

ABSTRACT

Content Management Systems are mostly used for website development. Websites are the main targets of various malicious attackers, and therefore it is necessary to be knowledgeable about the security level of websites. This will describe some features of the well-known open source Content Management System platforms: Drupal, WordPress and Joomla. The security of such web applications depends as much on vulnerabilities found in plugins as it does in vulnerabilities in the application core. One of the biggest problems facing the IT security industry is the use of vulnerabilities in legitimate software to launch malware attacks. Malicious programs can use these vulnerabilities to infect a Content of Websites without attracting the attention of the user and in some cases, without triggering an alert from security software. The cyber-attacks, or more specifically denial of service attacks, were launched by the Cyber fighters of Izz Ad-Din Al Qassam also known as Qassam Cyber Fighters. Operation Ababil was one of a series of cyber-attacks starting in 2012, targeting various American financial institutions and carried out by a group of Izz Ad-Din Al Qassam.

LIST OF FIGURES

Fig. No.	Name of Figure	Page No.
1.	Vulnerabilities by types	3
2.	Malicious Sites	5
3.	Architecture Diagram	13
4.	Use case diagram	14
5.	Class Diagram	15
6.	Activity Diagram	16
7.	Sequence Diagram	17
8.	Data flow diagram	18
9.	CMS Hacking Probabilities	22
10.	Admin access	23
11.	LOIC Attack	25
12.	Nmap TCP Port Scanning	30
13.	Nmap all port Scanning	31
14.	Nmap 3-way Handshake	32
15.	Wireshark IP search	34
16.	Wireshark http request	35
17.	Wireshark Packet Capturing	36
18.	HOIC Packet Capturing	37
19.	Wireshark TCP Attack	37
20.	Wireshark 3-way handshake	39
21.	Wireshark TCP stream analysis	40

22.	Wireshark Display Filter	40
23.	DVWA Command Injection	46
24.	DVWA CSRF	47
25.	SQL Injection	48
26.	DVWA XSS	49
27.	DVWA File upload	50
28.	Drupal website main	57
29.	Drupal Login	57
30.	Drupal Dashboard	58
31.	Drupal Configuration	58
32.	HOIC Attack	59
33.	DVWA Login	59
34.	DVWA Dashboard	60
35.	SQL injection attack	60

LIST OF TABLES

TABLE NO.	NAME OF TABLE	PAGE NO.
1.	Software requirement	10
2.	Hardware requirement	10
3.	Documentation	11
4.	Total Vulnerabilities by year	20
5.	Total Vulnerabilities by CMS	21
6.	Operating System Vulnerabilities	21

LIST OF ABBREVIATIONS

ACRONYM	ABBREVIATION
IEEE	Institute of Electrical and Electronics Engineers
CMS	Content Management System
GPL	General Public Licence
PHP	Hypertext Pre-Processor
XSS	Cross-Site Scripting
CSRF	Cross-Site Request Forgery
SQL	Structured Query Language
UML	Unified Modelling Language
OWASP	Open Web Application Security Project
DOS	denial of service
NMAP	Network Mapper
DDOS	Distributed Denial of Service Attack
LOIC	Low Orbit Ion Canon
HOIC	High Orbit Ion Canon
HTTP	Hyper-Text Transfer Protocol
DVWA	Damn Vulnerable Web App

INDEX

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	VIII
	LIST OF FIGURES	IX
	LIST OF TABLES	X
	LIST OF ABBREVIATIONS	XI
1.	INTRODUCTION	
	1.1.OVERVIEW OF THE PROJECT	01
	1.2.VULNERABILITIES	03
	1.3.PROBLEM STSTATEMENT	03
	1.4.TYPES OF CMS	04
	1.5.SECURITY ISSUES	05
2.	SYSTEM ANALYSIS	
	2.1. EXISING SYSTEM	06
	2.1.1 DISADVANTAGES	06
	2.2. PURPOSED SYSTEM	07
	2.2.1 ADVANTAGES	07
3.	FEASIBILITY STUDY	
	3.1. TECHNICAL EASIBILITY	08
	3.2. ECONOMICAL FEASIBILITY	08
	3.3. OPERATIONAL FESIBILITY	09
4.	REQUIREMENT ANALYSIS	
	4.1. SOFTWARE REQUIREMENTS	10

	4.2. HARDWARE REQUIREMENTS	10
	4.3. DOCUMENTATION	11
5.	SYSTEM DESIGN	
	5.1. ARCHITECTURE DIAGRAM	13
	5.2. USE CASE DIAGRAM	14
	5.3. CLASS DIAGRAM	15
	5.4. ACTIVITY DIAGRAM	16
	5.5. SEQUENCE DIAGRAM	17
	5.6. DATA FLOW DIAGRAM	18
6.	FUNCTIONAL MODULES	
	6.1. SYSTEM MODEL	19
	6.2. SYSTEM MODULES	20
	6.2.1. VULNERABILITIES	20
	6.2.1.1. DATABASE VULNERABILITIES	20
	6.2.1.2. WEB SERVER VULNERABILITIES	21
	6.2.1.3. SERVER VULNERABILITIES	21
	6.2.1.4. CMS VULNERABILITIES	22
	6.2.2. ADMIN ACCESS	22
	6.2.3. DOS ATTACK	23
	6.2.4. SQL INJECTION ATTACK	24
	6.2.5. ANALYZE NETWORK	24
	6.2.6. NETWORK SCANNING	24
7.	IMPLEMENTATION	
	7.1. DDOS ATTACK	25

	7.1.1. ATTACK CONFIGURATION	26
	7.2. NMAP	28
	7.3. FILTERING PACKETS	33
	7.4. SQL INJECTION	41
8.	SYSTEM TESTING	
	8.1. GENERAL	44
	8.2. PENETRATION TESTING	45
	8.2.1. COMMAND INJECTION	45
	8.2.2. CSRF	46
	8.2.3. SQL INJECTION ATTACK	47
	8.2.4. XSS	48
	8.2.5. UPLOAD	49
9.	CODING	51
10.	SECURING CMS	55
11.	CONCLUSION	56
	APPENDICES	57
	REFERENCES	61