04

Live · Course 04 of 08

Web Application Penetration Testing

Hunt real web vulnerabilities with Burp Suite: the OWASP Top 10, XSS, SQL injection, CSRF, SSRF, command injection, file inclusion, XXE and access control.

AT A GLANCE

Language
Telugu

Certificate
On completion

Lab
ACEP Tech Electronics

AFTER THIS COURSE

- [x] Test a web app end to end with Burp Suite
- [x] Find and exploit the OWASP Top 10 and 20+ more bug classes
- [x] Write findings the way bug bounty programs and clients expect

TOOLS YOU'LL USE

Burp Suite · sqlmap · Burp Collaborator · DVWA · bWAPP · OWASP WebGoat

SYLLABUS · 12 MODULES · 82 TOPICS

01 Introduction to WAPT

7 topics

- What is web application penetration testing
- Vulnerability assessment vs penetration testing
- Bug hunting methodology
- Web application vs website
- DBMS architecture
- URL structure
- Lab setup: DVWA, bWAPP, OWASP WebGoat

02 OWASP Top 10 (2021)

10 topics

- A01 Broken Access Control
- A02 Cryptographic Failures

02 OWASP Top 10 (2021) (continued)

- A03 Injection
- A04 Insecure Design
- A05 Security Misconfiguration
- A06 Vulnerable and Outdated Components
- A07 Identification and Authentication Failures
- A08 Software and Data Integrity Failures
- A09 Security Logging and Monitoring Failures
- A10 Server-Side Request Forgery

03 Burp Suite

4 topics

- Proxy configuration
- Repeater
- Web crawling
- Target scanning

04 Cross-Site Scripting (XSS)

6 topics

- JavaScript event handlers
- Reflected XSS
- Stored XSS
- DOM-based XSS
- Cookie theft with XSS
- XSS exploitation

05 SQL Injection

7 topics

- Error-based
- Union-based
- Blind: boolean-based and time-based
- Manual injection
- Automated scanning

05 SQL Injection (continued)

- Admin panel bypass
- sqlmap

06 Cryptographic Failures

5 topics

- ColdFusion vulnerability
- BREACH attack
- Heartbleed
- Missing HSTS
- POODLE attack

07 Broken Authentication & Sessions

6 topics

- Credential stuffing
- Improper admin login
- Insecure login forms
- Insecure logout
- Session hijacking
- Session ID exposed in the URL

08 CSRF

4 topics

- Change email
- Change address
- Add to cart
- CSRF exploitation

09 SSRF

4 topics

- SSRF stock checker
- SSRF to an internal API
- Blind SSRF
- Burp Collaborator

10 Shell, Command Execution & File Inclusion

5 topics

- File upload vulnerabilities
- Remote code execution
- OS command injection
- Local file inclusion (LFI)
- Remote file inclusion (RFI)

11 XXE (XML External Entity)

7 topics

- Introduction to XML and entities
- Document Type Definitions (DTD)
- XXE injection
- Billion laughs (DoS)
- XXE through file upload
- XXE to remote code execution
- XSS via XXE

12 Additional Vulnerabilities

17 topics

- IDOR
- Host header attacks
- HTTP request smuggling
- HTML injection
- Open redirection
- Path and directory traversal
- Insecure CORS
- Clickjacking
- Missing rate limits
- Parameter tampering
- JWT attacks
- Negative quantity
- Race conditions (coupons)
- Mass assignment

12 Additional Vulnerabilities (continued)

- OTP bypass
- Insecure deserialization
- SSTI

Ready to start Web App Pentesting?

Free live demo: Saturday 6:00 – 7:00 PM · Sunday 11:00 AM – 12:00 PM · Sunday 7:00 – 8:00 PM (IST). Reply **DEMO** on WhatsApp.

+91 81250 59380 · Call or WhatsApp

contact@secueyes.in

secueyes.in

Scan for this course

SecuEyes

YOUR INSTRUCTOR

Taught by a hacker who investigates cybercrime.



Every class is taught by **Chaitanya Eshwar Prasad**. He doesn't teach from slides: he teaches what he does every week, investigating real cybercrime cases and finding real vulnerabilities.

He started exploring technology in 7th class and was hunting security bugs by 10th. Today he supports cybercrime investigations as a forensic investigator, holds national records for his work, and has taught thousands of students on campus and through his Telugu YouTube channel.

7+	100+	33K+	9+
Years in cybersecurity	Bugs reported & secured	YouTube learners	Campuses as guest speaker

Anisetti Chaitanya Eshwar Prasad
Founder & Lead Instructor, Secueyes

SECURITY RESEARCH · HACKED & REPORTED

Google · YouTube · PayPal · Lenovo · Nokia · Epic Games · Unreal Engine · Rakuten · Kik · CoWIN (Winning Over Covid-19) · MCA, Govt of India · Govt of Telangana

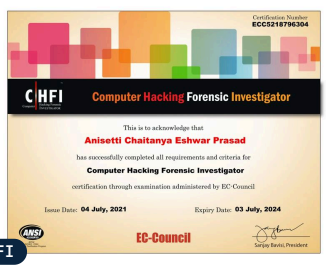
INVITED AS GUEST SPEAKER · UNIVERSITIES & COLLEGES

KL University · Anurag University · GRIET · VNRVJIET · KPRIT · ACE Engineering College · KL SAC · SJB Institute of Technology · Rishi MS Institute for Women

EC-COUNCIL CERTIFICATIONS



CEH



CHFI



CSA