ASL IT SECURITY

BEGINNERS WEB HACKING AND EXPLOITATION

V 2.0

Overview: Learn the various attacks like sql injections, cross site scripting, command execution and many advanced web attacks and become an expert in web application penetration testing. This training will enhance your skills to find and exploit vulnerabilities in your client's website fast and give you an inshight to patch those. You will learn to bypass complex filters and web application firewalls and the techniques used by underground hackers to compromise websites.

Description: Beginners Web Hacking and Exploitation is a beginner to intermediate level training where you learn various web attacks like SQLi, XXS, CSRF, File Inclusions etc in detail. You will learn to detect, exploit and mitigate each vulnerability manually and also with automated tools. More of the focus in this training is however given to manual methods so that you can learn what exactly happens when you run a scanner on a website. After this training you will be able to find a vulnerability manually which even a scanner misses and exploit it successfully bypassing various WAF and filters. Also you will learn various techniques useful during the exploitation phase in a pentest such as uploading shell to various popular CMS such as joomla, wordpress, and vbulletin, compromising websites on shared server by symlinks, local root exploits and much more.

Trainers:

Abhishek Sahni has seven years of experience in web application penetration testing. He had reported security vulnerabilities to yahoo and AOL. Abhishek had conducted successful security trainings on various topics for government agencies in India and abroad. He had performed many web application penetration tests and faced really challenging scenarios and found methods to overcome them.

Marco is an expert penetration tester and programmer. As he had performed several penetration tests for clients on complex web applications he has a good knowledge of developing custom reliable tools and exploits according to the requirement during pentests. In free time Marco enjoys coding complex, realistic and interesting web hacking labs for training the ASL IT Security's pentesting team.

Who Should Attend This Training?

Anyone who want to make a carrier in web penetration testing

Penetration testers who want to take their skills to next level

Anyone who wants to learn about web hacking and security

Web developers who want to learn about security issues in codes

Student Prerequisites:

This is a beginner level training so no previous knowledge is required. But knowledge of web programming languages like php, asp and databases is a plus but not required.

Deliverables:

Complete documentation

HD videos

Virtual labs developed by professionals for hands on training

Course Outline:

Module 1-Web Vulnerability Assessment and Penetration testing

1. What is vulnerability Assessment and Penetration Testing
2. Manual VS automated Testing
3. OWASP Top 10
4. Automated Tools
5. Archani
6. Owasp Zap
7. W3AF
8. Comparison of various web security scanners
9. Google Dorks (finding sensitive information)
10. BigDump.php
11. What are DOT NET NUKE and DNN VULNERABILITIES?
12. Google dorks to find DNN
13. Hacking DNN
14. Impact
15. Countermeasures

Module-2 ASL HackMe Labs

1. XAMPP Installation and getting started
2. Setting up ASL Hackme labs

Module-3 Sql injections introduction

1. What are Sql injections?
2. History of Sql Injections
3. Inband and out of band sqli
4. Sql Injection Login Bypass
5. URL based sql injection
6. String type and integer based injections

7. Using UNION SELECT to extract data
8. Using LIMIT to get data
9. INSERT_INTO method
10. Using Double query to inject the database
11. NAME_CONST method
12. UPDATEXML and EXTRACTVALUE method
13. User-Agent based SQL Injections
14. Cookie Based SQL Injectionss
15. Blind SQL Injection
16. Uploading Web Shell using SQL Injection
17. LOAD_FILE with sql injection (reading system files)
18. Web Application Firewall bypass 1
19. Web Application Firewall bypass 2
20. Web Application Firewall bypass 3
21. Web Application Firewall bypass 4
22. More WAF Evasion Methods
23. Mssql and postgres sql injection syntax
24. Complete OS takeover with SQL Injections
25. Impact
26. Automated tools
27. Countermeasures

Module 4-Cross Site Scripting

1. What is Cross Site Scripting?
2. Reflective and persistent XSS
3. Detecting XSS and attacking manually
4. Filter Bypassing
5. User-Agent and Referral based XSS
6. XSS through SQL Injections
7. Useful tools to find and exploit XSS
8. Payloads (cookie stealing, redirection, etc)
9. Session Hijacking
10. XSS frameworks

11. Impact
12. Countermeasures

Module-5 Cross Site Request Forgery

1. Introduction
2. Detection and Attacking
3. Limitations
4. Impact
5. Cross Site History Manipulation (XSHM)
6. Useful tools
7. Countermeasures

Module 6-File Include

1. What is Local File Inclusion
2. Exploiting LFI
3. Uploading webshell through LFI
4. What is Remote File Inclusion
5. Exploiting RFI
6. PHP Wrapper injections exploitations
7. WAF bypassing
8. Impact
9. Useful tools
10. Countermeasures

Module 8-Command Execution

1. Introduction toCommand Execution Flaws

2. System() and shell_exec()
3. Exploiting Command execution vulnerabilities
4. Command Execution through Logs Poisoning
5. Impact
6. Countermeasures

Module 9-Configuration Flaws

1. Full path Disclosure Vulnerabilities
2. Impact
3. Unencrypted logins
4. Impact
5. Countermeasures
6. Header Injections
7. Impact
8. Countermeasures
9. Clickjacking
10. Impact
11. Countermeasures

Module 10-Threats on shared hosting

1. Why shared hosting is a risk
2. Finding sites hosted on same servers
3. Using dorks to find vulnerable sites fast
4. Privilege Escalation Windows
5. Privilege Escalation Linux
6. Back Connecting
7. Finding Exploits
8. Using Local Root Exploits
9. Gaining access to sites on same server using symbolic links
10. Impact
11. Countermeasures