How to Mitigate an L7 Attack

Sometimes the goal of a cyber attack isn't to slow down or make a website unavailable, but to compromise it. Such attacks include SQL and command injections, Cross-Site Scripting, Cross-Site Request Forgery, Path / Directory Traversal, File Inclusion, as well as known vulnerability exploits and vulnerability scanning.

These attacks target the web application, rather than the server, so they are handled at L7 by the WAF (Web Application Firewall).

Identifying the Attack

Attacks aiming to compromise websites tend to target dynamic pages and endpoints (login pages, search and forms), authentication-related resources, file-handling endpoints and other sensitive paths, such as **/admin**, **/config** and similar.

Spikes of activity targeting potentially sensitive URLs are signs of such an attack. Logs will also often show errors, as attackers are probing for targets.

Example

Let's examine a specific log file for the **(www.)bank.cz** domain, specifically the Top 10 URLs.

b2b@wedos.com
WEDOS.com
WEDOS Group SA
7 Rue Robert Stümper
L - 2557 Luxembourg
Luxembourg
EU

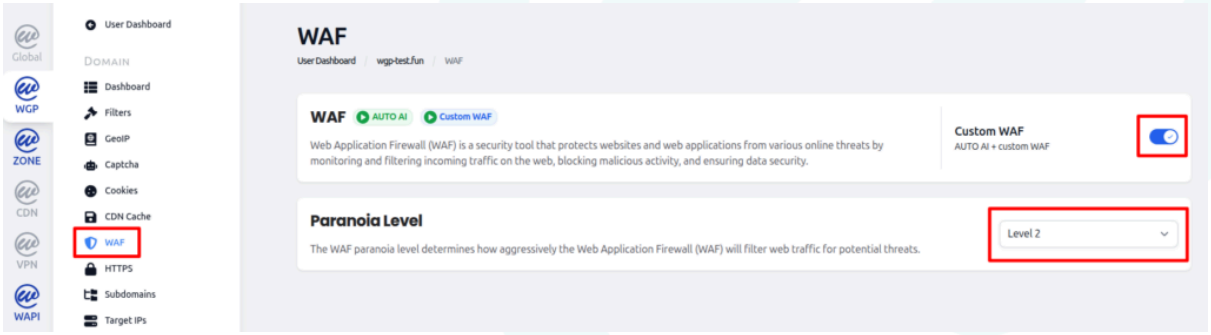
bank.cz + www.bank.cz top 10 URL's

Request Path	Count	Request Host
/captcha_verify?/wp-login.php	199	bank.cz
/robots.txt	102	bank.cz
/robots.txt	31	www.bank.cz
/captcha_verify?/robots.txt	85	bank.cz
/captcha_verify?/robots.txt	36	www.bank.cz
/xmlrpc.php	66	bank.cz
/favicon.ico	20	www.bank.cz
/favicon.ico	10	bank.cz
/captcha_verify?//2019/wp-includes/...	7	bank.cz
/captcha_verify?//blog/wp-includes/...	7	bank.cz

We notice frequent attempts to access **/captcha-verify/?wp-login.php** and **xmlrpc.php**. These may include brute-force login attempts, likely prevented by the captcha page, as well as attempts to exploit content, core or plugin vulnerabilities.

Manual Attack Mitigation

The recommended first response is to increase the WAF paranoia level. This will enforce strict traffic checks and block any suspicious activity, returning a 456 error whenever the firewall blocks such a request.



These errors should then appear in the Anomalies in Location table in Grafana. After increasing the paranoia level, monitor the anomalies in Grafana, as well as the website function and performance in general.

Anomalies in location: All

Timestamp	Location	Client IP	Code	Request Host	Method	Request Path	Useragent
2026-02-03 01:16:46	ac40-Sevilla	149.50.97.162	456	bank.cz	HEAD	/	Mozilla/5.0 (compatible; ...
2026-02-03 00:56:29	ac113-Paris	85.203.15.114	456	bank.cz	GET	/ALFA_DATA/alfacgiapi/p...	Mozilla/5.0 (Windows NT ...
2026-02-02 14:59:43	ac36-Chisinau	91.92.241.108	456	bank.cz	GET	/.env	Mozilla/5.0 (X11; Linux x8...
2026-02-02 13:42:17	ac32-Manchester	51.89.129.206	456	bank.cz	GET	/	Mozilla/5.0 (compatible; A...
2026-02-02 12:47:57	ac41-Alicante	172.190.142.176	456	bank.cz	GET	//wp-includes/css/about....	
2026-02-02 12:47:47	ac41-Alicante	172.190.142.176	456	bank.cz	GET	//wp-content/uploads/ind...	
2026-02-02 12:47:41	ac41-Alicante	172.190.142.176	456	bank.cz	GET	//wp-includes/ID3/index....	
2026-02-02 12:47:40	ac41-Alicante	172.190.142.176	456	bank.cz	GET	//wp-includes/customize/...	
2026-02-02 12:47:39	ac41-Alicante	172.190.142.176	456	bank.cz	GET	//wp-includes/ID3/index....	
2026-02-02 12:47:38	ac41-Alicante	172.190.142.176	456	bank.cz	GET	//wp-includes/css/about....	

1 2 3 1 - 10 of 28 rows

Resolution

If the site is running satisfactorily at the WAF paranoia level 2, consider leaving it set at that level indefinitely.

If either level of WEDOS.protection WAF causes the website to not function correctly, or if data decryption on the proxy is a security or performance concern, you can always enable HTTPS Pass Thru mode and set up your own Firewall or other security solution on your server.