

Cyber Security [Web, Network and Computer]: Basic Lab Practice Manual

By

Venkatesan Subramanian and Sandeep Kumar Shukla

Note: This manual is only for the learners who studied the different web, computer and network security concepts and interested in simulating the attack and mitigation techniques.

Acknowledgement: We referred various web sources to practice. We would like to thank all the authors, web sources and blogs.

Chapter 1 Web Security

1. IFRAME Hack	5
1.1 Message posting between frames	5
1.1 Exploitation.....	6
1.2 Protection Measure: Disable IFRAME	6
2. Enable SSL in Apache	7
3. Restrict Directory Listing.....	9
4. PHPMYADMIN access from remote machine.....	9
5. bash_history Access Control.....	10
6. Always Run Apache with non-privileged account.....	10
7. Remove the server signature [Customize the error].....	10
8. Referrer policy	11
9. Cross Origin Resource Sharing (CORS).....	12
10. Session	13
10.1 Creation.....	13
10.2 Session Fixation Vulnerability.....	13
10.2.1 Solution:	14
10.3 Session Hijacking.....	14
10.4 Plaintext Password in the header	14
10.5 HTTP Auth.....	15
10.6 Cookie based Session.....	16
10.7 Hidden Field.....	16
10.8 Proper logout.....	17

10.9 Password Strength.....	17
10.10 Captcha	18
11. Log Information - Apache.....	19
12. Cross Site Scripting.....	20
12.1 Testing the possibility of Cross Site Scripting.....	20
12.2 Reflected XSS.....	20
12.3 DOM based XSS.....	21
13. File vulnerability	22
13.1 File Injection	22
13.2 SVG File Vulnerability	22
14. Cross Site Request Forgery.....	23
15. Denial of Service – Client Side.....	24
15.1 Infinite Alert.....	24
15.2 Disabling the back button	25
15.3 Fill History	25
15.4 Logout.....	26
16. Reverse Tabnabbing.....	26
17. Upgrade Insecure requests using the following	27
18. Code Injection Attack	27
19. SQL Injection Attack	27
19.1 First order SQL Injection	28
19.2 Second Order SQL Injection.....	29
19.3 OAST Attack	29
19.4 Attention required with MySQL	30
20. Solution for SQLI and other Injections.....	30
20.1 Prepared Statement	30
20.2 Sanitization of the input	32
20.2.1 Use basename function	32
21. Authorization [Access Control]	33
21. 1 Folder Issue and solutions.....	34
21.2 HTACCESS	34
22. XML External Entity (XXE) Injection	36

22.1 Exploit.....	38
23. Preventing Google Link tracking.....	38
24. Robots.txt.....	38
25. Damn Vulnerable Web Application.....	39
26. CURL based login attempt.....	40

Chapter 2 Network Security

1. TCP SYN flooding.....	41
1.1 Other information.....	42
2. UDP echo-charge flooding.....	42
3. Packet Flow control using IP tables.....	43
3.1 On Flow Rate.....	43
3.2 On Packet Count.....	45
4. PING command vulnerabilities.....	46
4.1 Flooding.....	47
4.2 Ping of Death.....	47
4.3 Covert Channel.....	47
4.4 Smurf Attack.....	47
4.5 OS fingerprint.....	48
4.5.1 Solution.....	49
4.6 OS fingerprinting through Other Methods.....	49
4.7 Path Identification.....	50
5. Port Knocking.....	51
6. ARP Cache Poisoning.....	54
6.1 ARP Table.....	54
6.2 Exploit.....	55
6.3 Sniff the Outgoing packets from the victim on Attacker.....	56
6.4 Sniff the incoming packets of the victim.....	56
6.5 Important Note for MITM:.....	57
7. Wireless Penetration Testing.....	57
7.1 Interface.....	58
7.2 Monitor Interface.....	58

7.3 Monitoring	59
7.4 Use of ivstools.....	59
7.5 Password crack.....	59
7.6 Key extraction using IVs	60
7.7 Use of airdecap-ng	61
7.8 Use of airbase-ng.	61
8. MQTT Using mosquitto.....	62
8.1 Run the Subscriber	62
8.2 Run the Publisher	62
8.3 Multiple MQTT broker on same host	63
8.4 Possible Vulnerabilities	63
8.5 Password Authentication	64
8.6 Denial of Service.....	65
9. IPSec using Strongswan.....	65
9.1 Installation.....	66
9.2 Wireshark Interpretation	69
Chapter 1 Computer Security	
1. Reverse Shell	70
2. Stack Overflow Attack.....	72
3. Format String Attack.....	74

Chapter 1 Web Security
