Vulnerability test of PMS website:

1. Cross-Domain Misconfiguration :

POST: <https://pms.gplex.com/pms-back/public/api/login>

Solution:

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to

allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

Reference:

https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5\_overly\_permissive\_cors\_policy

##### 2. [X-Frame-Options Header Not Set](file:///C:\Users\Gsl\PMS-ZAP-Report-.html#alert-type-1) (3)

GET https://pms.gplex.com

GET https://pms.gplex.com/

GET https://pms.gplex.com/sitemap.xml

Solution:

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

Reference:

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

##### 3. [Incomplete or No Cache-control Header Set](file:///C:\Users\Gsl\PMS-ZAP-Report-.html#alert-type-2) (6)

1. GET https://pms.gplex.com
2. GET https://pms.gplex.com/
3. GET https://pms.gplex.com/manifest.json
4. GET https://pms.gplex.com/robots.txt
5. GET https://pms.gplex.com/sitemap.xml
6. POST https://pms.gplex.com/pms-back/public/api/login

Solution:

Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate.

Reference:

https://cheatsheetseries.owasp.org/cheatsheets/Session\_Management\_Cheat\_Sheet.html#web-content-caching

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

##### 4. [Timestamp Disclosure - Unix](file:///C:\Users\Gsl\PMS-ZAP-Report-.html#alert-type-3) (19)

1. GET https://pms.gplex.com
2. GET https://pms.gplex.com/
3. GET https://pms.gplex.com/sitemap.xml
4. GET https://pms.gplex.com/static/css/2.3fe668a2.chunk.css
5. GET https://pms.gplex.com/static/css/2.3fe668a2.chunk.css
6. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
7. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
8. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
9. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
10. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
11. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
12. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
13. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
14. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
15. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
16. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
17. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
18. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
19. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js

Solution:

Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Reference:

http://projects.webappsec.org/w/page/13246936/Information%20Leakage

##### 5. [X-Content-Type-Options Header Missing](file:///C:\Users\Gsl\PMS-ZAP-Report-.html#alert-type-4) (15)

1. GET https://pms.gplex.com
2. GET https://pms.gplex.com/
3. GET https://pms.gplex.com/favicon.ico
4. GET https://pms.gplex.com/logo192.png
5. GET https://pms.gplex.com/manifest.json
6. GET https://pms.gplex.com/robots.txt
7. GET https://pms.gplex.com/sitemap.xml
8. GET https://pms.gplex.com/static/css/2.3fe668a2.chunk.css
9. GET https://pms.gplex.com/static/css/main.1c726e1f.chunk.css
10. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
11. GET https://pms.gplex.com/static/js/main.ad379070.chunk.js
12. GET https://pms.gplex.com/static/media/call-center.924fd342.png
13. GET https://pms.gplex.com/static/media/dot.9cd441dc.svg
14. GET https://pms.gplex.com/static/media/gplex-logo.e8b46eb2.png
15. POST https://pms.gplex.com/pms-back/public/api/login

Solution:

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Reference:

http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx

https://owasp.org/www-community/Security\_Headers

##### 6. [Information Disclosure - Suspicious Comments](file:///C:\Users\Gsl\PMS-ZAP-Report-.html#alert-type-5) (2)

1. GET https://pms.gplex.com/static/js/2.6c6e6069.chunk.js
2. GET https://pms.gplex.com/static/js/main.ad379070.chunk.js

Solution:

Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

| **Alert type** | **Risk** | **Count** |
| --- | --- | --- |
| [**Cross-Domain Misconfiguration**](file:///C:\Users\Gsl\PMS-ZAP-Report-.html#alert-type-0) | Medium | 1  (2.2%) |
| [**X-Frame-Options Header Not Set**](file:///C:\Users\Gsl\PMS-ZAP-Report-.html#alert-type-1) | Medium | 3  (6.5%) |
| [**Incomplete or No Cache-control Header Set**](file:///C:\Users\Gsl\PMS-ZAP-Report-.html#alert-type-2) | Low | 6  (13.0%) |
| [**Timestamp Disclosure - Unix**](file:///C:\Users\Gsl\PMS-ZAP-Report-.html#alert-type-3) | Low | 19  (41.3%) |
| [**X-Content-Type-Options Header Missing**](file:///C:\Users\Gsl\PMS-ZAP-Report-.html#alert-type-4) | Low | 15  (32.6%) |
| [**Information Disclosure - Suspicious Comments**](file:///C:\Users\Gsl\PMS-ZAP-Report-.html#alert-type-5) | Informational | 2  (4.3%) |
| **Total** |  | 46 |