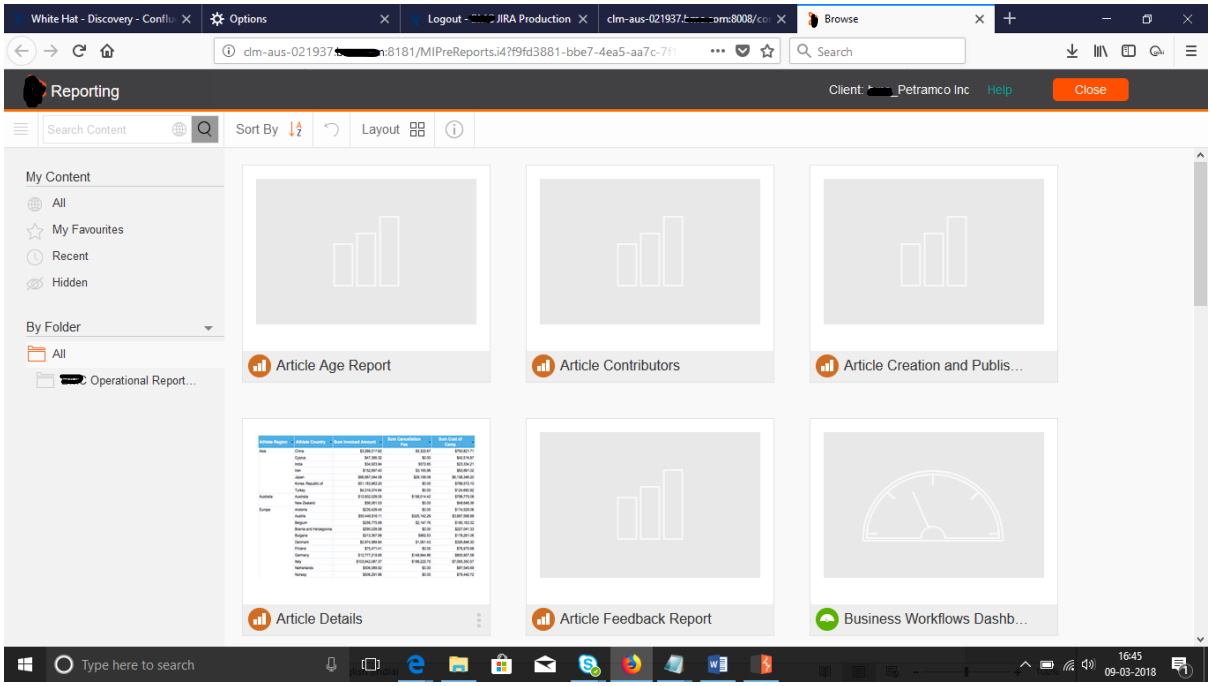
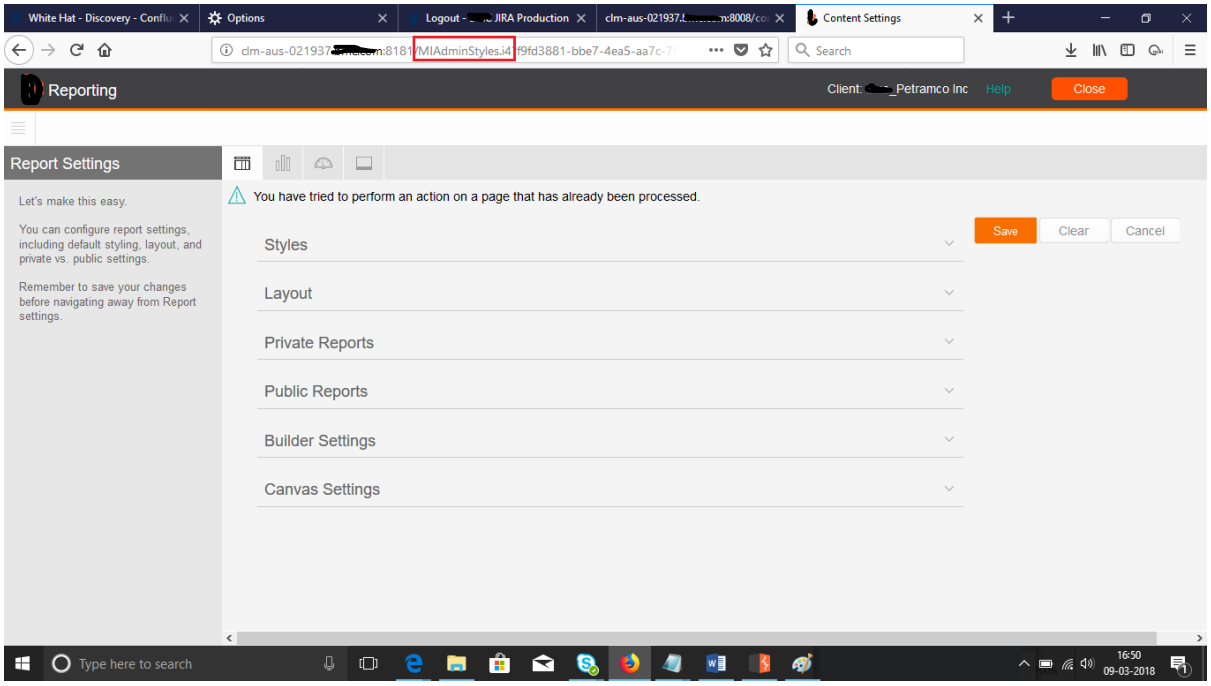
Stored XSS happened through privileges escalation which affects the Normal user and Admin both.

Login to the application with normal user at [http://clm-aus-021937.[redacted]:8008/com[redacted].bwfa/index.html#/login](http://clm-aus-021937.[redacted]:8008/com[redacted].bwfa/index.html#/login) . Go to the report tab (yellow fin)

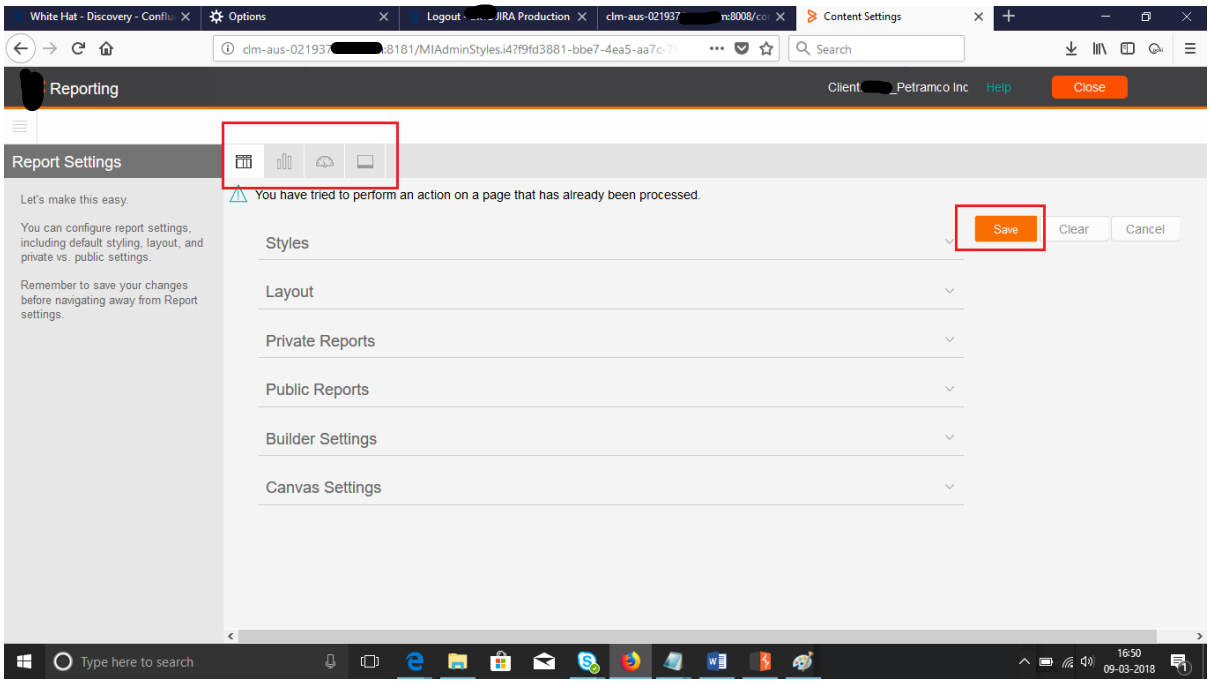


[http://clm-aus-021937.[redacted]:8181/MIPreReports.i4?f9fd3881-bbe7-4ea5-aa7c-7f1eb045688b=38d6af98-4b19-44b9-9971-30ae0eedf82b](http://clm-aus-021937.[redacted]:8181/MIPreReports.i4?f9fd3881-bbe7-4ea5-aa7c-7f1eb045688b=38d6af98-4b19-44b9-9971-30ae0eedf82b)

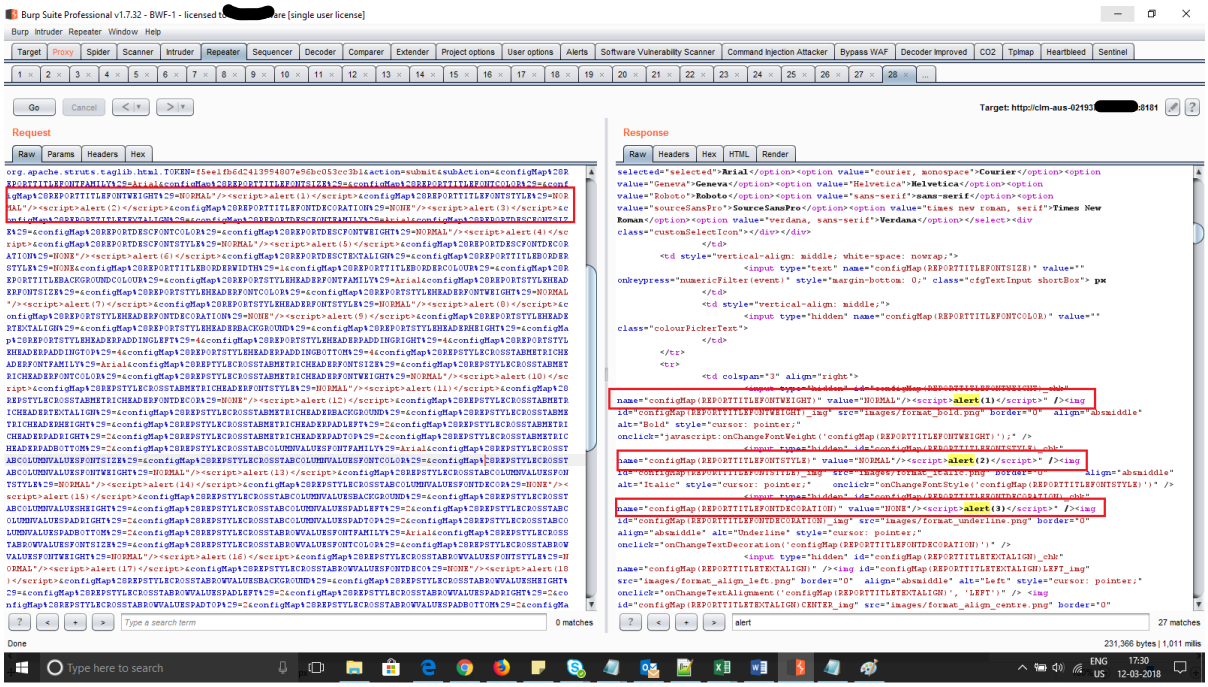
In the above link it is mentioned **MIPreReports.i4** , if we replace this with **MIAdminStyles.i4** we get the panel which is only accessible by admin . As shown in the image below.



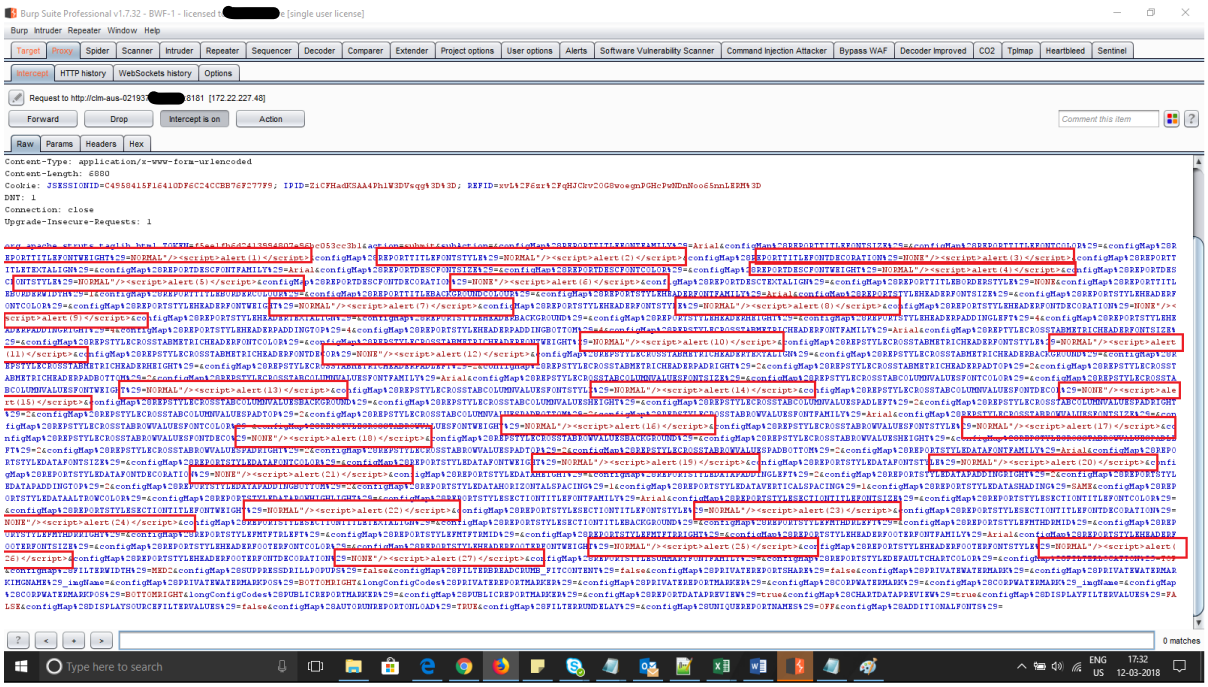
Intercept the request on burp while trying to click the save button or one of the tabs next to Report Settings .



Intercepting requests using burp, as shown below



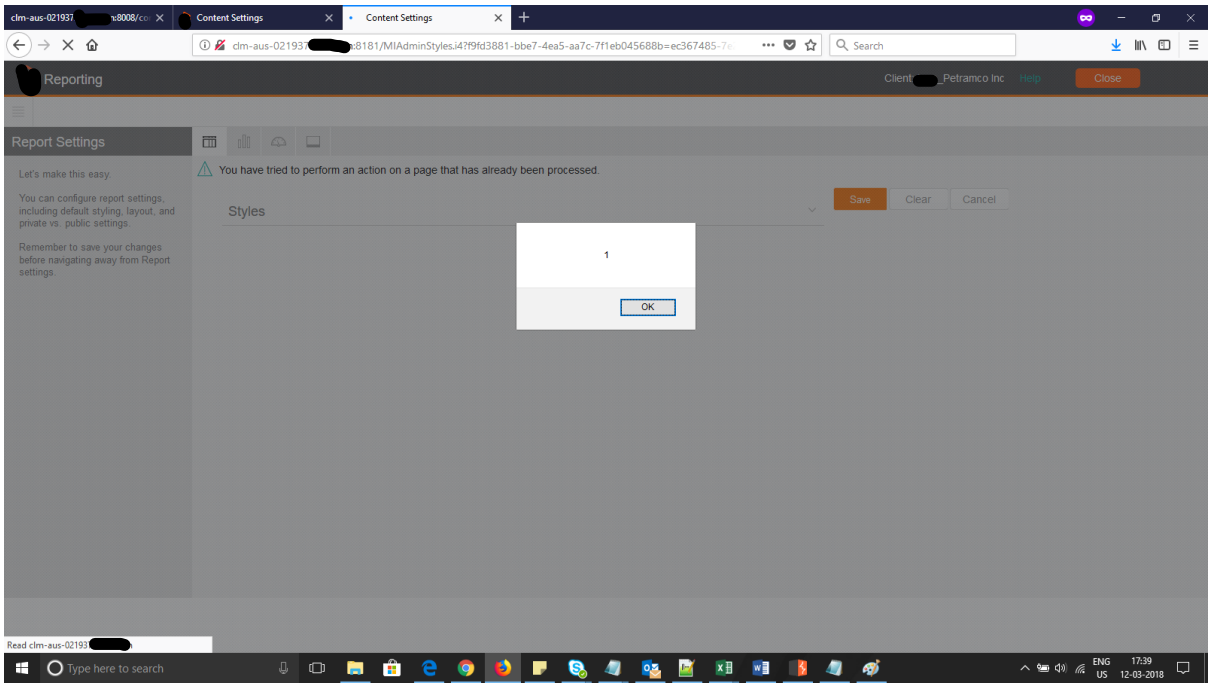
Add the payload (**“/><script>alert(1)</script>**) in all the highlighted parameters as shown below and click Forward.

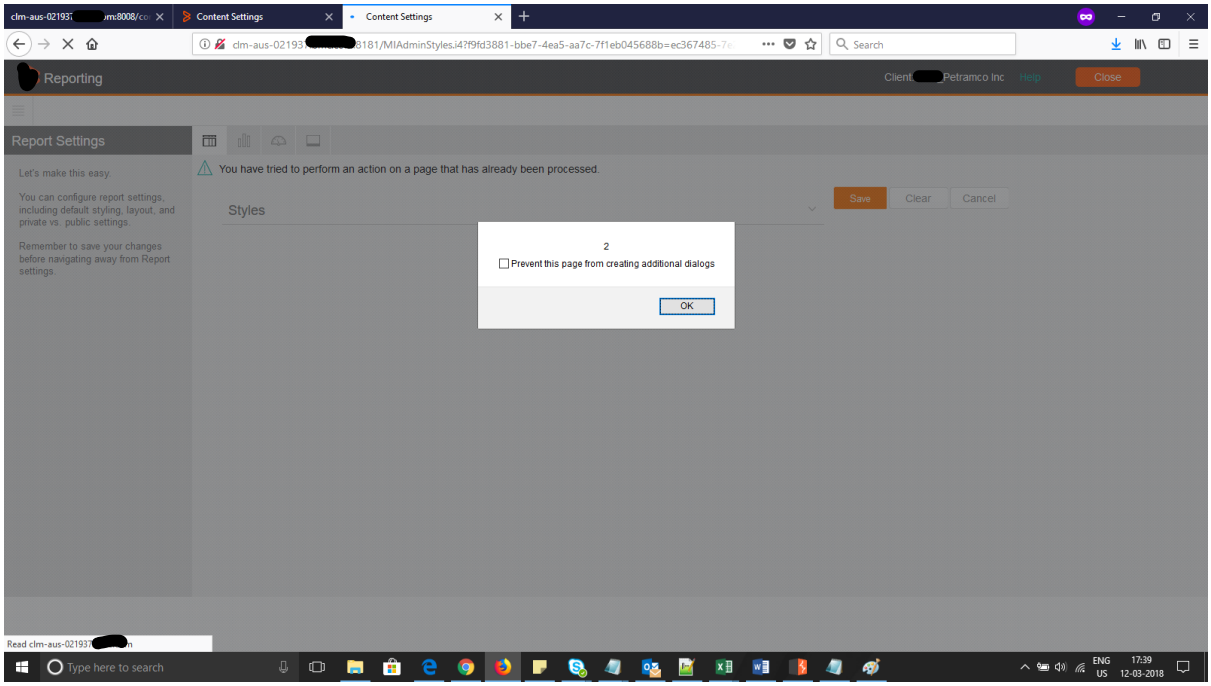


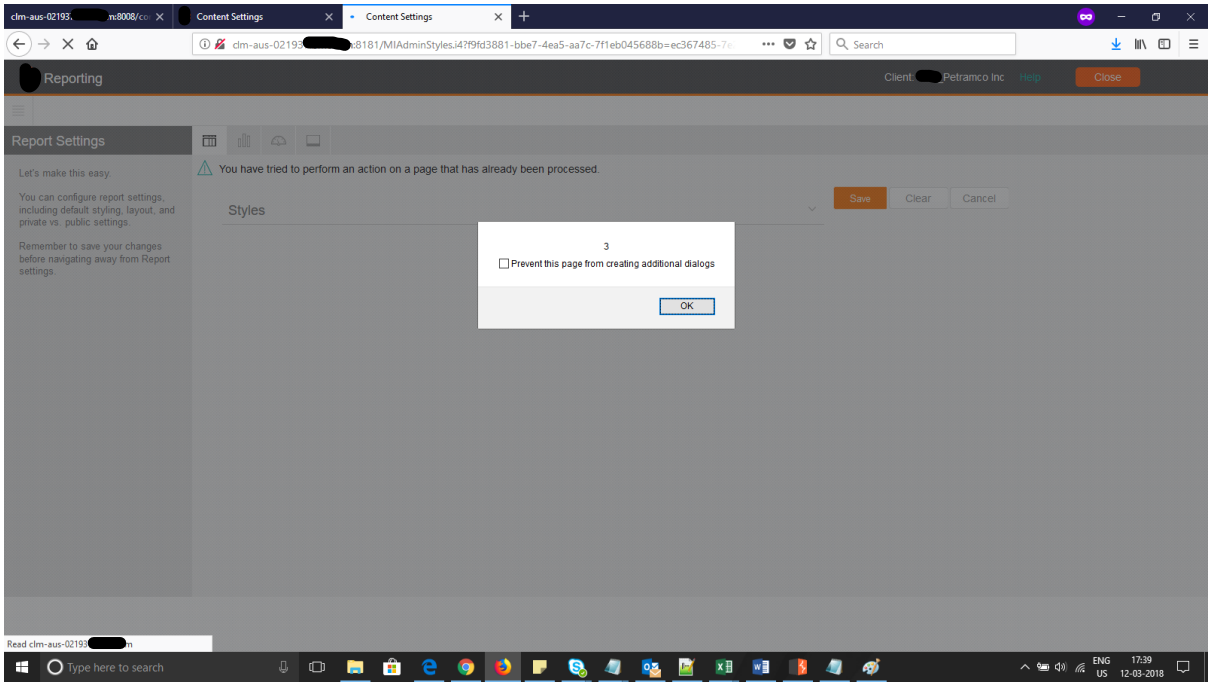
Below are the vulnerable parameters.

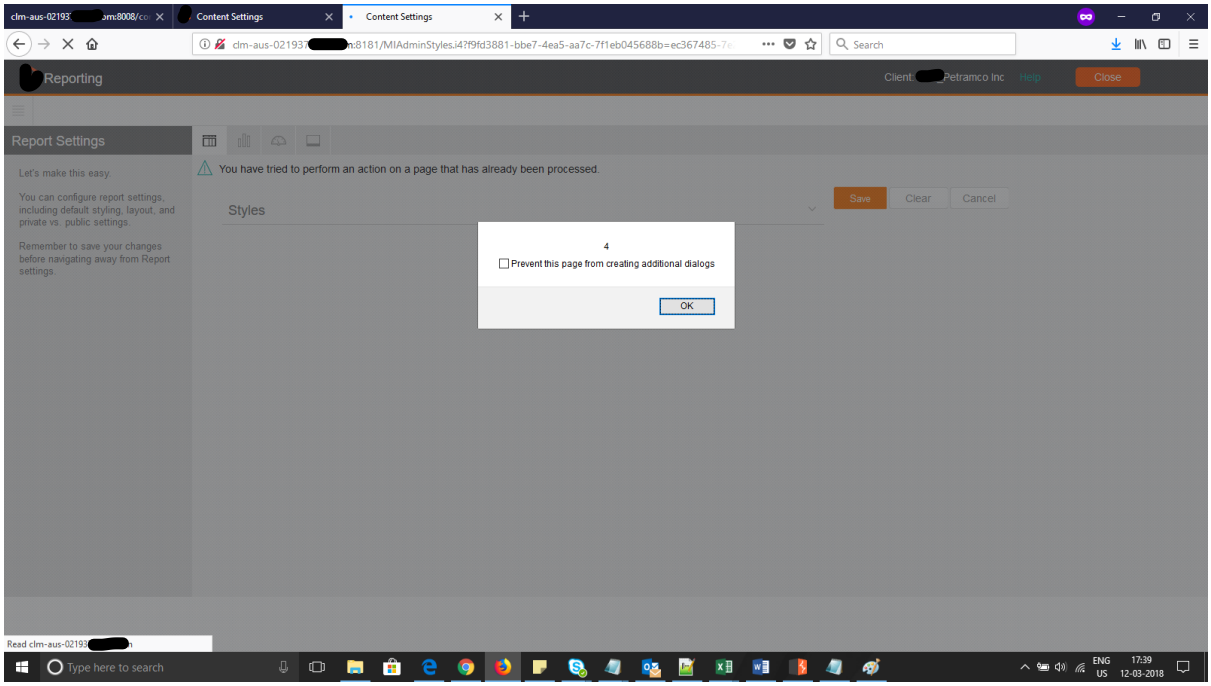
1. name="configMap(REPORTTITLEFONTWEIGHT)"
2. name="configMap(REPORTTITLEFONTSTYLE)"
3. name="configMap(REPORTTITLEFONTDECORATION)"
4. name="configMap(REPORTDESCFONTWEIGHT)"
5. name="configMap(REPORTDESCFONTSTYLE)"
6. name="configMap(REPORTDESCFONTDECORATION)"
7. name="configMap(REPORTSTYLEHEADERFONTWEIGHT)"
8. name="configMap(REPORTSTYLEHEADERFONTSTYLE)"
9. name="configMap(REPORTSTYLEHEADERFONTDECORATION)"
10. name="configMap(REPSTYLECROSSTABMETRICHEADERFONTWEIGHT)"
11. name="configMap(REPSTYLECROSSTABMETRICHEADERFONTSTYLE)"
12. name="configMap(REPSTYLECROSSTABMETRICHEADERFONTDECOR)"
13. name="configMap(REPSTYLECROSSTABCOLUMNVALUESFONTWEIGHT)"
14. name="configMap(REPSTYLECROSSTABCOLUMNVALUESFONTSTYLE)"
15. name="configMap(REPSTYLECROSSTABCOLUMNVALUESFONTDECOR)"
16. name="configMap(REPSTYLECROSSTABROWVALUESFONTWEIGHT)"
17. name="configMap(REPSTYLECROSSTABROWVALUESFONTSTYLE)"
18. name="configMap(REPSTYLECROSSTABROWVALUESFONTDECO)"
19. name="configMap(REPORTSTYLEDATAFONTWEIGHT)"
20. name="configMap(REPORTSTYLEDATAFONTSTYLE)"
21. name="configMap(REPORTSTYLEDATAFONTDECORATION)"
22. name="configMap(REPORTSTYLESECTIONTITLEFONTWEIGHT)
23. name="configMap(REPORTSTYLESECTIONTITLEFONTSTYLE)"
24. name="configMap(REPORTSTYLESECTIONTITLEFONTDECORATION)"
25. name="configMap(REPORTSTYLEHEADERFOOTERFONTWEIGHT)"
26. name="configMap(REPORTSTYLEHEADERFOOTERFONTSTYLE)"
27. name="configMap(REPORTSTYLEHEADERFOOTERFONTDECORATION)"

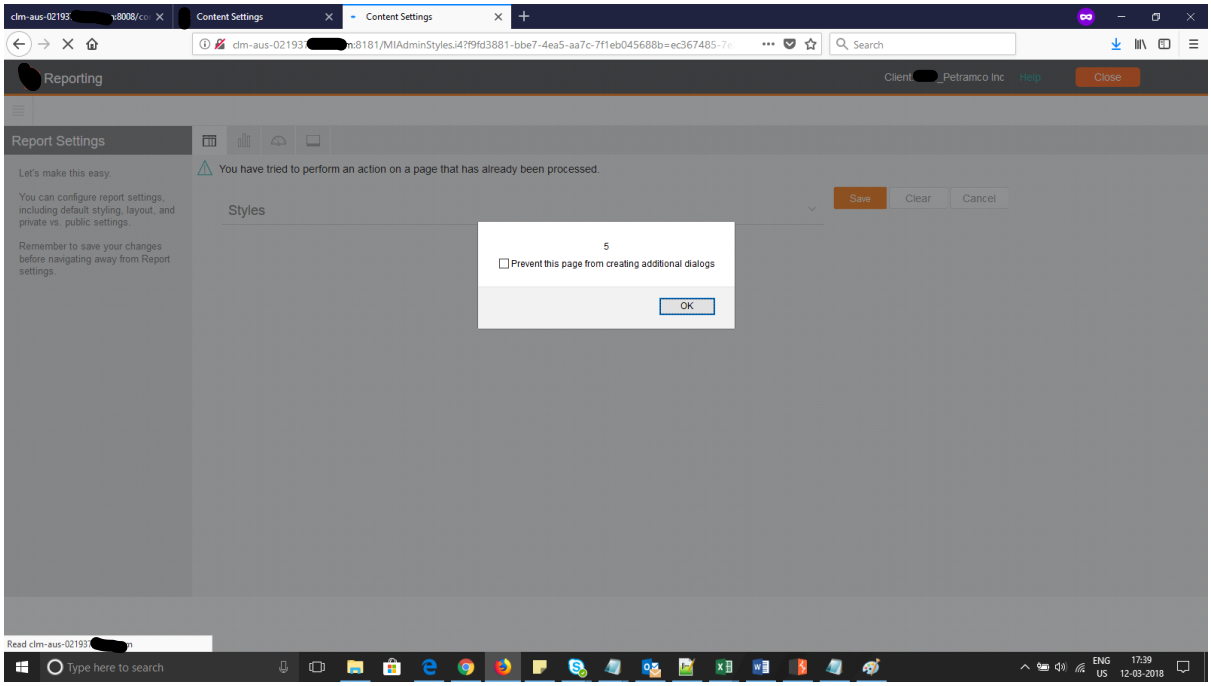
Then you will see the scripts getting executed on the browsers as shown below.

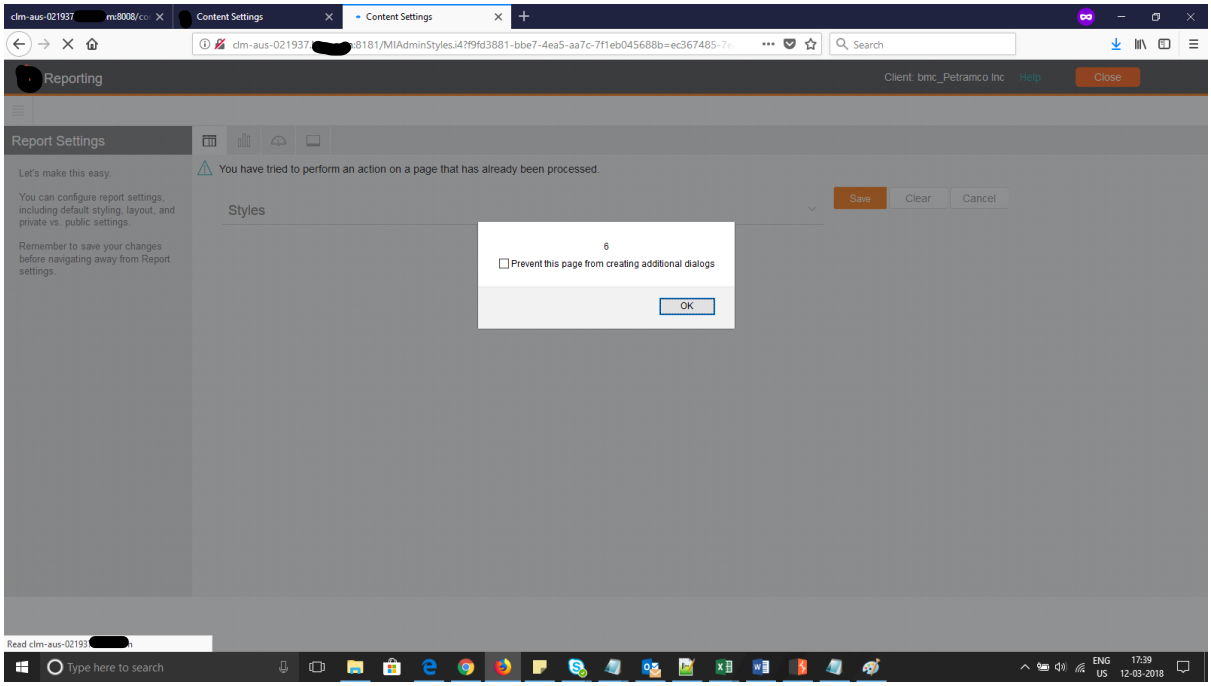


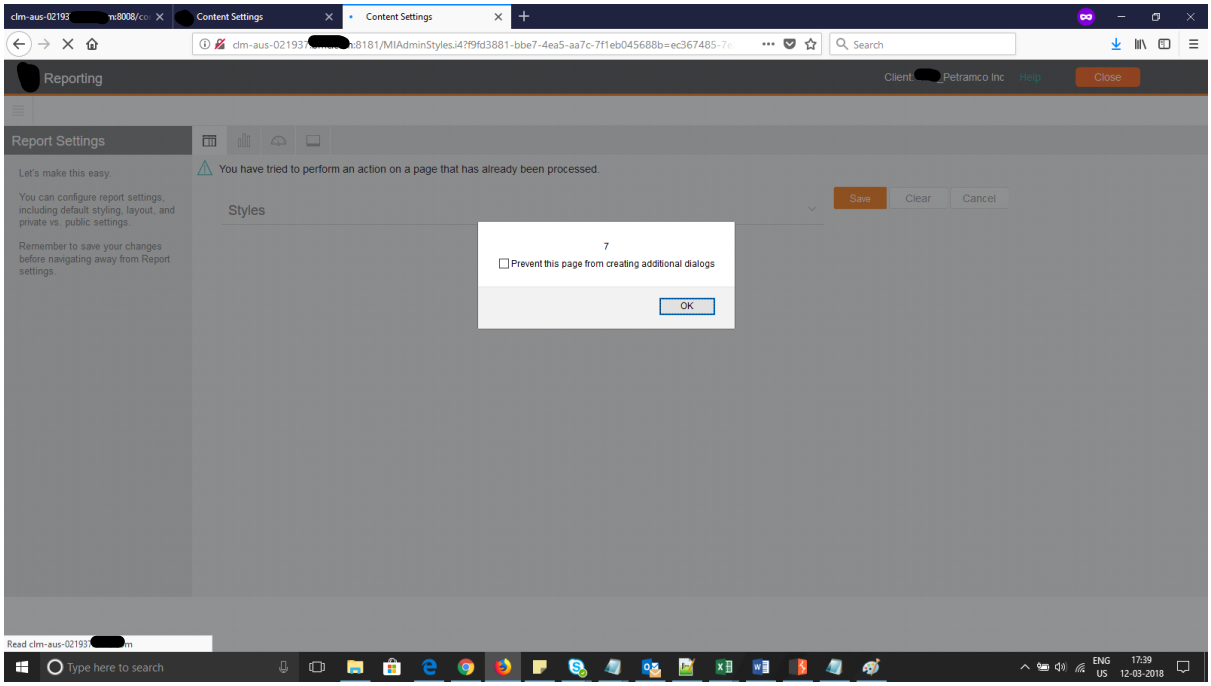

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
2
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:39
12-03-2018

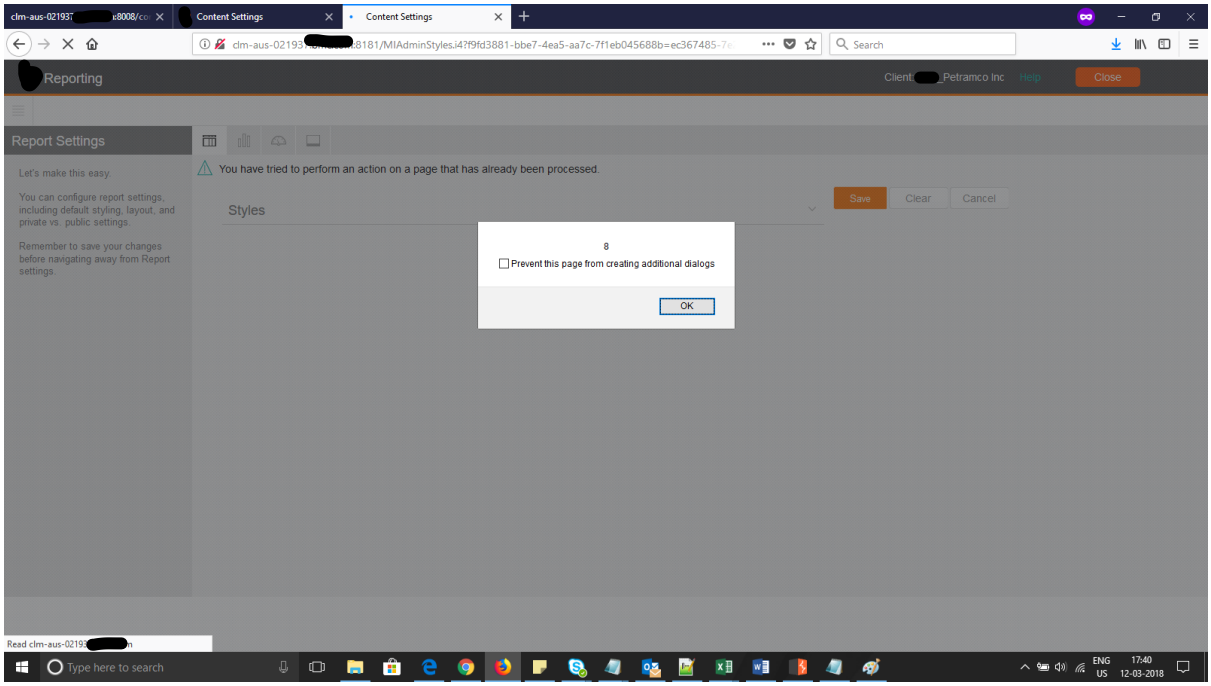

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
3
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:39
12-03-2018

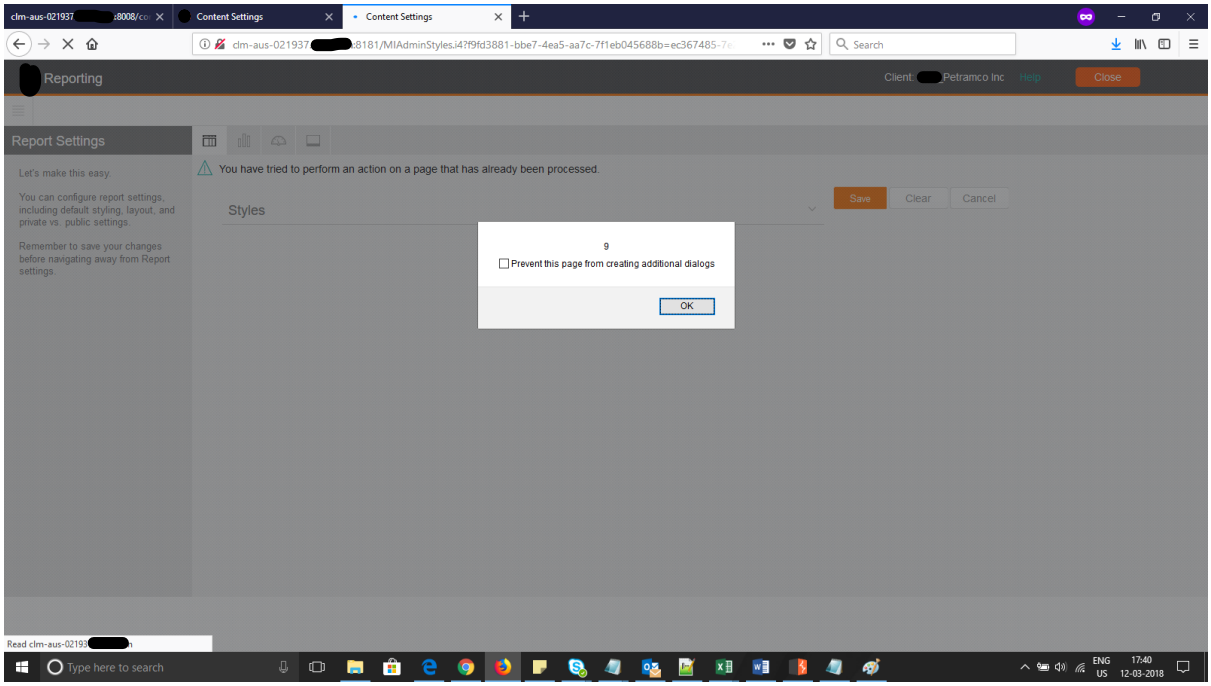

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
4
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:39
12-03-2018

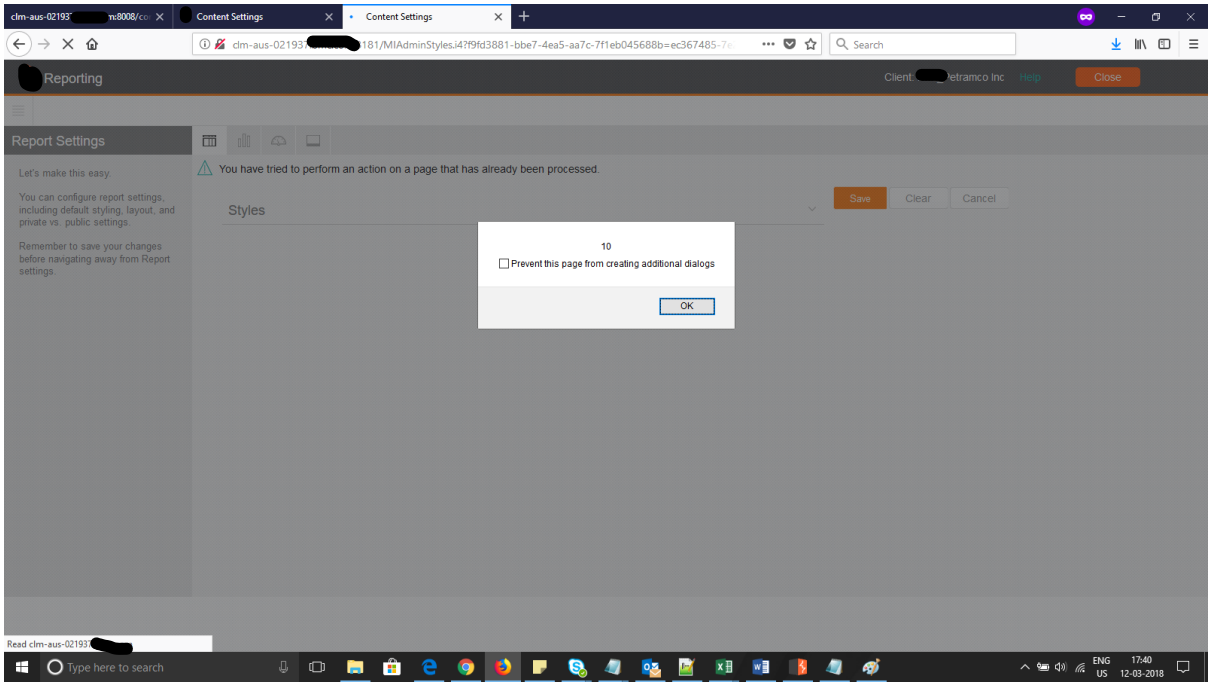

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
5
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:39
12-03-2018

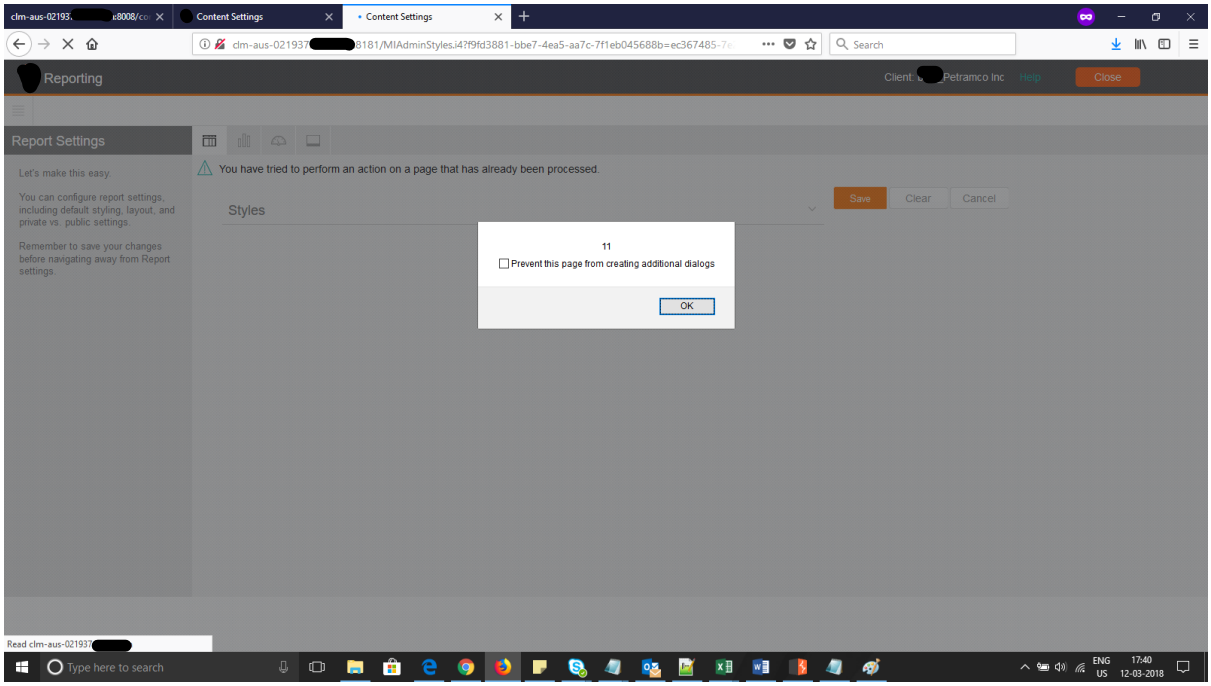

Content Settings
Content Settings
Search
Reporting
Client: bmc_Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
6
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:39
12-03-2018

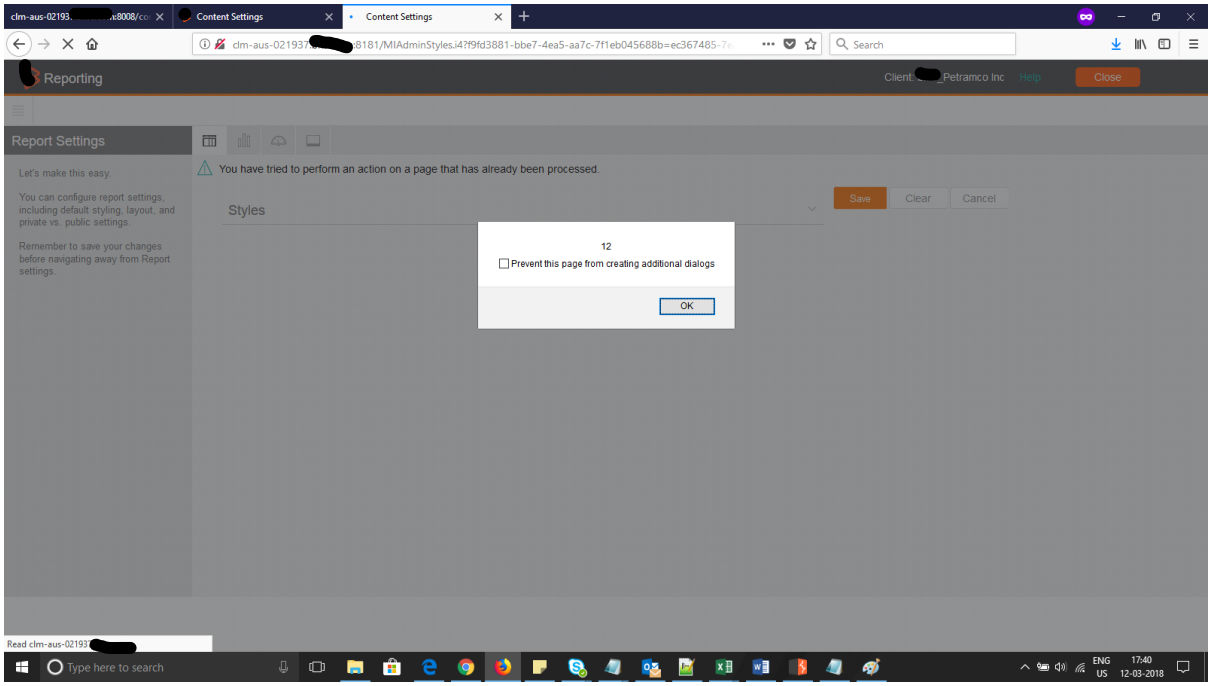

Content Settings
Content Settings
Search
Reporting
Client: _Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
7
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:39
12-03-2018

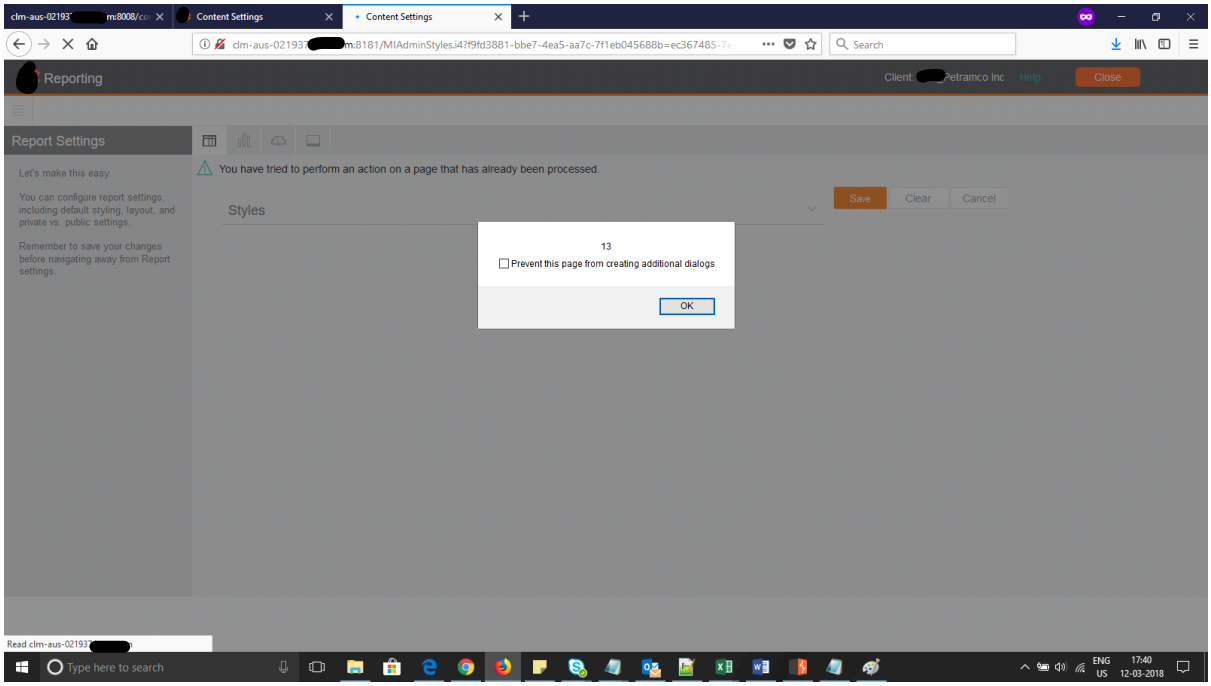

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
8
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:40
12-03-2018

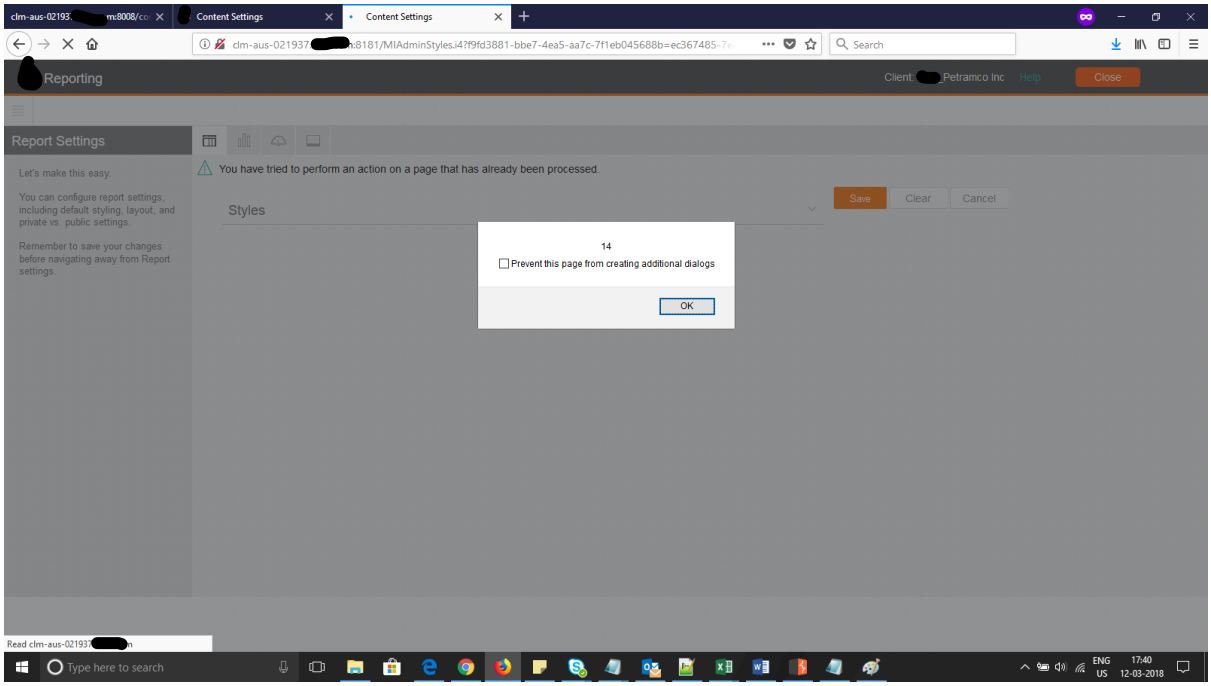

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
9
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:40
12-03-2018

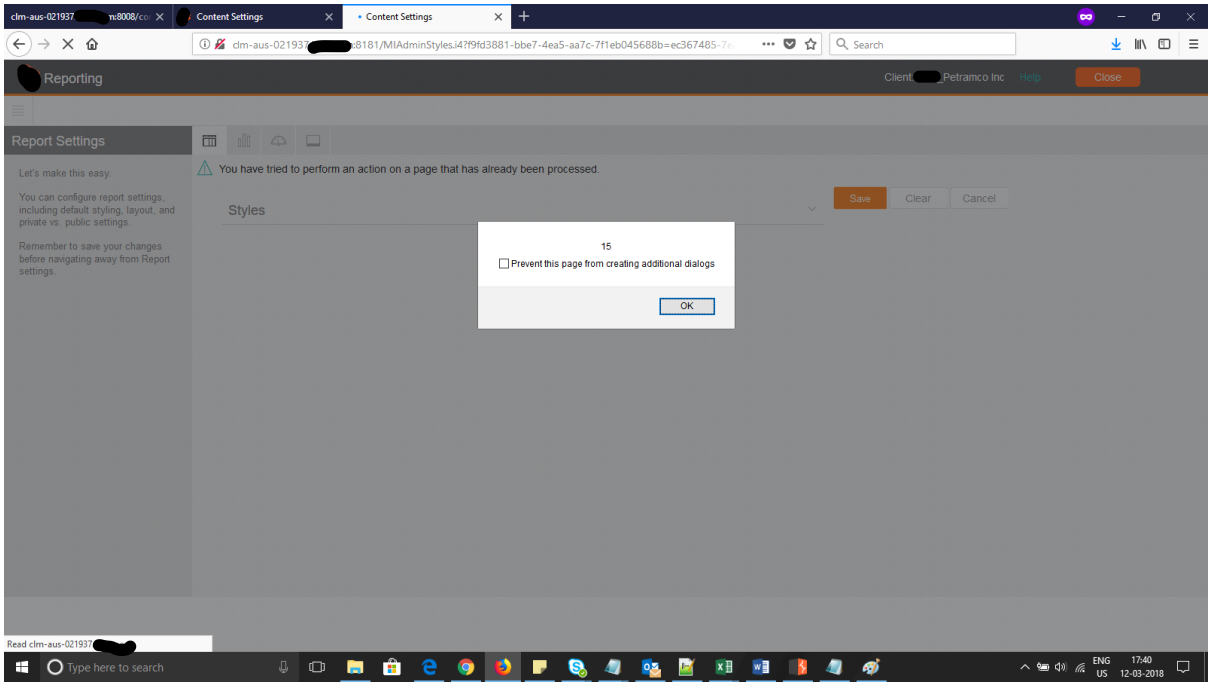

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
10
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:40
12-03-2018

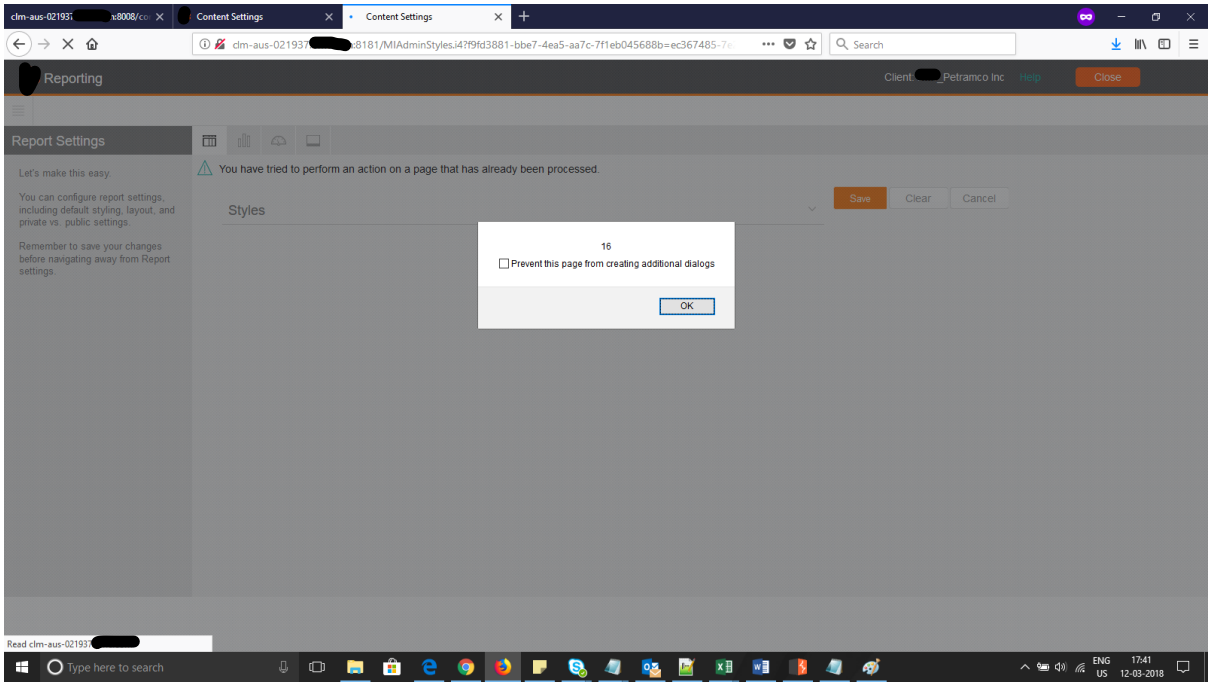

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
11
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:40
12-03-2018

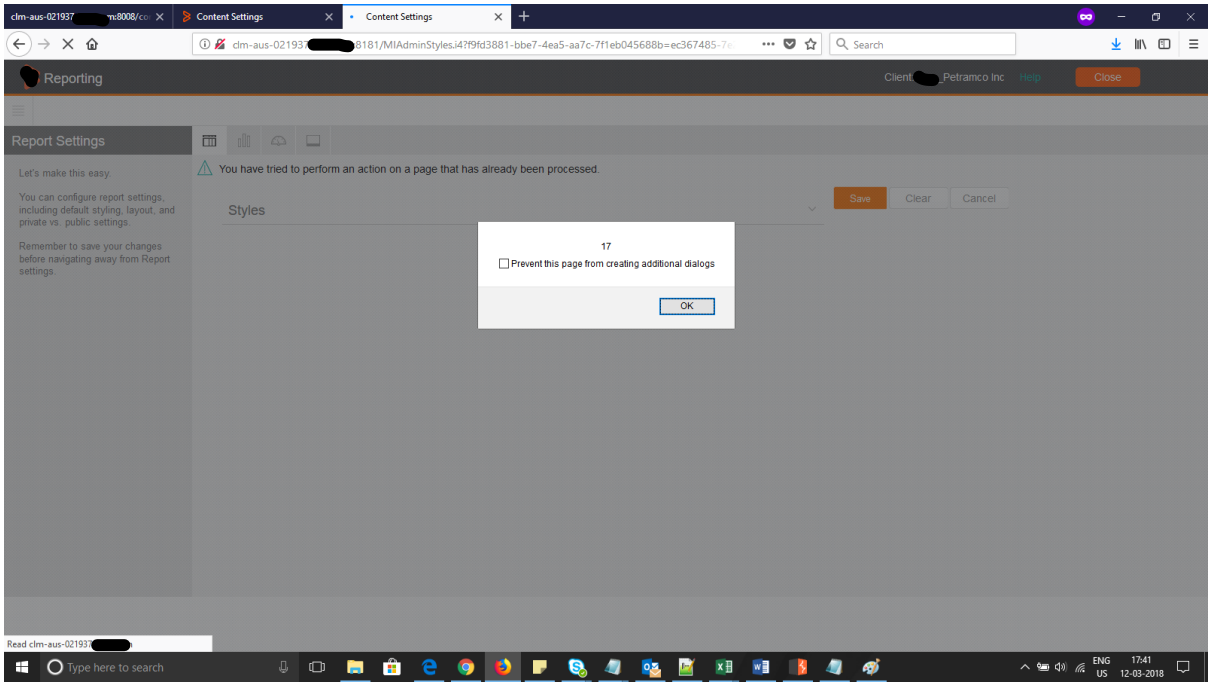

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
12
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:40
12-03-2018

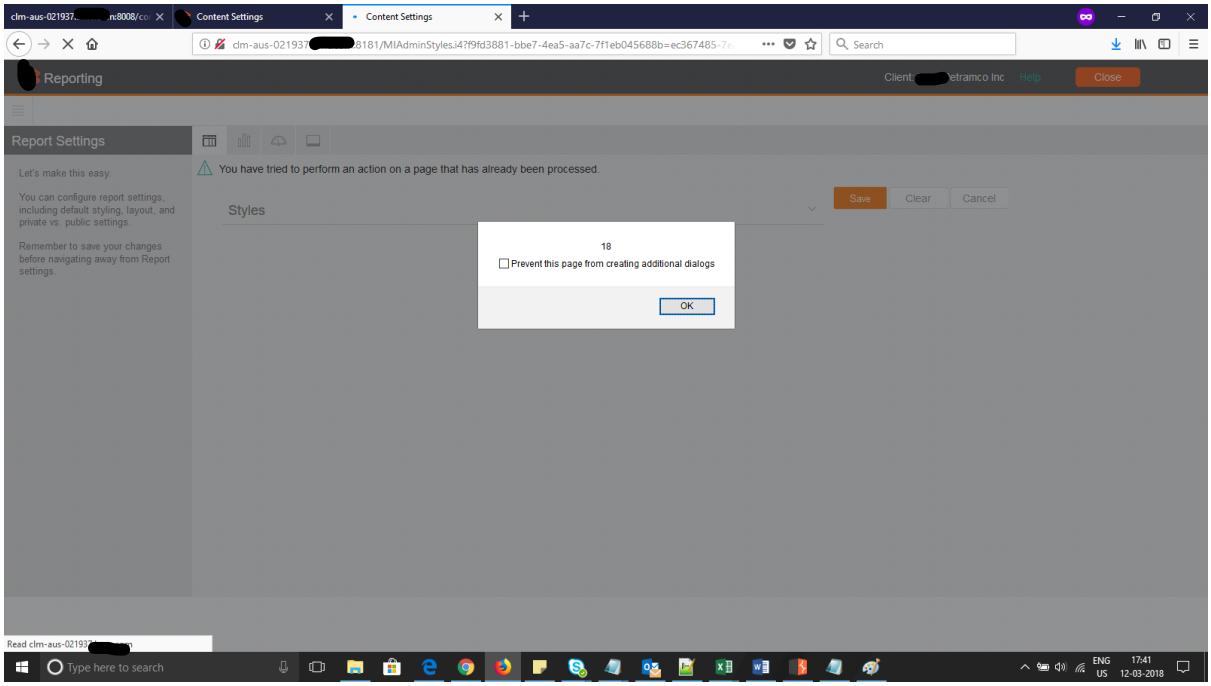

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
13
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:40
12-03-2018

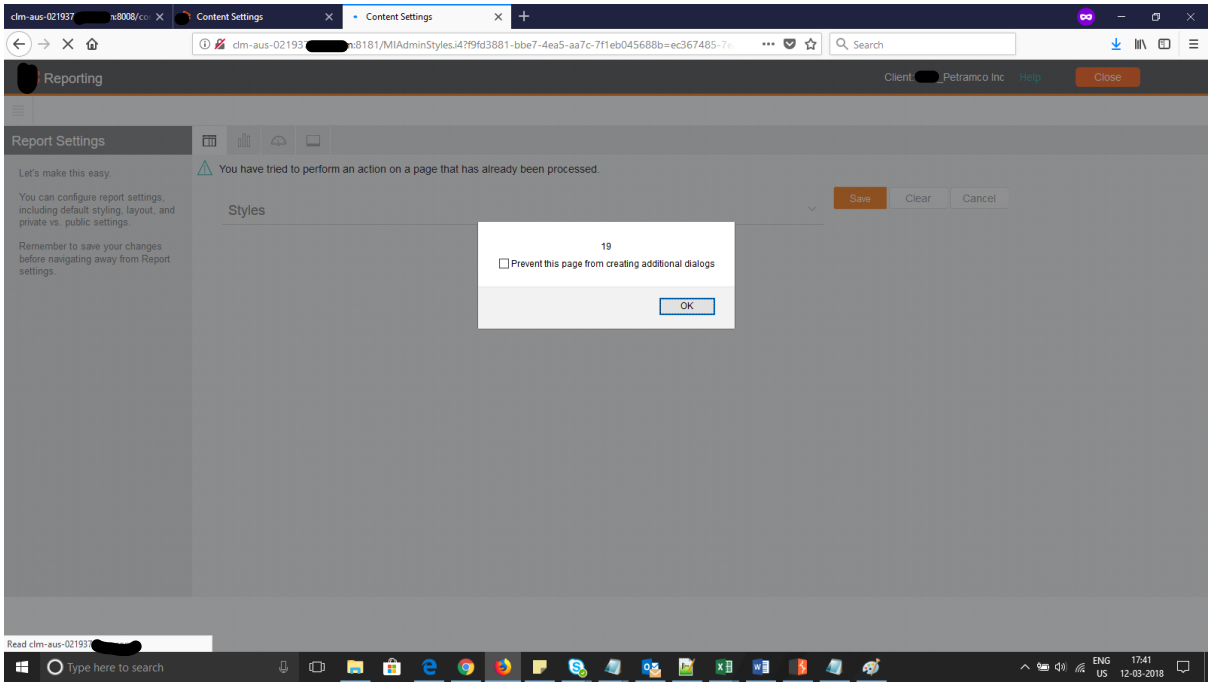

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
14
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:40
12-03-2018

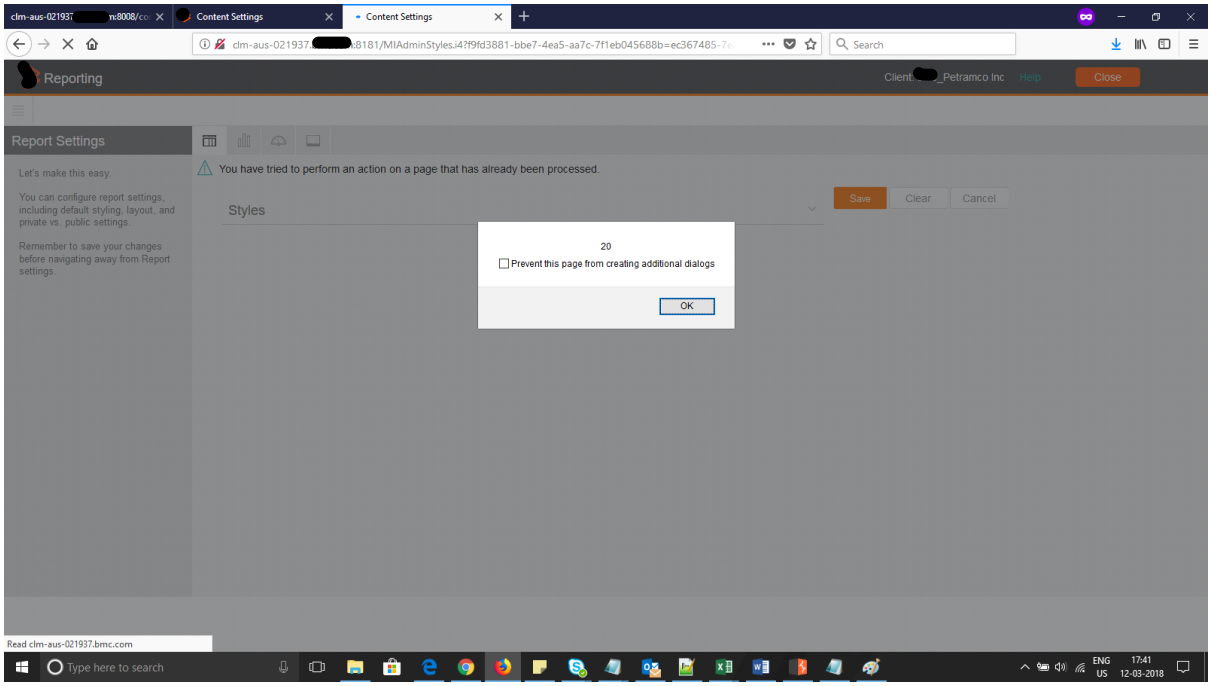

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
15
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:40
12-03-2018

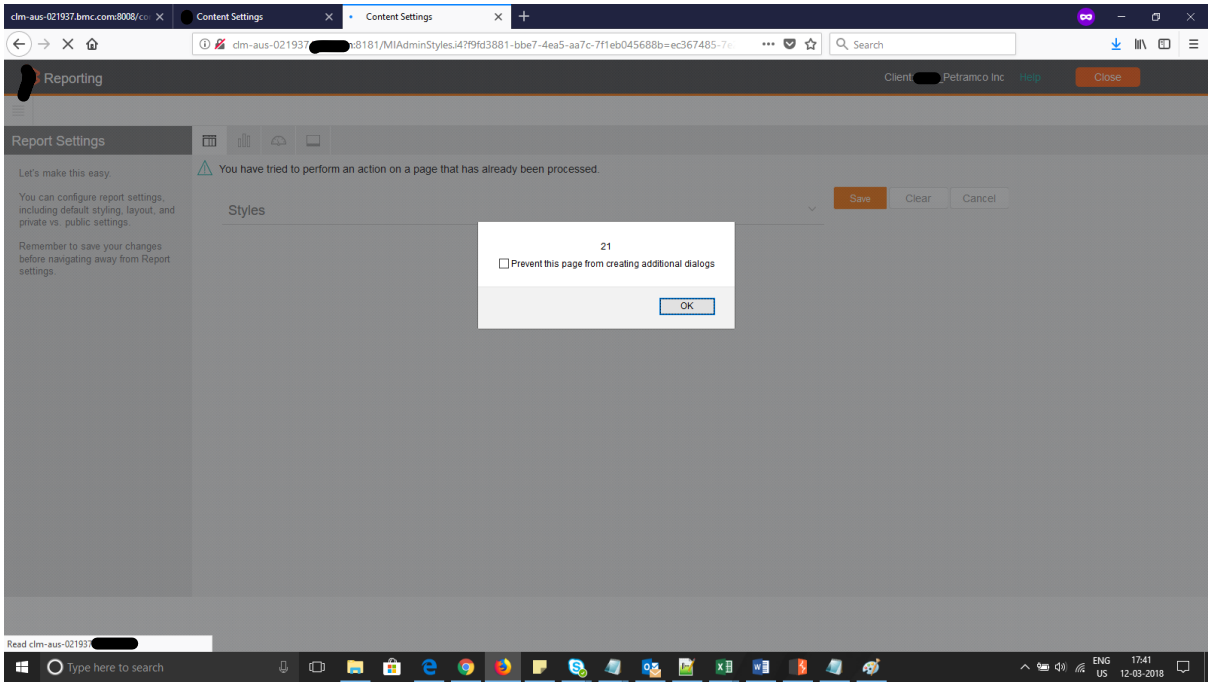

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
16
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:41
12-03-2018

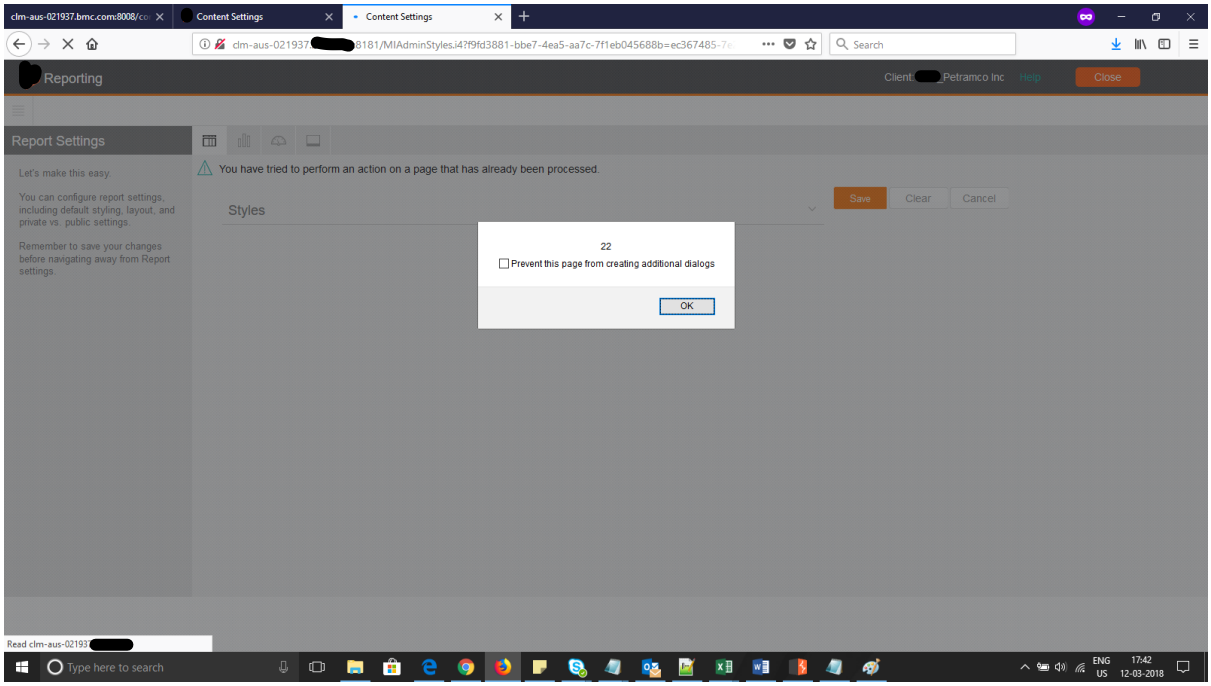

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
17
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:41
12-03-2018

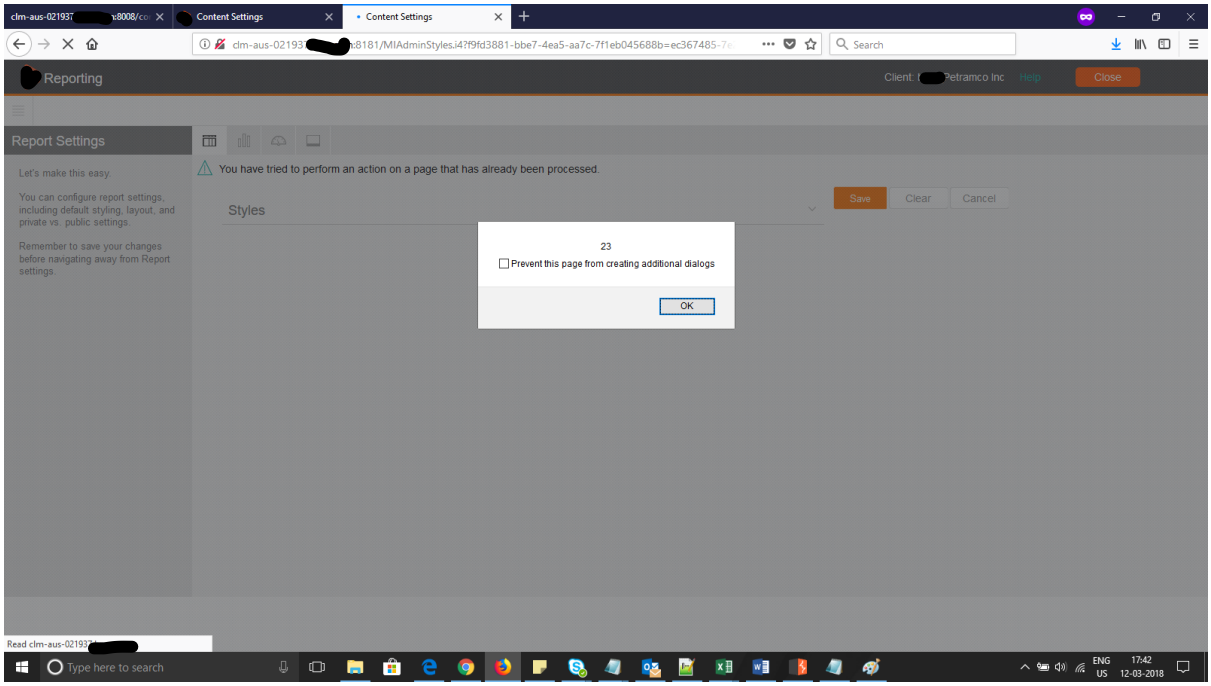

Content Settings
Content Settings
Search
Reporting
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
18
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:41
12-03-2018

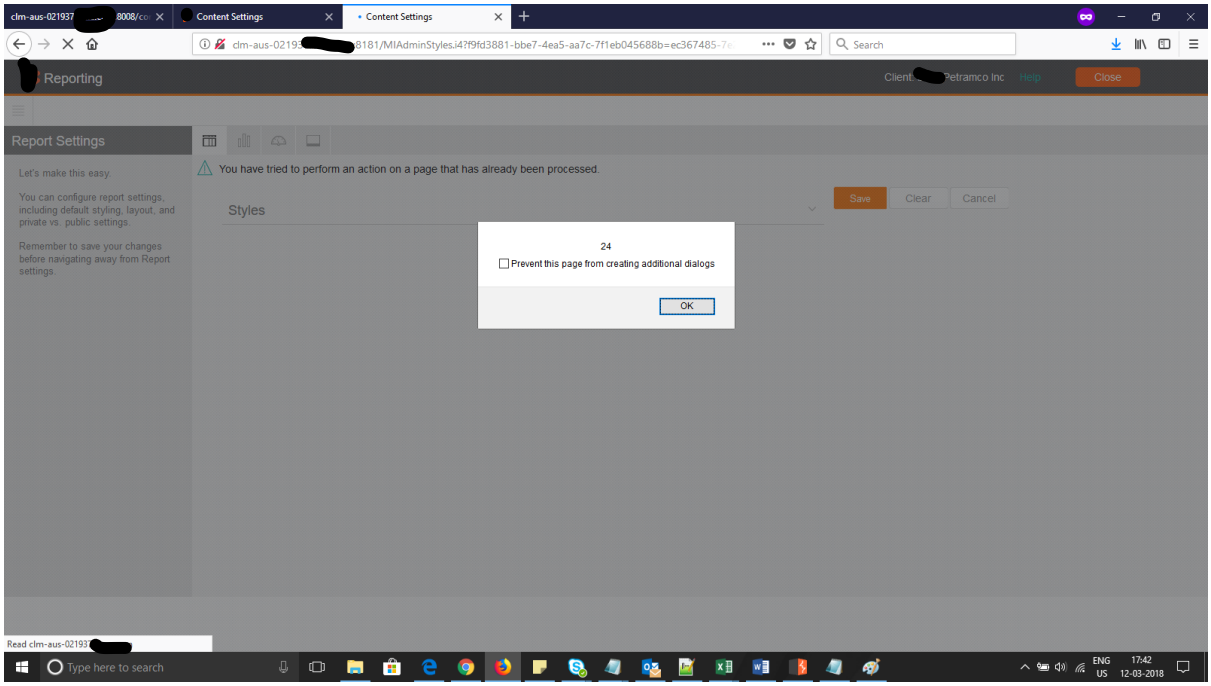

Content Settings
Content Settings
Search
Reporting
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
19
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:41
12-03-2018

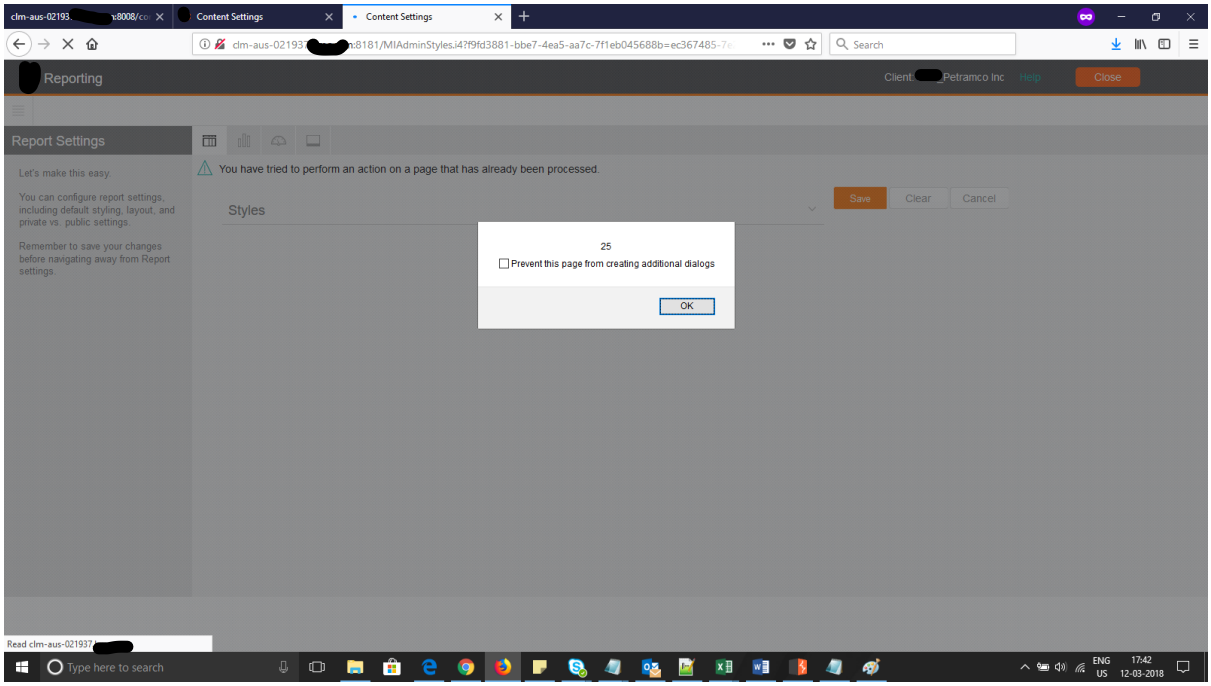

Content Settings
Content Settings
Reporting
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
20
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:41
12-03-2018

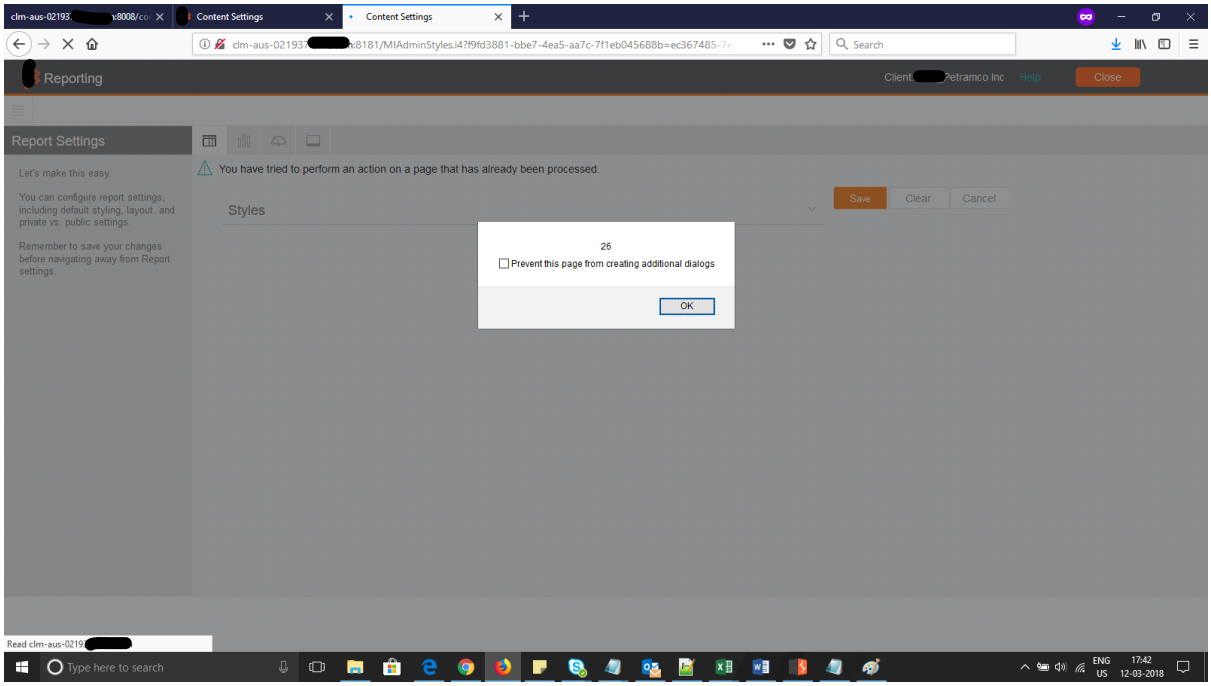

Content Settings
Content Settings
Reporting
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
21
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:41
12-03-2018

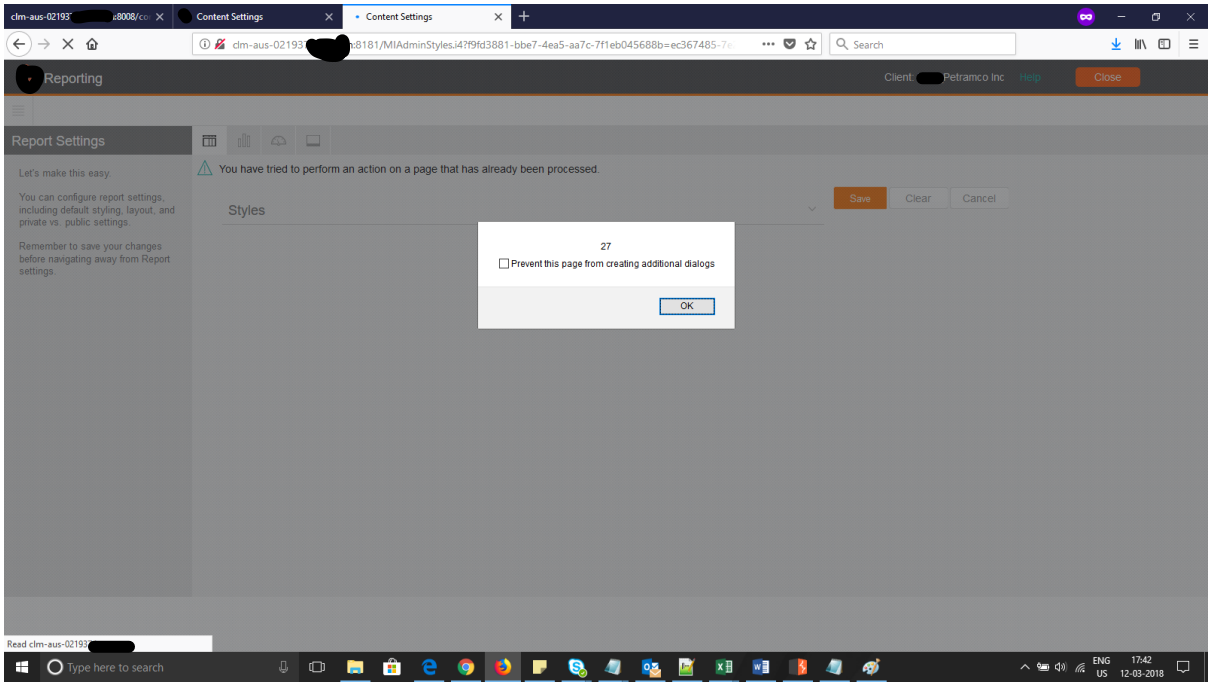

Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
22
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:42
12-03-2018


Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
23
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:42
12-03-2018


Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
24
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:42
12-03-2018


Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
25
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:42
12-03-2018


Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
26
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:42
12-03-2018


Content Settings
Content Settings
Search
Reporting
Client: Petramco Inc
Help
Close
Report Settings
Let's make this easy.
You can configure report settings, including default styling, layout, and private vs. public settings.
Remember to save your changes before navigating away from Report settings.
You have tried to perform an action on a page that has already been processed.
Styles
Save
Clear
Cancel
27
Prevent this page from creating additional dialogs
OK
Type here to search
ENG
US
17:42
12-03-2018