detectify

EXECUTIVE SUMMARY

parapp.accept.paqt.io

Scan Started

2023-05-16T11:11:49+00:00

Scan Finished

2023-05-17T04:50:27+00:00

Your findings

Your scan was completed with the following findings discovered.

Critical	High	Medium	Low	Information
0	0	0	0	6

Listed below are your most recent findings, with the most severe listed first. To improve your threat score, prioritise these top issues.

Severity	Issue Type	Times found
INFORMATION	Fingerprinted Software	1
INFORMATION	Deprecated Security Header / X-XSS-Protection	1
INFORMATION	HTML Comments	1
INFORMATION	Discovered Host	1
INFORMATION	Crawled URL's	1
INFORMATION	Service Providers	1

1 Fingerprinted Software

Summary

What does this mean?

Invalid fingerprints may cause a audit to take longer, and the lack of fingerprints may cause Detectify to miss running specific tests.

What can happen?

When Detectify audits an application, it collects various fingerprints that indicate what software is running. These fingerprints then allow Detectify to run specific tests when the time is right.

Found at		CVSS Score
1.1	parapp.accept.paqt.io	0

2 Deprecated Security Header

Summary

What does this mean?

It may be possible to do some client side attacks that was assumed to be mitigated.

What can happen?

We found a security header that is no longer maintained (or supported) by most modern browsers. This may cause you to believe a certain attack vector is mitigated, while it offer no real protection in practice.

Found at	CVSS Score
2.1 https://parapp.accept.paqt.io/	0

3 HTML Comments

Summary

What does this mean?

The snippets of code within comments will remain inactive until you remove the comment brackets. The comments might also contain sensitive information not meant for the public.

What can happen?

HTML comments, used to store temporary code written by the developers, are visible to the public. Read more at our [https://support.detectify.com/support/solutions/articles/48001048959-html-comments|knowledge base].

Found at	CVSS Score
3.1 https://parapp.accept.paqt.io/customers/22/couplings/create	0

4 Discovered Host(s)

Summary

What can happen?

Detectify has found the following hosts. This is in no way a vulnerability, but should be considered an indicator for what has been covered.

Read more [https://support.detectify.com/support/solutions/articles/48001048970-discovered-endpoint|here].

Found at		CVSS Score
4.1	parapp.accept.paqt.io	0

5 Crawled URL's

Summary

What does this mean?

A scan might take too long due to representative content on the application. Vulnerabilities may also be missed if Detectify lack coverage in some area of the application. If you suspect Detectify can perform better, then take a look at the associated CSV.

What can happen?

This finding is generated for debugging purposes. A link is associated with this finding containing a CSV file with all crawled URL's.

Found at		CVSS Score
5.1	parapp.accept.paqt.io	0

6 Service Providers

Summary

What does this mean?

Anyone can retrieve this data. It's only here to serve as an indicator of what vendors have access to.

What can happen?

The listed providers are authorized to host different parts of your infrastructure.

Read more [https://support.detectify.com/support/solutions/articles/48001048980-service-providers|here].

Found at		CVSS Score
6.1	parapp.accept.paqt.io	0