# PakWheels Scanning Report

Generated with ZAP on Sun 18 Dec 2022, at 21:04:47

## Contents

# About this report

## Report parameters

### Contexts

No contexts were selected, so all contexts were included by default.

### Sites

The following sites were included:

- `https://www.pakwheels.com`

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

### Risk levels

Included: `High`, `Medium`, `Low`, `Informational`

Excluded: None

### Confidence levels

Included: `User Confirmed`, `High`, `Medium`, `Low`

Excluded: User Confirmed, High, Medium, Low, False Positive

# Summaries

## Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

| | | Confidence | | | | |
|---|---|---|---|---|---|---|
| | | User Confirmed | High | Medium | Low | Total |
| | High | 0<br>(0.0%) | 0<br>(0.0%) | 0<br>(0.0%) | 0<br>(0.0%) | 0<br>(0.0%) |
| | Medium | 0<br>(0.0%) | 1<br>(7.1%) | 2<br>(14.3%) | 1<br>(7.1%) | 4<br>(28.6%) |
| Risk | Low | 0<br>(0.0%) | 1<br>(7.1%) | 4<br>(28.6%) | 1<br>(7.1%) | 6<br>(42.9%) |
| | Informational | 0<br>(0.0%) | 0<br>(0.0%) | 1<br>(7.1%) | 3<br>(21.4%) | 4<br>(28.6%) |
| | Total | 0<br>(0.0%) | 2<br>(14.3%) | 7<br>(50.0%) | 5<br>(35.7%) | 14<br>(100%) |

## Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

| | | Risk | | | |
|---|---|---|---|---|---|
| | | High<br>(= High) | Medium<br>(>= Medium) | Low<br>(>= Low) | Informational<br>(>= Informational) |
| Site | https://www.pakwheels.com | 0<br>(0) | 4<br>(4) | 6<br>(10) | 4<br>(14) |

## Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

| Alert type | Risk | Count |
|---|---|---|
| Absence of Anti-CSRF Tokens | Medium | 1287<br>(9,192.9%) |
| Content Security Policy (CSP) Header Not Set | Medium | 365<br>(2,607.1%) |
| Cross-Domain Misconfiguration | Medium | 413<br>(2,950.0%) |
| Missing Anti-clickjacking Header | Medium | 346<br>(2,471.4%) |
| Total | | 14 |

| Alert type | Risk | Count |
|---|---|---|
| Application Error Disclosure | Low | 3<br>(21.4%) |
| Cookie without SameSite Attribute | Low | 399<br>(2,850.0%) |
| Cross-Domain JavaScript Source File Inclusion | Low | 1998<br>(14,271.4%) |
| Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) | Low | 407<br>(2,907.1%) |
| Strict-Transport-Security Header Not Set | Low | 1<br>(7.1%) |
| Timestamp Disclosure - Unix | Low | 2262<br>(16,157.1%) |
| Information Disclosure - Suspicious Comments | Informational | 1140<br>(8,142.9%) |
| Modern Web Application | Informational | 354<br>(2,528.6%) |
| Re-examine Cache-control Directives | Informational | 312<br>(2,228.6%) |
| User Controllable HTML Element Attribute (Potential XSS) | Informational | 13<br>(92.9%) |
| Total | | 14 |

# Alerts

### Risk=Medium, Confidence=High (1)

#### https://www.pakwheels.com (1)

#### Content Security Policy (CSP) Header Not Set (1)

▶ GET https://www.pakwheels.com/

### Risk=Medium, Confidence=Medium (2)

#### https://www.pakwheels.com (2)

#### Cross-Domain Misconfiguration (1)

▶ GET https://www.pakwheels.com/robots.txt

#### Missing Anti-clickjacking Header (1)

▶ GET https://www.pakwheels.com/

### Risk=Medium, Confidence=Low (1)

#### https://www.pakwheels.com (1)

#### Absence of Anti-CSRF Tokens (1)

▶ GET https://www.pakwheels.com/

### Risk=Low, Confidence=High (1)

#### https://www.pakwheels.com (1)

#### Strict-Transport-Security Header Not Set (1)

▶ GET https://www.pakwheels.com/accessories-spare-parts/united/632418

### Risk=Low, Confidence=Medium (4)

#### https://www.pakwheels.com (4)

#### Application Error Disclosure (1)

▶ GET https://www.pakwheels.com/fetch_used_cars_featured_ads

#### Cookie without SameSite Attribute (1)

▶ GET https://www.pakwheels.com/*.js

#### Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.pakwheels.com/

#### Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

▶ GET https://www.pakwheels.com/*.js

### Risk=Low, Confidence=Low (1)

#### https://www.pakwheels.com (1)

#### Timestamp Disclosure - Unix (1)

▶ GET https://www.pakwheels.com/

### Risk=Informational, Confidence=Medium (1)

### https://www.pakwheels.com (1)

#### Modern Web Application (1)

▶ GET https://www.pakwheels.com/

### Risk=Informational, Confidence=Low (3)

### https://www.pakwheels.com (3)

#### Information Disclosure - Suspicious Comments (1)

▶ GET https://www.pakwheels.com/

#### Re-examine Cache-control Directives (1)

▶ GET https://www.pakwheels.com/robots.txt

#### User Controllable HTML Element Attribute (Potential XSS) (1)

▶ GET https://www.pakwheels.com/used-cars/search/-/featured_1/?nf=true

# Appendix

## Alert types

This section contains additional information on the types of alerts in the report.

### Absence of Anti-CSRF Tokens

| | |
|---|---|
| Source | raised by a passive scanner (Absence of Anti-CSRF Tokens) |
| CWE ID | 352 |
| WASC ID | 9 |
| Reference | ▪ http://projects.webappsec.org/Cross-Site-Request-Forgery<br>▪ http://cwe.mitre.org/data/definitions/352.html |

### Content Security Policy (CSP) Header Not Set

| | |
|---|---|
| Source | raised by a passive scanner (Content Security Policy (CSP) Header Not Set) |
| CWE ID | 693 |
| WASC ID | 15 |
| Reference | ▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy<br>▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html<br>▪ http://www.w3.org/TR/CSP/<br>▪ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html<br>▪ http://www.html5rocks.com/en/tutorials/security/content-security-policy/ |

- http://caniuse.com/#feat=contentsecuritypolicy
- http://content-security-policy.com/

### Cross-Domain Misconfiguration

| | |
|---|---|
| Source | raised by a passive scanner (Cross-Domain Misconfiguration) |
| CWE ID | 264 |
| WASC ID | 14 |
| Reference | - https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy |

### Missing Anti-clickjacking Header

| | |
|---|---|
| Source | raised by a passive scanner (Anti-clickjacking Header) |
| CWE ID | 1021 |
| WASC ID | 15 |
| Reference | - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options |

### Application Error Disclosure

| | |
|---|---|
| Source | raised by a passive scanner (Application Error Disclosure) |
| CWE ID | 200 |

| | |
|---|---|
| WASC ID | 13 |

### Cookie without SameSite Attribute

| | |
|---|---|
| Source | raised by a passive scanner (Cookie without SameSite Attribute) |
| CWE ID | 1275 |
| WASC ID | 13 |
| Reference | - https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site |

### Cross-Domain JavaScript Source File Inclusion

| | |
|---|---|
| Source | raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion) |
| CWE ID | 829 |
| WASC ID | 15 |

### Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

| | |
|---|---|
| Source | raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)) |
| CWE ID | 200 |
| WASC ID | 13 |
| Reference | - http://blogs.msdn.com/b/varunm/archive/2013/0 |

4/23/remove-unwanted-http-response-headers.aspx

- http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

### Strict-Transport-Security Header Not Set

| | |
|---|---|
| Source | raised by a passive scanner (Strict-Transport-Security Header) |
| CWE ID | 319 |
| WASC ID | 15 |
| Reference | https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html<br>https://owasp.org/www-community/Security_Headers<br>http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security<br>http://caniuse.com/stricttransportsecurity<br>http://tools.ietf.org/html/rfc6797 |

### Timestamp Disclosure - Unix

| | |
|---|---|
| Source | raised by a passive scanner (Timestamp Disclosure) |
| CWE ID | 200 |

| | |
|---|---|
| WASC ID | 13 |
| Reference | - http://projects.webappsec.org/w/page/13246936/Information%20Leakage |

### Information Disclosure - Suspicious Comments

| | |
|---|---|
| Source | raised by a passive scanner (Information Disclosure - Suspicious Comments) |
| CWE ID | 200 |
| WASC ID | 13 |

### Modern Web Application

| | |
|---|---|
| Source | raised by a passive scanner (Modern Web Application) |

### Re-examine Cache-control Directives

| | |
|---|---|
| Source | raised by a passive scanner (Re-examine Cache-control Directives) |
| CWE ID | 525 |
| WASC ID | 13 |
| Reference | - https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching<br>- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control |

- https://grayduck.mn/2021/09/13/cache-control-recommendations/

### User Controllable HTML Element Attribute (Potential XSS)

| | |
|---|---|
| **Source** | raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS)) |
| **CWE ID** | 20 |
| **WASC ID** | 20 |
| **Reference** | - http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute |