**Checkmarks**

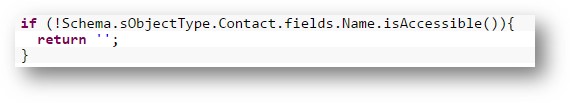
Please see detailed summary based on our discussion

**Dereferenced Field**

-          The issues like FLS\_Create, FLS\_Update, FLS\_Delete and dereferenced field comes under same category where on server side it is necessary to check if the user who is executing current apex class has appropriate permission on every SOQL that are executed within the class. Usually this verification follow the strategy of having all validation on server side instead of having them on through client login session. (as client login session can also be hacked). This scenario is more applicable in case of managed package for distribution where access to managed package is defined at higher level, and users who has access to package may get failure to run some part of it, because they do not have appropriate permission on fields or records.

-          In our scenario, since we are not planning for any managed package security review, this can be taken on lower priority.

This can be handled using methods like isAccessible() which enforces CRUD permissions inside the controller



**Client DOM XSRF**

-          As I see this issue has been taken care at most of the places by encoding the URL parameter data, please refer to existing snippet and follow the encode/decode mechanism on remaining occurrences.

In ConsumerDetail page, you can refer the use of JSENCODE to encode the URL parameters:



**XSRF With VF Call**

-          Client DOM XSRF can be **false positive in most of the cases**, one need to individually visit all these occurrences to see  if really using the parameter data any data damage can be performed.

-          E.g. Upon clicking delete button, the URL is being executed with parameter that is read into controller code which runs on server to perform certain action that can harm your data. If any hacker, run the similar URL with some id parameter, he will still be able to execute the delete operation with different parameters. This is unavoidable in some case, where we can apply one of following solution

o   Use POST method to submit the id value instead of GET method that makes your value as part of query string.

o   Introduce the confirmation box before actually deleting or updating the record, in our case the business team may not allow this.



**URL Redirection Attack**

-          Seems to be all serious issues, even though marked at medium priority should be fixed as early as possible.

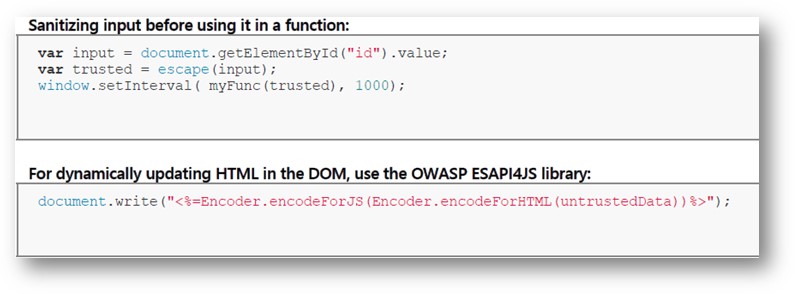
-          In this case, the parameter passed on as query string is actually being used for URL Redirection. Instead of passing URL to query string (like retVal), use some constants or codes to identify the page to be redirected. E.g. instead of passing  myPage as querystring parameter in “/somepage?retURL=myVFPage” we can pass an identifier as “/somepage?retURL=1” and then use this value 1,2 or 3 to identify the page where we want re-direction to be performed.

**VF Remoting Client Potential XSRF**

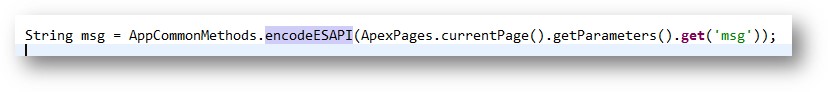
-          Update the platform settings appropriately (Please see the screenshot below. Make sure the CSRF Protection is checked)

-          Use encoding library from ESAPI package to encode the values while dealing with those variables within JavaScript.

As provided in the Checkmarx report:



     We can also encode the parameters on controller side by using the ESAPI method. This has been added in the AppCommonMethods class, and can be used in the following way:





**XSRF**

-          Update the platform settings appropriately

-          Use POST method to submit the id value instead of GET method that makes your value as part of query string. OR Introduce the confirmation box before actually deleting or updating the record, in our case the business team may not allow this.

**Client Use Of JQuery Outdated Version**

-          Upgrade JQuery library inclusion to the latest version, this does not seem to be developers mistake but since JQuery is continuously evolving and issues are getting fixed as identified it is necessary to use recent version as much possible. It is recommended to use JQuery in static resource, so that upgrading to newer version should be an easy thing to do.

-          Also observed that one of the instance is referring to geopointe managed package, which seems to be not in use. If really not required, then remove this package from org before next submission.

**VF Remoting Client Potential XSS**

-          Encode the data when it is received by your remoting callback and decode it before using, also some length or char validation can be applied. In case of HTML text returning, validate it with string size range and beginning and ending char of contents.

-          **Chances are high that most of these are false positive.**

**Note**: Check with the platform settings which could help you fixing many of these issues without code change, you can find this at Setup->Session Settings