# Website Vulnerability Scanner Report (Light)

Unlock the full capabilities of this scanner

**See what the DEEP scanner can do**

Perform in-depth website scanning and discover high risk vulnerabilities.

| Testing areas | Light scan | Deep scan |
|---|---|---|
| Website fingerprinting | ✓ | ✓ |
| Version-based vulnerability detection | ✓ | ✓ |
| Common configuration issues | ✓ | ✓ |
| SQL injection | — | ✓ |
| Cross-Site Scripting | — | ✓ |
| Local/Remote File Inclusion | — | ✓ |
| Remote command execution | — | ✓ |
| Discovery of sensitive files | — | ✓ |

✓ **https://qrshot.kz/**

Target added due to a redirect from https://qrshot.kz

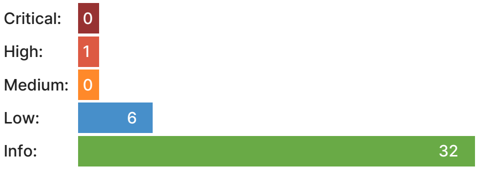
The Light Website Scanner didn't check for critical issues like SQLi, XSS, Command Injection, XXE, etc. Upgrade to run Deep scans with 40+ tests and detect more vulnerabilities.

## Summary

**Overall risk level:**

High

**Risk ratings:**



**Scan information:**

| | |
|---|---|
| Start time: | Dec 08, 2025 / 11:10:56 UTC+02 |
| Finish time: | Dec 08, 2025 / 11:11:35 UTC+02 |
| Scan duration: | 39 sec |
| Tests performed: | 39/39 |
| Scan status: | Finished |

## Findings

### Vulnerabilities found for nginx 1.18.0

port 443/tcp

| CVE | CVSS | EPSS Score | EPSS Percentile | Summary |
|---|---|---|---|---|
| CVE-2021-23017 | 7.7 | 0.73166 | 0.98724 | A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact. |

| | | | | |
|---|---|---|---|---|
| CVE-2023-44487 | 7.5 | 0.94419 | 0.99977 | The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023. |
| CVE-2021-3618 | 7.4 | 0.00492 | 0.64771 | ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer. |
| CVE-2022-41742 | 7.1 | 0.00082 | 0.24412 | NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted audio or video file. The issue affects only NGINX products that are built with the module ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. |
| CVE-2022-41741 | 7.0 | 0.00968 | 0.75891 | NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module. |

Details

**Risk description:**
The risk is that an attacker could search for an appropriate exploit (or create one himself) for any of these vulnerabilities and use it to attack the system.

Since the vulnerabilities were discovered using only version-based testing, the risk level for this finding will not exceed 'high' severity. Critical risks will be assigned to vulnerabilities identified through accurate active testing methods.

**Recommendation:**
In order to eliminate the risk of these vulnerabilities, we recommend you check the installed software version and upgrade to the latest version.

**Classification:**
EPSS score : 0.94419
EPSS percentile : 0.99977
CISA KEV: False
CVE : CVE-2021-23017, CVE-2023-44487, CVE-2021-3618, CVE-2022-41742, CVE-2022-41741
CVSS V3 : 7.7
CWE : CWE-1035

## Missing security header: Strict-Transport-Security

CONFIRMED

port 443/tcp

| URL | Evidence |
|---|---|
| https://qrshot.kz/ | Response headers do not include the HTTP Strict-Transport-Security header<br>Request / Response |

Details

**Risk description:**
The risk is that lack of this header permits an attacker to force a victim user to initiate a clear-text HTTP connection to the server, thus opening the possibility to eavesdrop on the network traffic and extract sensitive information (e.g. session cookies).

**Recommendation:**
The Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

```
Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]
```

The parameter `max-age` gives the time frame for requirement of HTTPS in seconds and should be chosen quite high, e.g. several months. A value below 7776000 is considered as too low by this scanner check.
The flag `includeSubDomains` defines that the policy applies also for sub domains of the sender of the response.

**Classification:**

CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

## Missing security header: Referrer-Policy

CONFIRMED

port 443/tcp

| URL | Evidence |
|---|---|
| https://qrshot.kz/ | Response headers do not include the Referrer-Policy HTTP security header as well as the <meta> tag with name 'referrer' is not present in the response.<br>Request / Response |

Details

**Risk description:**
The risk is that if a user visits a web page (e.g. "http://example.com/pricing/") and clicks on a link from that page going to e.g. "https://www.google.com", the browser will send to Google the full originating URL in the `Referer` header, assuming the Referrer-Policy header is not set. The originating URL could be considered sensitive information and it could be used for user tracking.

**Recommendation:**
The Referrer-Policy header should be configured on the server side to avoid user tracking and inadvertent information leakage. The value `no-referrer` of this header instructs the browser to omit the Referer header entirely.

**References:**
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

**Classification:**
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

## Missing security header: Content-Security-Policy

CONFIRMED

port 443/tcp

| URL | Evidence |
|---|---|
| https://qrshot.kz/ | Response does not include the HTTP Content-Security-Policy security header or meta tag<br>Request / Response |

Details

**Risk description:**
The risk is that if the target application is vulnerable to XSS, lack of this header makes it easily exploitable by attackers.

**Recommendation:**
Configure the Content-Security-Header to be sent with each HTTP response in order to apply the specific policies needed by the application.

**References:**
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

**Classification:**
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

## Missing security header: X-Content-Type-Options

CONFIRMED

port 443/tcp

| URL | Evidence |
|---|---|
| https://qrshot.kz/ | Response headers do not include the X-Content-Type-Options HTTP security header<br>Request / Response |

Details

**Risk description:**
The risk is that lack of this header could make possible attacks such as Cross-Site Scripting or phishing in Internet Explorer browsers.

**Recommendation:**
We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff`.

**References:**
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

**Classification:**
CWE : CWE-693
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

## Password Submitted in URL

port 443/tcp

UNCONFIRMED

| URL | Method | Parameters | Evidence |
|---|---|---|---|
| https://qrshot.kz/ | GET | **Headers:**<br>User-Agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 | The following form sends inputs of type password plainly in the URL:<br>`<form id="landingAuthForm">`<br>`<input type="text" name="username" placeholder="ÐÐ¾Ð³Ð¸Ð½" required>`<br>`<input type="password" name="password" placeholder="ÐÐ°ÑÐ¾Ð»Ñ" required>`<br>`<div class="auth-message" aria-live="polite"></div>`<br>`<button type="submit">ÐÐ¾Ð¹ÑÐ¸</button>`<br>`</form>`<br>Request / Response |

Details

**Risk description:**
Passwords submitted in URLs have a higher chance of being leaked. The main reason is that URLs can be leaked in browser cross-site requests via the Referer header. Additionally, URLs are usually stored in all kinds of logs. If any access or error logs of the server were publicly accessible, an attacker could also harvest password from it.

**Recommendation:**
You should submit passwords using POST rather than GET. This way sensitive data won't be shared to other locations via URLs.

**References:**
https://developer.mozilla.org/en-US/docs/Web/Security/Referer_header:_privacy_and_security_concerns

**Classification:**
OWASP Top 10 - 2021 : A4 - Insecure Design

## Server software and technology found

port 443/tcp

UNCONFIRMED

| Software / Version | Category |
|---|---|
| cdnjs | CDN |
| Font Awesome 6.4.0 | Font scripts |
| Google Font API | Font scripts |
| Nginx 1.18.0 | Web servers, Reverse proxies |
| Cloudflare | CDN |
| reCAPTCHA | Security |
| Ubuntu | Operating systems |

⌄ Details

**Risk description:**
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

**Recommendation:**
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

**References:**
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html

**Classification:**
OWASP Top 10 - 2017 : A6 - Security Misconfiguration
OWASP Top 10 - 2021 : A5 - Security Misconfiguration

CONFIRMED

## Nothing was found for client access policies.

## Nothing was found for robots.txt file.

## Nothing was found for absence of the security.txt file.

## Nothing was found for use of untrusted certificates.

## Nothing was found for enabled HTTP debug methods.

## Nothing was found for enabled HTTP OPTIONS method.

## Nothing was found for secure communication.

## Nothing was found for directory listing.

## Nothing was found for passwords submitted unencrypted.

## Nothing was found for error messages.

## Nothing was found for debug messages.

## Nothing was found for code comments.

## Nothing was found for domain too loose set for cookies.

## Nothing was found for mixed content between HTTP and HTTPS.

Nothing was found for cross domain file inclusion.

Nothing was found for internal error code.

Nothing was found for HttpOnly flag of cookie.

Nothing was found for Secure flag of cookie.

Nothing was found for login interfaces.

Nothing was found for secure password submission.

Nothing was found for sensitive data.

Nothing was found for unsafe HTTP header Content Security Policy.

Nothing was found for OpenAPI files.

Nothing was found for file upload.

Nothing was found for SQL statement in request parameter.

Nothing was found for password returned in later response.

Nothing was found for Path Disclosure.

Nothing was found for Session Token in URL.

Nothing was found for API endpoints.

Nothing was found for emails.

Nothing was found for missing HTTP header - Rate Limit.

## Scan coverage information

### List of tests performed (39/39)

- ✓ Test connection
- ✓ Scanned for passwords submitted in URLs
- ✓ Scanned for missing HTTP header - Strict-Transport-Security
- ✓ Scanned for missing HTTP header - Referrer
- ✓ Scanned for missing HTTP header - Content Security Policy
- ✓ Scanned for missing HTTP header - X-Content-Type-Options
- ✓ Scanned for website technologies
- ✓ Scanned for version-based vulnerabilities of server-side software
- ✓ Scanned for client access policies
- ✓ Scanned for robots.txt file
- ✓ Scanned for absence of the security.txt file
- ✓ Scanned for use of untrusted certificates
- ✓ Scanned for enabled HTTP debug methods
- ✓ Scanned for enabled HTTP OPTIONS method
- ✓ Scanned for secure communication
- ✓ Scanned for directory listing
- ✓ Scanned for passwords submitted unencrypted
- ✓ Scanned for error messages
- ✓ Scanned for debug messages
- ✓ Scanned for code comments
- ✓ Scanned for domain too loose set for cookies
- ✓ Scanned for mixed content between HTTP and HTTPS
- ✓ Scanned for cross domain file inclusion
- ✓ Scanned for internal error code
- ✓ Scanned for HttpOnly flag of cookie
- ✓ Scanned for Secure flag of cookie
- ✓ Scanned for login interfaces
- ✓ Scanned for secure password submission
- ✓ Scanned for sensitive data
- ✓ Scanned for unsafe HTTP header Content Security Policy
- ✓ Scanned for OpenAPI files
- ✓ Scanned for file upload
- ✓ Scanned for SQL statement in request parameter
- ✓ Scanned for password returned in later response
- ✓ Scanned for Path Disclosure
- ✓ Scanned for Session Token in URL
- ✓ Scanned for API endpoints
- ✓ Scanned for emails
- ✓ Scanned for missing HTTP header - Rate Limit

### Scan parameters

| | |
|---|---|
| target: | https://qrshot.kz/ |
| scan_type: | Light |
| authentication: | False |

### Scan stats

| | |
|---|---|
| Unique Injection Points Detected: | 8 |
| URLs spidered: | 18 |
| Total number of HTTP requests: | 30 |
| Average time until a response was received: | 123ms |