GRAND ACADEMIC PORTAL
RESEARCH JOURNALS

GAP INDIAN JOURNAL
OF FORENSICS AND BEHAVIOURAL SCIENCES
(ISSN – 2582-8177)
Globally peer-reviewed and open access journal.

ENHANCING CYBERSECURITY POSTURE IN INDIAN GOVERNMENT INFRASTRUCTURE: THE STRATEGIC ROLE OF WEB APPLICATION FIREWALLS (WAF)

[1]Akash Khunt, [2]Kiran Dodiya, [3]Dr Kapil Kumar

1. Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA (akpatel950@gmail.com)

2. Research Scholar, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA (kirandodiya01@gmail.com)

3Coordinator, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat, INDIA

Abstract

In the era of digital governance and rapid adoption of e-services, Indian government portals have become high-value targets for cyberattacks. Web Application Firewalls (WAFs) serve as a critical defence layer against web-based threats, including SQL injection, cross-site scripting (XSS), and API abuse. This research explores the architecture, functions, and deployment models of WAFs, evaluates their effectiveness in protecting Indian e-Governance infrastructure, and discusses real-world scenarios where WAFs mitigated potential attacks. The paper also analyses the challenges of implementation, reviews select WAF logs, and proposes policy-level recommendations to standardise WAF adoption under national cybersecurity frameworks.

Keywords: *WAF, Threats, Governance, Vulnerability, Logs, Government*

1. INTRODUCTION

The shift in India towards digital transformation has resulted in the emergence of platforms such as Digital India, UMANG, e-Hospital, and multiple state-level portals, among others. Although these services help increase citizen participation and administrative efficiency, they also expose the government to sophisticated cyberattacks. Not only do attacks on government websites create disruption, but they also have political and economic motivations. Web Application Firewalls (WAFs) play a critical role in preventing data breaches, minimising service disruptions, and preserving the integrity of government web applications.[1].

1.1 Understanding WAF: Functions and Architecture

The Web Application Firewall (WAF) is an intermediary between web applications and the internet. It tracks, queues, and prevents HTTP requests from and to a web application. However, WAFs protect against application-layer threats, unlike network firewalls, which interface at ports and IP addresses.[2].

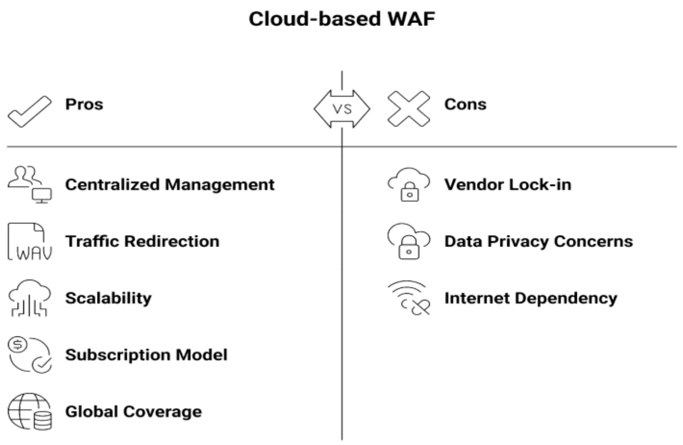


Figure 1 Cloud-Based WAF

2. KEY FUNCTIONS

2.1 Threat Detection and Prevention:

Web application firewalls are primarily deployed for protection against known web application attacks, such as SQL Injection (SQLi), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and remote code execution. These threats pose a serious risk to government portals that handle sensitive public data or services.[3]. In the case of India, where platforms such as DigiLocker, RTI Online, and the National Scholarship Portal are used by millions, WAFs ensure that applications remain robust against exploitation attempts using known vulnerability patterns.[4], [5].

2.2 Rate Limiting and Bot Filtering:

It can block malicious bots, identify suspicious behaviour, and rate-limit requests through a WAF. Government sites are often targeted by automated scanners, scraping tools, and brute-force attacks, with the aim of either overloading the system or extracting sensitive data.[6]. For example, in the Government e-Marketplace (GeM) and portals like MyGov, WAFs protect against denial-of-service attacks and unauthorised automated activity, such as scraping, by filtering and throttling bots, ensuring that authorised users can access services without interruption.[7].

2.3 API Protection:

Several Indian e-governance initiatives are increasingly involving the use of mobile applications and third-party integration, making the security of APIs important.[8]. WAFs could inspect payload content, validate content structure, and reject unauthorised API calls. For Aadhaar-enabled services and e-KYC integrations, they could strengthen protection by rejecting malformed or malicious requests, and help enforce the essential privacy principles — confidentiality and overall integrity of transmitted data — as per the privacy legislation (IT Act and DPDP Act).

2.4 Virtual Patching:

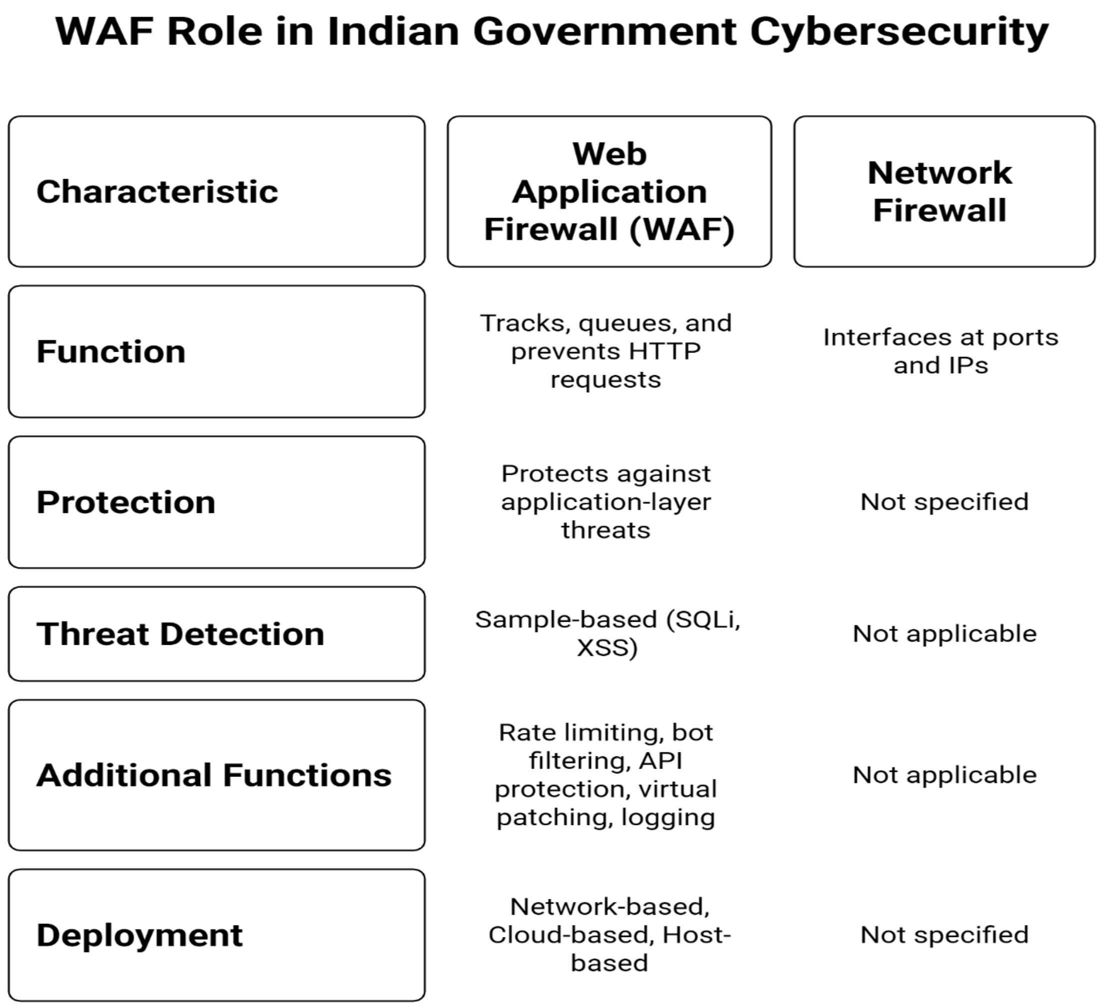
Many public sector applications in the country are running on legacy systems. Suppose the web app is built on legacy systems, or IT does not have the source code of the application. In that case, the modern WAFs (which are also called virtual patching) can fill the gap by blocking known vulnerabilities with custom rules, thus providing immediate coverage to protect applications that do not require application code modifications.[9]. We have already discussed how modern WAFs provide virtual patching which allows enterprise applications, which in many cases were built and are sitting on legacy systems to be protected by custom rules that block known vulnerabilities and provide functionality coverage immediately and without ever touching the application code, many of the public sector applications in India are legacy systems and fall under this category. This reduces the exposure window for discovering the vulnerability and deploying a patch.[10].

2.5 Logging and Forensic Analysis:

WAFs generate detailed logs of all web traffic, including both allowed and blocked requests, as well as those deemed suspicious. This is critical for government agencies to perform forensic investigations during security incidents.[11]. Logs can be exported to SIEM systems, such as Wazuh or QRadar, for centralised analysis. As mandated by CERT-In guidelines, these logs facilitate auditing, compliance reporting, and real-time threat correlation, thereby enhancing national cybersecurity posture and accountability.

2.6 Deployment Models:

WAFs can be deployed in various formats to suit different scales and environments. Network-based WAFs (typically hardware appliances) are ideal for central agencies, such as the NIC. Cloud-based WAFs (offered by AWS, Cloudflare, or Azure) provide scalable, SaaS-based protection with minimal setup. Host-based WAFs such as ModSecurity can be embedded directly within servers used by state or departmental applications.[12]. Each deployment model supports flexibility in defending different parts of India's decentralised digital governance infrastructure, as well as the role of WAF in the context of the Indian Government.



WAF Role in Indian Government Cybersecurity

Characteristic	Web Application Firewall (WAF)	Network Firewall
Function	Tracks, queues, and prevents HTTP requests	Interfaces at ports and IPs
Protection	Protects against application-layer threats	Not specified
Threat Detection	Sample-based (SQLi, XSS)	Not applicable
Additional Functions	Rate limiting, bot filtering, API protection, virtual patching, logging	Not applicable
Deployment	Network-based, Cloud-based, Host-based	Not specified

Figure 2 WAF Role in the Indian Government Cyber Security

3. THREAT LANDSCAPE IN THE INDIAN PUBLIC SECTOR

3.1 Targeted Attacks on Public Infrastructure

India's public sector has experienced a surge in cyberattacks over the past decade, primarily due to the exponential growth of digital services and the sensitive nature of the data being handled. Common attacks include website defacements, particularly of central and state-level government portals such as those hosted by the National Informatics Centre (NIC). These attacks are often politically motivated, intended to cause reputational damage or to broadcast ideological messages (CERT-In, 2022). In 2020, multiple state-level websites were compromised by foreign threat actors, exploiting outdated web infrastructure and inadequate patch management (Saxena & Arora, 2021).

Furthermore, data leaks-especially those involving Aadhaar numbers and personal identifiers—have exposed millions of citizens to identity theft. For example, a Tribune report on the Aadhaar data leak revealed the importance of securing citizen database security by preventing unauthorised access to Aadhaar records through illicit marketplaces (Bhalla, 2018). At the same time, DoS and DDoS attacks have been used against key government services, such as the Income Tax portal and e-filing systems, during peak filing times, denying users access to these systems (Kumar and Sharma, 2020). These patterns underscore the need for protection mechanisms at the web application level that can identify malicious payloads and anomalous traffic in real-time.

3.2 Regulatory Compliance and Security Directives

In response to these increasing threats, India's nodal cybersecurity agency, the Computer Emergency Response Team - India (CERT-In), has issued guidelines that mandate protection for government web applications (April 2022) by requiring organizations to monitor, log, and analyze network events and to install security technologies such as firewalls, intrusion detection systems, and WAFs with real-time defense capabilities and post-incident forensic capabilities (CERT-In, 2022).In addition, the National Cyber Security Policy (NCSP) defines Critical

Information Infrastructure (CII), or any system that relates to national defense, finance, health, or public safety and which can affect national security and economic stability if compromised, as a threat to national security and financial stability, and states that disruptions of CII assets are also threats to the national security and economic stability (Meity 2013). Given this situation, WAFs have become necessary for protecting against attacks on CII assets by virtually patching known vulnerabilities, blocking common attacks, and monitoring HTTP/S traffic patterns. Not only is compliance with such guidelines a matter of law, but it also plays into the trust we place in public digital systems.

3.3 Alignment with Digital Governance Missions

The National e-Governance Plan (NeGP) and India's ambitious Digital India Mission have accelerated the implementation of digital infrastructure across state and ministry administrations. These measures have made it simpler to launch mobile and web apps that provide services such as identification verification and online property records. Security of online applications is a significant concern, as although these programs enhance citizen satisfaction, they also increase the attack surface.

To ensure safe and inclusive access, the Guidelines for Indian Government Websites (GIGW) were established by the Ministry of Electronics and Information Technology (MeitY), offering directives on accessibility, content structure, and security. Among these, web application security is a critical pillar. WAFs are central to meeting GIGW security requirements as they provide automated mitigation against OWASP Top 10 threats, allow secure API exposure, and log all transactional activity for audit and compliance purposes (MeitY, 2020). Their deployment across public-facing portals not only aligns with strategic missions, such as Digital India, but also strengthens the nation's cybersecurity posture.

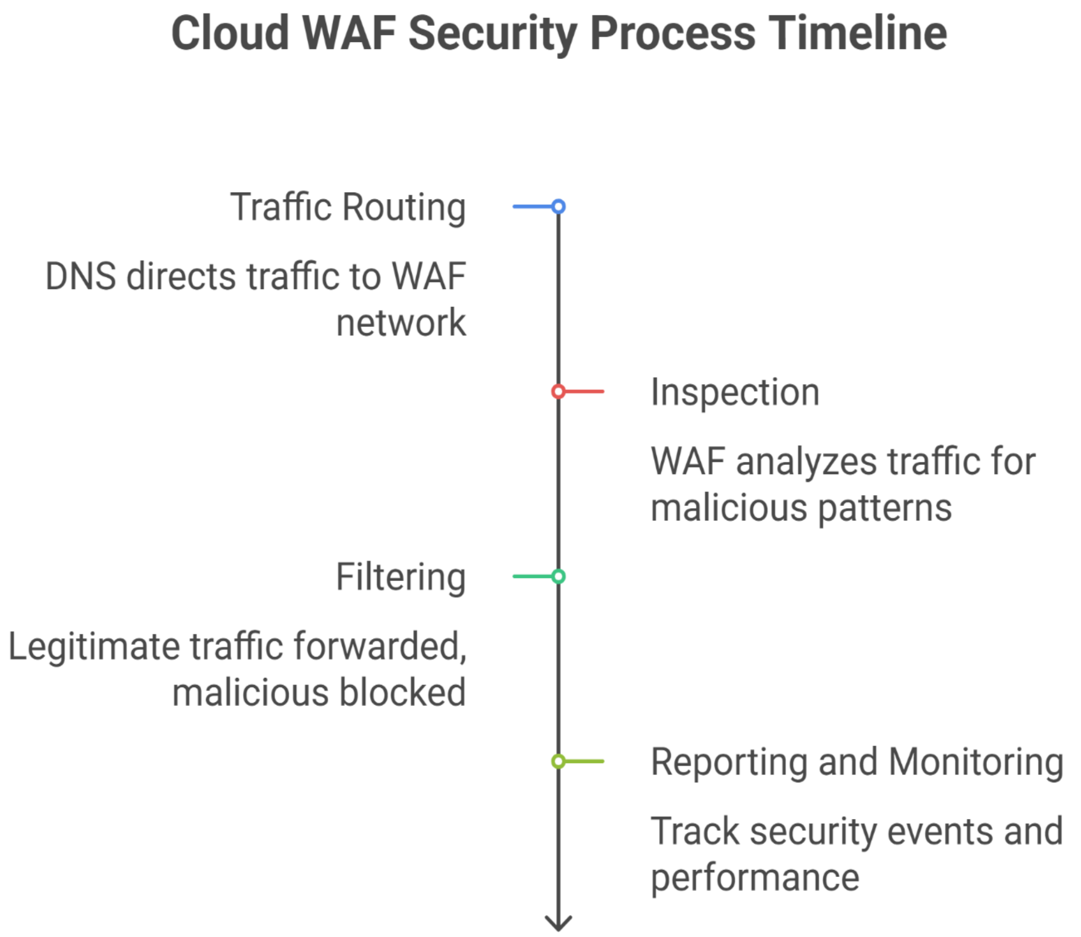

Cloud WAF Security Process Timeline
Traffic Routing
DNS directs traffic to WAF network
Inspection
WAF analyzes traffic for malicious patterns
Filtering
Legitimate traffic forwarded, malicious blocked
Reporting and Monitoring
Track security events and performance

Figure 3 Cloud WAF Security Process Timeline

4. SAMPLE WAF LOGS

```
[2025-06-15 18:30:45] [BLOCK] [XSS] Request from 203.92.23.14 to /admin/login.php    Matched Rule: "<script>
injection"    Action: Blocked | Severity: High
```

```
[2025-06-16 02:17:08] [BLOCK] [SQLi] Request from 115.241.19.102 to /search.php?q=' OR 1=1 --    Matched
Rule: SQL Injection Attempt    Action: Blocked | Severity: Critical
[2025-06-16 07:45:13] [ALLOW] [NORMAL] Request from 106.51.78.199 to /home    Status: Clean traffic
[2025-06-17 11:02:55] [BLOCK] [API Abuse] Request from 182.74.159.101 to /api/v1/userinfo    Matched Rule:
Rate limit exceeded (100 req/min)    Action: Temporarily Blocked | Severity: Medium
[2025-06-15 18:30:45] [BLOCK] [XSS] Request from 203.92.23.14 to /admin/login.php    Matched Rule: "<script>
injection"    Action: Blocked | Severity: High
[2025-06-16 02:17:08] [BLOCK] [SQLi] Request from 115.241.19.102 to /search.php?q=' OR 1=1 --    Matched
Rule: SQL Injection Attempt    Action: Blocked | Severity: Critical
[2025-06-16 07:45:13] [ALLOW] [NORMAL] Request from 106.51.78.199 to /home    Status: Clean traffic
[2025-06-17 11:02:55] [BLOCK] [API Abuse] Request from 182.74.159.101 to /api/v1/userinfo    Matched Rule:
Rate limit exceeded (100 req/min)    Action: Temporarily Blocked | Severity: Medium
```

5. CHALLENGE RELATED TO WAF (WEB APPLICATION FIREWALL) ADOPTION IN GOVERNMENT SYSTEMS

5.1 Cost and Procurement Delays in Public Sector:

Government agencies often operate under strict budgetary constraints and multi-tiered procurement procedures, and acquiring WAF solutions is a time-consuming and bureaucratic process. High-end WAF products, especially hardware-based appliances or enterprise-grade SaaS solutions, are tied to not only expensive upfront expenditures but also ongoing license fees to maintain the service. Public procurement rules, which may vary from country to country, can cause delays and thus expose systems to vulnerabilities in the meantime.

5.2 Lack of Trained Personnel for Configuration and Analysis:

A Web Application Firewall (WAF) functions well only with experts in analysing web traffic and identifying possible threats. One of the most ongoing problems, though, is that most government IT teams often lack sufficient personnel with the right skill sets to deploy, manage effectively, and—perhaps most crucially—properly calibrate these essential security systems. WAFs are potent tools, but they can easily become ineffective without appropriate configuration and ongoing monitoring, either missing real attacks or, on the other hand, generating numerous false positive alerts – both of which put the wider security strategy at risk.

5.3 High False Positive Rate Causing Service Downtimes

Configured with overly strict or broad policies, Web Application Firewalls (WAFs) can misread genuine user behaviour as an attack. This problem becomes more intense with public-facing systems, such as digital identities or citizen grievance portals, where obstructing real users can cause a serious block and raise substantial public ire. Events like these not only erode the public's trust, but they may also lead to system administrators relaxing or disabling security entirely — the very thing WAFs are supposed to protect against.

5.4 Compatibility Challenges with Existing Systems

A significant challenge is that many government systems still use legacy platforms and old web applications that are incompatible with new security technologies. Often, the integration of a Web Application Firewall (WAF) in these environments comes with significant technical debt and typically requires customisations or, in some cases, even code-level changes. These complications can lead to extended deployment cycles, soaring costs, and a heightened risk of outages, particularly if adequate documentation is unavailable or vendor support has been dropped.

RECOMMENDATIONS

Mandatory WAF Deployment: Deploy Web Application Firewalls across all publicly-accessible applications by the policies and procedures outlined in CERT-In.

Consolidate WAF Monitoring: To get WAF feeds under one umbrella, integrate them for monitoring action on WAF feeds with Security Information and Event Management (SIEM) systems that are hosted within the state and central data centres. This will help with centralised visibility in turn.

Focus on Workforce Development: Also, offer targeted training programs and certifications for National Informatics Centre (NIC) officials and state IT departments to enable them to manage WAF solutions with their experience.

Promote National Development: Produce your Web Application Firewalls. This initiative aims to reduce procurement costs and strengthen national data sovereignty by minimising dependency on foreign technologies.

CONCLUSION

With the digital world rapidly advancing, securing the Indian government's infrastructure has become a priority task. Web Application Firewalls (WAFs) serve as a safety net, stopping SQL injections, cross-site scripting (XSS), and illicit access to APIs for public authority sites and applications. The capability to achieve virtual patching, detect real-time web traffic, and collaborate with SIEM systems makes them ideal for improving digital security. Even considering the challenges, such as tighter budgets, a lack of skilled personnel, and the complexity of integrating with legacy systems, the benefits presented by WAFs are of significant value. Their implementation can be more effective if clear regulatory guidelines are provided, dedicated training programs are developed, and centralised monitoring is done. This will also help the government's flagship programs, such as Digital India, by expanding the use of WAFs across platforms. Even more importantly, protecting digital services is not just an IT matter, but also a matter of public trust and national resilience.

REFERENCES

[1] "(PDF) Analysis of Web Application Firewalls, Challenges, and Research Opportunities." Accessed: Jul. 09, 2025. [Online]. Available: https://www.researchgate.net/publication/356066472_Analysis_of_Web_Application_Firewalls_Challenges_and_Research_Opportunities

[2] S. V. Pingale and S. R. Sutar, "Analysis of Web Application Firewalls, Challenges, and Research Opportunities," *Lecture Notes in Electrical Engineering*, vol. 783, pp. 239–248, 2022, doi: 10.1007/978-981-16-3690-5_21.

[3] F. M. Alotaibi and V. G. Vassilakis, "Toward an SDN-Based Web Application Firewall: Defending against SQL Injection Attacks," *Future Internet 2023, Vol. 15, Page 170*, vol. 15, no. 5, p. 170, Apr. 2023, doi: 10.3390/FI15050170.

[4] "Top 20 Recent Cyber Attacks in India 2025, Latest Cyber Crime Cases in India." Accessed: Jul. 09, 2025. [Online]. Available: https://eventussecurity.com/cybersecurity/india/cyber-attacks/?utm_source=chatgpt.com

[5] "Web Application Firewall - Protect Website From Threats ." Accessed: Jul. 09, 2025. [Online]. Available: https://technologymoment.com/web-application-firewall-protect-your-website/?utm_source=chatgpt.com

[6] "Experience-Based Comparison of WAF Solutions in 2025." Accessed: Jul. 09, 2025. [Online]. Available: https://research.aimultiple.com/waf-solutions/?utm_source=chatgpt.com

[7] J. M. Silva, D. Ribeiro, L. F. Ramos, and V. Fonte, "A worldwide overview on the information security posture of online public services," Oct. 2023, Accessed: Jul. 09, 2025. [Online]. Available: https://arxiv.org/pdf/2310.01200

[8] B. R. Dawadi, B. Adhikari, and D. K. Srivastava, "Deep Learning Technique-Enabled Web Application Firewall for the Detection of Web Attacks," *Sensors 2023, Vol. 23, Page 2073*, vol. 23, no. 4, p. 2073, Feb. 2023, doi: 10.3390/S23042073.

[9] "Virtual Patching: A Lifesaver for Web App Security | Qualys." Accessed: Jul. 09, 2025. [Online]. Available: https://blog.qualys.com/product-tech/2017/05/04/virtual-patching-a-lifesaver-for-web-app-security

[10] G. Betarte, E. Giménez, R. Martínez, and Á. Pardo, "Machine learning-assisted virtual patching of web applications," Mar. 2018, Accessed: Jul. 09, 2025. [Online]. Available: https://arxiv.org/pdf/1803.05529

[11] "(PDF) WEB APPLICATION FIREWALL." Accessed: Jul. 09, 2025. [Online]. Available: https://www.researchgate.net/publication/387187876_WEB_APPLICATION_FIREWALL

[12] "The WAF Evasion Playbook: Know Your Enemy's Techniques." Accessed: Jul. 09, 2025. [Online]. Available: https://sikasecurity.com/a-comprehensive-review-of-waf-evasion-and-obfuscation-techniques