MyProject

- Dashboard
- My Projects
- Holiday List
- More
  Help

- R

- Ramakrishnan V
  Manage Profile Preference Change Password
  Logout

Discussions (PAMAC (Cloud Version))

Home Requirements Discussions Documents Daily Updates Changes Bugs

Posted By : Manas Dasgupta
Assigned To : (All Members)
D211
Date & Time : 18-11-2019 09:28:AM
Bhavana Pachpande | RES - VAPT

Hello,

Please note below attached RES - VAPT excel sheet, we shall use this thread to post any discussion or new update and changes regarding VAPT here.

RES VAPT.xlsx
↧ Download

Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 21-11-2019 04:58:PM
Hello mam,

As discussed high level threat points VAPT points to be done around next week. As such no new development and deployment will take place in live server, in case of any query regarding development please discuss with Sir Siddharth.

First VAPT high points will be done and then will go with medium and finally low points.
Each of them will be updated in country demo and live server both.

Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 25-11-2019 11:15:AM
Hello mam,

As discussed on phone, VAPT high points changes :

1) No direct URL access i.e copying and pasting any menu url won't work you need to click on links inorder to navigate to desired menu.

2) Menu access as per designation rights. Any lower designation employee cannot access higher level designation menu if they know the menu URL and directly access it in browser tab.

3) XSS filtering will be added to avoid Cros Site Scripting attacks after discussion of which characters to allow or to reject , as per VAPT point they have mentioned the following statement:

"The application should not accept any script, special character or HTML in fields whenever not required. It should escape special characters that may prove to be harmful. Some of the main characters used in scripts that must be escaped are as follows:
( ) ' " / ; * ; : = { } `(backtick) % + ^ ! - x00-x20 (x is a hexadecimal notation ; it includes Space, Tab, CarriageReturn, and LineFeed.)"

Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 02-12-2019 10:22:AM
Hello mam,

VAPT Point No. 7 : "Missing HTTP Headers" are updated in demo and live server both.
Please check.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 02-12-2019 02:45:PM
Hello mam,

As discussed on phone due to addition of new headers for XSS filter, issue was seen in chrome browser during send to client. As such following 2 lines are commented for now till we find any alternative solution.

Header always set X-XSS-Protection "1; mode=block"
Header always set X-Content-Type-Options nosniff
Posted By : Dipika Yedge
Assigned To : Bhavana Pachpande
D211
Date & Time : 04-12-2019 04:49:PM
Hi,

As discussed with Ajit Sir please upload the changes on live site.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 04-12-2019 04:53:PM
Hi,

Found some minor issues while testing in demo server, fixed them and update code also.

Will prepare files tomorrow and upload in live server.
Posted By : Bhavana Pachpande

Assigned To : Dipika Yedge
D211
Date & Time : 05-12-2019 01:37:PM
Hello mam,

VAPT point changes pushed to live server, please check and confirm.

Please logout and login again to see changes in effect.
Posted By : Super Admin
Assigned To : (All Members)
D211
Date & Time : 06-12-2019 07:21:AM
All points completed?
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 06-12-2019 06:03:PM
Hello sir,

VAPT point -1 high priority change is completed and uploaded on live server. Next will update codeigniter version and then move to point 2(XSS filtering) and then point 3 (CSRF token).

Hello mam,

As per email received documentation for VAPT point-1 changes is prepared, please check excel sheet.

As per discussion with Sir Kailash pamac php framework "**Codeigniter**" version is to be updated to the latest stable version.

Current **Codeigniter** version is 2.1.4 and latest stable version is CodeIgniter 3.1.11

Reference URL : https://codeigniter.com/download

RES VAPT Point-1 Documentation_06-12-2019.xlsx
↧ Download
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 10-12-2019 09:11:AM
Hello mam,

Web app i.e php framework " **Codeigniter** " version update done to 3.1.11 from 2.1.4.
Files are updated in country demo server, will prepare the same for live server today.

Please check thoroughly before uploading files in live server. We will check from our end also.
Posted By : Dipika Yedge
Assigned To : Bhavana Pachpande
D211
Date & Time : 11-12-2019 12:19:PM
Hi,

Have process test case on demo, no issue found while processing.

Posted By : Bhavana Pachpande

Assigned To : Dipika Yedge
D211
Date & Time : 11-12-2019 05:12:PM
Hello mam,

As discussed will update files tomorrow morning for version update in live server.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 12-12-2019 07:58:AM
Hello mam,

Web app version is updated to 3.1.11, please check in case of any issue let us know. Will monitor today for any issues.

Also VAPT point No. 7 "Missing HTTP Headers" is also updated in live server with XSS headers. Exception only the "X-Content-Type-Options nosniff" won't work in "Send to client" and "Export" menus. Please inform Sir Ajit also. As both these menus are causing issue due to activation of nosniff header.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 17-12-2019 09:07:AM
Hello mam,

Form View related design issue after version upgrade are fixed and updated in both live and demo server. Please check and confirm.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 02-01-2020 11:50:AM
Hello mam,

VAPT point -2 (XSS filtering) high priority change is completed and uploaded on demo server.
Please check and confirm before upload in live server.
Posted By : Super Admin
Assigned To : (All Members)
D211
Date & Time : 03-01-2020 07:40:AM
All completed VAPT high priority changes go online next week on India & Dubai server without further writing for confirmation.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 07-01-2020 12:26:PM
Hello mam,

VAPT point -2 (XSS filtering) high priority change is completed and uploaded on live server. In case of any related issue please let us know.
Posted By : Manas Dasgupta
Assigned To : Dipika Yedge
D211
Date & Time : 10-01-2020 01:03:PM
Currently working on emergency bug B413 : Dubai case id issue as per discussion with Mam Dipika. Will resume vapt task once completed.

Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 13-01-2020 09:48:AM
Hello mam,

VAPT point no - 4 (**Session cookie attributes are not set properly**) is updated in both demo and live server. In case of any related issue please let us know.

Total - VAPT - 4 points updated in live server. (1,2,4,7)

Note : **Exceptions >**

--

1) Point -2 : XSS filter
a) It is removed for "/user/reports" module due to issue occurred as discussed on phone for excel file showing direct sql query and Case details mis is blank. Will check and modify xss code for this module manually and update here once done.

b) Due to Dubai bug **B413** >> **part of XSS** filtering is modified per new codeigniter version 3 for (% space) in any string converted to garbage character thus causing string to truncate at that point(% space) and save in database .

Ref URL 1: Issue >> https://github.com/bcit-ci/CodeIgniter/issues/4877
Ref URL 2: Fix >> https://github.com/bcit-ci/CodeIgniter/issues/5225

2) Point -4 : Cookie path is kept (/) rather than any specific path as per mentioned in the VAPT excel doc. Because it was causing issue while logging in when path is set to any other than (/) i.e root path.

3) **Point -7 : (Missing HTTP Headers) Below code is added in server config file (.htaccess)**

#XSS- Protection : REF URL : https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection?utm_source=mozilla&utm_medium=devtools-netmonitor&utm_campaign=default

```
<FilesMatch ".(htm|html|php|jpe?g|png|gif|js|ico|pdf|txt|xls|xlsx|csv|xml|woff|swf|zip)$">
   Header always set X-XSS-Protection "1; mode=block"
   Header always append X-Frame-Options SAMEORIGIN
   Header always set Content-Security-Policy "default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; font-src 'self' https://fonts.gstatic.com;"
   #Header always set X-Content-Type-Options nosniff # Issue in send to client and export module
   Header always set Strict-Transport-Security "max-age=16070400; includeSubDomains; preload" env=HTTPS
   Header always set Referrer-Policy origin
   Header always edit Set-Cookie ^(.*)$ "$1; HTTPOnly; Secure; SameSite=Strict"
</FilesMatch>
```

a) Here **extra security** is added for asset(Ex js,css,images..) loading to be done from same domain. Except for fonts (https://fonts.gstatic.com) using below code

Header always set Content-Security-Policy "default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline'; font-src 'self' https://fonts.gstatic.com;"

b) Here ::<< **Header always set X-Content-Type-Options nosniff >>** is commented and using in coding php files directly due to issue in send to client in chrome browser which was directly printing the javascript code in browser as such send to client/export module are removed from '**nosniff**"

Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 20-01-2020 02:43:PM
Hello mam,

VAPT point-6 is updated in live server. Please let us know in case of any issue. Jquery main library is updated to latest version 3.4.1

Also css and js are minified to improve load time.

Note : For some Jquery library like fancytree, jquery.scrolltable, fancybox their version of jquery is used if the version is updated to latest then it is causing error like no scrollbar on list pages no popups, client assign tree structure disappears due to js errors.
Posted By : Super Admin
Assigned To : (All Members)
D211
Date & Time : 22-01-2020 11:06:AM
Note : For some Jquery library like fancytree, jquery.scrolltable, fancybox their version of jquery is used if the version is updated to latest then it is causing error like no scrollbar on list pages no popups, client assign tree structure disappears due to js errors.

We must resolve the conflict in long term. No old versions should be used.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 23-01-2020 04:42:PM
Ok sir, we will search for alternative plugins if no other solution is found.

Also tomorrow Manas will be working on bug B415 as per discussion with Pamac Team.
Mam Dipika please confirm.
Posted By : Dipika Yedge
Assigned To : Bhavana Pachpande
D211
Date & Time : 23-01-2020 04:49:PM
Hi

It is ok to search for alternate plugins for the resolutions.

However bugs resolution is always the priority so Manas will work as discussed.
Posted By : Super Admin
Assigned To : (All Members)
D211
Date & Time : 24-01-2020 09:02:AM
I hope PAMAC team understand security compromise and data breach.
They are better aware of Financial data and bank concerns.

I will have further discussion with PAMAC Management, if we should decide team schedule or PAMAC?

Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 24-01-2020 05:25:PM
Please note as of BUG - B419 Dubai google map issue 2 major updates in VAPT point have been done.
1) .htaccess : Point No 7 updated to allow google api urls for image loading

Header always set Content-Security-Policy "default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://maps.googleapis.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; font-src 'self' https://fonts.gstatic.com; img-src 'self' https://maps.gstatic.com https://maps.google.com https://maps.googleapis.com data:"

2)XSS(VAPT point 2) - unable to create google map image for case id 102039126. The base64 code of image send through post after XSS filtering was getting corrupted.
Function name mapToJpg() >path> controllers/userlogin/mapToJpg.
Removed XSS filtering from there.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 29-01-2020 05:18:PM
Please note as of BUG - B415 PDF export issue 1 minor update in VAPT point has been done.

1) /models/Commonfunmodel.php >> Function >> post_removeTags()

Because of XSS filtering applied in pdf design report format the function >> post_removeTags() used to remove script tags added <!DOCTYPE.. in the final html thus causing the html in pdf to break if multiple cases are exported at the same time. For a single case it works ok.

Now function is modified to use string replace instead of PHP HTML DOMPARSER.

Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 31-01-2020 12:39:PM
Hello mam,

VAPT Point-5 sql query in http request changes are done and updated demo and live server.
In case of any issue please let us know we shall revert.

Also as discussed should the same change be done on **Templates** > **Report Creation** menu ?
Posted By : Dipika Yedge
Assigned To : Bhavana Pachpande
D211
Date & Time : 31-01-2020 12:53:PM
Should the same change be done on **Templates** > **Report Creation** menu ? -
As discussed with Ganesh Sir, no need to change existing menu

Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 31-01-2020 01:46:PM
Ok mam. As such VAPT point - 5 is completed to remove sql from http request for user reports.

Remaining one major VAPT point-3 , CSRF changes, Here as per excel sheet only one URL is given to make changes should we do it in entire application or for that URL only.

URL >> https://pms.resoftech.com/admin/master/index/employeeassign
Posted By : Super Admin

Assigned To : (All Members)
D211
Date & Time : 03-02-2020 09:59:AM
Bhavana, This question should not be asked.
Security is TOP priority, you should consult everything with me for VAPT.

Posted By : Bhavana Pachpande
Assigned To : (All Members)
D211
Date & Time : 13-02-2020 07:57:AM
ok sir.
Posted By : Manas Dasgupta
Assigned To : Dipika Yedge
D211
Date & Time : 13-02-2020 04:52:PM
Hello mam,

Currently VAPT point is on hold as i am working on bugs now.
Posted By : Super Admin
Assigned To : Manas Dasgupta
D211
Date & Time : 09-03-2020 10:29:AM
Which Point remain, and when we are completing it?
Posted By : Manas Dasgupta
Assigned To : Dipika Yedge
D211
Date & Time : 24-03-2020 10:07:AM
Point 3 CSRF is remaining will complete this after Dubai domain bug is completed.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 17-04-2020 03:31:PM
Hello mam,

Point 3 CSRF is remaining will complete this as per new task list priority.
Posted By : Dipika Yedge
Assigned To : Bhavana Pachpande
D211
Date & Time : 20-05-2020 06:31:PM
Okay
Posted By : Super Admin
D211
Date & Time : 20-05-2020 09:52:PM
Question is on Hold.
Posted By : Bhavana Pachpande
Assigned To : Ajit Kedare
D211
Date & Time : 27-05-2020 04:54:PM
Hello sir,

As per today's telephonic discussion regarding VAPT remaining points i.e related to point 3 : CSRF token, it is a huge change throughout application as all the forms in res needs to be modified to allow add of token. Minimum 10 days will require for development till demo server. Please check Task list for assigned priority of this task mentioned in **D217**.

Also note:
1) It can cause issue in form submitting if user tries to submit form again by clicking on reload button because f token mismatch. Page must be properly reloaded for new token to generate.
2) Ajax call won't be included for token checking. Ajax call are used for dynamic dropdown and a few other function where page is not fully loaded.

Posted By : Super Admin
Assigned To : Ajit Kedare
D211
Date & Time : 28-05-2020 11:54:AM
Hope this helps, you may submit working progress report.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 05-10-2020 05:37:PM
Hello mam,

As discussed VAPT point CSRF will affect all forms in web application for both India and Dubai domain.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 07-10-2020 04:34:PM
Hello ,

As discussed CSRF changes till date are updated on demo server, for you to check. There will be issues in some form submits and dependable dropdown , please report when found.

If major issue occurs we will disable it as Vendor related testing will start from your ops team.
Posted By : Manas Dasgupta
Assigned To : Dipika Yedge
D211
Date & Time : 13-10-2020 05:22:PM
Hello mam,

Please note below **points** :
1) One form must be submitted at a time when CSRF token regeneration is disabled.
2) Token is valid for 2hrs if not used.
3) If token regeneration is not required then one single token can be used throughout session for all form submition. This can be helpful when submitting multiple forms in different tabs.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 29-10-2020 04:36:PM
Hello mam,

CSRF protection is enabled in country demo server for testing, in case of any issue please let us know.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 24-11-2020 03:38:PM
Hello mam,

Fix for dependable dropdown due to csrf token issue is added in demo server, and also hr related modules.

Please check in case o any issue let us know.

Posted By : Bhavana Pachpande
Assigned To : (All Members)
D211
Date & Time : 30-11-2020 08:50:AM
Hello,

As discussed with Sir Siddharth please let us know when we can prepare files for live, as without this point on live server we can not do Server fall back test.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 14-12-2020 04:49:PM
Hello mam,

As discussed it will take upto 5 days to prepare files in live copy and upload.
Posted By : Bhavana Pachpande
Assigned To : Dipika Yedge
D211
Date & Time : 22-12-2020 12:55:PM
Hello mam,

Changes are uploaded in live server for India and Dubai server both. Please check and let us know in case of any issue.
Posted By : Dipika Yedge
Assigned To : Bhavana Pachpande
D211
Date & Time : 04-01-2021 11:40:AM
Please close this discussion
Posted By : Super Admin
D211
Date & Time : 15-01-2021 07:15:AM
Question is closed.

Reply Cancel