION (SQLi)

- SQL injection types
- Manual exploitation
- Automated exploitation

NotSoSecure part of claranet cyber security

mind Hacking Point

CHECK POINT

XML EXTERNAL ENTITY (XXE) ATTACKS
- XXE basics
- XXE exploitation

INSECURE FILE UPLOADS
- Attacking file upload functionality
- Executing remote code through malicious file upload

COMPONENTS WITH KNOWN VULNERABILITIES
- Understanding the risk introduced by known vulnerabilities
- Known vulnerabilities leading to critical exploits
- Log4J attacks

INSUFFICIENT LOGGING AND MONITORING
- Understanding importance of logging and monitoring
- Evaluate the logging events
- Common pitfalls in logging and monitoring

What you'll get

- Certificate of completion
- 30 days lab access after the course (with the opportunity to extend)
- 8 Continuing Professional Education (CPE) credits awarded per day of training fulfilled
- Learning pack: question & answer sheets, setup documents, and command cheat sheets

Course highlights

What delegates love:
- Intensive format: two days of focused learning that can be immediately applied to pentesting initiatives
- Our labs: probably the biggest selling point for our courses. Not only will you spend most of the course hacking hands-on in a lifelike web environment, you'll get 30+ days access to practice your new skills afterwards.
- Dedicated Kali instance: you'll have your own infrastructure to play with, enabling you to hack at your own speed.
- Real-world learning: where many of the leading cybersecurity training courses
- are based on theory, our scenario-led, research-based approach ensures you learn how real threat actors think and behave.
- Specialist-led training: you'll learn from highly skilled and experienced practicing penetration testers and red teamers.

Outcomes for budget holders

This course is designed to develop web application security testing competency within your organization, helping you:
- Respond to the security skills shortage from the ground up
- Take the first steps towards building an advanced web application security testing team
- Create a stronger case for securing your organization's software development and procurement practices
- Build a closer relationship between development and security teams
- Nurture and retain passionate, highly skilled, and security conscious employees
- Keep your own web security knowledge up to date
- Demonstrate commitment to security through training, compliance, and change management
- Develop the organization's competitive advantage for security-conscious customers

NotSoSecure part of claranet cyber security