MyProject

Discussions (PAMAC (Cloud Version))

Home Requirements Discussions Documents Daily Updates Changes Bugs

Posted By : Ajit Kedare
Assigned To : (All Members)
D279
Date & Time : 10-06-2023 08:14:PM
Megha Gavankar | VAPT web and mobile app mitigatin

Hi,
VAPT for web and mobile app conducted, please find attached observations , also sharing the VAPT report for reference.
we need to mitigate the observations and confirm the vendor for post mitigation testing
please help closing the same

password for the attachment will be shared seperatly.

Mob and app VAPT.xlsx
↧ Download
Mobile_Application_Security_Testing_Report_PAMAC_RES 2 8 2_Android_v1 0.pdf
↧ Download
Web_Application_Security_Testing_Report_of_PAMAC_Online_System_V1 0-2.pdf
↧ Download
Posted By : Manas Dasgupta
Assigned To : Ajit Kedare
D279
Date & Time : 19-06-2023 08:25:AM
Hello sir,

Please confirm if this thread is of high priority now. Should i start checking and working on Vapt we app ?
Posted By : Manas Dasgupta
Assigned To : Ajit Kedare
D279

Date & Time : 19-06-2023 04:56:PM
Hello sir,

For vapt point 1 : Sensitive Data Exposed ; the info.php file is removed from demo India aws server.

It is not present in live server. Screenshot attached.

↧ Download
Posted By : Manas Dasgupta
Assigned To : Ajit Kedare
D279
Date & Time : 21-06-2023 11:29:AM
Hello sir,

Excel sheet for new 2023 VAPT points are updated, please check.
Each task will be worked on, in the order as mentioned in the excel.

Note: For **mobile app VAPT** points please discuss with Android developer and let us know if any more new changes are to be done in webservice. Old Mobile app VAPT points are present in demo server only and not live server for both India and Dubai.
Refer discussion: **D222**

Mob and app VAPT.xlsx
↧ Download
Posted By : Manas Dasgupta
Assigned To : Ajit Kedare
D279
Date & Time : 22-06-2023 12:55:PM
Hello sir,

As discussed with Sir Siddharth, please set priority of task new added in support task point 92 and 93.
Which is to be done first ?
Posted By : Manas Dasgupta
Assigned To : Ajit Kedare
D279
Date & Time : 22-06-2023 01:27:PM
Hello sir,

Few more updates are added for VAPT web application, please check excel for updated Shimbi remarks.

For point 2 - The server supports weak SSL/TLS ciphers and weak TLS version.

Below is the response from yrhost, email is also forwarded :

"2. The server supports weak SSL/TLS ciphers and weak TLS version." in pdf file.

We can remove old TLS versions and ciphers but that would mean old windows OS, old andriod versions and old browser will no longer be able to load webpage under https.

Please confirm and we can remove it. Also note it is marked as "LOW" risk under pdf.

Mob and app VAPT.xlsx
↧ Download
Posted By : Ajit Kedare
Assigned To : Manas Dasgupta
D279
Date & Time : 22-06-2023 02:51:PM
Dea Manas,

please refer attached excel, i have updated the comments
kindly share your availability for arranging the call with VAPT vendor.

Mob and app VAPT.xlsx
↧ Download
Posted By : Manas Dasgupta
Assigned To : Ajit Kedare
D279
Date & Time : 22-06-2023 02:52:PM
Hello sir,

We can discuss tomorrow 11 am or 11:30 am, let me know.
Posted By : Ajit Kedare
Assigned To : Manas Dasgupta
D279
Date & Time : 22-06-2023 04:07:PM
Dear Manas,

i discussed with VAPT vendor, they will be available for discussion on Monday 26-june-2023 at 11:30 AM they will be sharing the meeting link for the same. will share the link once received from vendor.
Posted By : Manas Dasgupta
Assigned To : Ajit Kedare
D279
Date & Time : 22-06-2023 04:18:PM
Hello sir,

On Monday i will be on leave, please schedule for Tuesday.
Posted By : Ajit Kedare
Assigned To : Manas Dasgupta
D279
Date & Time : 22-06-2023 05:32:PM
Dear Manas

Please find meeting link for Tuesday 27 june 2023 at 11:30 am

https://meet.google.com/cig-qqte-uty

Posted By : Manas Dasgupta
Assigned To : Ajit Kedare
D279
Date & Time : 27-06-2023 05:49:PM
Hello sir,

As discussed in today's meeting below is the attached updated excel.

Mob and app VAPT.xlsx
↧ Download
Posted By : Manas Dasgupta
Assigned To : Dipika Yedge
D279
Date & Time : 07-07-2023 02:18:PM
Hello mam,

VAPT web app, Point 3 and Point 6 changes are updated in demo server for both India and Dubai, please check if any issue in login for any users as changes are present in login.

Note:
1) Check bank login URL also.
2) RSA public/private key pair with passphrase is used for **password** encryption and decryption during the process of login form submission and verification.
Posted By : Dipika Yedge
Assigned To : Manas Dasgupta
D279
Date & Time : 10-07-2023 02:31:PM
Hi,

As discussed it's working proper.

Please upload the changes on live server
Posted By : Manas Dasgupta
Assigned To : Dipika Yedge
D279
Date & Time : 10-07-2023 05:03:PM
ok mam, will start changes for live and push tomorrow.

Also point 4 changes are uploaded in demo server. Related to js file update.
Posted By : Manas Dasgupta
Assigned To : Ajit Kedare
D279
Date & Time : 10-07-2023 05:03:PM
Hello sir,

Reply for TLS update in server came for rollback, please check email and let us know what is to be done.
Posted By : Manas Dasgupta
Assigned To : Dipika Yedge
D279
Date & Time : 11-07-2023 09:21:AM
Hello mam,

VAPT web app, Point 3 and Point 6 changes are updated in live server for both India and Dubai, please check now logins for both bank url and normal login.

Posted By : Manas Dasgupta
Assigned To : Dipika Yedge
D279
Date & Time : 11-07-2023 02:03:PM
Hello mam,

VAPT web app, Point 4 changes are updated in live server for both India and Dubai, please let us know in case of any complain for UI related issues.
Posted By : Manas Dasgupta
Assigned To : Ajit Kedare
D279
Date & Time : 18-07-2023 05:13:PM
Hello sir,

For VAPT point 5, simultaneous login there are 2 options, please let us know which to implement :

1) The last time user logged in will be treated as a valid login and if same user was logged in previously in any web app device will be logged out after 5 min. For this a server request will be send every 5 min for every user logged in or we can logout the previous user if he does any action like click on menu or button.

2) The first time use logged in will be treated as a valid login and if the same user tries to login in next time in any web app device then it won't allow it.

Note point 2 Drawback: Unless the user logged in first time, logs out next login won't happen. Also in case user closes the browser or system i.e session lost without click on logout menu then the user can never login next time.
He has to inform Res to request for new login or we can set an fixed hour for next login.
Posted By : Megha Gavankar
Assigned To : Manas Dasgupta
D279
Date & Time : 27-09-2023 03:39:PM
Hello sir,

As Discuss on call VAPT list is already shared in this please check
Posted By : Megha Gavankar
Assigned To : (All Members)
D279
Date & Time : 27-09-2023 03:42:PM
Hello Sir,

Current task update on VAPT mobile.

VAPT Mobile Task Update.xls
↧ Download
Posted By : Ajit Kedare
Assigned To : (All Members)
D279
Date & Time : 30-10-2023 04:57:PM
As discussed in call today, please refer attached update on VAPT,
need to start patching as per assignment.

Mob and app VAPT.xlsx
↧ Download

Posted By : Manas Dasgupta
Assigned To : Megha Gavankar
D279
Date & Time : 09-11-2023 10:16:AM
Hello mam,

Below is the password policy used in web app:

1) minimum password character length is **8**
2) maximum password character length is **16**
3) Must not match last password
4) Allow alpha numeric special characters as below rule (regular expression shared):
---
a) ATLEAST_ONE_NUMBER - "/^[A-Za-z]*$/"
b) ATLEAST_ONE_CHAR - "/^[0-9]*$/"
c) ATLEAST_ONE_UPPERCASE_CHAR - "/[A-Z]/"
d) ATLEAST_ONE_LOWERCASE_CHAR - "/[a-z]/"
e) ATLEAST_ONE_SPECIAL_CHAR - "#[~`!@#$%^&*()_-+={}[]|:;<>.,'"s?/\\]+#"

Reply Cancel