

COURSE PROFILE:

Advanced Web Hacking

5 day **Advanced** training



NotSoSecure part of
claranet cyber security®

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 it's 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 you'll 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 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 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 it's 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.

Our syllabuses are revised regularly to reflect the latest in-the-wild hacks, the newest Burp Suite releases, and whatever proof of concepts we've been developing in our own research. Because they remain so up to date with the threat landscape and security industry standard, **many delegates return every 1-2 years** to update their skills and get a refresh.



NotSoSecure part of

claranet cyber security®

What's in the syllabus

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

INTRODUCTION

- Lab setup and architecture overview
- Burp Suite features recap

ATTACKING AUTHENTICATION AND SINGLE SIGN ON (SSO)

- Token hijacking attacks
- Logical bypass/boundary conditions
- Bypassing 2-Factor Authentication (2FA)
- Authentication bypass using subdomain takeover
- JSON Web Token (JWT) and JSON Web Signature (JWS) attacks
- Security Assertion Markup Language (SAML) authorization bypass
- Open Authorization (OAuth) issues

PASSWORD RESET ATTACKS

- Session poisoning
- Host header validation bypass
- Case study: common password reset fails

BUSINESS LOGIC FLAW AND AUTHORISATION FLAWS

- Mass assignment
- Invite/promo code bypass
- Replay attack
- API authorization bypass
- HTTP Parameter Pollution (HPP)

EXTENSIBLE MARKUP LANGUAGE (XML) EXTERNAL ENTITY (XXE) ATTACK

- XXE basics
- Advanced XXE exploitation over out-of-band (OOB) channels
- XXE through SAML
- XXE in file parsing

BREAKING CRYPTOGRAPHY

- Known plaintext attack (faulty password reset)
- Padding oracle attack
- Hash length extension attacks
- Auth bypass using .NET machine key
- Exploiting padding oracles with fixed initialization vectors (IVs)
- ECDSA nonce reuse attack

REMOTE CODE EXECUTION (RCE)

- Java deserialization attack
 - Binary

- XML
- serialVersionUID mismatch
- .Net deserialization attack
- PHP deserialization attack
- Python deserialization attack
- Server-side template injection
- Exploiting code injection over OOB channels

SQL INJECTION (SQLi) MASTERCLASS

- Second-order injection
- OOB exploitation
- SQLi through cryptography
- OS code execution via PowerShell
- Advanced topics in SQLi
- Advanced SQLMap usage and web application firewall (WAF) bypass

TRICKY FILE UPLOAD

- Malicious file extensions
- Circumventing file validation checks
- Exploiting hardened web servers
- SQLi via file metadata

SERVER-SIDE REQUEST FORGERY (SSRF)

- SSRF to query internal network
- SSRF to exploit templates and extensions
- SSRF filter bypass techniques

ATTACKING THE CLOUD

- SSRF exploitation
- Serverless exploitation
- Google dorking in the cloud era
- Cognito misconfiguration to data exfiltration
- Post-exploitation techniques on cloud-hosted applications
- Case studies: SSRF to RCE in containers
 - SSRF to Amazon Elastic Compute Cloud (EC2) takeover
 - AWS credentials Leaked (Netflix, TD Bank)

ATTACKING HARDENED CONTENT MANAGEMENT SYSTEMS (CMS)

- Identifying and attacking various CMS
- Attacking hardened WordPress, Joomla, and Microsoft SharePoint

WEB CACHING ATTACKS

- Web cache deception attack
- Web cache poisoning attack
 - Web cache poisoning in Drupal 8

MISCELLANEOUS VULNERABILITIES

- Unicode normalization attacks
- Second order insecure direct object references (IDOR) attack
- Exploiting misconfigured code control systems
- Pentesting GraphQL
 - Introspection based attacks on GraphQL
- HTTP desync attack

VARIOUS CASE STUDIES

- A collection of weird and wonderful XSS and CSRF attacks

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 realistic web environment, you'll get 30+ days' lab 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 of the leading cybersecurity training courses are based on theory, our scenario-based syllabus teaches you how real threat actors think and behave.
- Specialist training guaranteed: you'll learn from highly skilled and experienced practicing penetration testers and red teamers.
- Up-to-date content: our syllabus remains so relevant and current, delegates come back year on 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.

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

Outcomes for budget holders

This course is designed to bring your organization's web application security testing competency up to an advanced industry standard, helping you:

- Lower the likelihood of security incidents by identifying high-impact vulnerabilities in your web infrastructure
- Improve your understanding of the organization's risk posture based on the frequency and severity of vulnerabilities identified
- Create a stronger case for securing your organization's software development and procurement practices
- Build a closer relationship between development and security teams
- Internally pentest new tools and systems before making an investment
- Nurture and retain passionate, skilled, and security conscious employees
- Keep your own web application security knowledge relevant
- Demonstrate commitment to security through training, compliance, and change management
- Develop the organization's competitive advantage for security-conscious customers



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®

