Ordu Üniversitesi Bilim ve Teknoloji Dergisi
Ordu Üniv. Bil. Tek. Derg.

Ordu University Journal of Science and Technology
Ordu Univ. J. Sci. Tech.

E-ISSN: 2146-6459 2026, 16 Araştırma Makalesi / Research Article
Makale Sayısı / Article Number: 6 http://doi.org/10.54370/ordubtd.1919389

An Evaluation of the Web Security Posture of University Websites in Turkey: A Case Study

Osman Güray Özcüre[1], Özgür Tonkal[1]

[1]Samsun University, Faculty of Engineering and Natural Sciences, Department of Software Engineering, Samsun

Geliş Tarihi / Received Date: 30.03.2026 Kabul Tarihi / Accepted Date: 08.06.2026

Abstract

This study assessed the web security posture of 205 universities in Turkey that had a main website as of August 23, 2025. The lack of a comprehensive study focusing on Web Application Firewall (WAF) usage and vulnerability assessment of main university websites in Turkey motivated the research. In the study, the scanning tools wafw00f and ZAP were initially used, followed by the inclusion of Mozilla's HTTP Observatory to cross-check ZAP's findings for a more trustworthy evaluation, due to certain limitations exhibited by ZAP. In addition, an additional ZAP scan was conducted on academic staff web pages to extend the scope of the vulnerability assessment. Each tool was used in a non-intrusive way to prevent causing harm to the websites. The scans were performed using wafw00f on August 23, 2025; with ZAP between September 4 and 12, 2025; and finally with HTTP Observatory between October 3 and 4, 2025. Later, an additional ZAP scan of academic staff web pages was conducted between December 12 and 15, 2025. Only findings marked as High Confidence by ZAP were included in the evaluation to maintain scientific consistency. The results were analysed in relation to the Open Web Application Security Project (OWASP) Top Ten 2021 and the associated risks. The findings show that many universities lack a WAF and have missing or misconfigured Content Security Policy (CSP) and Strict-Transport-Security headers. These issues fall under A05:2021 - Security Misconfiguration and may increase the risk of A03:2021 - Injection, suggesting that university web security remains vulnerable and would benefit from further improvement.

Keywords: web application security, universities, WAF, vulnerability assessment, OWASP top ten 2021

Türkiye'deki Üniversitelerin Web Sitelerinin Güvenlik Durumunun Değerlendirilmesi: Bir Durum Çalışması

Öz

Bu çalışma, 23 Ağustos 2025 itibarıyla ana web sitesine sahip olan Türkiye'deki 205 üniversitenin web güvenliği durumunu değerlendirmiştir. Türkiye'deki üniversitelerin ana web sitelerinde Web Uygulama Güvenlik Duvarı (WAF) kullanımı ve güvenlik açığı değerlendirmesine odaklanan kapsamlı bir çalışmanın bulunmaması bu araştırmayı motive etmiştir. Çalışmada başlangıçta wafw00f ve ZAP tarama araçları kullanılmış, ZAP'ın bazı sınırlılıkları nedeniyle daha güvenilir bir değerlendirme elde etmek amacıyla Mozilla'nın HTTP Observatory aracı, ZAP bulgularını doğrulamak üzere sürece dahil edilmiştir. Ayrıca, güvenlik açığı değerlendirmesinin kapsamını genişletmek amacıyla akademik personel web sayfaları üzerinde ek bir ZAP taraması gerçekleştirilmiştir. Her bir araç, web sitelerine zarar verilmesini önlemek amacıyla müdahaleci olmayan (non-intrusive) şekilde kullanılmıştır. Taramalar; 23 Ağustos 2025'te wafw00f ile, 4-12 Eylül 2025 arasında ZAP ile ve 3-4 Ekim 2025 arasında HTTP Observatory ile gerçekleştirilmiştir. Daha sonra, ZAP ile 12-15 Aralık 2025 arasında akademik personel web sayfaları üzerinde ek bir tarama yapılmıştır. Bilimsel tutarlılığı sağlamak amacıyla değerlendirmeye yalnızca ZAP tarafından High Confidence olarak işaretlenen bulgular dahil edilmiştir. Elde edilen sonuçlar, Open Web Application Security Project (OWASP) Top Ten 2021'de yer alan güvenlik açıkları ve bunların potansiyel riskleri dikkate alınarak analiz edilmiştir. Bulgular, üniversitelerin çoğunun WAF kullanmadığını ve Content Security Policy (CSP) ile Strict-Transport-Security başlıklarının eksik veya hatalı yapılandırıldığını göstermiştir. Bu zafiyetler, OWASP Top Ten 2021 kapsamında A05:2021-Security Misconfiguration kategorisi ile örtüşmekte olup A03:2021-Injection riskinde potansiyel bir artışa işaret etmekte ve üniversitelerin web güvenliğinin belirli ölçüde zafiyet içererek iyileştirme gerektirdiğini göstermektedir.

Anahtar Kelimeler: web uygulama güvenliği, üniversiteler, WAF, güvenlik açığı değerlendirmesi, OWASP top ten 2021

Sorumlu Yazar / Corresponding Author: Osman Güray Özcüre osmangurayozcure.akademik@gmail.com

Introduction

Web applications are among the most important assets of organisations, and their security continues to be a global concern. This is evident in recent reports. For example, 53% of organisations reported a lack of confidence in their application security in 2024, while 30% experienced breaches linked to stolen credentials in 2025 (Fortinet, 2024; Fortinet, 2025). Together, these findings suggest that the overall security posture of web applications remains vulnerable and still requires improvement.

Given this widespread weakness, different types of organisations face similar risks. Universities, however, stand out due to the large number of users they serve and the critical information they manage. Regardless of the web technologies used, web applications can still contain exploitable vulnerabilities, attracting both attackers and researchers. Among the organisations working in this area, the Open Web Application Security Project (OWASP) provides a widely accepted framework of common web vulnerabilities, which is updated periodically rather than on a fixed annual basis. In this study, OWASP Top Ten 2021, the most recent version available at the time, was used as a reference framework (OWASP, 2021).

Due to these vulnerabilities, many websites remain at risk. This risk can be mitigated by detecting and remediating vulnerabilities before exploitation, with vulnerability scanning playing an important role.

Vulnerability scanning is an action that tries to find available logical errors and vulnerable components of the system, causing vulnerabilities (Altulaihan, Alismail, & Frikha, 2023). Scanning approaches are generally categorised as active or passive. In a comparative study, Ecik (2021) found that passive vulnerability scanning can produce more accurate results in less time, without causing potential harm to target systems. This makes it particularly suitable for large-scale assessments.

In addition to vulnerability scanning, Web Application Firewalls (WAFs) provide an additional layer of protection. A WAF is a security solution designed to protect websites against common web-based attacks, particularly injection attacks such as Cross-Site Scripting (XSS) and SQL Injection (SQLi). It also helps prevent intrusion attempts by filtering and monitoring web traffic to block malicious requests (Ghanbari et al., 2015).

WAFs can generally be divided into two types based on their detection methods: rule-based and anomaly-based. A rule-based WAF operates by filtering traffic through predefined allow or deny rules, while an anomaly-based WAF identifies unusual patterns in web requests to flag potential attacks (Clincy & Shahriar, 2018). Figure 1 illustrates the role of a WAF in filtering web traffic between clients and web applications.

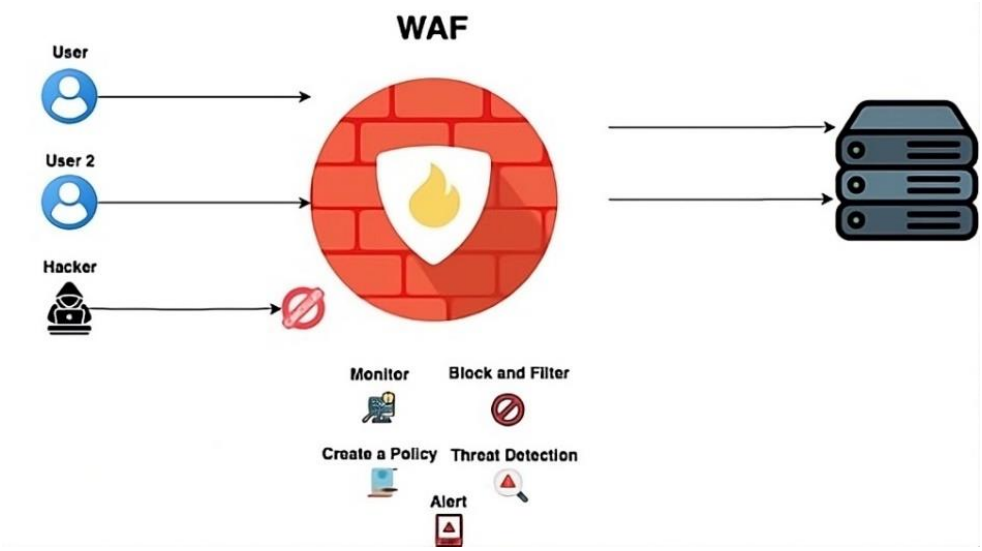

Figure 1. The Role of a WAF

As shown in Figure 1, a WAF filters incoming web traffic to block malicious requests while allowing legitimate ones. Considering the importance of WAF usage and vulnerability assessment, this study aimed to evaluate the web security posture of main university websites in Turkey. Figure 2 illustrates the research process.

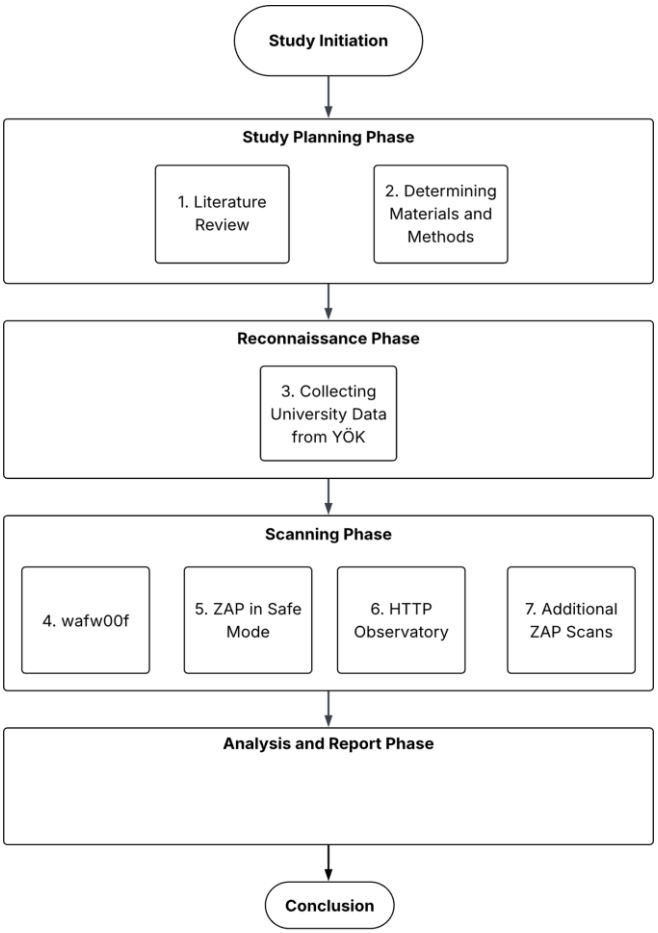

Figure 2. Overview of the Research Process

As illustrated in Figure 2, the study followed a structured process consisting of planning, reconnaissance, scanning, and analysis phases. The analysis used wafw00f, ZAP (Safe Mode), and HTTP Observatory, with an additional ZAP scan of academic staff web pages. All tools were used in a non-intrusive manner.

In this context, the main contributions of this study are as follows:

1. Unique Scope: Analysis of 205 main university websites in Turkey,
2. Novel Perspective: An evaluation of web security posture together with WAF usage, which has been largely overlooked in prior studies,
3. Validation: ZAP findings were cross-checked using HTTP Observatory,

These contributions provide new insights and distinguish this study from prior studies.

Related Work

Several studies have examined the security of university websites using different vulnerability scanning tools. Adha et al. (2023) evaluated a university website using ZAP and OpenVAS tools, reporting that ZAP detected more vulnerabilities and performed more efficiently. Similarly, Muin et al. (2022) used Nessus to assess multiple university websites and identified medium-level security risks, highlighting the importance of configuration-related vulnerabilities such as DNS weaknesses.

Prasetyo and Hassanah (2021) compared Nessus and ZAP alongside reconnaissance tools, showing that different scanners may identify different vulnerabilities, thus emphasizing the benefit of using multiple tools. Satria et al. (2024) used ZAP and Nessus to assess university websites under the ac.id domain and mapped the identified vulnerabilities to the OWASP Top Ten 2021 framework, providing a structured classification of the vulnerabilities.

In a study on universities in Turkey, Macakoğlu et al. (2022) analysed 147 university web pages intended for prospective students. The study focused on accessibility, availability, and security, using automated testing tools such as Sucuri's SiteCheck for vulnerability assessment. The findings showed that most institutions had moderate security levels, although issues related to accessibility and availability were also identified.

To provide a structured comparison and highlight the key differences of prior studies and this study, Table 1 is presented. In the table, Active Vulnerability Scanning, Passive Vulnerability Scanning, and Vulnerability Assessment are abbreviated as AVS, PVS, and VA, respectively.

Table 1. Comparison of Previous Studies and This Study

Studies	Targets	Tools	Methods	WAF Analysis
Prasetyo and Hassanah (2021)	Universitas Internasional Batam	Nessus & ZAP (VA); nslookup, whois & nmap (reconnaissance)	AVS	No
Muin et al. (2022)	web1, web2, web3	Nessus	AVS	No
Macakoğlu et al. (2022)	147 university web pages for prospective students in Turkey	SiteCheck; automated tools for accessibility, availability	PVS	No
Adha et al. (2023)	Mataram University	ZAP & OpenVAS	AVS	No
Satria et al. (2024)	5 websites operating under ac.id domain	Nessus & ZAP	AVS	No
This Study	205 main websites of universities in Turkey	wafw00f, ZAP & HTTP Observatory	PVS	Yes

VA: Vulnerability Assessment; AVS: Active Vulnerability Scanning; PVS: Passive Vulnerability Scanning

As shown in Table 1, a review of the literature indicates that no study has evaluated the web security of universities in terms of WAF usage. Most prior studies, except for Macakoğlu et al. (2022), relied primarily on active vulnerability scanning, which may potentially harm target websites. To avoid such risks, this study adopted a safer, non-intrusive approach similar to that of Macakoğlu et al. (2022), while focusing specifically on vulnerabilities mapped to the OWASP Top Ten 2021 and incorporating WAF usage analysis using wafw00f, ZAP in Safe Mode, and Mozilla's HTTP Observatory. Accordingly, accessibility and availability aspects were excluded.

The study by Macakoğlu et al. (2022) also differed from this study in several ways that highlight its novelty. Unlike this study, the earlier study did not validate its results by cross-checking with another tool or assess WAF usage, relying solely on Sucuri's SiteCheck for vulnerability assessment. In contrast, this study cross-verified the results obtained from ZAP using Mozilla's HTTP Observatory to enhance reliability. Moreover, Macakoğlu et al. (2022) examined 147 web pages created for prospective students, whereas this study focused on 205 main university websites. Taken together, these differences show the novelty of this study.

Material and Method

This section describes the reconnaissance and scanning phases of the study, as well as the accuracy of the tools, exhibited limitations by the tools, and handling of false positives.

Reconnaissance

The reconnaissance phase involved collecting university names and main website URLs from YÖK's Higher Education Information Management System on August 23, 2025. Although 208 universities were identified, only 205 with active main websites were included in the analysis (Yükseköğretim Kurulu, 2025).

Scanning

The scanning phase consisted of four steps: detecting WAF usage using wafw00f, conducting non-intrusive vulnerability assessment using ZAP in Safe Mode, cross-checking the ZAP findings with Mozilla's HTTP Observatory, and performing an additional ZAP scan of academic staff web pages.

For the initial ZAP scan, the scope was limited to main university websites with ".edu.tr" domains, and three representative pages (e.g., a contact page) were scanned for each university. The additional ZAP scan was conducted on academic staff web pages to extend the scope of the analysis. Since the initial ZAP findings had already been cross-checked using HTTP Observatory, repeating the same validation process for the additional scan of academic staff web pages was considered unnecessary. In addition, the additional ZAP scan revealed vulnerabilities largely consistent with those identified in the initial ZAP scan, suggesting that similar configuration-related issues were present regardless of web page type.

The scans were conducted as follows: on August 23, 2025 with wafw00f; between September 4 and 12, 2025 with ZAP; between October 3 and 4, 2025 with HTTP Observatory; and between December 12 and 15, 2025 for the additional ZAP scan.

The selected tools were chosen based on their reliability and widespread use in web security assessments. wafw00f is commonly used for WAF detection, while ZAP is an open-source tool widely adopted in both industry and academia, as also observed in prior studies such as Adha et al. (2023). HTTP Observatory was included as a non-intrusive tool with a similar scope to ZAP in Safe Mode, enabling cross-validation of the findings and improving the reliability of the evaluation.

Accuracy and Limitations of the Tools

Although the tools were generally effective, some limitations were observed during scanning. wafw00f scanned 204 out of 205 universities, except for Ordu University when attempting to connect to its university website. On the other hand, ZAP scanned 187 out of 205 universities. For 18 universities, scanning was limited due to timeouts, access restrictions, or connection issues. These limitations are summarized in Table 2.

Table 2. Exhibited Limitations by ZAP

University	Exhibited Limitation (ZAP)
Acıbadem Mehmet Ali Aydınlar University	Connection failure
Burdur Mehmet Akif Ersoy University	HTTP communication error
Demiroğlu Bilim University	DNS resolution error
Gümüşhane University	Access denied (403)
Haliç University	Connection timeout
İstanbul Aydın University	Access denied (403)
İstanbul Beykent University	Access denied (403)
İstanbul Medeniyet University	Connection failure
İstanbul Rumeli University	Access denied (403)
İzmir Bakırçay University	Connection failure
Kahramanmaraş İstiklal University	Blank page response
Kapadokya University	Blank page response
Kırklareli University	SSL/TLS error
Kocaeli University	Connection failure
Özyeğin University	Network connection error
Türk Hava Kurumu University	Connection failure
Yaşar University	Access denied (403)
Yeditepe University	Connection failure

As shown in Table 2, the observed limitations varied across universities and were mainly related to access restrictions, connection failures, DNS resolution issues, SSL/TLS errors, and blank page responses. In particular, "Access denied (403)" responses might be related to automated scanning bot detection or, potentially, Intrusion Detection/Prevention Systems (IDS/IPS). Mozilla's HTTP Observatory also exhibited certain limitations during scanning, although it successfully scanned 199 out of 205 universities, compared to 187 for ZAP. The observed limitations are presented in Table 3.

Table 3. Exhibited Limitations by HTTP Observatory

University	Exhibited Limitation (HTTP Observatory)
Burdur Mehmet Akif Ersoy University	HTTP communication error
Demiroğlu Bilim University	DNS resolution error
Gümüşhane University	Access denied (403)
İstanbul Beykent University	Access denied (403)
İstanbul Medeniyet University	Connection failure
Kahramanmaraş İstiklal University	Blank page response

As shown in Table 3, similar to the limitations observed for ZAP, the limitations of HTTP Observatory included HTTP communication errors, DNS resolution errors, access restrictions, connection failure, and blank page responses. For example, an "Access denied (403)" response was returned for Gümüşhane University, similar to the limitation observed for ZAP, possibly due to automated scanning bot detection. Additionally, HTTP Observatory encountered an unexpected case for Burdur Mehmet Akif Ersoy University, in which the website responded with an "HTTP communication error", more specifically HTTP status code 404. However, this website was accessible in the browser (i.e. Google Chrome), yet the reason behind this limitation remains unclear. Despite these limitations, HTTP Observatory provided reliable results for cross-checking the findings obtained from ZAP.

Technical Limitations and Handling of False Positives and Negatives

The tools used in this study have inherent limitations due to their non-intrusive nature. ZAP and HTTP Observatory primarily identify observable configuration-level issues, meaning that vulnerabilities requiring active interaction or authenticated access may go undetected. Similarly, wafw00f may fail to detect WAF solutions that are configured to suppress identifiable responses.

Also, to improve reliability of the findings, three steps were taken. All tools were used in a non-intrusive manner, which helped reduce the risk of inaccurate detections. In addition, only High Confidence findings from ZAP were considered, and the results were cross-checked using HTTP Observatory. Together, these steps reduced the risk of false positives and false negatives and strengthened the overall reliability of the analysis.

Results and Discussion

This section presents the findings obtained from wafw00f, ZAP, and HTTP Observatory in their respective subsections. Taken together, these results reflect the overall web security posture of universities. Since HTTP Observatory was used to cross-check ZAP findings, the results did not always fully align, thereby improving the reliability of the evaluation. Additionally, as noted in the Related Work section, no prior studies were identified that used these tools in the context of universities in Turkey, which makes direct comparison with prior studies difficult.

WAF Usage Overview

wafw00f detected WAF usage for 204 of the 205 universities. For Ordu University, the scan could not be completed, even though the website was accessible. Figure 3 shows the distribution of WAF usage across the universities.

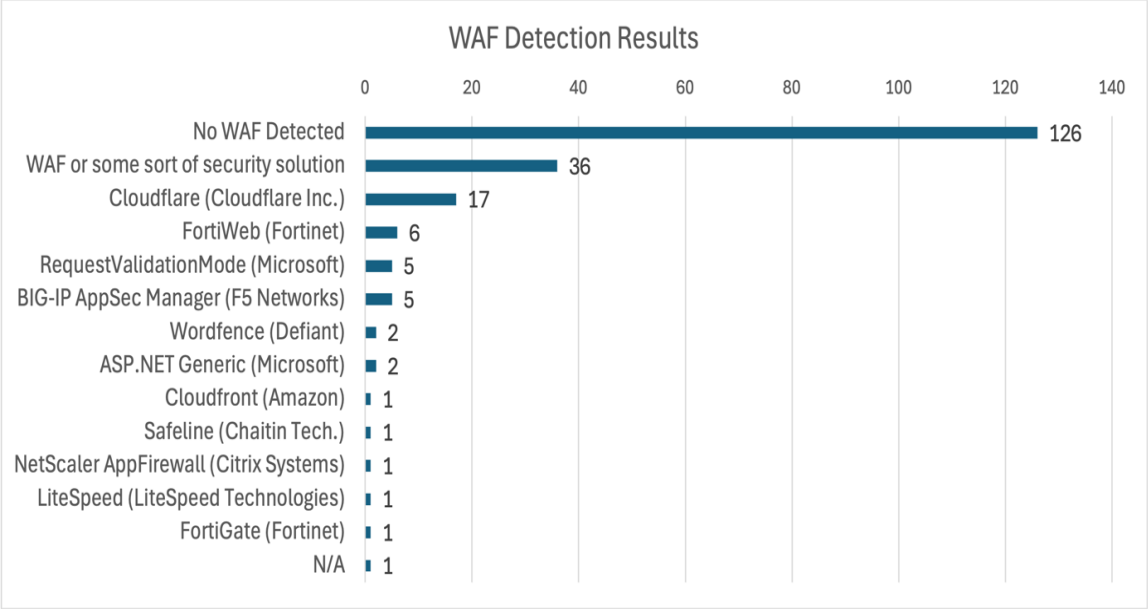

Figure 3. Findings of wafw00f

As shown in Figure 3, 126 universities were detected to have no WAF solution. In contrast, 78 universities had some form of protection, either through a detected WAF or another security mechanism. Among these, 42 universities had identifiable WAF solutions.

These findings suggest that while some universities implement protective measures against attacks such as XSS and SQLi, most remain without a WAF, increasing their exposure to these risks. The identified issues are associated with OWASP Top Ten 2021 categories, particularly A03: Injection and A05:Security Misconfiguration.

Among the detected WAF solutions, Cloudflare was the most widely used, with significantly higher use than alternatives such as FortiWeb. This difference may be related to factors such as cost, ease of deployment, and brand recognition.

Microsoft-related solutions, including RequestValidationMode and ASP.NET Generic, were also observed, suggesting that universities using Microsoft-based web technologies may prefer security features built into that ecosystem. Other WAF solutions were used less frequently, likely reflecting lower market presence compared to more established providers.

Overall, the limited use of WAF solutions suggests that many universities rely on alternative security measures such as server configurations or hosting-level protections. However, these may not provide sufficient protection against common web vulnerabilities. To reduce these risks, universities without a WAF could consider deploying one or strengthening their existing security configurations.

As shown in Figure 3, 126 universities were detected to have no WAF solution. In contrast, 78 universities had some form of protection, either through a detected WAF or another security mechanism. Among these, 42 universities had identifiable WAF solutions.

These findings suggest that while some universities implement protective measures against attacks such as XSS and SQLi, most remain without a WAF, increasing their exposure to these risks. The identified issues are associated with OWASP Top Ten 2021 categories, particularly A03: Injection and A05:Security Misconfiguration.

Among the detected WAF solutions, Cloudflare was the most widely used, with significantly higher use than alternatives such as FortiWeb. This difference may be related to factors such as cost, ease of deployment, and brand recognition.

Microsoft-related solutions, including RequestValidationMode and ASP.NET Generic, were also observed, suggesting that universities using Microsoft-based web technologies may prefer security features built into that ecosystem. Other WAF solutions were used less frequently, likely reflecting lower market presence compared to more established providers.

Overall, the limited use of WAF solutions suggests that many universities rely on alternative security measures such as server configurations or hosting-level protections. However, these may not provide sufficient protection against common web vulnerabilities. To reduce these risks, universities without a WAF could consider deploying one or strengthening their existing security configurations.

Vulnerability Assessment with ZAP Overview

ZAP revealed several common vulnerabilities in university websites. Figure 4 shows their distribution across the universities.

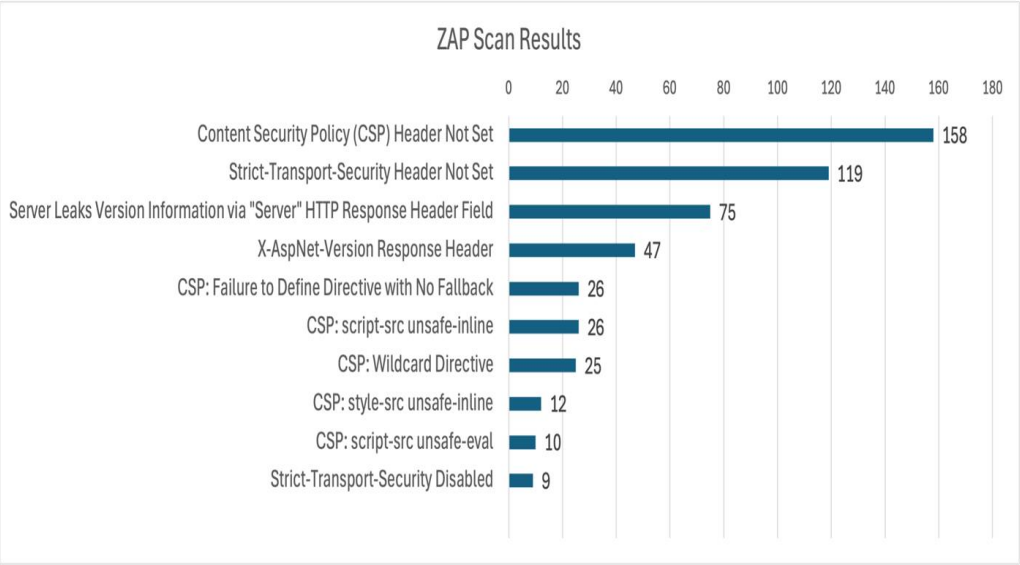

Figure 4. Findings of ZAP

Figure 4 shows that the most frequent vulnerabilities were CSP Header Not Set (158), Strict-Transport-Security Header Not Set (119), Server Leaks Version Information via “Server” HTTP Response Header Field (75), and X-AspNet-Version Response Header (47).

CSP Header Not Set was the most common vulnerability, indicating that many universities did not enforce content security policies and were therefore more exposed to attacks such as XSS and clickjacking.

Other CSP-related vulnerabilities were also identified, although less frequently. Table 4 summarises these findings. In Table 4, “CSP: Failure to Define Directive with No Fallback” is shortened to “CSP: Failure to Define Directive” for clarity.

Table 4. Other CSP-Related Vulnerabilities

Vulnerability	Description	Risk	Mitigation
CSP: Failure to Define Directive	Directive not defined	XSS, clickjacking	Define directives or set default-src fallback
CSP: script-src unsafe-inline	Inline scripts allowed	XSS	Remove inline scripts (use nonces/hashes)
CSP: Wildcard Directive	Any source allowed	XSS	Restrict sources (avoid “*”)
CSP: style-src unsafe-inline	Inline styles allowed	XSS, UI manipulation	Remove inline styles
CSP: script-src unsafe-eval	eval() function allowed	XSS	Disable unsafe-eval

As shown in Table 4, CSP-related vulnerabilities extended beyond missing headers to include frequent directive-level misconfigurations. This suggests that even when CSP is implemented, it is sometimes ineffective due to misconfiguration, which weakens protection against attacks such as XSS and clickjacking.

Apart from CSP-related vulnerabilities, several other configuration issues were observed, including Strict-Transport-Security Header Not Set (119), Server Leaks Version Information via “Server” HTTP Response Header Field (75), X-AspNet-Version Response Header (47), and Strict-Transport-Security Disabled (9). Although these were classified as low risk by ZAP, they may still contribute to security weaknesses.

Strict-Transport-Security Header Not Set vulnerability indicates that HTTPS is not enforced, whereas Strict-Transport-Security Disabled vulnerability refers to cases where it is explicitly turned off. Both vulnerabilities can be mitigated by configuring the web server to enforce HTTPS and disable HTTP.

On the other hand, both Server Leaks Version Information via “Server” HTTP Response Header Field and X-AspNet-Version Response Header vulnerabilities expose version information by the server, which may enable more targeted attacks. For example, if a web application uses an outdated technology (e.g., PHP 5.6), known vulnerabilities specific to that version can be exploited.

Taken together, the findings from ZAP suggest that both CSP-related and other configuration-related vulnerabilities may affect the overall web security posture. Additionally, these vulnerabilities primarily correspond to OWASP Top Ten 2021 category A05: Security Misconfiguration and may also increase the risk of A03: Injection, particularly in the case of CSP-related issues.

Findings of HTTP Observatory

HTTP Observatory was used to cross-check the findings obtained from ZAP. Table 5 presents a comparison of the results obtained from both tools.

Table 5. Cross-Checking of ZAP Findings Using HTTP Observatory

HTTP Observatory (Cross-Check)	ZAP Findings
CSP header not implemented (171)	CSP Header Not Set (158)
CSP implemented unsafely (25)	Various CSP-related misconfigurations (99)
Strict-Transport-Security header not implemented (131)	Strict-Transport-Security Header Not Set (119)
Strict-Transport-Security header set to less than six months (18)	Not detected by ZAP

As shown in Table 5, the findings of both tools were largely consistent, with only minor differences in the number of detected cases. For example, ZAP identified 158 instances of missing CSP headers, while HTTP Observatory reported 171. Similarly, the difference for Strict-Transport-Security header absence was relatively small. These similarities suggest that both tools identified comparable configuration-related issues, supporting the reliability of the findings. Differences in counts may be attributed to variations in detection methods and fewer observed limitations in HTTP Observatory, allowing more universities to be scanned.

An additional finding from HTTP Observatory that is not detected by ZAP, was the presence of Strict-Transport-Security header set to less than six months (18), indicating incomplete HTTPS enforcement. This can be mitigated by increasing the duration to at least one year.

Taken together, the results from both tools consistently highlight configuration-related weaknesses, demonstrating that cross-checking with multiple tools can improve the reliability of web security evaluations.

Additional Vulnerability Assessment of Academic Staff Web Pages

The additional scan using ZAP revealed that academic staff web pages were affected by many of the same vulnerabilities observed in the previous scan, which consisted of three randomly selected representative web pages. However, two additional vulnerabilities were also detected. Figure 5 shows the distribution of these findings.

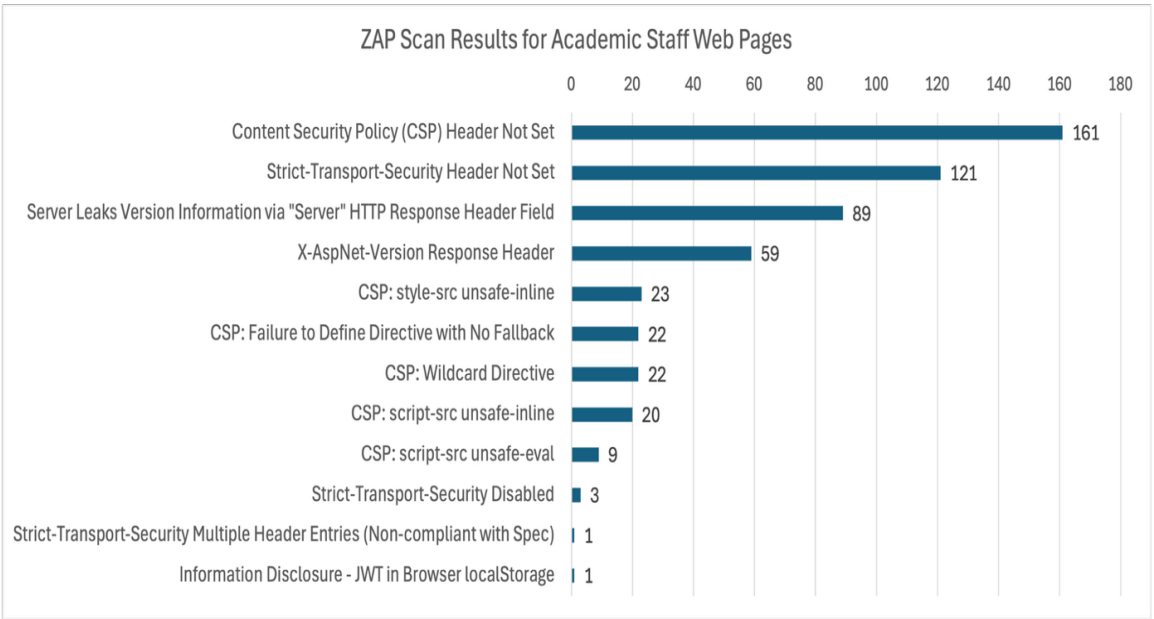

Figure 5. Findings of Additional Scan

Figure 5 shows that the additional scan found similar vulnerabilities in academic staff web pages to those identified in the initial ZAP scan (see the subsection Vulnerability Assessment with ZAP Overview), along with two additional ones. These were Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec) and Information Disclosure - JWT in Browser localStorage.

Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec) vulnerability involves multiple conflicting headers, which may lead to inconsistent enforcement of HTTPS policies. Similarly, Information Disclosure - JWT in Browser localStorage vulnerability may expose sensitive information on the client side. Although less frequent, these vulnerabilities further highlight configuration-related weaknesses in web applications.

Taken together with the initial ZAP findings, the results suggest that these vulnerabilities occur consistently across different types of web pages rather than being limited to specific categories. This further supports the presence of A05: Security Misconfiguration.

Conclusion and Recommendations

This study evaluated the web security posture of 205 universities with a main website as of August 23, 2025. wafw00f was used to detect WAF usage, while ZAP was used in Safe Mode to assess vulnerabilities in a non-intrusive manner. HTTP Observatory was also used to cross-check the initial ZAP findings, which improved the reliability of the evaluation. Also, the additional ZAP scan of academic staff web pages showed that similar vulnerabilities were present across different types of pages, indicating that these issues were not limited to specific sections.

This study contributes to the literature by jointly evaluating WAF usage and web vulnerabilities, focusing on High Confidence findings and using non-intrusive, cross-checked methods. This perspective has not been identified in prior studies.

The findings showed that most universities did not have a WAF solution in place, which increases their exposure to vulnerabilities such as XSS and SQLi. These are primarily associated with OWASP Top Ten 2021 category A05: Security Misconfiguration. However, having a WAF solution in place should not be interpreted as being completely secure in web applications. Overreliance on WAF solutions may lead to a false sense of security, potentially causing universities to neglect secure coding and configuration practices, as well as regular vulnerability assessments. In addition, CSP headers were often missing or improperly configured, and Strict-Transport-Security headers were

either absent or misconfigured, further supporting this category. The additional scan of academic staff web pages confirmed that similar configuration-related vulnerabilities were present across different types of pages. Taken together, the results suggest that the web security posture of universities in Turkey may require improvement, particularly in terms of configuration-related practices.

To improve security, universities should consider deploying WAF solutions, enforcing HTTPS consistently, implementing CSP with properly defined directives, and minimizing the exposure of version information in response headers. In addition, university IT departments could benefit from periodically implementing automated vulnerability assessment routines to identify potential weaknesses at an early stage.

Finally, future studies conducting legally authorized active vulnerability scanning may reveal higher-impact vulnerabilities and further contribute to improving web application security awareness and practices across universities in Turkey.

Author Contribution

Osman Güray Özcüre, prepared the experimental setup and followed the experimental process. *Özgür Tonkal*, carried out the data collection and statistical analyses. The authors wrote, read, and approved the manuscript together.

Ethics

There are no ethical issues regarding the publication of this article.

Conflict of Interest

The authors declare that there is no conflict of interest.

ORCID

Osman Güray Özcüre https://orcid.org/0009-0003-4003-9831

Özgür Tonka https://orcid.org/0000-0001-7219-9053

Kaynaklar

Adha, M., Kwa, Z. D., & Muhammad, A. H. (2023). Website security test at the University of Mataram using vulnerability assessment. *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), 8*(2), 647–655. https://doi.org/10.29100/jipi.v8i2.3830

Altulaihan, E. A., Alismail, A., & Frikha, M. (2023). A survey on web application penetration testing. *Electronics, 12*(5), 1229. https://doi.org/10.3390/electronics12051229

Clincy, V., & Shahriar, H. (2018, July). Web application firewall: Network security models and configuration. In *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)* (Vol. 1, pp. 835–836). IEEE. https://doi.org/10.1109/COMPSAC.2018.00144

Ecik, H. (2021, December). Comparison of active vulnerability scanning vs. passive vulnerability detection. In *2021 International Conference on Information Security and Cryptology (ISCTURKEY)* (pp. 87–92). IEEE. https://doi.org/10.1109/ISCTURKEY53027.2021.9654331

Fortinet. (2024). *2024 application security report. Fortinet.* Retrieved July 22, 2025, from https://www.cybersecurity-insiders.com/portfolio/2024-application-security-report-fortinet/

Fortinet. (2025). *2025 web application security report. Fortinet.* Retrieved July 22, 2025, from https://www.fortinet.com/uk/resources/reports/application-security-report

Ghanbari, Z., Rahmani, Y., Ghaffarian, H., & Ahmadzadegan, M. H. (2015, November). Comparative approach to web application firewalls. In *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)* (pp. 808–812). IEEE. https://doi.org/10.1109/KBEI.2015.7436148

Macakoğlu, Ş. S., Peker, S., Medeni, İ. T., & Medeni, T. D. (2022). Türk üniversitelerinin aday öğrenci web sayfalarının erişilebilirlik, kullanılabilirlik ve güvenlik açısından değerlendirilmesi. *Bilişim Teknolojileri Dergisi, 15*(3), 261–274. https://doi.org/10.17671/gazibtd.1066330

Muin, M. A., Kapti, K., & Yusnanto, T. (2022). Campus website security vulnerability analysis using Nessus. *International Journal of Computer and Information System, 3*(2), 79–82. https://doi.org/10.29040/ijcis.v3i2.72

OWASP. (2021). *OWASP Top 10: 2021. OWASP.* Retrieved July 26, 2025, from https://owasp.org/Top10/

Prasetyo, S. E., & Hassanah, N. (2021). Analisis keamanan website Universitas Internasional Batam menggunakan metode ISSAF. *Jurnal Ilmiah Informatika, 9*(2), 82–86. https://doi.org/10.63866/jpst.v1i2.76

Satria, B. N., Wicaksono, S. R., & Setiawan, R. (2024). Integrating OWASP and MOORA for comprehensive vulnerability assessment and prioritization in educational web applications. *Proceedings of the National Conference on Electrical Engineering, Informatics, Industrial Technology, and Creative Media*, 4(1), 1154–1162

Yükseköğretim Kurulu. (2025). *Yükseköğretim bilgi yönetim sistemi*. Retrieved August 23, 2025, from https://istatistik.yok.gov.tr/