Check Point Certified Advanced Web Hacking (CCPE-AW)

Zetlan Technologies

Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Course Modules

1. INTRODUCTION

- Lab setup and architecture overview
- Burp Suite features recap

2. 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 Languge (SAML) authorization bypass
- Open Authorization (OAuth) issues

3. PASSWORD RESET ATTACKS

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

4. BUSINESS LOGIC FLAW AND AUTHORISATION FLAWS

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

5. EXTENSIBLE MARKUP LANGUAGE (XML) EXTERNAL ENTITY (XXE)

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

6. 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

7. REMOTE CODE EXECUTION (RCE)

- Java deserializtn attack- Binary- XML- Serial Version UID mismatch
- .Net deserialization attack
- PHP deserialization attack
- Python deserialization attack
- Server-side template injection
- Exploiting code injection over OOB channels

8. 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 app firewall (WAF) bypass

9. TRICKY FILE UPLOAD

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

10. SERVER-SIDE REQUEST FORGERY (SSRF)

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

11. ATTACKING THE CLOUD

- SSRF exploitation
- Serverless exploitation
- Google Dorking in the cloud era
- Post-exploitation techniques on cloud-hosted applications
- SSRF to RCE in containrs- SSRF to Amazon Elastic Compute Cloud

12. ATTACKING HARDENED CONTENT MANAGEMNT SYSTEMS (CMS)

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

13. WEB CACHING ATTACKS

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

14. 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

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474