COURSE PROFILE:

Ultimate Web Hacking

5 days | **Advanced training**

Version 8

claranet cyber security | NotSoSecure Training

Your Course

Web application security is one of the biggest and fastest-moving specializations within cybersecurity today. Only with a comprehensive, well-rehearsed arsenal of modern ethical hacking skills can it be mastered. Join this hands-on, 5-day course to push your web hacking to the next level and widen your career prospects. Get your hands dirty with our popular virtual labs and learn from experienced, practicing penetration testers with a legacy of training at Black Hat.

Who is it for?

- Penetration testers and red teamers
- Security consultants and architects
- CSIRT/SOC analysts and engineers/blue teams
- Developers with in-depth security experience
- Security/IT managers and team leads.

This course is suitable for in-house security teams from intermediate to pro level. It's also relevant to other security and IT practitioners and managers who want to understand the current threat landscape and defend their organization.

Delegates must have the following to make the most of the course:

- Intermediate knowledge of web application security (at least 2 years' experience)
- Common command line syntax competency
- Experience using virtual labs for pentesting and/or offensive research
- Basic working knowledge of Burp Suite (download here)

Top 3 Takeaways

- Many of the latest and most complex web hacking and penetration testing techniques
- The skills and knowledge to hack the OWASP Top 10
- Knowledge of how to remediate as well as exploit web application vulnerabilities

What will you learn?

This course uses a Defense by Offense methodology based on real-world engagements and offensive research (not theory). That means everything we teach has been tried and tested on live environments and in our labs, so you can put it into practice as soon as the training is over. By the end of the course, you'll know:

- How to think and behave like an advanced, real-world threat actor.
- How to identify commonly used vulnerabilities known to have caused damage and disruption in recent months.
- How to deploy the latest and most common web application hacks (including many novel techniques that can't be detected by scanners)
- How to analyze vulnerabilities within your own organization and customize your hacking techniques in response.

What will you 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 environments.
- Trying out different hacking techniques to exploit the OWASP Top 10 and other common vulnerabilities.
- Discussing case studies with your course leader to understand the impact of the hacks covered.

Why is it relevant?

All modern organizations rely on web applications, making them the attack vector of choice for many threat actors. However, scanners alone are neither powerful nor smart enough to find the more complex and often more damaging vulnerabilities that would threaten your organization's ability to stay online. And with so many vulnerabilities open to exploitation, remediation must be prioritized according to risk and impact. What's needed is a thorough, contextual understanding of how and why web applications get targeted and what happens when those attacks succeed. Our Advanced Web Hacking course provides delegates with this knowledge and more, helping push their existing offensive testing and remediation skills to the next level.

What is in the Syllabus?

Note: Our syllabus is subject to change based on new vulnerabilities found and exploits released.

MODULES	WHAT YOU WILL LEARN
INTRODUCTION	This module is an overview of offensive security for web applications, focusing on understanding the necessary tools and techniques for successful security testing. The module dives into web application architecture and introduces foundational concepts such as HTTP protocol, web proxies, and penetration testing methodologies. It emphasizes the importance of a secure development lifecycle (SDLC) and how it relates to the security testing process to prepare attendees to master web application penetration testing. • Lab Setup and Architecture Overview • Burp Suite 101

ATTACKING AUTHENTICATION AND SINGLE SIGN ON (SSO)	This module introduces various authentication protocols used in modern web applications and discusses various techniques for exploiting and bypassing them. Participants will learn how to identify common authentication vulnerabilities such as vulnerable JWT implementations, vulnerabilities in SAML authorization, and misconfigurations in OAuth.
	Additionally, the module includes case studies that demonstrate how to bypass 2-factor authentication (2FA) mechanisms and exploit authentication bypasses using subdomain takeover techniques.
	• Exploiting JWT and JWS Implementation
	• SAML Authorization Bypass
	• Case Studies:
	  ○ Bypassing 2-Factor Authentication (2FA)
	  ○ Authentication Bypass using Subdomain Takeover
	  ○ OAuth Misconfiguration Attack

PASSWORD RESET ATTACKS	The module introduces techniques to attack and bypass validation mechanisms, such as Host Header Validation Bypass, which can be used to bypass password reset validation across different domains. The attendees will also learn about Bypassing IP Based Brute Force Protections, where attackers can leverage cloud services to carry out brute-force attacks against password reset tokens. • Host Header Validation Bypass • Bypassing IP Based Brute Force Protections
BUSINESS LOGIC FLAW AND AUTHORIZATION FLAWS	The module educates attendees on identifying and exploiting common web application business logic and authorization flaws and provides them with in-depth knowledge of the different types of flaws. Covering Mass Assignment, which occurs when information is unnecessarily indexed or written in fields that should remain blank, and Second Order Insecure Direct Object Reference (IDOR), where an attacker can indirectly manipulate data without an ID. Additionally, the module introduces

	attendees to race conditions in web applications, a type of flaw that arises when multiple requests make an unpredicted effect on the intended function. • Mass Assignment • Second Order IDOR • Identifying and Exploiting Race Conditions in Web Apps • WebSocket Authorization Bypass
API PENTESTING	This module focuses on application programming interface (API) security testing, which is critical for securing web applications that rely on them. Attendees will learn how to identify and exploit authorization bypass vulnerabilities in REST APIs using different techniques. Moreover, the module includes training on exploiting GraphQL APIs that have become popular due to their flexibility in handling complex data queries. Additionally, the module covers gRPC endpoints and how to identify and exploit them effectively. • API Authorization Bypass - REST API • Exploiting GraphQL APIs
XML EXTERNAL ENTITY (XXE) ATTACK	This module is designed to give attendees an in-depth understanding of XML External Entity (XXE) attacks, which can be exploited to gain unauthorized system access. The module covers the basics of XXE, then moves to explain advanced XXE exploitation techniques such as exfiltrating data through out-of-band (OOB) channels and techniques to exploit XXE through SAML. The module also demonstrates the use of XXE in applications that parse files containing XML, such as MS Office documents. • XXE through bypassing WAF • Advanced XXE Exploitation over Out-of-Band (OOB) Channels • XXE Through SAML • XXE in File Parsing
BREAKING CRYPTOGRAPHY	This module focuses on cryptography testing and attacks which was commonly found in web applications. Attendees will learn how to identify and exploit different cryptography vulnerabilities to understand the importance of utilizing strong & modern cryptography implementations for web application security. The module covers the basics of cryptography with examples of how cryptography can be used in password reset workflows and how to exploit the known plaintext attack in these scenarios. Furthermore, it covers Hash Length Extension Attacks, which can be used to spoof a valid hash signature and alter the contents of data. Finally, it dives into authentication bypasses using .NET Machine Keys that have been leaked or exposed to the internet. • Known Plaintext Attack (Faulty Password Reset) • Exploiting padding oracles with fixed IV's • Hash Length Extension Attacks • Auth Bypass using .NET Machine Key

REMOTE CODE EXECUTION (RCE)	This module covers deserialization attacks that can lead to Remote Code Execution (RCE) vulnerability in web applications. It educates attendees on methods to exploit insecure deserialization against various coding languages, including PHP, Java, & Python. The module then moves to less conventional RCE attacks such as Git misconfigurations, and Server-side Template Injection. The module demonstrates real-life examples of how these attacks can be exploited and also highlights the importance of secure coding practices to mitigate the risks of these attacks in web applications.
	• PHP Deserialization Attack
	• Java Deserialization Attack
	  ○ Binary
	  ○ XML
	  ○ SerialVersionUID Mismatch
	• Python Deserialization Attack
	• Leverage Git Misconfiguration to ViewState Deserialization
	• Server-side Template Injection

SQL INJECTION (SQLi) MASTERCLASS	This module is devoted to mastering SQL Injection (SQLi), one of the most dangerous vulnerabilities that allow attackers to execute unauthorized SQL queries. The module outlines Advanced SQL injection techniques such as Second-order Injection and Out-of-Band (OOB) Exploitation, which can be used to bypass modern-day security measures such as Web Application Firewalls (WAFs). Additionally, it covers SQLi through Cryptography, where the attacker can manipulate input parameters or fields using different cryptographic techniques. The module demonstrates exploiting the Operating System through PowerShell and covers advanced SQLMap usage, which is a potent SQL injection tool. • Second-order Injection • OOB Exploitation • SQLi through Cryptography • Advanced SQLMap - usage of eval for runtime payload generation • SQLi – Data Exfiltration over DNS • Advanced SQLMap Usage and Web Application Firewall (WAF) Bypass
TRICKY FILE UPLOAD	This module delves into some less commonly identified methods to bypass file validation checks. Attendees will learn about the importance of preventing unauthorized executable code from being uploaded onto the web server and how attackers can exploit file upload vulnerabilities. The module emphasizes the use of malicious file extensions, such as asp or phtml, that can pass through validation protocols not designed to detect executable files. Additionally, the module covers strategies to identify and exploit hardened web servers that have implemented security measures against file upload attacks. • Malicious File Extensions • Circumventing File Validation Checks • Exploiting Hardened Web Servers

SERVER-SIDE REQUEST FORGERY (SSRF)	This module provides attendees with an in-depth understanding of Server-Side Request Forgery (SSRF) attacks and how they can be exploited to gain unauthorized access to sensitive information on internal networks, often bypassing firewall restrictions. • SSRF to Query Internal Network and metadata API • SSRF to Exploit Templates and Extensions • SSRF Filter Bypass Techniques ○ SSRF Filter Bypass via DNS Rebinding

ATTACKING THE CLOUD	This module is focused on attacking various cloud services and outlines different techniques attackers can use to exploit vulnerabilities in cloud services. It covers Serverless Exploitation and gaining code execution via Lambda functions, Google Dorking in the Cloud Era, AWS Cognito Misconfigurations leading to Data Exfiltration, and SSRF to RCE in Legacy AWS Web Applications. This module is designed to empower individuals to proactively address security challenges within various cloud infrastructures.
	• Serverless Exploitation
	• Google Dorking in the Cloud Era
	• Cognito Misconfiguration to Data Exfiltration
	• SSRF to RCE in Legacy AWS Web Applications
	• Case studies:
	  ○ SSRF to Amazon Elastic Compute Cloud (EC2) takeover
	  ○ AWS credentials Leaked (Netflix, TD Bank)

AI / LLM VULNERABILITIES	This AI security section focuses on the risks introduced when applications rely on large language models for decision-making or automation. The attendees will understand on how attackers manipulate model behaviour through both direct and indirect prompt injection. The module also highlights common design flaws in AI plugins and tool integrations, where the attendees will learn to leverage and trick the AI bot into executing remote code. • Direct vs Indirect Prompt Injection • Insecure Plugin Design • Preventive Measures in Securing
DEPENDENCIES AND SUPPLY CHAIN VULNERABILITIES	This module looks at the often-overlooked risks hidden inside third-party code, open-source libraries, and CMS extensions that modern web applications depend on. Even a fully patched core system can be compromised by a vulnerable plugin or an outdated dependency. Through practical examples, the module shows how attackers trace and exploit these components, chain known vulnerabilities inside trusted packages, and execute vulnerabilities with known components. • Supply Chain Security • Attacking Components with Known Vulnerabilities • Exploiting Hardened CMS

WEB CACHING ATTACKS	This module covers the Web Cache Poisoning Attack, where an attacker can manipulate the content that the cache serves to all the users, often bypassing typical security measures. The attendees will learn how attackers can manipulate the cache mechanisms to execute cache poisoning attacks and the impact of cascading cache poisoning attacks. Furthermore, the module highlights the importance of secure coding practices when designing caching mechanisms, emphasizing the strategies to prevent caching attacks effectively. • Web Cache Deception • Web Cache Poisoning Attack • Web Cache Poisoning in Drupal8

BUGS IN THE CODE AND CLIENT-SIDE VULNERABILITIES	This module covers how attack chaining works where upon identifying vulnerabilities in the code can lead to RCE. This module also covers vulnerabilities related to client side bypasses, where an attacker can analyse the client-side JavaScript file and identify the potential vulnerability which leads to XSS or sensitive information leakage in case of post message bugs. In modern application it has implemented the protection of integrity of data supplied in HTTP request which prevents from further testing of the web application, here by creating your own burp suite custom plugins we can update the parameter at runtime which was used to protect the integrity allow an attacker to modify the request data and test the entire application for security vulnerabilities.
	• Attack Chain: Finding Bugs in Code to RCE
	• Exploiting Post Message Bugs
	• HTTP Desync Attack
	• Writing your own Burp Plugins to Bypass Integrity Checks
	  ○ Understanding the Limitation
	  ○ Understanding Burp Montaya APIs
	  ○ Writing your Burp Plugin
	  ○ Exploiting the Application

VARIOUS CASE STUDIES	• A collection of weird and wonderful XSS, CSRF, SSRF, RCE attacks

Bonus Exercises During Extended 30-Day Lab Period

Boundary Condition	JWT KID Claim Bypass	Invite Promocode Bypass
UUID Brute Force	Cookie Swap Attack	HTTP Parameter Pollution
XXE via XInclude	Unicode Normalization Attack	ECDSA Nonce Reuse Attack
Padding Oracle Attack	Jackson JSON Deserialization Attack	Python Deserialization Attack
Log4Shell	Server-Side Template Injection in YouTrack	.Net Deserialization Attack
Second order SQL Injection on Joomla	SQLi via File Metadata	NoSQL Injection
PHP Object Injection	HTTP Desync Attack	Cookie Swap

What will you get?

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

Course Highlights

What delegates love:

- **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, but you'll also have 30+ days of access to practice your new skills afterwards.
- **Individual access:** You'll have your own infrastructure to play with, enabling you to hack at your own speed.
- **Real-world learning:** Where many leading cybersecurity training courses are based on theory, our scenario-led, research-based approach ensures you learn how real threat actors think and act.
- **Specialist-led training:** You'll learn from highly skilled and experienced practicing penetration testers and red teamers.
- **Up-to-date content:** Our syllabus remains so relevant that delegates come back year after year for more.
- **Remediations included:** You'll learn how to fix as well as find vulnerabilities.
- **Course topics**: Cryptography, SQL injection, and RCE often come out on top.

Outcomes for Budget Holders

This course is designed to bring your in-house cloud security testing competency up to the industry standard, helping you:

- Lower the likelihood of security incidents by identifying weaknesses in your cloud infrastructure.
- Improve your understanding of the organization's risk posture based on the frequency and severity of weaknesses identified.
- Improve the organization's approach to access control management.
- Create a stronger case for securing software development, cloud deployment, and governance practices.
- Develop a secure cloud roadmap that balances growth and risk.
- Implement cloud-based attack detection and response tactics.
- Build a closer relationship between development and security teams.
- Internally pentest new tools and systems before making an investment.
- Nurture and retain passionate, highly skilled, and security-conscious employees.

WHY NOTSOSECURE?

We **hack**. We **teach**.

NotSoSecure is Claranet's dedicated training division and part of its global penetration testing practice. We're one of the largest training partners at Black Hat and a respected provider of web, mobile, and network penetration testing.

All our trainers are experienced, practicing, accredited penetration testers with their own field of excellence. This translates into our course syllabuses, where each module is designed around real-world engagements and in-the-wild research. No other provider of cybersecurity training is modelled in this way. The delegates we train leave our courses armed with knowledge and skills based on current and authentic attacker tactics and tradecraft, not theory alone.

It's our mission to help organizations raise the bar when it comes to their cybersecurity, and to inspire and empower the next generation of IT and security professionals to remain relevant in the way they think and hack. We achieve this by delivering practical content, giving delegates the hands-on experience needed to understand the context behind each offensive and defensive technique. They go on to use this with confidence in their own work, be that within an organisation or their personal research.

WE HACK.
WE TEACH.

claranet cyber security®