

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. TLS Version Restriction	9
4. Restrict Directory Listing.....	9
5. PHPMYADMIN access from remote machine.....	10
6. Bash_history Access Control	10
7. Always Run Apache with non-privileged account.....	11
8. Remove the server signature [Customize the error].....	11
9. Referrer policy	12
10. Cross Origin Resource Sharing (CORS).....	13
10.1 CORS Example with Access-Control-Allow-Origin header	14
11. Session	15
11.1 Creation.....	15
11.2 Session Fixation Vulnerability.....	15
11.2.1 Solution:	16
11.3 Session Hijacking.....	16
11.4 Plaintext Password in the header	16
11.5 HTTP Auth.....	17
11.6 Cookie based Session.....	18

11.7	Hidden Field.....	19
11.8	Proper logout.....	19
11.9	Password Strength.....	20
11.10	Captcha	20
12.	Log Information - Apache.....	21
13.	Cross Site Scripting.....	22
13.1	Testing the possibility of Cross Site Scripting.....	22
13.2	Reflected XSS.....	22
13.3	DOM based XSS.....	23
14.	File vulnerability	24
14.1	File Injection	24
14.2	SVG File Vulnerability	25
15.	Cross Site Request Forgery.....	25
16.	Denial of Service – Client Side.....	29
16.1	Infinite Alert.....	29
16.2	Disabling the back button	30
16.3	Fill History	30
16.4	Logout.....	31
17.	Reverse Tabnabbing.....	31
18.	Upgrade Insecure requests using the following.....	32
19.	Code Injection Attack	33
20.	SQL Injection Attack	33
20.1	First order SQL Injection	33
20.2	Second Order SQL Injection.....	35
20.3	OAST Attack	35
20.4	Attention required with MySQL	36
21.	Solution for SQLI and other Injections.....	36
21.1	Prepared Statement	36
21.2	Sanitization of the input	38
21.2.1	Use basename function	38
22.	Authorization [Access Control]: Insecure Direct Object References	39
22.1	Folder Issue and solutions.....	40

22.2	HTACCESS	40
23.	XML External Entity (XXE) Injection	42
23.1	Exploit.....	44
24.	Preventing Google Link tracking.....	44
25.	Robots.txt.....	44
26.	Damn Vulnerable Web Application.....	45
27.	CURL based login attempt.....	46
28.	Clipboard Data stealing.....	46
29.	CRLF Injection	48
30.	Local File Includes and Remote Code Execution	50

Chapter 2 Network Security

1.	TCP SYN flooding.....	51
1.1	Other information.....	53
2.	SCTP Simulation	53
3.	UDP echo-charge flooding.....	54
4.	Packet Flow control using IP tables	55
4.1	On Flow Rate	55
4.2	On Packet Count	58
5.	PING command vulnerabilities.....	59
5.1	Flooding	59
5.2	Ping of Death	60
5.3	Covert Channel	60
5.4	Smurf Attack.....	60
5.5	OS fingerprint	61
5.5.1	Solution.....	62
5.6	OS fingerprinting through Other Methods.....	62
5.7	Path Identification	63
6.	Port Knocking	64
7.	ARP Cache Poisoning.....	67
7.1	ARP Table	67
7.2	Exploit.....	68

7.3 Sniff the Outgoing packets from the victim on Attacker	69
7.4 Sniff the incoming packets of the victim	69
7.5 Important Note for MITM:	70
8. Wireless Penetration Testing	70
8.1 Interface	70
8.2 Monitor Interface	71
8.3 Monitoring	72
8.4 Use of ivstools.....	72
8.5 Password crack.....	72
8.6 Key extraction using IVs	73
8.7 Use of airdecap-ng	74
8.8 Use of airbase-ng.	74
9. MQTT Using mosquito.....	75
9.1 Run the Subscriber	75
9.2 Run the Publisher	75
9.3 Multiple MQTT broker on same host	76
9.4 Possible Vulnerabilities	76
9.5 Password Authentication	77
9.6 Denial of Service.....	77
10. IPSec using Strongswan.....	78
10.1 Installation.....	79
10.2 Wireshark Interpretation	81
11. DNSSEC	83
 Chapter 2 Computer Security	
1. Reverse Shell	84
2. Stack Overflow Attack.....	85
3. Format String Attack.....	87