

# **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 .....	12
9. Cross Origin Resource Sharing (CORS).....	13
10. Session .....	13
10.1 Creation.....	13
10.2 Session Fixation Vulnerability.....	14
10.2.1 Solution: .....	14
10.3 Session Hijacking.....	14
10.4 Plaintext Password in the header .....	15
10.5 HTTP Auth.....	15
10.6 Cookie based Session.....	16
10.7 Hidden Field.....	17
10.8 Proper logout.....	17

10.9 Password Strength.....	18
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.....	22
13. File vulnerability .....	22
13.1 File Injection .....	22
13.2 SVG File Vulnerability .....	23
14. Cross Site Request Forgery.....	23
15. Denial of Service – Client Side.....	25
15.1 Infinite Alert.....	25
15.2 Disabling the back button .....	25
15.3 Fill History .....	26
15.4 Logout.....	26
16. Reverse Tabnabbing.....	26
17. Upgrade Insecure requests using the following .....	27
18. Code Injection Attack .....	28
19. SQL Injection Attack .....	28
19.1 First order SQL Injection .....	28
19.2 Second Order SQL Injection.....	29
19.3 OAST Attack .....	30
19.4 Attention required with MySQL .....	31
20. Solution for SQLI and other Injections.....	31
20.1 Prepared Statement .....	31
20.2 Sanitization of the input .....	33
20.2.1 Use basename function .....	33
21. Authorization [Access Control] .....	34
21. 1 Folder Issue and solutions.....	35
21.2 HTACCESS .....	35
22. XML External Entity (XXE) Injection .....	37

22.1 Exploit.....	39
23. Preventing Google Link tracking.....	39
24. Robots.txt.....	39
25. Damn Vulnerable Web Application.....	40
26. CURL based login attempt.....	41
27. Clipboard Data stealing.....	41
28. CRLF Injection .....	43

## Chapter 2 Network Security

1. TCP SYN flooding.....	45
1.1 Other information.....	46
2. UDP echo-charge flooding.....	46
3. Packet Flow control using IP tables .....	47
3.1 On Flow Rate .....	47
3.2 On Packet Count .....	49
4. PING command vulnerabilities.....	50
4.1 Flooding.....	51
4.2 Ping of Death .....	51
4.3 Covert Channel .....	51
4.4 Smurf Attack.....	51
4.5 OS fingerprint .....	52
4.5.1 Solution.....	53
4.6 OS fingerprinting through Other Methods.....	53
4.7 Path Identification.....	54
5. Port Knocking .....	55
6. ARP Cache Poisoning.....	58
6.1 ARP Table .....	58
6.2 Exploit.....	59
6.3 Sniff the Outgoing packets from the victim on Attacker .....	60
6.4 Sniff the incoming packets of the victim .....	60
6.5 Important Note for MITM: .....	61
7. Wireless Penetration Testing .....	61

7.1 Interface .....	62
7.2 Monitor Interface .....	62
7.3 Monitoring .....	63
7.4 Use of ivstools.....	63
7.5 Password crack.....	63
7.6 Key extraction using IVs .....	64
7.7 Use of airdecap-ng .....	65
7.8 Use of airbase-ng. ....	65
8. MQTT Using mosquitto.....	66
8.1 Run the Subscriber .....	66
8.2 Run the Publisher .....	66
8.3 Multiple MQTT broker on same host .....	67
8.4 Possible Vulnerabilities .....	67
8.5 Password Authentication .....	68
8.6 Denial of Service.....	69
9. IPSec using Strongswan.....	69
9.1 Installation.....	70
9.2 Wireshark Interpretation .....	73
 <b>Chapter 3 Computer Security</b>	
1. Reverse Shell .....	75
2. Stack Overflow Attack.....	76
3. Format String Attack.....	78