FINCALC

DAST notes

c/o O&M Pensions Solutions
5 Kings Court Newcomen Way,
Colchester
Essex, CO4 9RA

Tel. 01206 803210
Email. sales@fincalc.co.uk

Introduction

At FinCalc, we take the security of our customer data very seriously. As part of our commitment to data security we undertake monthly Dynamic Application Security Testing (DAST) on our FinCalc platform to ensure that it remains as secure as possible. This is in addition to the annual penetration testing that is completed externally.

The internal testing is completed using Burp Suite Pro, you can find more information on their software here.

Both authenticated and unauthenticated tests are completed. Unauthenticated tests are run using no credential access to the application, whereas we run authenticated tests as a Power User (the role with the most permissions available on the application).

While completing these tests we have found that there are false positives, these notes are designed to give a reason as to why these results are false positives and provide our reasoning as to why we have decided to ignore these report issues.

Tests that generate a false positive issue

Test	**N**otes
Cross-origin resource sharing	The majority of external resources used in the FinCalc app are stored locally apart from a few which must be called externally but are managed by an explicit whitelist.
Cross-site scripting (DOM-based)	While on occasion we do pass data to JavaScript it is always sanitised before use.
TLS cookie without secure flag set	A cookie is added by Azure for load balancing which causes this warning.
Cross-origin resource sharing: arbitrary origin trusted	Our CORS policy is managed by both Azure and IIS. We ensure only trusted origins are accepted.
Link manipulation (reflected DOM-based)	Mitigated by having strong input validation and output encoding.
HTTP request smuggling	Issue arises on unauthenticated routes so not at risk to this threat