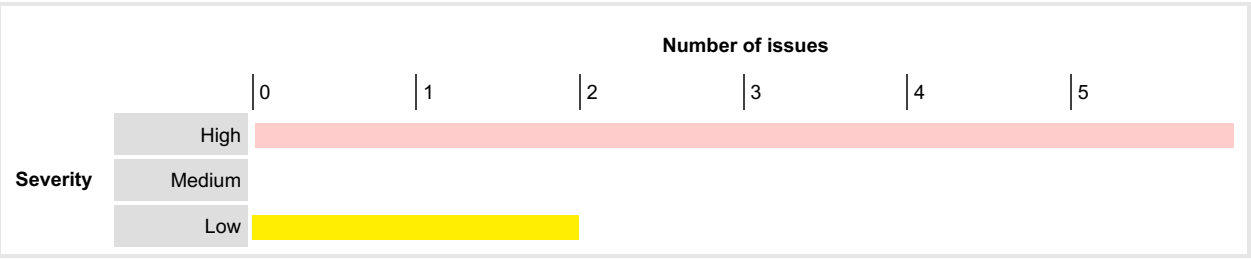
FinCalc DAST Test Report

Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severity as High, Medium, Low or Information. This reflects the likely impact of each issue for a typical organization. Issues are also classified according to confidence as Certain, Firm or Tentative. This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	0	0	6	6
	Medium	0	0	0	0
	Low	2	0	0	2
	Information	15	0	0	15

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issues with a confidence level of Certain, and the bars fade as the confidence level falls.



Contents

1. Cross-site scripting (DOM-based)

There are 6 instances of this issue:

- /cgi-bin/
- /cgi-bin/
- /login
- /login
- /login/request_new_password
- /login/request_new_password

1.1. https://app.fincalc.co.uk/cgi-bin/

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**https://app.fincalc.co.uk**
Path:	**/cgi-bin/**

Static analysis

Data is read from **document.location** and passed to **$()** via the following statements:

- `var url = document.location.toString();`
- `$('.nav-tabs a[href="#' + url.split('#')[1] + '"]').tab('show');`

1.2. https://app.fincalc.co.uk/cgi-bin/

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**https://app.fincalc.co.uk**
Path:	**/cgi-bin/**

Static analysis

Data is read from **location** and passed to **$()** via the following statement:

- `var path = $(location).attr('pathname');`

1.3. https://app.fincalc.co.uk/login

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**https://app.fincalc.co.uk**
Path:	**/login**

Static analysis

Data is read from **document.location** and passed to **$()** via the following statements:

- `var url = document.location.toString();`
- `$('.nav-tabs a[href="#' + url.split('#')[1] + '"]').tab('show');`

1.4. https://app.fincalc.co.uk/login

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**https://app.fincalc.co.uk**
Path:	**/login**

Static analysis

Data is read from **location** and passed to **$()** via the following statement:

- `var path = $(location).attr('pathname');`

1.5. https://app.fincalc.co.uk/login/request_new_password

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**https://app.fincalc.co.uk**
Path:	**/login/request_new_password**

Static analysis

Data is read from **document.location** and passed to **$()** via the following statements:

- `var url = document.location.toString();`
- `$('.nav-tabs a[href="#' + url.split('#')[1] + '"]').tab('show');`

1.6. https://app.fincalc.co.uk/login/request_new_password

Summary

Severity:	**High**
Confidence:	**Tentative**
Host:	**https://app.fincalc.co.uk**
Path:	**/login/request_new_password**

Static analysis

Data is read from **location** and passed to **$()** via the following statement:

- `var path = $(location).attr('pathname');`

---

2. Unencrypted communications

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**http://app.fincalc.co.uk**
Path:	**/**

---

3. Strict transport security not enforced

Summary

Severity:	**Low**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/**

4. Cross-origin resource sharing

There are 9 instances of this issue:

- http://app.fincalc.co.uk/robots.txt
- https://app.fincalc.co.uk/cgi-bin/
- https://app.fincalc.co.uk/css/custom.css
- https://app.fincalc.co.uk/libraries/bootstrap-3.3.7/bootstrap.min.css
- https://app.fincalc.co.uk/libraries/fontawesome-5.14.0/css/all.min.css
- https://app.fincalc.co.uk/libraries/jquery-ui-1.12.1/jquery-ui.min.css
- https://app.fincalc.co.uk/login/check_login
- https://app.fincalc.co.uk/login/request_new_password
- https://app.fincalc.co.uk/robots.txt

4.1. http://app.fincalc.co.uk/robots.txt

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**http://app.fincalc.co.uk**
Path:	**/robots.txt**

4.2. https://app.fincalc.co.uk/cgi-bin/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/cgi-bin/**

4.3. https://app.fincalc.co.uk/css/custom.css

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/css/custom.css**

4.4. https://app.fincalc.co.uk/libraries/bootstrap-3.3.7/bootstrap.min.css

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**

Path:	**/libraries/bootstrap-3.3.7/bootstrap.min.css**

4.5. https://app.fincalc.co.uk/libraries/fontawesome-5.14.0/css/all.min.css

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/libraries/fontawesome-5.14.0/css/all.min.css**

4.6. https://app.fincalc.co.uk/libraries/jquery-ui-1.12.1/jquery-ui.min.css

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/libraries/jquery-ui-1.12.1/jquery-ui.min.css**

4.7. https://app.fincalc.co.uk/login/check_login

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/login/check_login**

4.8. https://app.fincalc.co.uk/login/request_new_password

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/login/request_new_password**

4.9. https://app.fincalc.co.uk/robots.txt

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/robots.txt**

5. TLS cookie without secure flag set

There are 2 instances of this issue:

- /cgi-bin/
- /robots.txt

5.1. https://app.fincalc.co.uk/cgi-bin/

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/cgi-bin/**

5.2. https://app.fincalc.co.uk/robots.txt

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/robots.txt**

6. Cross-domain script include

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/login/request_new_password**

7. Robots.txt file

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/robots.txt**

8. Cacheable HTTPS response

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/robots.txt**

9. TLS certificate

Summary

Severity:	**Information**
Confidence:	**Certain**
Host:	**https://app.fincalc.co.uk**
Path:	**/**

Report generated by Burp Suite web vulnerability scanner v2022.5.1, at Monday Jun 20 21:19:32 GMT 2022.