



- [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 : Bhavana Pachpande

Assigned To : (All Members)

D222

Date & Time : 27-11-2020 12:02:PM

Ajit Kedare | VAPT Point for Mobile App

Hello team,

As discussed below files are attached regarding VAPT points for Mobile application.

Password for pDF :

passworld: qseap@pamac2020

Mobile_APP_VAPT_observations.xlsx

↓ Download

Qseap-Pamac_RES Mobile Application security Report_v1.0.pdf

↓ Download

Posted By : Bhavana Pachpande

Assigned To : Dipika Yedge

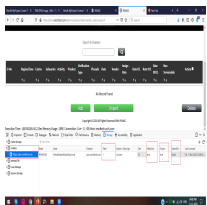
D222

Date & Time : 11-12-2020 04:12:PM

Hello mam,

As discussed please check attached screenshot for Mobile VAPT point : 16 (Session cookie path attribute not set).

This is for web in Live India server.



↓ Download

Posted By : Jayshree

Assigned To : Bhavana Pachpande

D222

Date & Time : 14-12-2020 08:01:PM

HI,

As discussed with manas sir Vulnerabilities An adversary can check other user's cases and submit it by changing request parameter and An adversary can bypass authentication using response manipulation need jwt for sever site validation.

SQL Injection attack might be possible on the application =Its done from res app mobile ,must sanitize the input string to avoid an SQL injection attack from server side .

and for Sensitive information such as username and passwords are transmitted in plain text,here we are Doing RND on that.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 15-12-2020 05:15:PM

Hello,

SQL Injection attack might be possible on the application =Its done from res app mobile ,must sanitize the input string to avoid an SQL injection attack

As per discussion webservice is updated for login for xss filter and remove =.
Please check now.

Posted By : Dipika Yedde

Assigned To : Bhavana Pachpande

D222

Date & Time : 22-12-2020 02:00:PM

Hi Manas,

As discussed please start to work on it,

Posted By : Super Admin

Assigned To : (All Members)

D222

Date & Time : 23-12-2020 06:42:AM

Can you add what was discuss here? This is essential to keep track of every updates.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 23-12-2020 12:50:PM

Hello,

SQL Injection attack might be possible on the application =Its done from res app mobile ,must sanitize the input string to avoid an SQL injection

As per discussion webservice is updated for login for xss filter and remove =.

Please check and update here so that we can put changes on live also.

Posted By : Jayshree

Assigned To : Bhavana Pachpande

D222

Date & Time : 24-12-2020 07:07:PM

hi,

As discussed with manas sir AES encryption algorithm will be implement from mobile app site. for web site refer

<https://aesencryption.net/>

<https://stackoverflow.com/questions/44234719/encryption-between-php-java>.

here searching how to make disable Trace method is enabled .

Posted By : Super Admin

Assigned To : (All Members)

D222

Date & Time : 15-01-2021 07:15:AM

Where we now?

Posted By : Manas Dasgupta

Assigned To : (All Members)

D222

Date & Time : 15-01-2021 07:54:AM

We are working on the xss filter and encryption/decryption of data when exchanged to and from mobile app to our web server.

2nd we will work on JWT implementation. Token based data exchange.

Posted By : Super Admin

Assigned To : (All Members)

D222

Date & Time : 18-01-2021 06:43:AM

Ok thanks for updates

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 22-01-2021 05:33:PM

Hello,

As per email send to you please find the alternative for encryption and decryption using JAVA for mobile app.

We will use `openssl_encrypt()` method : with "AES-256-CBC" algorithm. Same for decryption.

File attached.


PHP Ref URL :

Ref. URL : <https://www.php.net/manual/en/function.openssl-encrypt.php>

For testing you can check below url : after the /test/ in url add any string it will show the output

Test URL: https://country-pamac.urdemo.net/web-service/api_live_2_3/test

 enc-dec.zip

 Download

Posted By : Super Admin

Assigned To : Jayshree

D222

Date & Time : 27-01-2021 06:23:AM

Hope this helps ...

By when we can close this thread?

Posted By : Jayshree

Assigned To : Super Admin

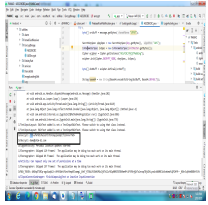
D222

Date & Time : 10-02-2021 05:53:PM

hi,

Encryption decryption done from mobile app site.

In php code have used secret_key is 14 character but in app site need 16 character so we have added two more character after that its get execute successfully,please check code.



Download

after testing got this result.

encry_decrypt_code.txt

Download

From above php reference,we have implemented in our java code app site.you can check this file

Posted By : Super Admin

Assigned To : Manas Dasgupta

D222

Date & Time : 11-02-2021 06:24:AM

Please check and see what else remain here...

Please conclude thread if all done

Posted By : Manas Dasgupta

Assigned To : Jayshree

D222

Date & Time : 11-02-2021 05:34:PM

Hello team,

Task list is updated and shared by Mam Dipika D217. Please check priority.

Also as per current task Revised VAPT point for web are to be done first and then Mobile app VAPT points.

@Jayshree, please discuss with Sir Ajit for any query.

For secret_key 14 character but in app site need 16 character, i will make changes in test webservice tomorrow and update you for the same.

Posted By : Manas Dasgupta

Assigned To : Jayshree

D222

Date & Time : 12-02-2021 04:15:PM

Hello Jayshree,

I have updated login method to decrypt the encrypted data of username and password. Please make changes from you end in mobile app and send the encrypted format of username and password.

And check if you are able to login from mobile app.

Also in order to test you can change the login end point to :

https://country-pamac.urdemo.net/webservice/api_live_2_3/test

It will response with the decrypted Username and Password.

Posted By : Jayshree

Assigned To : Manas Dasgupta

D222

Date & Time : 16-02-2021 06:02:PM

hi,

With the help of manas sir,

We have updated the same from mobile app side,

encrypted format of username and password we are sending from mobile to the server,and its get successfully decrypting from server.

Posted By : Manas Dasgupta

Assigned To : Jayshree

D222

Date & Time : 22-02-2021 02:44:PM

Hello,

As discussed please confirm if we can put this point on live server for both India and Dubai domain.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 04-03-2021 05:23:PM

Hello team,

As discussed will start implementation of JWT for webservice from 08-03-2021.

This point will require webservice changes first for token creation , after that mobile app changes will have to be done to save the token received during login and send it back with every request for data validation.

And also handle error if any.

Posted By : Jayshree

Assigned To : Bhavana Pachpande

D222

Date & Time : 24-03-2021 05:06:PM

hi,

In res demo login updated jwt token by manas sir,

We have checked with android studio , received token in response,
now need to update token given api

UserApi

@POST

<https://country-pamac.urdemo.net/sendDataToServerWFile>

@POST

<https://country-pamac.urdemo.net/changePassword>

CaseApi

@POST

<https://country-pamac.urdemo.net/sendList>

@POST

<https://country-pamac.urdemo.net/sendReject>

@POST

<https://country-pamac.urdemo.net/sendFeLog>

@POST

<https://country-pamac.urdemo.net/sendRequest>

@POST

<https://country-pamac.urdemo.net/uploadFile>

@GET

<https://country-pamac.urdemo.net/downloadFileByUrl>

Posted By : Manas Dasgupta

Assigned To : Jayshree

D222

Date & Time : 25-03-2021 10:34:AM

Hello team,

Following method is not found in webservice :

<https://country-pamac.urdemo.net/sendDataToServerWFile>

Also i think the urls mentioned above are wrong it should be like :

https://country-pamac.urdemo.net/webservice/api_live_2_3/**methodName**

Posted By : Jayshree

Assigned To : Manas Dasgupta

D222

Date & Time : 30-03-2021 06:03:PM

Dear sir,

sorry....Yes,url like https://country-pamac.urdemo.net/webservice/api_live_2_3/**methodName**

We have implemented getJWTtoken successfully while changing password in res app and also implemented in saveFeLog.

Posted By : Manas Dasgupta

Assigned To : Jayshree

D222

Date & Time : 31-03-2021 10:30:AM

Hi,

Please check below mentioned endpoints are not found in country demo server webservice file.

Not found:

<https://country-pamac.urdemo.net/sendDataToServerWFile>

<https://country-pamac.urdemo.net/sendList>

<https://country-pamac.urdemo.net/sendReject>

<https://country-pamac.urdemo.net/sendRequest>

<https://country-pamac.urdemo.net/uploadFile>

<https://country-pamac.urdemo.net/downloadFileByUrl>

Posted By : Jayshree
Assigned To : Manas Dasgupta
D222
Date & Time : 31-03-2021 01:13:PM
Hi,

After checked Api_live_2_3 file from manas sir api is like that

for sendDataToServerWFile

https://country-pamac.urdemo.net/webService/api_live_2_3/saveData

for sendList and sendReject

https://country-pamac.urdemo.net/webService/api_live_2_3/caseAck

for sendRequest

https://country-pamac.urdemo.net/webService/api_live_2_3/checkClosedCases

for uploadFile

https://country-pamac.urdemo.net/webService/api_live_2_3/downloadImages

Posted By : Manas Dasgupta
Assigned To : Jayshree
D222
Date & Time : 31-03-2021 03:39:PM
Hello mam,

As discussed, changes for token validation are done and uploaded in demo server. Please make changes from your end also and check entire flow. In case of any issue please update here.

Points to do:

- 1) For token expiry or invalid or any other exception, please logout **user from mobile app**.
- 2) During **logout** process please add a callback to webservice api with token to capture fe logout date time in server side also and we can also store the logout reason if required for log.
- 3) Please discuss with **Sir Ajit or Sir Ganesh** and update here to set token expiry time. Currently it is set to 24 hours in demo server.

Posted By : Jayshree
Assigned To : Manas Dasgupta
D222
Date & Time : 31-03-2021 06:01:PM
Dear sir,

Token implementation for all api done from mobile app side and also tested end to end point.
token expiry logic part is not completed.we are working on that.

Discussed with ajit sir, they said keep session 24 hours as it is.

Posted By : Manas Dasgupta
Assigned To : Jayshree
D222
Date & Time : 01-04-2021 09:08:AM
ok mam

Posted By : Bhavana Pachpande
Assigned To : Jayshree
D222
Date & Time : 02-04-2021 04:04:PM
Hello,

As discussed for logout from mobile app due to

- 1) Token exception and
- 2) User Click on Logout from menu(New feature to be added by you on mobile app)

api will be called from your mobile application to webservice to capture the logout datetime.

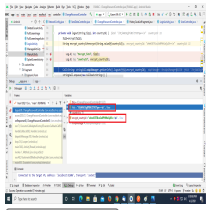
End Point : https://country-pamac.urdemo.net/webService/api_live_2_3/logout

Please make necessary changes and update here once done.

Posted By : Jayshree
Assigned To : Bhavana Pachpande
D222
Date & Time : 02-04-2021 07:16:PM

Dear sir,

we have consuming https://country-pamac.urdemo.net/webservice/api_live_2_3/logout api only in change password for testing and even we are encrypting feId and countryId while user login and logout,



Download

Please check screen shoot ,encrypted feId and countryId .

Posted By : Jayshree

Assigned To : Bhavana Pachpande

D222

Date & Time : 03-04-2021 06:23:PM

hi,

we have implemented token expiration logout api, used logoutController class in every api, please check encrypted feId and countryId.

Posted By : Manas Dasgupta

Assigned To : Jayshree

D222

Date & Time : 05-04-2021 04:32:PM

Hello mam,

As discussed on phone please check with playstore support team to upload app in google playstore as we need to put the mobile vapt point changes in live server also.

Also please do a invalid token test from mobile app to check if proper logout is done from all end points.

Posted By : Jayshree

Assigned To : Manas Dasgupta

D222

Date & Time : 06-04-2021 12:39:PM

Dear Sir,

We have checked invalid token test from mobile app and its done from all end points,

Yes, We are also trying to upload the apk on Google playstore.

Posted By : Manas Dasgupta

Assigned To : Jayshree

D222

Date & Time : 06-04-2021 05:15:PM

Hello mam,

Please let me know when upload is done. so that i can push changes in live server also.

Please note that this will also affect **Dubai mobile app**.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 14-04-2021 08:07:AM

Any updates ?

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 26-04-2021 05:11:PM

Hello mam,

Any updates ?

Posted By : Jayshree

Assigned To : Bhavana Pachpande

D222

Date & Time : 27-04-2021 05:14:PM

hi,

Mobile Vapt ponts have been done by our side. Also gave apk for testing.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 28-04-2021 12:03:PM

ok mam,

Please let us know when can we upload changes in live server.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 10-05-2021 02:57:PM

Hello mam,

Any updates when we can upload changes in live server.

Posted By : Jayshree

Assigned To : Bhavana Pachpande

D222

Date & Time : 10-05-2021 03:28:PM

hi,

I spoke to Ajit sir, He said that we do it live only after receiving the vapt test report.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 12-05-2021 10:24:AM

Hello mam,

And by when are we will get the test report ?

Posted By : Super Admin

Assigned To : Ganesh Sawant

D222

Date & Time : 24-05-2021 05:00:PM

How long only my team expected to wait?

Posted By : Jayshree


Assigned To : Super Admin

D222

Date & Time : 07-06-2021 03:38:PM

Dear sir manas,

As discussed on call some VAPT points report, here we are sharing excel, please check .

 Mobile VAPT post mitigation observations.xlsx

[Download](#)

PFA

Posted By : Super Admin

Assigned To : Manas Dasgupta

D222

Date & Time : 07-06-2021 04:03:PM

Masan for you

Posted By : Manas Dasgupta

Assigned To : Dipika Yedge

D222

Date & Time : 07-06-2021 05:09:PM

Hello mam,

Need to discuss task priority, please let me know if we can discuss tomorrow.

Posted By : Bhavana Pachpande

Assigned To : Ganesh Sawant

D222

Date & Time : 08-06-2021 03:21:PM

Hello sir,

As per discussion with Mam Kavita, please let us know if we can start working on mobile vapt new points.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 09-06-2021 04:44:PM

As discussed with Mam Kavita, we have started to work on this task from today.

Also for your query regarding development time, it will take 12 to 16 days.

For token expiry the entire jwt process token validation will have to be changed now, as it will be stateful now.

The firebase JWT library doesn't have any manual or forceful token expiry method, we have to store all token in db on logout and check on every request if it has already been used or not.

Posted By : Jayshree

Assigned To : Bhavana Pachpande

D222

Date & Time : 14-06-2021 05:42:PM

Dear sir manas,

change password using encryption

When We checked using encryption ,

after tried change the password in the mobile, got error message appears "Try again ,Invalid OLD password"

When trying to change the password without using encryption,

The password is allowed change, but unable log in with new change password, still it took old password.
need to check from backend side may be something went to wrong.

Recaptcha token:

IN res Login page and change password we are implemented recaptcha using token, here we creating token with the help of google API, that token we will send to server side

Posted By : Jayshree

Assigned To : Bhavana Pachpande
D222

Date & Time : 15-06-2021 12:57:PM
sir manas,

Discussed on call, encrypted change password :

feid
/Utj4AO3qjPl8H/ZTJOTqw==

oldpassword

vndwWbDghy0LRGU9zFrRTA==

newpassword

H3XfCF5qBwkdZHXwvbT6Cg==

for recaptcha verification using token :

refer from this site <https://www.javatpoint.com/using-google-recaptcha-in-android-application>.

used api String url = "<https://www.google.com/recaptcha/api/siteverify>";
for this you need two parameter

recaptcha_secret_key = 6Le2Q-EZAAAAAHKjuWcceVXk2coo35xSi5PxW0Fn

response= from my side // response token

Posted By : Bhavana Pachpande

Assigned To : Jayshree
D222

Date & Time : 15-06-2021 03:24:PM
Hello mam,

Please check change password webservice if working.

For captcha we will start after logout token expiry process is done.

Posted By : Jayshree

Assigned To : Bhavana Pachpande
D222

Date & Time : 16-06-2021 05:00:PM
hi,

Yes, We have checked, now change password is working properly.

Posted By : Bhavana Pachpande
Assigned To : Jayshree

D222
Date & Time : 18-06-2021 03:27:PM
Hello,

Changes for token blacklist using database store has been updated in demo server.
Please send token during logout also.

During logout token value will be stored in a table whether or not it is expired.

Now on every request it will check if the token was already used or not i.e present in that blacklist table.
If found you can logout the user.

let me know if you want a token regenerate api also for regenerating token in between ?

Please check.

Posted By : Manas Dasgupta

Assigned To : Jayshree

D222

Date & Time : 21-06-2021 11:15:AM

Hello mam,

For captcha please let us know which api you are going to use, also check if both php and android is supported.

Posted By : Jayshree

Assigned To : Manas Dasgupta

D222

Date & Time : 22-06-2021 06:13:PM

hi manas sir,

As discussed on call

for recaptcha verification using token :

refer from this site <https://www.javatpoint.com/using-google-recaptcha-in-android-application>.

used api String url = "<https://www.google.com/recaptcha/api/siteverify>";

for this you need two parameter

recaptcha_secret_key = 6Le2Q-EZAAAAAHKjuWcceVXk2coo35xSi5PxW0Fn

response= from my side // response token

Posted By : Manas Dasgupta

Assigned To : Jayshree

D222

Date & Time : 23-06-2021 08:14:AM

ok thanks will check and update here once done.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 25-06-2021 03:15:PM

Hello mam,

As discussed please send google captcha token in change password post field as "**captchaToken**".

Posted By : Jayshree

Assigned To : Bhavana Pachpande

D222

Date & Time : 25-06-2021 06:54:PM

HI,

We have implemented field "**captchaToken**" in app side ,as per discussion we are sending recaptchaToken on change password, Even also checked using debugger ,but when we tried to change password ,got toast message Token expire and got logout without changing password.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 29-06-2021 08:21:AM

Hello mam,

Please send us all the request post parameters, so that we can test it with postman.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 30-06-2021 04:23:PM

Hello mam,

As discussed please send google captcha token in login post field as "**captchaToken**".

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 15-07-2021 08:45:AM

Hello mam,

Is testing done, for token expiry ? Also please inform PAMAC team for discussion on when can we go live with webservice and mobile apk.

Posted By : Jayshree

Assigned To : Bhavana Pachpande

D222

Date & Time : 18-07-2021 02:00:PM

hi,

VAPT points is completed,

here we are doing testing on RES app side.

once will get approval from ajit sir then we will upload on playstore.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 19-07-2021 08:06:AM

ok thank you for the update. Keep posting here in case of approval received.

Posted By : Bhavana Pachpande

Assigned To : Jayshree

D222

Date & Time : 18-08-2021 01:27:PM

Hello mam,

Is it approved ? Can we go live.

Posted By : Jayshree**Assigned To :** Bhavana Pachpande

D222

Date & Time : 23-08-2021 04:10:PM

HI,

here having some error on DCR template,

Vaishnavi creating DCR template on demo server, Once get completed then we can check after that we can do live

Posted By : Bhavana Pachpande**Assigned To :** Jayshree

D222

Date & Time : 25-08-2021 05:21:PM

ok mam, thanks for the update.

Posted By : Bhavana Pachpande**Assigned To :** Jayshree

D222

Date & Time : 27-09-2021 09:23:AM

Hello mam,

Is it approved ? Can we go live. Can we please discuss and come to a estimated date for upload in live server.

Posted By : Bhavana Pachpande**Assigned To :** Jayshree

D222

Date & Time : 25-10-2021 08:36:AM

Hello mam,

Is it approved ? Can we go live. Can we please discuss and come to a estimated date for upload in live server.

Posted By : Bhavana Pachpande**Assigned To :** Jayshree

D222

Date & Time : 08-11-2021 08:45:AM

Hello mam,

Is it approved ? Can we go live. Can we please discuss and come to a estimated date for upload in live server.

Posted By : Bhavana Pachpande**Assigned To :** Dipika Yedge

D222

Date & Time : 28-01-2022 11:20:AM

Hello mam,

Is it approved ? Can we go live. Can we please discuss and come to a estimated date for upload in live server.

If no update can we hold this point.

Posted By : Ramakrishnan V**Assigned To :** Ganesh Sawant

D222

Date & Time : 08-04-2023 06:22:PM

I presume this is an issue of involving mobile app. (as i see jayashree was involved).

In my opinion, this should be closed and if the requirement is still needed we can consider a new ticket after our android developer joins and starts functioning full fledged.

Posted By : Ramakrishnan V**Assigned To :** Ajit Kedare

D222

Date & Time : 08-04-2023 06:23:PM

VAPT points is completed,

here we are doing testing on RES app side.

once will get approval from ajit sir then we will upload on playstore.

What are these and if they are purely Andoid related - let us close this and create a new ticket with more information (requirement document for android development)