

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

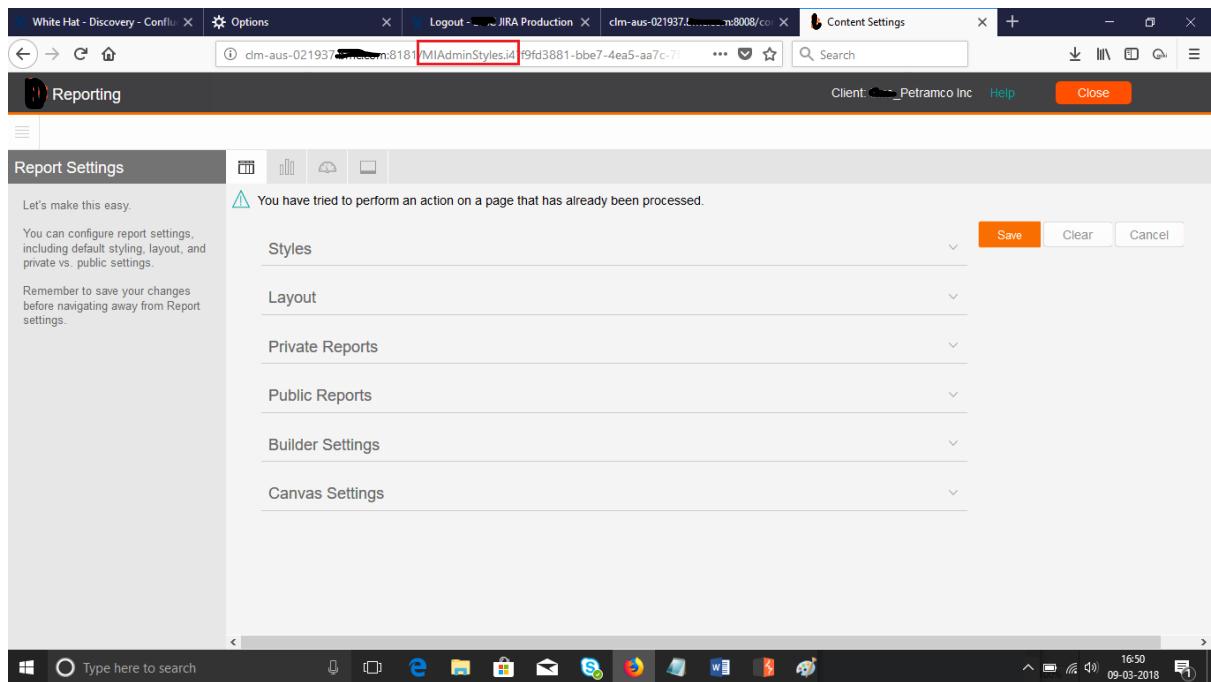
Login to the application with normal user at <http://clm-aus-021937.url.com:8008/com.ud.dsm.bwfa/index.html#/login>. Go to the report tab (yellow fin)

The screenshot shows a web interface for a reporting application. At the top, there are several tabs: "White Hat - Discovery - Conflu", "Options", "Logout", "JIRA Production", "clm-aus-021937.url.com:8008/com.ud.dsm.bwfa/index.html#/login", and "Browse". Below the tabs, the title bar says "Reporting" and shows the client as "Petramco Inc". The main area contains a sidebar with "My Content" and "By Folder" sections. The "By Folder" section has a link to "Operational Report...". There are six report cards displayed in a grid:

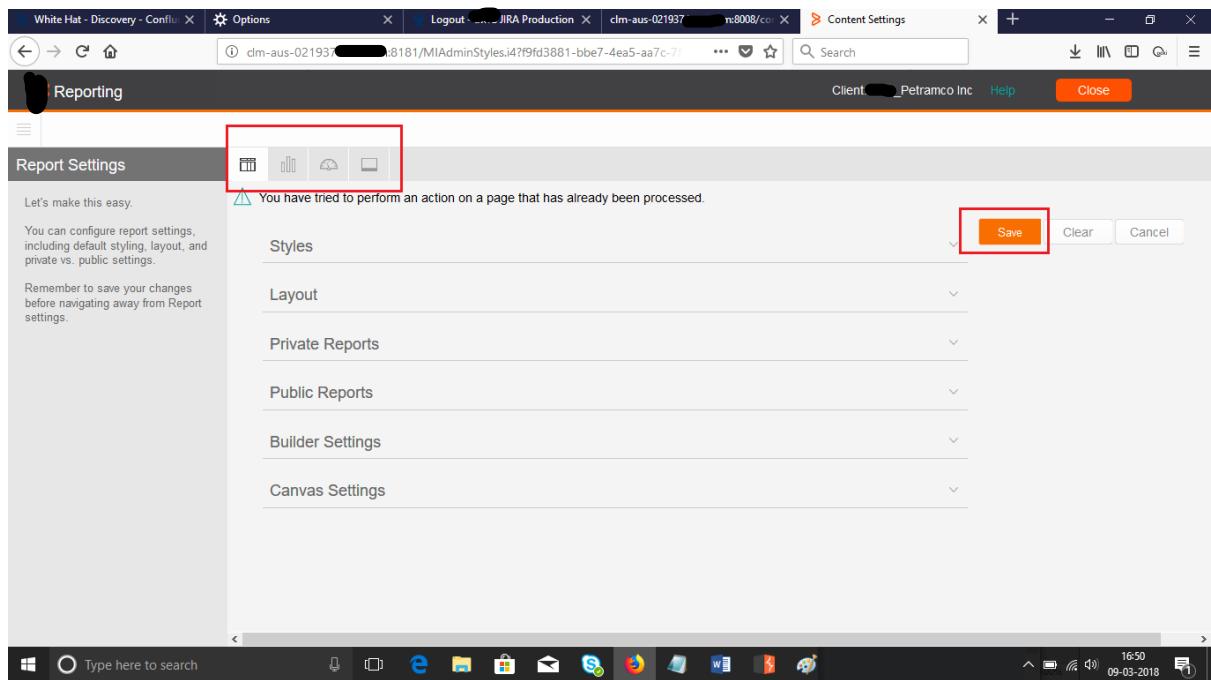
- Article Age Report: A bar chart with three bars of increasing height.
- Article Contributors: A bar chart with three bars of increasing height.
- Article Creation and Publis...: A bar chart with three bars of increasing height.
- Article Details: A table showing data for various countries across different dimensions like Sales Region, Delivery Country, Total Annual Amount, Pmt, Total Commission, and Total Profit. Some rows include "All" and "Grand Total".
- Article Feedback Report: A bar chart with three bars of increasing height.
- Business Workflows Dashb...: A gauge chart showing performance levels.

<http://clm-aus-021937.url.com: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(REPSTYLECROSSTABROWVALUESFONTDECOR)"
19. name="configMap(REPORTSTYLELEDATAFONTWEIGHT)"
20. name="configMap(REPORTSTYLELEDATAFONTSTYLE)"
21. name="configMap(REPORTSTYLELEDATAFONTDECORATION)"
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.

