

**Republic of the Philippines**

**Nueva Ecija University of Science and Technology**

**Atate, Palayan City, Nueva Ecija**

**Denial of Service (DoS) Attack on a Major News Website:**

**A Case Study on Vulnerabilities in Web Application Firewalls (WAFS)**

**Submitted by:**

Duque, Owen C.

Valdez, Ladylyn A.

Sumait, Princess L.

Pajarillo, Ruth P.

**Submitted to:**

Mr. Joey P. Dela Cruz

**Abstract:**

This case study investigates vulnerabilities in Web Application Firewalls (WAFs) that may be exploited by attackers to launch Denial of Service (DoS) attacks on major news websites. As the digital landscape continues to evolve, news organizations face increasing threats to the availability and integrity of their online platforms. DoS attacks pose a significant risk to the uninterrupted delivery of news content and undermine the trust and credibility of media sources.

**Introduction:**

The landscape of news consumption has shifted dramatically with the advent of digital platforms, where major news websites play a pivotal role in disseminating timely information to a global audience. However, this digital transformation has also exposed news organizations to a myriad of cyber threats, with Denial of Service (DoS) attacks emerging as a significant concern. Trends indicate a troubling escalation in the frequency, scale, and sophistication of such attacks, driven by the increasing reliance on online platforms for news dissemination and the growing commodification of cyber attack tools and services in underground markets.

Denial of Service (DoS) attacks represent a formidable challenge to the integrity and availability of major news websites, posing a direct threat to the public's access to reliable information. These attacks, which aim to disrupt the normal operation of web servers by overwhelming them with a flood of illegitimate traffic or requests, can have far-reaching consequences, ranging from service outages and data breaches to reputational damage and financial losses. Moreover, the evolving tactics and techniques used by adversaries to launch DoS attacks pose a continuous challenge to the effectiveness of traditional defense mechanisms, necessitating a proactive and adaptive approach to cyber security.

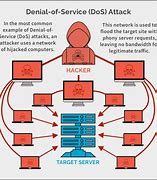
In light of these challenges, this study seeks to address the pressing need for enhanced cyber resilience among major news websites by focusing on vulnerabilities in Web Application Firewalls (WAFs) that may be exploited by attackers to launch DoS attacks. Specifically, the study aims to identify the underlying vulnerabilities in WAF implementations, assess their potential impact on the security posture of news websites, and propose effective mitigation strategies to bolster their defenses against DoS attacks. By achieving these objectives, the study aims to contribute to the broader goal of safeguarding the availability and reliability of online news platforms, thereby upholding the public's right to access accurate and timely information in the digital age.

This study holds significant implications for the fields of cyber security, media studies, and public policy. By shedding light on the vulnerabilities in WAFs that expose major news websites to DoS attacks, the study contributes to the ongoing efforts to strengthen the resilience of critical digital infrastructure against cyber threats. Furthermore, the findings of this research may inform the development of targeted defense strategies, regulatory frameworks, and industry standards aimed at mitigating the risk of DoS attacks on media organizations. Ultimately, by safeguarding the integrity and availability of online news platforms, this study seeks to uphold the fundamental principles of freedom of expression, democratic governance, and information transparency in the digital era.

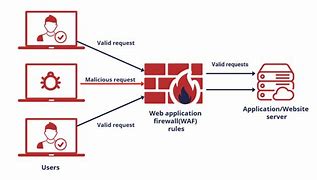
**Background**

The proliferation of digital technologies has revolutionized the way people consume news and information, with major news websites serving as primary sources for a global audience. This shift towards digital platforms has brought unprecedented opportunities for news organizations to reach wider audiences and deliver real-time updates. However, it has also exposed them to a host of cyber threats, including Denial of Service (DoS) attacks, which aim to disrupt the availability of online services by overwhelming web servers with malicious traffic.

**Denial of Service Attack (DoS)**

 DoS attacks have become increasingly prevalent and sophisticated, posing significant challenges to the resilience of major news websites. These attacks can result in service outages, degraded performance, and reputational damage, undermining the credibility and trustworthiness of media outlets. Moreover, the evolving nature of DoS attack techniques, coupled with the widespread availability of attack tools and services, makes it imperative for news organizations to adopt proactive measures to safeguard their digital infrastructure.

**Web Application Firewalls (WAFs)**

 Web Application Firewalls (WAFs) play a critical role in defending against DoS attacks by filtering and monitoring incoming web traffic, detecting and blocking malicious requests, and mitigating the impact of volumetric attacks. However, the effectiveness of WAFs in mitigating DoS

attacks depends on various factors, including the configuration settings, rule sets, and traffic patterns observed in their deployments.

Given the importance of WAFs in protecting major news websites from DoS attacks, there is a need for empirical research to identify vulnerabilities in WAF implementations and assess their impact on cyber resilience. By understanding the underlying causes of these vulnerabilities and proposing effective mitigation strategies, news organizations can enhance their defenses against DoS attacks and ensure the uninterrupted delivery of news content to their audiences.

Against this backdrop, this case study aims to investigate vulnerabilities in WAFs that may be exploited by attackers to launch DoS attacks on major news websites. By examining real-world scenarios, analyzing WAF configurations, and engaging with industry stakeholders, the study seeks to provide actionable insights for strengthening the cyber security posture of news organizations and upholding the availability and integrity of online news platforms.

**Prevention and Mitigation**

Preventing and mitigating Denial of Service (DoS) attacks on major news websites requires a multi-layered approach that combines proactive measures with robust incident response strategies. The following prevention and mitigation techniques can help safeguard against the disruptive effects of DoS attacks:

**Implementing WAF Best Practices:** News websites should adhere to best practices for configuring and managing Web Application Firewalls (WAFs). This includes regularly updating WAF rule sets, enabling rate limiting to prevent excessive traffic, and fine-tuning WAF settings to filter out known attack patterns.

**Distributed Traffic Management:** Deploying content delivery networks (CDNs) and load balancers can help distribute incoming traffic across multiple servers and data centers, reducing the impact of volumetric DoS attacks. By spreading the load and absorbing excess traffic, CDNs and load balancers can enhance the resilience of news websites against DoS attacks.

**Traffic Analysis and Anomaly Detection:** Implementing real-time traffic analysis tools and anomaly detection systems can help identify unusual patterns or spikes in web traffic indicative of DoS attacks. By monitoring traffic behavior and detecting deviations from normal patterns, news websites can proactively respond to potential threats and mitigate their impact.

**Rate Limiting and Request Throttling:** Enforcing rate limiting and request throttling mechanisms can help prevent DoS attacks by limiting the number of requests allowed from individual IP addresses or user agents. By imposing reasonable limits on request rates and enforcing strict access controls, news websites can mitigate the risk of resource exhaustion and service disruption caused by DoS attacks.

**Incident Response Planning:** Developing comprehensive incident response plans that outline roles, responsibilities, and escalation procedures in the event of a DoS attack is essential. News organizations should establish communication channels with stakeholders, including hosting providers, WAF vendors, and law enforcement agencies, to coordinate response efforts and minimize downtime.

**Regular Security Audits and Penetration Testing:** Conducting regular security audits and penetration testing exercises can help identify vulnerabilities in WAF configurations and web application code that may be exploited by attackers. By proactively identifying and remedying security weaknesses, news websites can bolster their defenses against DoS attacks and other cyber threats.

**Collaboration and Information Sharing:** Participating in information sharing and collaboration initiatives within the cyber security community can provide news organizations with valuable insights into emerging threats and effective mitigation strategies. By sharing threat intelligence, incident data, and best practices with peers and industry stakeholders, news websites can collectively enhance their resilience against DoS attacks and other cyber threats.

**Objectives**

The primary objectives of this case study are as follows:

**Identify Vulnerabilities in WAF Implementations:** The study aims to systematically identify vulnerabilities in Web Application Firewalls (WAFs) that may be exploited by attackers to launch Denial of Service (DoS) attacks on major news websites. By conducting a comprehensive assessment of WAF configurations, rule sets, and traffic patterns, the study seeks to pinpoint common weaknesses and misconfigurations that could undermine the effectiveness of WAF defenses.

**Assess Impact on Security Posture:** Once vulnerabilities are identified, the study aims to assess their potential impact on the overall security posture of major news websites. This involves evaluating the severity and exploitability of identified vulnerabilities, as well as their implications for service availability, data integrity, and user confidentiality. By quantifying the risk posed by WAF vulnerabilities, the study aims to provide actionable insights for prioritizing mitigation efforts and strengthening cyber resilience.

**Propose Mitigation Strategies:** Building on the findings of vulnerability assessment, the study aims to propose effective mitigation strategies for enhancing the resilience of WAFs against DoS attacks. These strategies may include recommendations for optimizing WAF configurations, updating rule sets, implementing additional security controls, and enhancing incident response procedures. By offering practical guidance and best practices, the study seeks to empower news organizations to proactively defend against DoS attacks and safeguard the availability of their online platforms.

**Contribute to Cybersecurity Knowledge:** Beyond the specific context of major news websites, the study aims to contribute to broader cybersecurity knowledge by shedding light on vulnerabilities in WAF implementations and their implications for cyber resilience. By sharing insights, lessons learned, and best practices, the study aims to foster a better understanding of the evolving threat landscape and empower organizations across industries to enhance their defenses against DoS attacks and other cyber threats.

Overall, the primary objectives of this case study revolve around identifying vulnerabilities in WAFs, assessing their impact on security posture, proposing mitigation strategies, and contributing to cybersecurity knowledge. By achieving these objectives, the study aims to strengthen the resilience of major news websites against DoS attacks and uphold the availability and integrity of online news platforms.

**Identifying vulnerabilities**

Identifying vulnerabilities in Web Application Firewalls (WAFs) is crucial for effectively mitigating Denial of Service (DoS) attacks on major news websites. Here are some key steps to identify vulnerabilities in WAF implementations:

**Configuration Review:**

Conduct a comprehensive review of the WAF configuration settings to identify potential misconfigurations or weaknesses. This includes examining rulesets, whitelists, blacklists, and security policies configured within the WAF interface. Look for any overly permissive rules, deprecated settings, or unused features that could introduce vulnerabilities or bypasses.

**Rule Set Analysis:**

Evaluate the effectiveness of the WAF rule sets in detecting and blocking malicious traffic. Analyze the coverage and specificity of rules, ensuring they align with the known attack patterns and vulnerabilities relevant to the web application. Look for gaps in rule coverage, false positives, and outdated signatures that may undermine the WAF's ability to detect and mitigate DoS attacks

**Traffic Pattern Monitoring:**

Monitor incoming web traffic patterns to detect anomalies and suspicious behavior indicative of DoS attacks. Use logging and monitoring tools to track key metrics such as request rates, bandwidth utilization, and server response times. Look for sudden spikes or fluctuations in traffic volume, repetitive requests from a single source, or patterns consistent with known DoS attack vectors.

**Security Testing:**

Conduct security testing exercises, such as vulnerability scanning and penetration testing, to identify potential weaknesses in the WAF deployment. Use automated scanning tools to assess the security posture of web applications and WAF configurations, identifying common vulnerabilities such as injection flaws, misconfigurations, and access control issues. Perform manual penetration testing to validate findings and identify complex attack vectors that may evade automated detection.

**Third-Party Audits:**

Engage third-party security experts or auditing firms to perform independent assessments of the WAF deployment. External auditors can provide objective insights into potential vulnerabilities and offer recommendations for enhancing the security posture of the WAF and web applications. Ensure the auditors have expertise in WAF technologies and understand the specific requirements and challenges of news website environments.

**Vendor Advisories and Updates:**

Stay informed about security advisories, patches, and updates released by WAF vendors. Regularly review vendor documentation, release notes, and security bulletins to identify vulnerabilities and recommended mitigations. Promptly apply security patches and updates to address known vulnerabilities and enhance the resilience of the WAF against emerging threats.

**Threat Intelligence Feeds:**

Leverage threat intelligence feeds and security information sharing platforms to gain insights into emerging threats and attack techniques targeting WAFs. Subscribe to reputable threat intelligence sources that provide real-time updates on DoS attacks, exploit kits, and malware campaigns. Use threat intelligence feeds to proactively adjust WAF configurations and implement targeted countermeasures against known threats.

**Successful attacks can indeed have severe consequences for major news websites, impacting both the organization and its audience in various ways:**

**Disruption of Service:** The primary goal of Denial of Service (DoS) attacks is to disrupt the normal operation of web servers, rendering them inaccessible to legitimate users. Successful attacks can lead to prolonged service outages, preventing audiences from accessing news content and updates. This disruption not only affects the user experience but also damages the reputation and credibility of the news website, potentially driving away visitors and subscribers.

**Loss of Revenue:** Major news websites often rely on advertising revenue, subscriptions, and e-commerce transactions to sustain their operations. A successful DoS attack can disrupt these revenue streams by interrupting website functionality and preventing users from engaging with advertisements or completing transactions. As a result, news organizations may experience financial losses and reduced profitability in the aftermath of an attack.

**Damage to Brand Reputation:** The availability and reliability of news websites are essential factors in building and maintaining trust with audiences. A successful DoS attack can tarnish the reputation of a news organization by highlighting vulnerabilities in its cyber defenses and signaling a lack of preparedness to safeguard user data and information. Negative publicity surrounding the attack may erode trust and confidence in the brand, leading to long-term reputational damage and loss of market share.

**Legal and Regulatory Consequences:** Depending on the nature of the attack and its impact, news organizations may face legal and regulatory consequences for failing to protect user data and maintain service availability. Regulatory bodies such as data protection authorities may impose fines or sanctions for non-compliance with data security standards and breach notification requirements. Moreover, affected users may pursue legal action against the news organization for negligence or breach of contract, further escalating the financial and reputational costs of the attack.

**Operational Disruption and Recovery Costs:** Responding to a successful DoS attack requires significant time, resources, and expertise to mitigate the impact and restore normal operations. News organizations may incur expenses related to incident response, forensic analysis, system restoration, and infrastructure upgrades to prevent future attacks. Additionally, downtime resulting from the attack may disrupt editorial workflows, collaboration tools, and content management systems, affecting the productivity and efficiency of newsroom operations.

In summary, successful DoS attacks can have severe consequences for major news websites, ranging from service disruptions and revenue losses to reputational damage and legal liabilities. Protecting against these attacks requires proactive measures, robust defenses, and effective incident response capabilities to safeguard the availability and integrity of online news platforms.

**Attack Scenario**

**Preparation and Reconnaissance:**

The attacker conducts reconnaissance to identify vulnerabilities in the website's infrastructure and security measures.

They gather information about the website's architecture, technologies, and potential entry points.

**Launch of DoS Attack:**

The attacker initiates a distributed Denial of Service (DDoS) attack using a botnet to flood the website's servers with malicious traffic.

The attack overwhelms the servers, causing service degradation or complete outage for legitimate users.

**WAF Bypass and Evasion:**

The attacker attempts to bypass or evade the defenses of the Web Application Firewall (WAF) by exploiting vulnerabilities or manipulating traffic patterns.

They may launch simultaneous attacks from multiple sources to overwhelm the WAF's capacity and evade detection.

**Impact on Website Availability:**

The sustained attack disrupts the website's availability, resulting in slow page load times, timeouts, or error messages for users.

The website experiences loss of audience engagement and reputational damage due to the outage.

**Response and Mitigation Efforts:**

The security team implements mitigation measures, such as rate limiting and IP blocking, to mitigate the attack and restore service availability.

Collaboration with ISPs and DDoS mitigation services helps mitigate attack traffic upstream and identify the perpetrators.

**Post-Incident Analysis and Remediation:**

A post-incident analysis identifies attack vectors, vulnerabilities exploited, and areas for improvement in cyber defenses.

Security enhancements, such as updating WAF rules and deploying additional DDoS mitigation solutions, are implemented to bolster resilience against future attacks.

**Conclusion**

Denial of Service (DoS) attacks pose significant threats to the availability and integrity of major news websites, disrupting service and undermining the trust of audiences. This study has explored the vulnerabilities in Web Application Firewalls (WAFs) that attackers exploit to orchestrate such attacks, along with the severe consequences that successful attacks can entail.

By identifying vulnerabilities in WAF implementations, assessing their impact on security posture, and proposing mitigation strategies, this study aims to empower news organizations to enhance their cyber resilience and mitigate the risk of DoS attacks. Prevention and mitigation efforts, including WAF configuration reviews, traffic pattern monitoring, and incident response planning, play critical roles in defending against attacks and preserving the availability of online news platforms.

In the face of evolving cyber threats, continuous vigilance, collaboration, and adaptation are essential. News organizations must remain proactive in fortifying their defenses, staying abreast of emerging threats, and refining their incident response capabilities to effectively mitigate the impact of DoS attacks and ensure uninterrupted access to reliable news content.

Ultimately, safeguarding the availability and integrity of major news websites is essential for upholding the principles of freedom of expression, democratic governance, and information transparency in the digital age. By addressing vulnerabilities in WAFs and strengthening cyber defenses, news organizations can fulfill their vital role as trusted sources of information and contribute to a safer and more resilient digital ecosystem.

**REFERENCES**

[**https://www.pewresearch.org/journalism/2020/12/08/measuring-news-consumption-in-a-digital-era/**](https://www.pewresearch.org/journalism/2020/12/08/measuring-news-consumption-in-a-digital-era/)

[**https://link.springer.com/article/10.1007/s10586-017-0730-x**](https://link.springer.com/article/10.1007/s10586-017-0730-x)

[**https://www.researchgate.net/publication/371575436\_Addressing\_the\_Digital\_Divide\_Access\_and\_Use\_of\_Technology\_in\_Education**](https://www.researchgate.net/publication/371575436_Addressing_the_Digital_Divide_Access_and_Use_of_Technology_in_Education)

[**https://www.researchgate.net/publication/375062115\_A\_Comprehensive\_Analysis\_of\_High-Impact\_Cybersecurity\_Incidents\_Case\_Studies\_and\_Implications**](https://www.researchgate.net/publication/375062115_A_Comprehensive_Analysis_of_High-Impact_Cybersecurity_Incidents_Case_Studies_and_Implications)

<https://blog.cloudflare.com/ddos-threat-report-2023-q4>

<https://www.researchgate.net/publication/326104043_Web_Application_Firewall_Network_Security_Models_and_Configuration>

<https://www.researchgate.net/publication/375062115_A_Comprehensive_Analysis_of_High-Impact_Cybersecurity_Incidents_Case_Studies_and_Implications>

<https://www.sciencedirect.com/science/article/pii/S2352484721007289>

<https://onlinelibrary.wiley.com/doi/full/10.1002/eng2.12697>

<https://www2.deloitte.com/us/en/insights/topics/cyber-risk/global-cybersecurity-threat-trends.html>

<https://ieeexplore.ieee.org/document/8511955>

<https://www.upguard.com/blog/cybersecurity-regulations-by-industry>

<https://www.researchgate.net/publication/351302051_Application_Layer_Denial-of-Service_Attacks_and_Defense_Mechanisms_A_Survey>

<https://www.tandfonline.com/doi/full/10.1080/10920277.2022.2034507>

<https://www.sciencedirect.com/science/article/pii/S2352484721007289>

<https://www.sciencedirect.com/science/article/abs/pii/B9780128162033000046>

<https://www.cisa.gov/sites/default/files/publications/understanding-and-responding-to-ddos-attacks_508c.pdf>

<https://www.linkedin.com/pulse/how-do-cyber-criminels-evolve-tactics-techniques-procedures>

<https://www.researchgate.net/publication/375062115_A_Comprehensive_Analysis_of_High-Impact_Cybersecurity_Incidents_Case_Studies_and_Implications>

<https://www.sciencedirect.com/science/article/pii/S0160791X19306840>

<https://www.sciencedirect.com/science/article/pii/S0167404823002626>

<https://journals.sagepub.com/doi/10.1177/00223433231220264>

<https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024>

<https://link.springer.com/article/10.1007/s10270-021-00898-7><https://securityscorecard.com/blog/common-web-application-vulnerabilities-explained/>

<https://dl.acm.org/doi/10.1007/978-3-319-26961-0_29>