

# Website Vulnerability Scanner Report

✓ <https://denikledec.cz/>

## Summary

### Overall risk level:

Medium

### Risk ratings:



### Scan information:

Start time: Nov 19, 2023 / 23:32:10  
 Finish time: Nov 19, 2023 / 23:32:42  
 Scan duration: 32 sec  
 Tests performed: 19/19  
 Scan status: **Finished**

## Findings

### 🚩 Insecure cookie setting: missing HttpOnly flag

CONFIRMED

URL	Cookie Name	Evidence
<a href="https://denikledec.cz/">https://denikledec.cz/</a>	ABc_VrvonpdNe-fh, qlguJ-rYIDRGPhH, saFPqVG, wassup7897c33c988ad8fefb4a045b28355dbe	The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag: Set-Cookie: ABc_VrvonpdNe-fh=wyViBP.5W_dQ6Htl Set-Cookie: qlguJ-rYIDRGPhH=_L5dOmyX7ehjw8t Set-Cookie: saFPqVG=6JwgBkl Set-Cookie: wassup7897c33c988ad8fefb4a045b28355dbe=MGJfMzQyNjRmMGM5MDc3NWNjNDQ2NWlZnzk5ZWQ2ODE3ZjUjzE3MDA0MzlyMzMjlyMjMjEyLjcxLjI1NS4xNTIjI3NjYW54NS5wZW50ZXN0LXRvb2xzLmNvbSMj

#### Details

#### Risk description:

A cookie has been set without the **HttpOnly** flag, which means that it can be accessed by the JavaScript code running inside the web page. If an attacker manages to inject malicious JavaScript code on the page (e.g. by using an XSS attack) then the cookie will be accessible and it can be transmitted to another site. In case of a session cookie, this could lead to session hijacking.

#### Recommendation:

Ensure that the HttpOnly flag is set for all cookies.

#### References:

<https://owasp.org/www-community/HttpOnly>

#### Classification:

CWE : [CWE-1004](#)  
 OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)  
 OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

### 🚩 Robots.txt file found

CONFIRMED

URL
<a href="https://denikledec.cz/robots.txt">https://denikledec.cz/robots.txt</a>

#### Details

#### Risk description:

There is no particular security risk in having a robots.txt file. However, this file is often misused by website administrators to try to hide some web pages from the users. This should not be considered a security measure because these URLs can be easily read directly from the robots.txt file.

**Recommendation:**

We recommend you to manually review the entries from robots.txt and remove the ones which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).


**References:**

<https://www.theregister.co.uk/2015/05/19/robotstxt/>























**Classification:**

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

 **Server software and technology found**

UNCONFIRMED ⓘ

Software / Version	Category
 PHP	Programming languages
 WordPress	CMS, Blogs
 MySQL	Databases
 Cloudflare	CDN
 RSS	Miscellaneous
 Open Graph	Miscellaneous
 HTTP/3	Miscellaneous
 Facebook Login	Authentication
 ThemeGrill ColorMag	WordPress themes
 ColorMag 3.0.7	WordPress themes
 AddToAny Share Buttons 1.1	WordPress plugins
 Contact Form 7 5.8.3	WordPress plugins
 Yoast SEO 21.5	SEO, WordPress plugins
 AddToAny	Widgets
 Complianz 6.5.5	A/B Testing, Cookie compliance, WordPress plugins
 Font Awesome	Font scripts
 Twitter Emoji (Twemoji) 14.0.2	Font scripts
 jQuery Migrate 3.4.1	JavaScript libraries
 jQuery 3.7.1	JavaScript libraries
 reCAPTCHA	Security
 Priority Hints	Performance
 HSTS	Security

▼ Details

**Risk description:**

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](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 - 2013 : A5 - Security Misconfiguration

OWASP Top 10 - 2017 : A6 - Security Misconfiguration

---

 Website is accessible.

 Nothing was found for vulnerabilities of server-side software.

---

 Nothing was found for client access policies.

---

 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 secure communication.

---

 Nothing was found for directory listing.

---

 Nothing was found for missing HTTP header - Strict-Transport-Security.

---

 Nothing was found for missing HTTP header - Content Security Policy.

---

 Nothing was found for missing HTTP header - X-Frame-Options.

---

 Nothing was found for missing HTTP header - X-Content-Type-Options.

---

 Nothing was found for missing HTTP header - Referrer.

---

 Nothing was found for domain too loose set for cookies.

 Nothing was found for Secure flag of cookie.

---

## Scan coverage information

---

### List of tests performed (19/19)

- ✓ Checking for website accessibility...
- ✓ Checking for HttpOnly flag of cookie...
- ✓ Checking for website technologies...
- ✓ Checking for vulnerabilities of server-side software...
- ✓ Checking for client access policies...
- ✓ Checking for robots.txt file...
- ✓ Checking for absence of the security.txt file...
- ✓ Checking for use of untrusted certificates...
- ✓ Checking for enabled HTTP debug methods...
- ✓ Checking for secure communication...
- ✓ Checking for directory listing...
- ✓ Checking for missing HTTP header - Strict-Transport-Security...
- ✓ Checking for missing HTTP header - Content Security Policy...
- ✓ Checking for missing HTTP header - X-Frame-Options...
- ✓ Checking for missing HTTP header - X-Content-Type-Options...
- ✓ Checking for missing HTTP header - Referrer...
- ✓ Checking for domain too loose set for cookies...
- ✓ Checking for Secure flag of cookie...
- ✓ Checking for unsafe HTTP header Content Security Policy...

### Scan parameters

Target: `https://denikledec.cz/`  
Scan type: `Light`  
Authentication: `False`

### Scan stats

Unique Injection Points Detected:	200
URLs spidered:	5
Total number of HTTP requests:	13
Average time until a response was received:	404ms

---