ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/382183250

Cyber Security & Ethical Hacking

Book · June 2024

CITATIONS
3

READS
12,063

1 author:

Mohammad Shakhawat Khan
Bangladesh University of Engineering and Technology

3 PUBLICATIONS **3** CITATIONS

SEE PROFILE

All content following this page was uploaded by Mohammad Shakhawat Khan on 16 December 2024.

The user has requested enhancement of the downloaded file.

Cyber Security & Ethical Hacking

By

Mohammad Shakhawat Khan

User ID - shakhawatkhan79

A thesis submitted in partial fulfillment of the requirements for the course of

Cyber Security & Ethical Hacking

AWS

Arena Web Security

NEW WINDOW OF WORLD WIDE WEB

Arena Web Security, Dhaka, Bangladesh
June, 2024

Declaration

I, Mohammad Shakhawat Khan currently a final year Bachelor student of Naval Architecture and Marine Engineering in Bangladesh University of Engineering and Technology, do hereby declare that the study presented in this paper titled **“Cyber Security and Ethical Hacking”** is my original work.

I have appropriately acknowledged and referred to all external sources of information and ideas in the text, and included them in the bibliography. I verify that this paper is not submitted to other university, institute and any diploma or internship program for any award, degree or qualification.

I have obtained the necessary permissions and approvals for the use of copyrighted materials, data, or other resources referenced in this thesis. I take full responsibility for the accuracy, integrity, and ethical conduct of this thesis and affirm my commitment to upholding academic honesty and integrity standards.

Signature of the Candidate

Mohammad Shakhawat Khan
User ID: shakhawatkhan79
Date:

Certificate of Thesis

This is to make sure that Mohammad Shakhawat Khan completed effectively the thesis titled "Cyber Security and Ethical Hacking" under my supervision as a supervisee at Arena Web Security. The thesis was conducted in partial fulfillment of the requirements for the course of Cyber Security & Ethical Hacking. The thesis was produced and the study was conducted with praiseworthy dedication, diligence, and academic discipline by **Mohammad Shakhawat Khan** during the course of this thesis. His thesis endeavors exemplified a high standard of academic excellence and provided valuable insights to the discipline of cyber security.

A comprehensive understanding of the subject matter is demonstrated by the thesis, This thesis represents an original contribution to knowledge. The thesis presents a comprehensive and scholarly approach to addressing the thesis objectives through the thesis methodologies, analyses, and conclusions.

I hereby confirm that Mohammad Shakhawat Khan has satisfactorily defended the thesis before the examination committee and has fulfilled the requirements for the completion of cyber security & ethical hacking at arena web security.

.

Supervisor

Tanjim Al Fahim

Chief Executive Officer (CEO)

Arena Web Security

Dhaka, Bangladesh

Dedicated To-

My Beloved Parents
&
Respected Teachers

Acknowledgement

I would like to express my profound gratitude to my thesis supervisor **Tanjim Al Fahim**, Chief Executive Officer of Arena Web Secuity, for giving me the opportunity to work on it. Without his continuous support, ideas, guidelines and encouragements this challenging work would not have been possible to be completed successfully.

I want to thank **Md Ashif Islam**, Faculty of Arena Web Security for teaching me the topics related to the course very elaborately.

I am also thankful to **Romaan Moonshi**, **Bijoy Chandra Mondal**, **Syed Sakib Alam Mubin** to support the whole journey of this course with their excellent technical support and advices.
I would like to thank all others who are directly or indirectly related to this thesis by sharing their ideas, suggestions and thus supporting us. Finally, I am grateful to my parents and other family members for their constant encouragement and support.

Mohammad Shakhawat Khan

User ID-shakhawatkhan79

Abstract

This thesis focuses on the fields of cybersecurity and ethical hacking, examining different methods, tools, and platforms used to protect digital assets and detect weaknesses. The study starts by providing an overview of ethical hacking and the fundamentals of SQL injection. It then covers various topics including OSINT techniques for monitoring specific individuals, DOS and DDOS attacks, session hijacking, both automatic and manual SQL injection methods, and methods for bypassing Web Application Firewalls (WAF) using error-based and post-based techniques. In addition, it explores the deployment of webshells, the uploading of shells, and the consequences of Bad USB and keyloggers. In addition, the thesis investigates LFI (Local File Inclusion), RFI (Remote File Inclusion), and RCE (Remote Code Execution) vulnerabilities, as well as CSRF (Cross-Site Request Forgery), XSS (Cross-Site Scripting), and social engineering assaults. Additionally, it offers valuable knowledge on effectively employing tools such as Burp Suite for doing web application security testing and resolving challenges presented in PortSwigger laboratories. Additionally, it examines the application of Kali Linux for ethical hacking and utilizes Nmap for doing port scanning, including FIN, XMAS, TCP, and UDP scans. Finally, it examines the methodology, tools, and vulnerabilities involved in website penetration testing. It also investigates the practice of outsourcing security testing through sites such as Fiverr, HackerOne, and Bugcrowd. This thesis intends to get a thorough comprehension of cybersecurity and ethical hacking techniques, tools, and platforms by conducting a detailed analysis of these subjects. The ultimate goal is to enable the creation of efficient strategies for safeguarding digital assets and reducing the impact of cyber attacks.

Table of Contents

DECLARATION ... I

CERTIFICATE OF THESIS ... II

ACKNOWLEDGEMENT ... IV

ABSTRACT ... V

TABLE OF CONTENTS ... VI

TABLE OF FIGURES ... IX

NOMENCLATURE ... XII

ACRONYMS ... XII

CHAPTER 1: ETHICAL HACKING & BASIC SQL INJECTION ... 1

1.1 EXPLORING ETHICAL HACKING: OPPORTUNITIES, IMPORTANCE, AND CAREER PATHS ... 1
1.2 BASIC SQL INJECTION ... 1

CHAPTER 2: OSINT ... 4

2.1 OSINT AND LIVE PROJECT ... 4
2.2 TRACKING OF A TARGET PERSON ... 5

CHAPTER 3: DOS, DDOS, LIVE DDOS & SESSION HIJACKING ... 6

3.1 DOS & DDOS ... 6
3.2 LIVE DDOS ATTACK ... 6
3.3 SESSION HIJACKING ... 7

CHAPTER 4: AUTOMATIC AND MANUAL SQL INJECTION ... 9

4.1 AUTOMATIC SQLI BY HAVIJ ... 9
4.2 MANUAL SQLI ... 11

CHAPTER 5: WAF BYPASS SQL INJECTION (ERROR BASED & X-PATH BASED) ... 13

5.1 WAF BYPASS SQL INJECTION ... 13
5.2 ERROR BASED SQL INJECTION ... 15
5.3 X-PATH BASED SQL INJECTION ... 16

CHAPTER 6: WEBSHELL ... 17

6.1 WEBSHELL ... 17
6.2 SHELL UPLOAD ... 17

CHAPTER 7: BAD USB & SKEYLOGGER ... 18

7.1 KEYLOGGER ... 18
7.2 RASPBERRY PI PICO ... 18
7.3 WIFI DUCKY ... 18
7.4 FLIPPERZERO ... 18
7.4 SKEYLOGGER ... 19

CHAPTER 8: LFI/RFI/RCE ... 20

8.1 LFI ... 20
8.2 RFI ... 21

CHAPTER 9: CSRF & XSS ... 22

9.1 Cross Site Request Forgery (CSRF) 22
9.2 Cross Site Scripting (XSS) 24

CHAPTER 10: BURP SUITE 26

10.1 Burp Suite 26

CHAPTER 11: PORTSWIGGER LAB SOLVE 28

11.1 Portswigger CSRF Lab Solve 28

CHAPTER 12: KALI LINUX 29

12.1 Kali Linux 29

CHAPTER 13: NMAP, FIX SCAN, TCP SCAN, UDP SCAN 33

13.1 NMAP 33
13.2 FIN Scan 35
13.3 XMAS Scan 36
13.4 TCP Scan 38
13.5 UDP Scan 39

CHAPTER 14: WEBSITE PENETRATION TESTING & VULNERABILITIES 40

14.1 Website Penetration Testing 40
14.2 Website Penetration Testing Tool 41
14.3 Vulnerabilities 42

CHAPTER 15: FIVERR 44

15.1 Fiverr 44

CHAPTER 16: HACKERONE & BUGCROUD 45

16.1 Outsourcing in Hackerone & Bugcroud 45

APPENDIX A: 46

A.1.1 Basic SQL Injection 46
A.2.1 Tracking of a Target Person 47
A.3.1 Live DDOS Attack 49
A.3.2 Session Hijacking 51
A.4.1 Automatic SQLI by Havij 53
A.4.2 Manual SQL Injection 55
A.5.1 WAF Bypass SQL Injection 59
A.5.2 Error Based SQL Injection 63
A.5.3 X-Path Based SQL Injection 67
A.6.1 Shell Upload 71
A.7.1 Skeylogger in Kali Linux 74
A.8.1 LFI 76
A.9.1 Cross Site Request Forgery 78
A.9.2 Cross Site Scripting 82
A.10.1 BURP Suite 83
A.11.1 Portswigger Lab Solve 87
A.12.1 Kali Linux 91
A.13.1 NMAP Scan 93
A.13.2 FIN Scan 98
A.13.3 XMAS Scan 98
A.13.4 TCP Scan 99
A.13.5 UDP Scan 99

A.14.1 ACUNETIX..100

Table of Figures

FIGURE 1.2.1 : LOGIN INTERFACE OF BASIC SQL VULNERABLE SITE. 3
FIGURE 1.2.2 : ADMIN PANEL ACCESS TAKEN BY BASIC SQL INJECTION. 3
FIGURE 2.1.1 : THE FAMILY PICTURE OF NAZIBUL ISLAM EXTRACTED USING OSINT. 4
FIGURE 2.2.1 : TRACKING DETAILS OF A TARGET PERSON WITH GPS LOCATION. 5
FIGURE 3.2.1 : LIVE DDOS ATTACK. 6
FIGURE 3.3.1 : ADMIN PAGE FINDING USING LINK. 8
FIGURE 3.3.2 : ADMIN PANEL ACCESS BY NO REDIRECT. 8
FIGURE 4.1.1 : ADMIN USERNAME AND PASSWD EXTRACTED USING HAVIJ. 10
FIGURE 4.2.2 : ADMIN ID AND PASSWORD IS EXTRACTED BY MANUAL INJECTION. 11
FIGURE 5.1.1 : WEB APPLICATION FIREWALL. 13
FIGURE 5.1.2 : USER ID AND PASSWORD EXTRACTED OF TARGET WEBSITE BY WAF BYPASS SQL INJECTION. 14
FIGURE 5.2.1 : DATA DUMP USING ERROR BASED SQL INJECTION. 15
FIGURE 5.3.1 : DATA DUMP USING X-PATH BASED SQL INJECTION. 16
FIGURE 6.2.1 : SHELL UPLOAD SUCCESSFUL. 17
FIGURE 7.4.1: SKEYLOGGER RECORD OF ALL THE KEY PRESSED AFTER INSTALLATION. 19
FIGURE 8.1.1 : LFI PAYLOAD TO A TARGET SITE 20
FIGURE 9.1.1 : CROSS SITE REQUEST FORGERY ATTACK 22
FIGURE 9.1.2 : SCRIPT IS CONVERTED TO URL AND DELIVERED FOR CSRF ATTACK EXECUTED SUCCESSFULLY. 23
FIGURE 9.2.1 : XSS ATTACK SUCCESSFUL EXECUTION ON TARGET SITE. 25
FIGURE 10.1.1 : INTERMEDIATE REQUEST TO GET IN TO A SERVER. 26
FIGURE 10.1 2: DIFFERENT USER ID AND PASSWORD PAYLOAD TEST USING BURP SUITE INTRUDER ATTACK. 27
FIGURE 11.1.1 : PORTSWIGGER CSRF LIVE LAB SOLVE 28
FIGURE 12.1.3 : ADMIN PANEL EXTRACTION USING FFUF IN KALI LINUX. 32
FIGURE 13.1.1 : NMAP SCAN. 34
FIGURE 13.1.2 : NMAP EXPLOIT DETECTION. 34
FIGURE 13.2.1 : NMAP FIN SCAN. 35
FIGURE 13.3.1 : NMAP XMAS SCAN. 37
FIGURE 13.4.1 : TCP SCAN. 38
FIGURE 13.5.1 : UDP SCAN. 39
FIGURE 14.3.1 : DIFFERENT TYPES OF VULNERABILITIES USING ACUNETIX. 43
FIGURE A.1.1.1 : TAKEN ACCESS OF A SITE BY BASIC SQL INJECTION. 46
FIGURE A.2.1.1 : CUSTOM URL CREATION BY GRABIFY. 47
FIGURE A.2.1.2 : CUSTOM URL CREATED BY GRABIFY. 47
FIGURE A.2.1.3 : TRACKING DETAILS OF A TARGET PERSON USING IP ADDRESS TRACKER. 48
FIGURE A.3.1.1 : HOIC SOFTWARE INTERFACE AND TARGET URL SETUP. 49
FIGURE A.3.1.2 : SETTING UP THE NUMBER OF THREADS FOR DDOS ATTACK. 49
FIGURE A.3.1.3 : DDOS ATTACK USING HOIC. 50
FIGURE A.3.2.1 : REDIRECT TO LOGIN PAGE INTERFACE 51
FIGURE A.3.2.2 : BLOCKING OF REDIRECT URL. 51
FIGURE A.3.2.3 : ADMIN PANEL ACCESS BY NO REDIRECT. 52
FIGURE A.4.1.1 : TARGET URL ADDED TO HAVIJ. 53
FIGURE A.4.1.2 : THE EXTRACTION OF USERNAME AND PASSWORD FOR THE TARGET WEBSITE. 54
FIGURE A.4.2.1 : SITE INTERFACE IN CYBERFOX BROWSER. 55
FIGURE A.4.2.2 : SITE INTERFACE AFTER POINT INJECTION IN CYBERFOX BROWSER. 55
FIGURE A.4.2.3 : FINDING THE TOTAL NUMBER OF TABLE. (HERE TABLE NUMBER IS 30) 56
FIGURE A.4.2.4 : VULNERABLE TABLE EXTRACTION. 57
FIGURE A.4.2.5 : VULNERABLE TABLE VERSION. 57
FIGURE A.4.2.6 : WEBSITE TABLE EXTRACTION BY DIOS. 58
FIGURE A.4.2.7 : USER ID AND PASSWORD EXTRACTED OF TARGET WEBSITE BY MANUAL SQL INJECTION. 58
FIGURE A.5.1.1 : SITE INTERFACE IN CYBERFOX BROWSER. 59
FIGURE A.5.1.2 : SITE INTERFACE AFTER POINT INJECTION IN CYBERFOX BROWSER. 59

Figure A.5.1.3 : Finding the total number of table. (Here table number is 6) 60
Figure A.5.1.4 : Vulnerable table extraction by WAF bypass.. (Here vulnerable table is 2 60
Figure A.5.1.5 : Website table extraction by WAF DIOS........ 61
Figure A.5.1.6 : User id and password extracted of target website by WAF bypass SQL injection........ 62
Figure A.5.2.1 : Vulnerability test of target site using cyberfox browser. 63
Figure A.5.2.2 : Number of column identification using cyberfox browser........ 64
Figure A.5.2.3 : Changed number of column by changing injection point. 65
Figure A.5.2.4 : Error based command to get the table version. 65
Figure A.5.2.5 : Data dump using error based SQL injection. 66
Figure A.5.3.1 : Vulnerability test of target site using cyberfox browser. 67
Figure A.5.3.2 : Number of column identification using cyberfox browser........ 68
Figure A.5.3.3 : Changed number of column by changing injection point. 69
Figure A.5.3.4 : X-PATH based command to get the table version. 69
Figure A.5.3.5 : Data dump using X-PATH based SQL injection. 70
Figure A.6.1.1 : Target site access by basic SQL injection. 71
Figure A.6.1.2 : An uploader to upload a shell. 71
Figure A.6.1.3 : Upload the shell. 72
Figure A.6.1.4 : Shell Upload Successful. 73
Figure A.7.1.1 : Skeylogger installation in kali linux. 74
Figure A.7.1.2 : Running System interface of kali linux. 75
Figure A.7.1.3 :Closing running System in kali linux. 75
Figure A.8.1.1 : LFI target site interface. 76
Figure A.8.1.2 : LFI payload directed to a php file. 76
Figure A.8.1.3 : LFI payload to a target site. 77
Figure A.9.1.1 : Creating and login to the account........ 78
Figure A.9.1.2 : CSRF token captured by BURP. 78
Figure A.9.1.3 : Generation of CSRF poc. 79
Figure A.9.1.4 : Modification of script using auto submit script. 80
Figure A.9.1.5 : Script is converted to url and delivered for CSRF attack executed successfully........ 81
Figure A.9.2.1 : Target interface for XSS vulnerability. 82
Figure A.9.2.2 : XSS attack successful execution on target site........ 82
Figure A.10.1.1 : BURP suite interface........ 83
Figure A.10.1.2 : BURP suite proxy connected to browser to intercept request. 84
Figure A.10.1.3 : BURP suite request send to intruder for payload attack. 84
Figure A.10.1.4 : BURP suite attack selected for buttering ram........ 85
Figure A.10.1.5 : BURP suite payload collection. 85
Figure A.10.1.6 : BURP suite no redirect selected for payload attack. 86
Figure A.10.1.7 : BURP suite results for successful access taken by payload test. 86
Figure A.11.1.1 : Lab session task by portswigger. 87
Figure A.11.1.2 : Change mail cookie and CSRF token captured by BURP suite. 87
Figure A.11.1.3 : Change POST method to GET method and generation of CSRF poc. 88
Figure A.11.1.3 : Extracted script is delivered exploit to victim. 89
Figure A.11.1.4 : Portswigger CSRF Live Lab Solve. 90
Figure A.12.1.1 : Key-mon, python installed. 91
Figure A.12.1.2: Admin panel extraction by FFUF. 92
Figure A.12.1.3 : Admin panel extraction using FFUF in kali linux. 93
Figure A.13.1.1 : Nmap interface in kali linux. 94
Figure A.13.1.2 : Nmap interface in VPS........ 94
Figure A.13.1.3 : Nmap exploit detection. 95
Figure A.13.1.4 : Nmap port scan. 96
Figure A.13.1.5 : Nmap top port scan. 97
Figure A.13.2.1 : Nmap FIN scan. 98
Figure A.13.3.1 : Nmap XMAS scan. 98

FIGURE A.13.4.1 : TCP SCAN. 99
FIGURE A.13.5.1 : UDP SCAN. 99
FIGURE A.14.1.1 : TARGET SITE SETUP AND FULL SCAN SELECTION. 100
FIGURE A.14.1.2 : DIFFERENT TYPES OF VULNERABILITYREPORT USING ACUNETIX. 102

Nomenclature

Acronyms

Symbol	Description
SQL	Structured Query Language
URL	Uniform Resource Locator
OSINT	Open Source Intelligence
IP	Internet Protocol
GPS	General Positioning System
DOS	Denial of Service
DDOS	Distributed Denial of Service
HOIC	High Orbit Ion Canon
DBMS	Database Management System
WAF	Web Application Firewall
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
ISP	Internet Service Provider
USB	Universal Serial Bus
LFI	Local File Inclusion
CSRF	Cross Site Request Forgery
XSS	Cross Site Scripting
POC	Proof of Concept
IOS	Iphone Operating System
FFUF	Fuzz Faster U Fool
UDP	User Datagram Protocol
TCP	Transmission Control Protocol

Symbol	Description
VPS	Virtual Private Server

For Full Access Contact
Thank You

View publication stats