examplewebsite48.com

Firewall activity

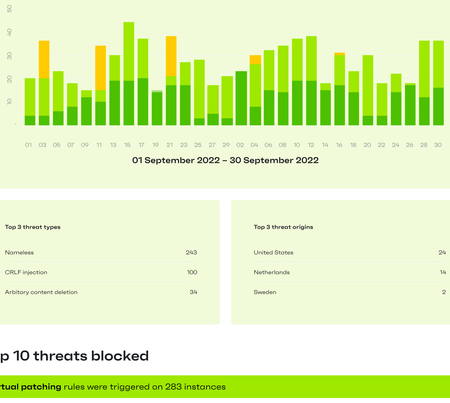
There are numerous rules applied at any given time however active attacks may not be always happening. See full log via dashboard.

450
Total number of threats blocked

50
Blocked by virtual patches
These rules protect the website from attacks against specific software.

200
Blocked by firewall
Universal web security ruleset to protects against a number of attacks.

137
Blocked by other rules
Custom firewall rules can be implemented as an extra security layer.



01 September 2022 – 30 September 2022

Top 3 threat types

Nameless	243
CRLF injection	100
Arbitary content deletion	34

Top 3 threat origins

United States	24
Netherlands	14
Sweden	2

Top 10 threats blocked

Virtual patching rules were triggered on 283 instances

Firewall ruleset to protect the website from attacks targeting specific software.

Top 10 rules triggered for	Version	Action	Instances
[redacted]	18.003	BLOCK	23
[redacted]	12.1	BLOCK	21
[redacted]	1.02	BLOCK	19
[redacted]	18.003	BLOCK	17
[redacted]	Set1	BLOCK	17
[redacted]	4.39	BLOCK	15
[redacted]	12.1	BLOCK	11
[redacted]	3.0	BLOCK	9
[redacted]	Set2	BLOCK	7
[redacted]	1.02	BLOCK	5

Firewall rules were triggered on 159 instances

Universal web security ruleset to protects your sites from a significant number of attacks such as SQL injection, cross site scripting, local file inclusion and more.

Top 10 rules triggered for	Module	Action	Instances
Stop self-executing JavaScript functions	OWASP	BLOCK	23
Block basic directory traversal	OWASP	BLOCK	21
Stop self-executing JavaScript functions	OWASP	BLOCK	19
Block Transposh WordPress Translation Vulnerability	BOTS	BLOCK	17
Block basic directory traversal	SMTHNGNW	BLOCK	17
Stop plugin enumeration attempts	OWASP	BLOCK	15
Block basic directory traversal	BOTS	BLOCK	11
Block Transposh WordPress Translation Vulnerability	SMTHNGNW	BLOCK	9
Stop self-executing JavaScript functions	OWASP	BLOCK	7
Stop plugin enumeration attempts	BOTS	BLOCK	5

Custom rules were triggered on 137 instances

Custom firewall rules implemented as an extra layer to protect the website. See documentation on writing custom firewall rules.

Top 10 rules triggered for	Module	Action	Instances
Stop self-executing JavaScript functions	OWASP	BLOCK	23
Block basic directory traversal	OWASP	BLOCK	21
Stop self-executing JavaScript functions	OWASP	BLOCK	19
Block Transposh WordPress Translation Vulnerability	BOTS	BLOCK	17
Block basic directory traversal	SMTHNGNW	BLOCK	17
Stop plugin enumeration attempts	OWASP	BLOCK	15
Block basic directory traversal	BOTS	BLOCK	11
Block Transposh WordPress Translation Vulnerability	SMTHNGNW	BLOCK	9
Stop self-executing JavaScript functions	OWASP	BLOCK	7
Stop plugin enumeration attempts	BOTS	BLOCK	5

2163 instances triggered in total for www.examplewebsite48.com.

4 suggested actions

Action	Software	Reason
Update	[redacted]	Vulnerable. Update to remove vulnerability.
Replace	[redacted]	Delete and install alternative software.
Update	[redacted]	A newer version is available.
Delete	[redacted]	Deactivated software can still be exploited.

Security vulnerabilities

2 low · 1 medium · 1 high · 0 critical

A security vulnerability is a weakness that can be exploited by an attacker with malicious intent. Resolved = vulnerability is no longer present, Mitigated = protected by virtual patches or firewall rules, Not mitigated = no protection needed or available, Exploited = known to be exploited on the wild

3 vulnerabilities not resolved

Vulnerability	Severity	Details	Date & time identified	Status
Remote code execution (RCE) [redacted] Successful attackers could redirect visitors and customers to a malicious website.	Medium CVSS 5.1	View ›	12 October 2022 NEW 18:04:20	Exploited Not mitigated
Remote code execution (RCE) [redacted] Successful attackers could redirect visitors and customers to a malicious website.	High CVSS 6.1	View ›	5 July 2022 18:04:20	Exploited Mitigated
Remote code execution (RCE) [redacted] Successful attackers could redirect visitors and customers to a malicious website.	Low CVSS 5.1	View ›	23 November 2021 18:04:20	Mitigated

Software overview

2 core · 19 plugins · 3 themes

This is a list of all the software installed on the website.

4 Vulnerable
Some software can have multiple vulnerabilities at once.

1 Likely abandoned
Delete and replace ASAP as no support seems discontinued.

4 Outdated
Always back up to auto-update ONLY vulnerable plugins.

2 Deactivated
Advised to delete as installed software can still be targeted.

14 Up to date
Check forms and dynamic content after updating.

Software		Version	Date & time
Plugin	[redacted]	4.48	Update available Vulnerable
Plugin	[redacted]	25.3b	Up to date Likely abandoned
Plugin	[redacted]	1.02	Up to date Deactivated Vulnerable
Plugin	[redacted]	2.2	Up to date Deactivated Mitigated Vulnerable
Plugin	[redacted]	58.2.2	Up to date Mitigated Vulnerable
Core	WordPress	7.2	Up to date Vulnerable
Plugin	[redacted]	10.01b	Up to date Vulnerable
Theme	[redacted]	1.1.12	Update available
Plugin	[redacted]	58.2.2-3	Up to date
Plugin	[redacted]	2.2	Up to date
Plugin	[redacted]	10.01b	Up to date
Theme	[redacted]	58.2.2	Up to date
Core	WordPress	7.2	Up to date
Plugin	[redacted]	58.2.2-3	Up to date
Plugin	[redacted]	1.02	Up to date
Plugin	[redacted]	58.2.2-3	Up to date
Plugin	[redacted]	2.2	Up to date
Plugin	[redacted]	10.01b	Up to date
Plugin	[redacted]	58.2.2	Up to date
Plugin	[redacted]	1.02	Up to date