ZAP Scanning Report

Generated with ZAP on Wed 14 Feb 2024, at 13:09:39

ZAP Version: 2.14.0

Contents

- About this report
  - Report parameters
- Summaries
  - Alert counts by risk and confidence
  - Alert counts by site and risk
  - Alert counts by alert type
- Alerts
  - Risk=High, Confidence=Medium (2)

- Risk=Medium, Confidence=High (5)
- Risk=Medium, Confidence=Medium (1)
- Risk=Low, Confidence=High (2)
- Risk=Low, Confidence=Medium (6)
- Risk=Low, Confidence=Low (1)
- Risk=Informational, Confidence=High (3)
- Risk=Informational, Confidence=Medium (3)
- Risk=Informational, Confidence=Low (4)

- Appendix
  - Alert types

About this report

Report parameters

Contexts

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

Sites

The following sites were included:

- https://identity.xero.com
- https://api.xero.com
- https://login.xero.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
Risk	High	0 (0.0%)	0 (0.0%)	2 (7.4%)	0 (0.0%)	2 (7.4%)
	Medium	0 (0.0%)	5 (18.5%)	1 (3.7%)	0 (0.0%)	6 (22.2%)
	Low	0 (0.0%)	2 (7.4%)	6 (22.2%)	1 (3.7%)	9 (33.3%)
	Informational	0 (0.0%)	3 (11.1%)	3 (11.1%)	4 (14.8%)	10 (37.0%)
	Total	0 (0.0%)	10 (37.0%)	12 (44.4%)	5 (18.5%)	27 (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 (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://api.xero.com	1 (1)	0 (1)	0 (1)	0 (1)
	https://login.xero.com	1 (1)	0 (1)	1 (2)	4 (6)

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
Total		27

Alert type	Risk	Count
Generic Padding Oracle	High	1 (3.7%)
SQL Injection - SQLite	High	14 (51.9%)
CSP: Wildcard Directive	Medium	5 (18.5%)
CSP: script-src unsafe-eval	Medium	1 (3.7%)
CSP: script-src unsafe-inline	Medium	1 (3.7%)
CSP: style-src unsafe-inline	Medium	4 (14.8%)
Content Security Policy (CSP) Header Not Set	Medium	1 (3.7%)
Missing Anti-clickjacking Header	Medium	1 (3.7%)
CSP: Notices	Low	5 (18.5%)
Total		27

Alert type	Risk	Count
Cookie No HttpOnly Flag	Low	30 (111.1%)
Cookie Without Secure Flag	Low	11 (40.7%)
Cookie with SameSite Attribute None	Low	13 (48.1%)
Cookie without SameSite Attribute	Low	30 (111.1%)
Cross-Domain JavaScript Source File Inclusion	Low	4 (14.8%)
Strict-Transport-Security Header Not Set	Low	31 (114.8%)
Timestamp Disclosure - Unix	Low	16 (59.3%)
X-Content-Type-Options Header Missing	Low	24 (88.9%)
Authentication Request Identified	Informational	1 (3.7%)
Total		27

Alert type	Risk	Count
CSP: X-Content-Security-Policy	Informational	1 (3.7%)
Information Disclosure - Suspicious Comments	Informational	2 (7.4%)
Loosely Scoped Cookie	Informational	48 (177.8%)
Modern Web Application	Informational	4 (14.8%)
Obsolete Content Security Policy (CSP) Header Found	Informational	1 (3.7%)
Re-examine Cache-control Directives	Informational	25 (92.6%)
Session Management Response Identified	Informational	96 (355.6%)
User Agent Fuzzer	Informational	429 (1,588.9%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	4 (14.8%)
Total		27

Alerts

Risk=High, Confidence=Medium (2)

https://api.xero.com (1)

SQL Injection - SQLite (1)

▶ POST https://api.xero.com/api.xro/2.0/Items

https://login.xero.com (1)

Generic Padding Oracle (1)

▶ GET https://login.xero.com/identity/connect/authorize/callback?client_id=856C66E3C16B41EBB2FF9936E2B1C1E0&redirect_uri=https%3A%2F%2Fmyxero-dev-ed.develop.my.salesforce.com%2Fapex%2FKTXero__XeroOAuthPage&response_type=code&scope=offline_access+openid+profile+email+accounting.transactions+accounting.settings+accounting.contacts+accounting.attachments+files+assets+projects&state=123&consentId=02a7f148-df0b-42f5-b76c-6f0ca8a522w1

Risk=Medium, Confidence=High (5)

Risk=Medium, Confidence=Medium (1)

Risk=Low, Confidence=High (2)

https://login.xero.com (1)

CSP: Notices (1)

▶ GET https://login.xero.com/identity/user/login?ReturnUrl=%2Fidentity%2Fconnect%2Fauthorize%2Fcallback%3Fclient_id%3D856C66E3C16B41EBB2FF9936E2B1C1E0%26redirect_uri%3Dhttps%253A%252F%252Fmyxero-dev-ed.develop.my.salesforce.com%252Fapex%252FKTXero__XeroOAuthPage%26response_type%3Dcode%26scope%3Doffline_access%2520openid%2520profile%2520email%2520accounting.transactions%2520accounting.settings%2520accounting.contacts%2520accounting.attachments%2520files%2520assets%2520projects%26state%3D123

Risk=Low, Confidence=Medium (6)

Risk=Low, Confidence=Low (1)

Risk=Informational, Confidence=High (3)

https://login.xero.com (3)

Authentication Request Identified (1)

▶ POST https://login.xero.com/identity/user/login

CSP: X-Content-Security-Policy (1)

▶ GET https://login.xero.com/identity/connect/authorize?client_id=xero_api_authoriser&redirect_uri=https%3A%2F%2Fauthorize.xero.com%2Fsignin-oidc&response_type=code%20id_token&scope=openid%20profile%20email&response_mode=form_post&nonce=638434862813013816.MzAwZWE5ZTYtNWUxNi00ODFmLThjZTUtZDdmMDQ4NTQ1ZWRkYmZkNjQyNjMtMjgxZi00OTRhLThhYWYtYzU3ODg1OTc3Njll&state=CfDJ8K9lNSh5LjlJj-XwApQde0GZ69sRUNTaLwdZ58PGrzicrN4QCoM_i16nIuycwLm_l_KmwqvJ3TACiIIxjI6AJZS2Ay6fYNwrooZF_COIaI1f6JI_3kUt4AEo5hwWz-lK9Zaa419Agfj1bHzmJOCyTA_GkofmBcuA5JLdMpCrsu8aYIX1bl_VDvvR5mv3JkC7K8-Wnk8ijsr7VM_BuwzGSKAsDXpa8Xed4yQ0tB73NbH4NMaaR2v9AWhrxJcMfMdGCKkDGYrnRi_rcwCnVewYj4cSUgZ7hC7pwDqXhwVFiLkjhjMFMUhYu4WxE6IvD8JnnOEWk6SeqdE6bq_b6bbVRhid1B4N27ZoXIqiGKL0CiLzoX6hzi3RT7_mxwq_FsG_nxVmJdlWgEknSnelPDICv8g3ZTCKIsZSu-lGGjQTkGnXln9PbVTlVCKPXD1Yr3S0BqOzBYMNar0aW7PZwU3sa7tCFXP6CvXMRFwLuEky58zgPnUze6cW8KoLnT_BwPUT4g4_q6-4Y6hN-F9vMirgHZ5NZPApSVfMwQD2E4k2Q8Wg6V2dysza9YvFSoi8DE0Ky3AIXoqCs58AH2-1cV7HDvAMu_bpK9PtaqTQteIMzzwMibE0X9iN_JL5ie3cFatS6aDwihYJdIsoE_u6YQ8yOAo7DHsTy8G9F2hw40s_AGxd34rG-f17ErOWHdg9Iq5i0v8Lvm-Wt8m9TP2xRdF-wy1tyCtYm8GopIaEZ570y9vf2acNETPio8ud7AQiQL4g4HYtt3CkZMsl41Vq4rgmBTyFCowbpd7TPJozRsdMBlBwhm3_gSqJtmFEsPqkwq0ft7DHE8-18a_WkQmjOu-7pbJ9Po5gR9sqI7msZ1SQY33qTRhK7IlDmy07Z9eqvqFT-fvzmQPnuCYtITubfQ2jRrAj0kYdN9W-mGgNbeR5EzK1jHOkT6bRtihCsowoQp7XHVMpA_rbdhx4XfCUURyxAqRlT0-z6EV6hyr_FG-_uoP6&x-client-SKU=ID_NETSTANDARD2_0&x-client-ver=5.5.0.0

Obsolete Content Security Policy (CSP) Header Found (1)

▶ GET https://login.xero.com/identity/connect/authorize?client_id=xero_api_authoriser&redirect_uri=https%3A%2F%2Fauthorize.xero.com%2Fsignin-oidc&response_type=code%20id_token&scope=openid%20profile%20email&response_mode=form_post&nonce=638434862813013816.MzAwZWE5ZTYtNWUxNi00ODFmLThjZTUtZDdmMDQ4NTQ1ZWRkYmZkNjQyNjMtMjgxZi00OTRhLThhYWYtYzU3ODg1OTc3Njll&state=CfDJ8K9lNSh5LjlJj-

XwApQde0GZ69sRUNTaLwdZ58PGrzicrN4QCoM_i16nIuycwLm_l_KmwqvJ3TACiIIxjI6AJZS2Ay6fYNwrooZ
F_COIaI1f6JI_3kUt4AEo5hwWz-
lK9Zaa419Agfj1bHzmJOCyTA_GkofmBcuA5JLdMpCrsu8aYIX1bl_VDvvR5mv3JkC7K8-
Wnk8ijsr7VM_BuwzGSKAsDXpa8Xed4yQ0tB73NbH4NMaaR2v9AWhrxJcMfMdGCKkDGYrnRi_rcwCnVewYj4cS
UgZ7hC7pwDqXhwVFiLkjhjMFMUhYu4WxE6IvD8JnnOEWk6SeqdE6bq_b6bbVRhid1B4N27ZoXIqiGKL0CiLzo
X6hzi3RT7_mxwq_FsG_nxVmJdlWgEknSnelPDICv8g3ZTCKIsZSu-
lGGjQTkGnXln9PbVTlVCKPXD1Yr3S0BqOzBYMNar0aW7PZwU3sa7tCFXP6CvXMRFwLuEky58zgPnUze6cW8Ko
LnT_BwPUT4g4_q6-4Y6hN-
F9vMirgHZ5NZPApSVfMwQD2E4k2Q8Wg6V2dysza9YvFSoi8DE0Ky3AIXoqCs58AH2-
1cV7HDvAMu_bpK9PtaqTQteIMzzwMibE0X9iN_JL5ie3cFatS6aDwihYJdIsoE_u6YQ8yOAo7DHsTy8G9F2hw
40s_AGxd34rG-f17ErOWHdg9Iq5i0v8Lvm-Wt8m9TP2xRdF-
wy1tyCtYm8GopIaEZ570y9vf2acNETPio8ud7AQiQL4g4HYtt3CkZMsl41Vq4rgmBTyFCowbpd7TPJozRsdMB
lBwhm3_gSqJtmFEsPqkwq0ft7DHE8-18a_WkQmjOu-
7pbJ9Po5gR9sqI7msZ1SQY33qTRhK7IlDmy07Z9eqvqFT-fvzmQPnuCYtITubfQ2jRrAj0kYdN9W-
mGgNbeR5EzK1jHOkT6bRtihCsowoQp7XHVMpA_rbdhx4XfCUURyxAqRlT0-z6EV6hyr_FG-_uoP6&x-
client-SKU=ID_NETSTANDARD2_0&x-client-ver=5.5.0.0

Risk=Informational, Confidence=Medium (3)

https://login.xero.com (1)

User Agent Fuzzer (1)

▶ GET https://login.xero.com

Risk=Informational, Confidence=Low (4)

Appendix

Alert types

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

Generic Padding Oracle

Source	raised by an active scanner (Generic Padding Oracle)
CWE ID	209
WASC ID	20
Reference	▪ https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-070 ▪ https://www.mono-project.com/docs/about-mono/vulnerabilities/ ▪ https://bugzilla.redhat.com/show_bug.cgi?id=623799

SQL Injection - SQLite

Source	raised by an active scanner (SQL Injection - SQLite)
CWE ID	89
WASC ID	19
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://developers.google.com/web/fundamentals/security/csp#pol

	icy_applies_to_a_wide_variety_of_resources

CSP: script-src unsafe-eval

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: script-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693

WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp

	▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

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 ▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html ▪ https://www.w3.org/TR/CSP/ ▪ https://w3c.github.io/webappsec-csp/ ▪ https://web.dev/articles/csp ▪ https://caniuse.com/#feat=contentsecuritypolicy ▪ https://content-security-policy.com/

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

CSP: Notices

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://developers.google.com/web/fundamentals/security/csp#pol

	icy applies to a wide variety of resources

Cookie No HttpOnly Flag

Source	raised by a passive scanner (Cookie No HttpOnly Flag)
CWE ID	1004
WASC ID	13
Reference	▪ https://owasp.org/www-community/HttpOnly

Cookie Without Secure Flag

Source	raised by a passive scanner (Cookie Without Secure Flag)
CWE ID	614
WASC ID	13
Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Cookie with SameSite Attribute None

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

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

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 ▪ https://owasp.org/www-community/Security_Headers ▪ https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security ▪ https://caniuse.com/stricttransportsecurity ▪ https://datatracker.ietf.org/doc/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

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	▪ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) ▪ https://owasp.org/www-community/Security_Headers

Authentication Request Identified

Source	raised by a passive scanner (Authentication Request Identified)
Reference	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/

CSP: X-Content-Security-Policy

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ https://www.w3.org/TR/CSP/ ▪ https://caniuse.com/#search=content+security+policy ▪ https://content-security-policy.com/ ▪ https://github.com/HtmlUnit/htmlunit-csp ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Information Disclosure - Suspicious Comments

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

Loosely Scoped Cookie

Source	raised by a passive scanner (Loosely Scoped Cookie)
CWE ID	565
WASC ID	15
Reference	▪ https://tools.ietf.org/html/rfc6265#section-4.1 ▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html ▪ https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

Modern Web Application

Source	raised by a passive scanner (Modern Web Application)

Obsolete Content Security Policy (CSP) Header Found

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 ▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html ▪ https://www.w3.org/TR/CSP/ ▪ https://w3c.github.io/webappsec-csp/ ▪ https://web.dev/articles/csp ▪ https://caniuse.com/#feat=contentsecuritypolicy ▪ https://content-security-policy.com/

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_Managem

	ent_Cheat_Sheet.html#web-content-caching ▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control ▪ https://grayduck.mn/2021/09/13/cache-control-recommendations/

Session Management Response Identified

Source	raised by a passive scanner (Session Management Response Identified)
Reference	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id

User Agent Fuzzer

Source	raised by an active scanner (User Agent Fuzzer)
Reference	▪ https://owasp.org/wstg

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	▪ https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html