JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Mitigating Distributed Denial of Service Attacks For Web Security

R.Thenmalar
Assistant Professor
Dept of Computer Science & Engineering
RVS College of Engineering & Technology,
Coimbatore, India.
thenmalarcbe@gmail.com

M.Harini
712821104018
Dept of Computer Science & Engineering
RVS College of Engineering & Technology,
Coimbatore, India.
mmharini21@gmail.com

M.Gokul
712821104013
Dept of Computer Science & Engineering
RVS College of Engineering & Technology,
Coimbatore, India.
Sachingokul009@gmail.com

K.K.Amaldas
712821104004
Dept of Computer Science & Engineering
RVS College of Engineering & Technology,
Coimbatore, India. das171018@gmail.com

A.Ajith
712821104003
Dept of Computer Science & Engineering
RVS College of Engineering & Technology,
Coimbatore, India.
ajithajith23744ak@gmail.com

Abstract-- WordPress is one of the most widely used content management systems (CMS), powering over 172 million websites, including e- commerce, personal blogs, news platforms, and online magazines. Due to its popularity, WordPress websites frequently become targets for cyberattacks, particularly Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. A common vulnerability, user enumeration, allows attackers to identify valid usernames, which facilitates brute force attacks and account takeovers. This paper focuses on analyzing security loopholes in WordPress websites and provides mitigation strategies for preventing DDoS and DoS attacks. Through controlled testing environments using SSH scripts, Python, and CGI scripts, we examined over 100 WordPress- powered websites, including three locally hosted instances. The findings highlight the importance of proactive security measures, including firewall configurations, user authentication hardening, and resource management, to mitigate attacks and ensure website availability.

Index Terms-- WordPress Security, Content Management System (CMS), Denial of Service (DoS), Distributed Denial of Service (DDoS), Cybersecurity, User Enumeration, Brute Force Attacks,

Account Takeover, Firewall Configurations, Authentication Hardening, Resource Management, Web Security.

1. Introduction

With over 3.2 billion users globally, the Internet has become an essential tool for communication, commerce, and governance. WordPress, powering nearly 30% of all websites, has emerged as a major target for cybercriminals. Attackers exploit vulnerabilities in WordPress plugins, outdated themes, and weak authentication mechanisms to compromise websites and launch DDoS attacks, disrupting services and causing financial loss. Common vulnerabilities affecting WordPress sites include: SQL Injection (SQLi) , Cross-Site Scripting (XSS), Broken Authentication & User Enumeration, Denial of Service (DoS) & DDoS Attacks, Security Misconfigurations & Outdated Plugins.

This study investigates the root causes of these vulnerabilities and implements mitigation strategies through penetration testing and defensive measures such as traffic filtering, IP blocking, and server resource optimization.

2. RELATED WORKS

1. Zargar, Joshi & Tipper (2013) – Reviewed various defense mechanisms against DDoS flooding attacks and classified mitigation strategies based on their effectiveness.

2. Wang, Zhang & Shin (2007) – Proposed a change-point monitoring method to detect DoS attacks in real time.

3. Singh & Patel (2021) – Focused on enhancing WordPress security by strengthening authentication mechanisms and securing plugins.

4. Johnson & Kumar (2019) – Analyzed traffic filtering techniques to differentiate between legitimate and malicious traffic.

5. Lee & Kim (2022) – Conducted a comparative analysis of cloud-based and edge computing solutions for DDoS mitigation.

3. THE PROPOSED CONSTRUCTION

The proposed solution involves identifying vulnerabilities, simulating attacks, and implementing mitigation techniques for WordPress-powered websites.

The approach includes the following phases:

3.1 Identification of Vulnerabilities:

1. Scanning WordPress plugins, themes, and core components for security flaws.
2. Utilizing tools like WPScan, Python scripts, and SSH-based penetration testing to detect weaknesses.
3. Conducting brute-force simulations to evaluate the impact of user enumeration attacks.

3.2 Attack Simulation and Traffic Analysis:

1. Deploying botnets and SSH scripts to launch simulated DDoS and DoS attacks on controlled test environments.

Figure 1.Simulation of DDoS

2. Monitoring network traffic using Wireshark and Snort to analyze attack patterns.

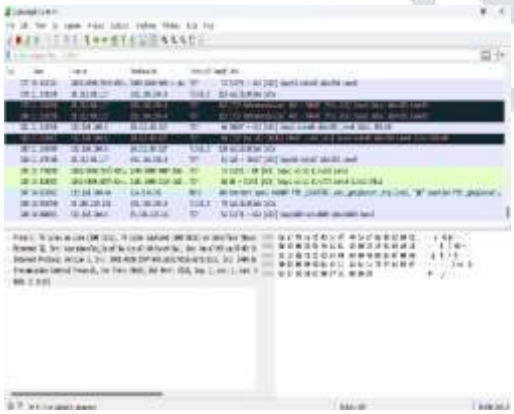

Figure 2.Traffic analysis

3. Evaluating the impact of resource exhaustion attacks on server availability.

3.3 Mitigation Strategies Implementation:

1. Traffic Filtering: Differentiating between normal and malicious traffic using rate-limiting and anomaly detection.

2. IP Blocking & Rate Limiting: Preventing excessive requests from a single source to avoid brute-force login attempts.

3. Firewalls & Access Control: Configuring Web Application Firewalls (WAFs) to block suspicious requests.

4. Strengthening Authentication: Implementing multi-factor authentication (MFA) and disabling user enumeration.

5. Content Delivery Networks (CDNs): Distributing traffic to prevent server overload.

Figure 3. Content Delivery networks

3.4 Performance Analysis & Validation:

1. Testing server response times, resource utilization, and attack resistance under different mitigation strategies.

2. Analyzing the effectiveness of firewalls, CDN configurations, and IP filtering against DDoS threats.

4. SYSTEM MODEL

1) **Attack Detection Model:** Uses Intrusion Detection Systems (IDS) and AI-based anomaly detection to identify suspicious traffic.

2) **Traffic Filtering Model:** Implements CAPTCHA verification, rate-limiting, and IP blocking to filter malicious requests.

3) **Cloud-Based Mitigation Model:** Employs cloud services such as AWS Shield and Cloudflare to absorb large-scale DDoS attacks.

4) **Machine Learning-Based Detection Model:** Uses AI to classify and differentiate between legitimate and malicious traffic patterns.

5) **Blockchain-Based Security Model:** Decentralized authentication for preventing unauthorized access.

6) **Load Balancing Model:** Distributes incoming requests across multiple servers to reduce load and prevent crashes.

7) **Edge Computing Model:** Filters traffic at network edge nodes before it reaches **the main web server.**

8) **Honeypot-Based Detection Model:** Uses decoy systems to trap attackers and gather intelligence on their tactics.

5. ACKNOWLEDGMENT

The authors would like to express their gratitude to **Lee & Kim (2022)** for their valuable research on cloud-based and edge computing solutions for DDoS mitigation, which provided significant insights and foundational

knowledge for our study.

6.Predction Table: Impact of DDOS Mitigation Techniques

Technique	Cost Level	Scalability
Rate Limiting	Low	Moderate
Web Application Firewall (WAF)	Medium	High
Ip Blacklisting	Low	Low
Traffic Filtering	Medium	Moderate

7.CONCLUSION

This study provides a comprehensive approach to mitigating DDoS attacks on WordPress-powered servers. By conducting vulnerability assessments, attack simulations, and implementing mitigation strategies, we demonstrate practical techniques for improving website security.

The findings show that: Traffic filtering and rate limiting significantly reduce the attack surface, CDNs and cloud- based security solutions mitigate large- scale DDoS threats Combining AI- based anomaly detection with firewalls enhances proactive defense mechanisms.

Future work will focus on integrating AI-driven threat intelligence and automated security frameworks for real-time attack prevention.

8.REFERENCES

[1] Lee & Kim (2022) – Conducted a comparative analysis of cloud- based and edge computing solutions for DDoS mitigation.

[2] S. K. Sahoo, S. Mohapatra, and S. K. Jena (2020)"A Study on Metasploit Framework: A Pen- Testing Tool".

[3] (2019)"Penetration Testing Using S. S. Sonar and S. S. Upadhyay Metasploit Framework".

[4] Johnson & Kumar (2019) – Analyzed traffic filtering techniques for distinguishing between legitimate and malicious traffic.

[5] Yongbin Zhou, Deyong Chen, and Wei Chen (2004),"Research and Implementation of Remote Desktop Protocol Service Security".