

# Assignment 4 – Mobile Mess

## Introduction

Your organization has decided that they want to make an Android application available for students who want to purchase NYU GiftCards. They took the liberty of hiring a contractor to create the application, but the code came back less useful than desired. Though your boss never told you which contracting company was hired, you're pretty sure it as Shoddy Corp's Cut-Rate Contracting. They also created a back-end for the application to interact with, but that was given to another member of your team at work to fix.

## Part 1 – Setting up environment

Followed directions given in assignment

1. Downloaded Android Studio
2. Created Virtual Device Pixel 3a with Build R
3. Imported Project GiftcardSite/ into Android Studio
4. Run Virtual Device and Launched AVD emulator and able to open up GiftcardSite

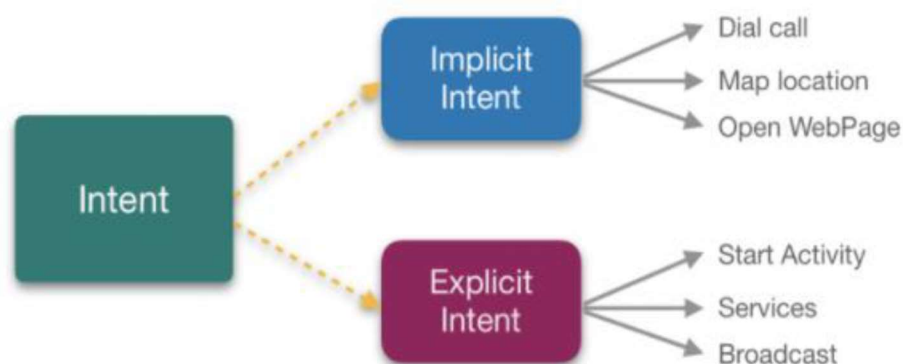
## Part 2 – It's all about intent

Android Intent is the message that is passed between components such as activities, content providers, broadcast receiver, services etc. Suppose you want to go from one screen to another screen or communication between applications, this activity in called Intent. For an application to work and navigate thru one screen to another screen within application or from one application to another application intents are used in Android.

### Part 2.1 - Intents

**Q1.** What are two types of Intent?

There are 2 types of Intent



**Explicit Intent** – An intent is explicit when an action uses or calls class/package or component within its own app to satisfy the need. For example, perform an activity to download a file but action is called within app

**Implicit Intent** – An intent is implicit when an action calls a component from another app or source to handle it. For example, a user wants to get location and action call google maps to provide need info. This is normally done using (Intent.ACTION\_VIEW) as in line # 69 in SecondFragment.kt:

```
var intent = Intent(Intent.ACTION_VIEW)
```

**Q2.** Which of the two types of Intents are more secure?

Explicit Intent is more secure as the actions are handled within an app. Since an implicit intent does not specify a particular application to receive the data, any application can process the intent by using an Intent Filter for that intent. This can allow untrusted applications to obtain sensitive data, cause privilege escalation or denial-of-service

**Q3.** What type of Intent is shown on lines 69 to 73 of SecondFragment.kt

The intent in lines 69 to 73 is an Implicit Intent. A URL is used to go thru a https service to get the index of products. See below

```
var intent = Intent(Intent.ACTION_VIEW) //Implicit Intent
intent.type = "text/giftcards-browse"
intent.data = Uri.parse("https://appsecclass.report/api/index")
intent.putExtra("User", loggedInUser);
```

Secondfragment is called by register new user (action/intent) and shows this implicit intent when the user is registered successfully. See below

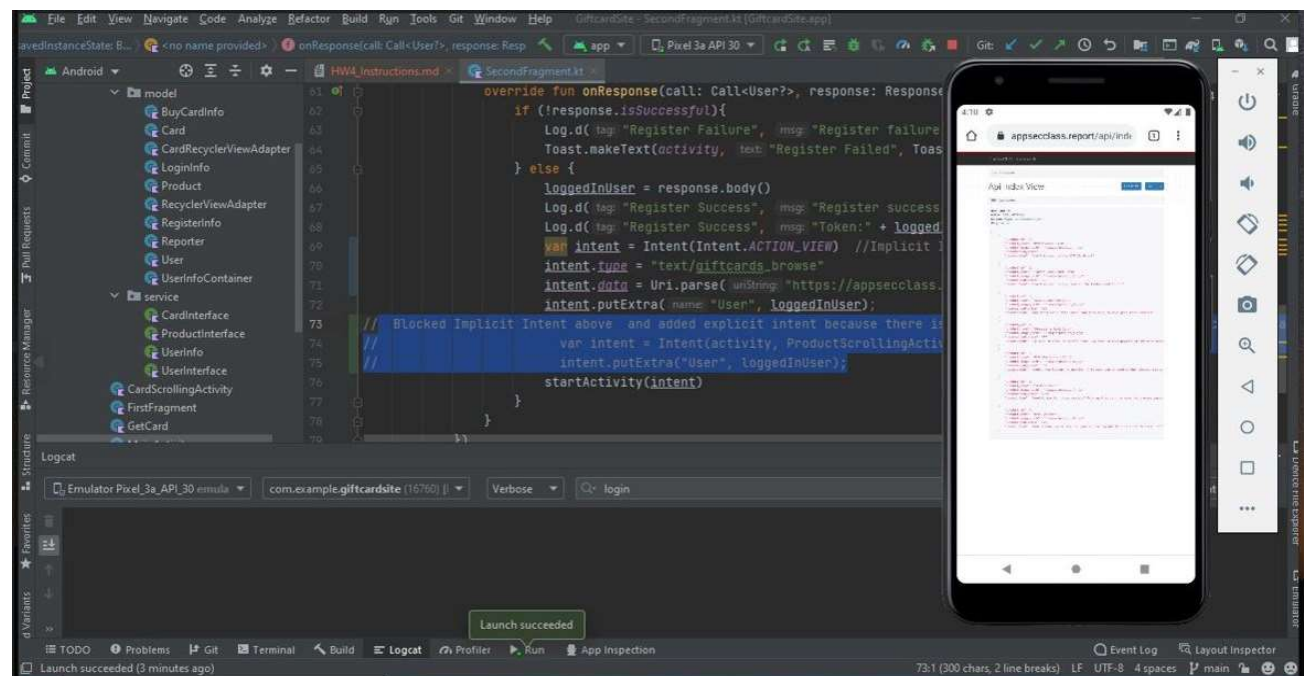


Figure stored in images/2ndFragment\_Implicit\_intent.JPG

**Q4.** What type of Intent is shown on line 68 to 70 of ThirdFragment.kt

In file ThirdFragment.kt lines 68 to 70 an Explicit intent is used by when ProductScrollingActivity class makes a call within the app to get the list of products. ThirdFragment is called when registered user uses the login screen. The application shows the products list. See below

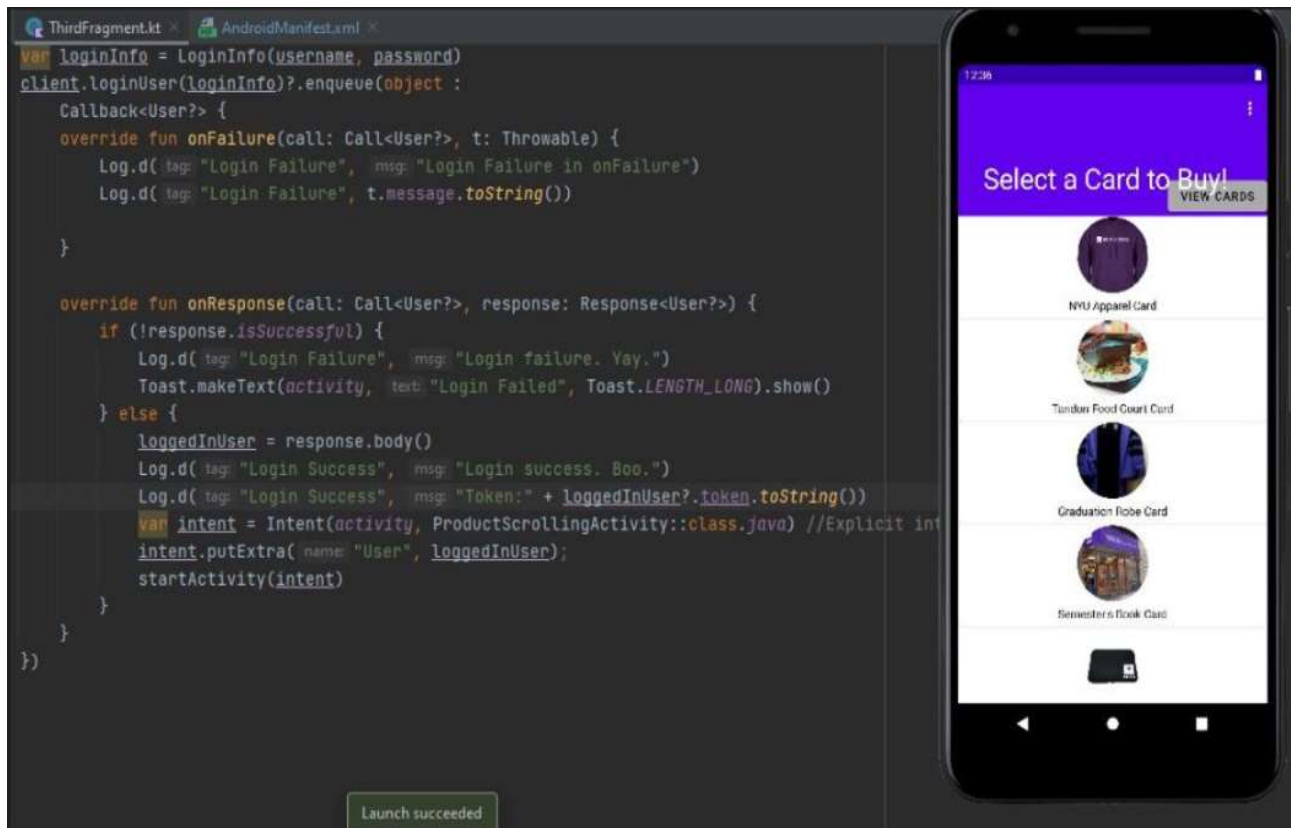


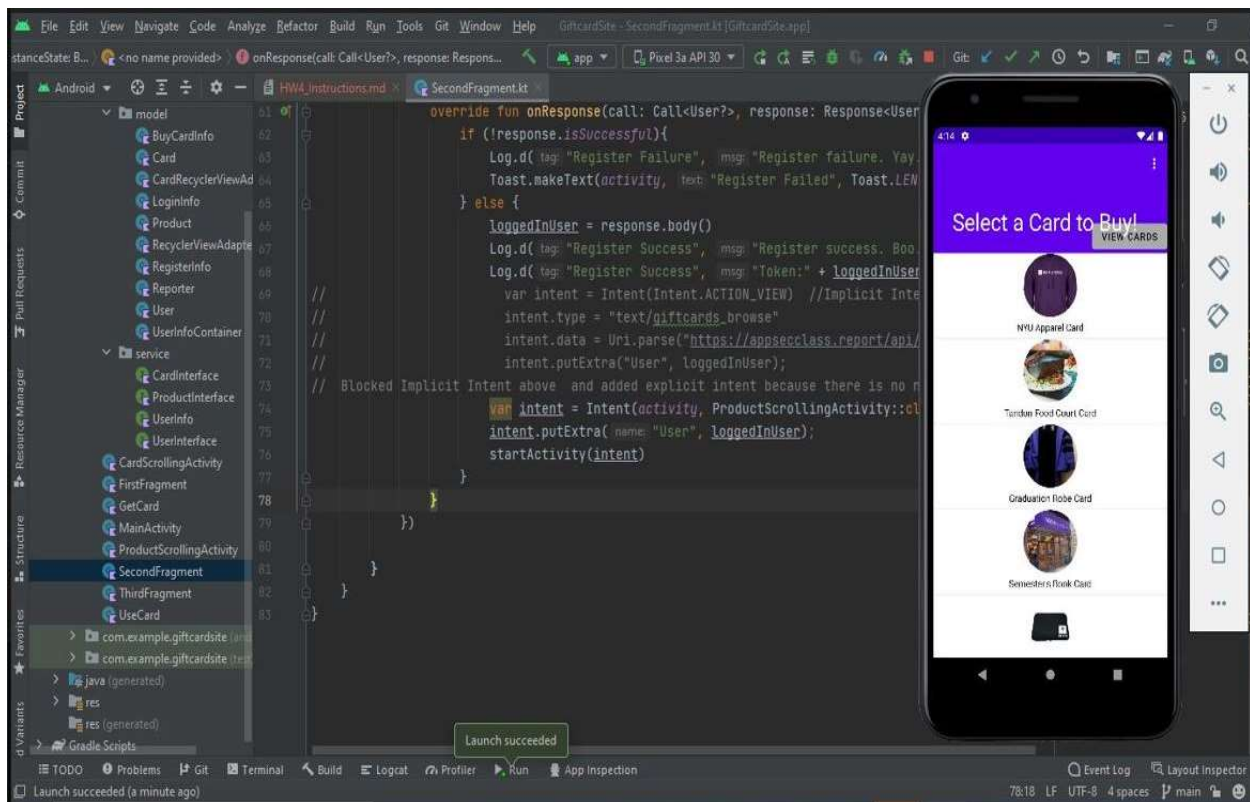
Figure stored in images/3rdFragment\_explicit\_intent.JPG

**Q5.** Which of these two Intents is the proper way to do an Intent?

Explicit intent is the proper way to do an Intent as it is more secure. However, sometimes there may be the need to use implicit intents. In those cases, secure practices must be implemented.

As stated above explicit intent are more secure to use. SecondFragment uses implicit intent to get product list.

Using Right Intent -- By looking at the output and clicking on the link used in SecondFragment, I compared the Products View (Same screen for Login workflow called in ThirdFragment), I was able to replace the implicit intent with an explicit intent by calling ProductScrollingActivity class to get the information within the application. The application worked without any issue. The change was also confirmed with registering new user which landed on Products view, similar to login screen using explicit intent as shown below



**Figured stored in images/2ndFragment\_explicit\_intent\_chage.JPG**

## Part 2.2 – Shutting out the world

In order to remove the possibility of other applications using Intents to launch activities of the application, I identified the following lines in the activity-filter section to stop not needed intents in the AndroidManifest.xml. I removed all activities (4) except main activity. The following screen shot is from UseCard activity. Similar lines removed from GetCard, ProductScrolling activity and CardScrollingActivity

```
<!--<intent-filter-->
<!-- <action android:name="android.intent.action.VIEW" />--> //commented to shutdown intent in all activities

<!-- <category android:name="android.intent.category.DEFAULT" />--> //commented to shutdown intent in all
activities

<!-- <data android:mimeType="text/giftcards use" />-->
<!-- <data android:scheme="gifcard" />-->
<!-- <data android:host="appsecclass.report"/>-->
<!--</intent-filter-->
```

## Part 3 -- Can you read me out there?

Communication non secure in transit is always vulnerable to attacks and the communication can be exposed. In order to make sure the communication is secure; we can use HTTPS. HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses, and to digitally sign those requests and responses. The following lines were changed

1. SecondFragment.kt – Line 48
2. ThirdFragment.kt –Line 45
3. CardScrollingActivity.kt – Lines 59, 98, and 123
4. ProductScrollingActivity.kt – Lines 61, 101, and 127
5. UseCard.kt – Lines 35 and 43
6. GetCard.kt – Lines 31 and 40
7. CardRecyclerViewAdapter.kt – Line 21
8. RecyclerViewAdapter.kt – Line 23

**Application Launched successfully after http to https changes.**

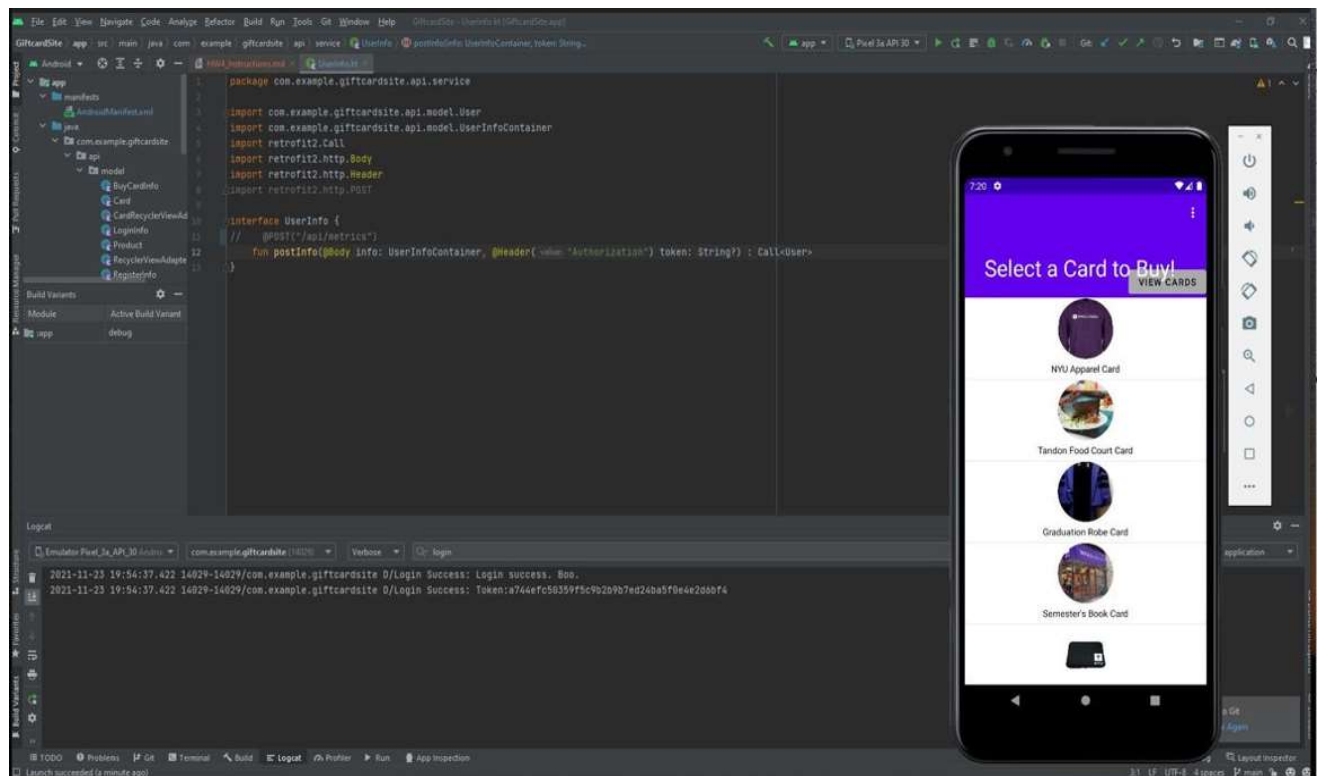
## Part 4: Oops, was that card yours?

While exploring the application for vulnerabilities, I used Android studio Logcat utility with filter “login” and verbose on option. The following lines were received after a successful login showing token issued to user (also in screenshot)

2022-12-08 19:54:37.422 14029-14029/com.example.giftcardsite D/Login Success: Login success. Boo.

2022-12-08 19:54:37.422 14029-14029/com.example.giftcardsite D/Login Success:

**Token:a744efc50359f5c9b2b9b7ed24ba5f0e4e2d6bf4**



**Figured stored in images/logcat\_login.JPG**

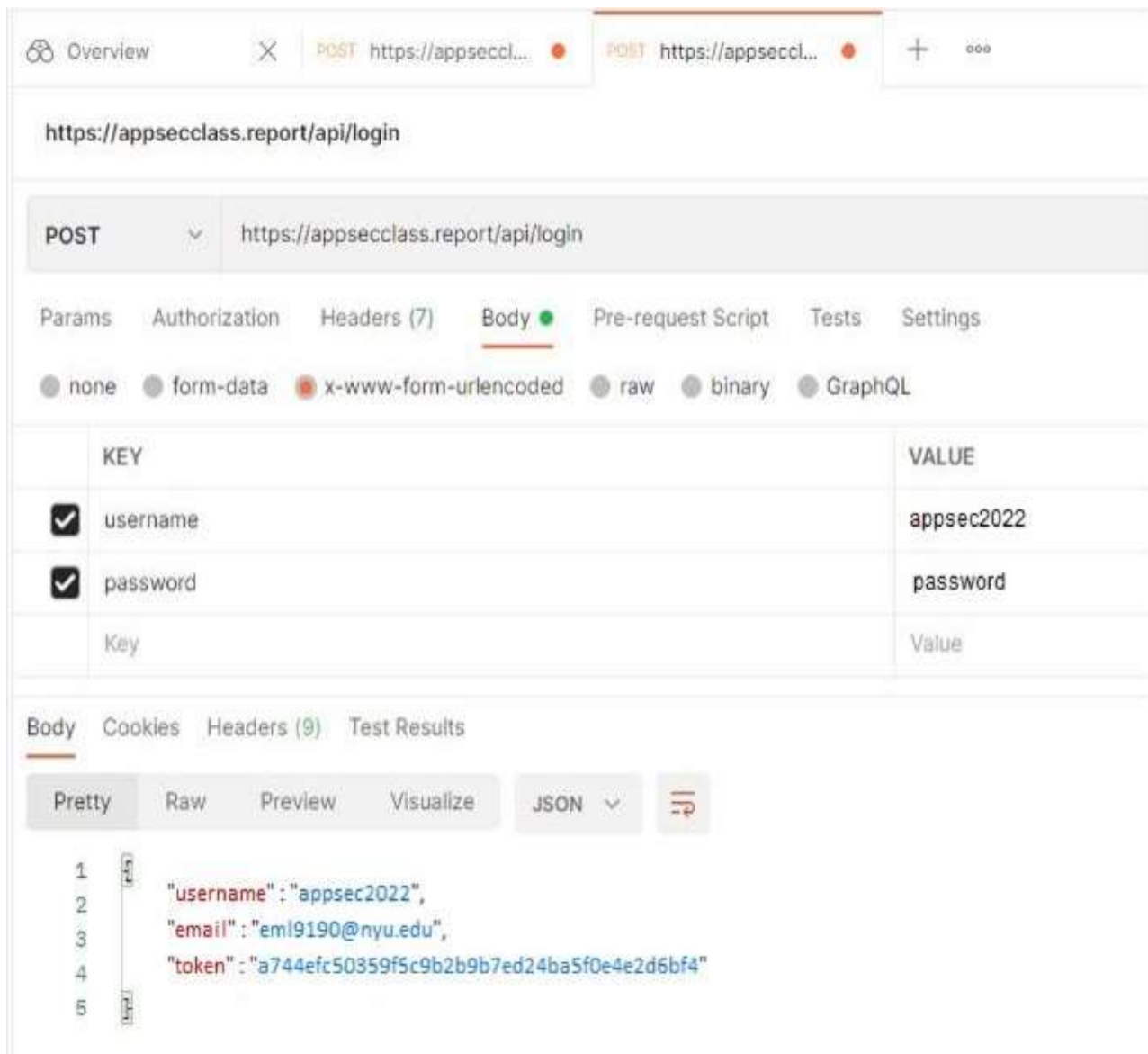


Solution: Logs proved my assumption that the sensitive data is easily accessible. Hence, code which writes to the log must be removed.

By further looking into files UseCard.kt and CarInterface.kt I got the api calls used for card list and card use

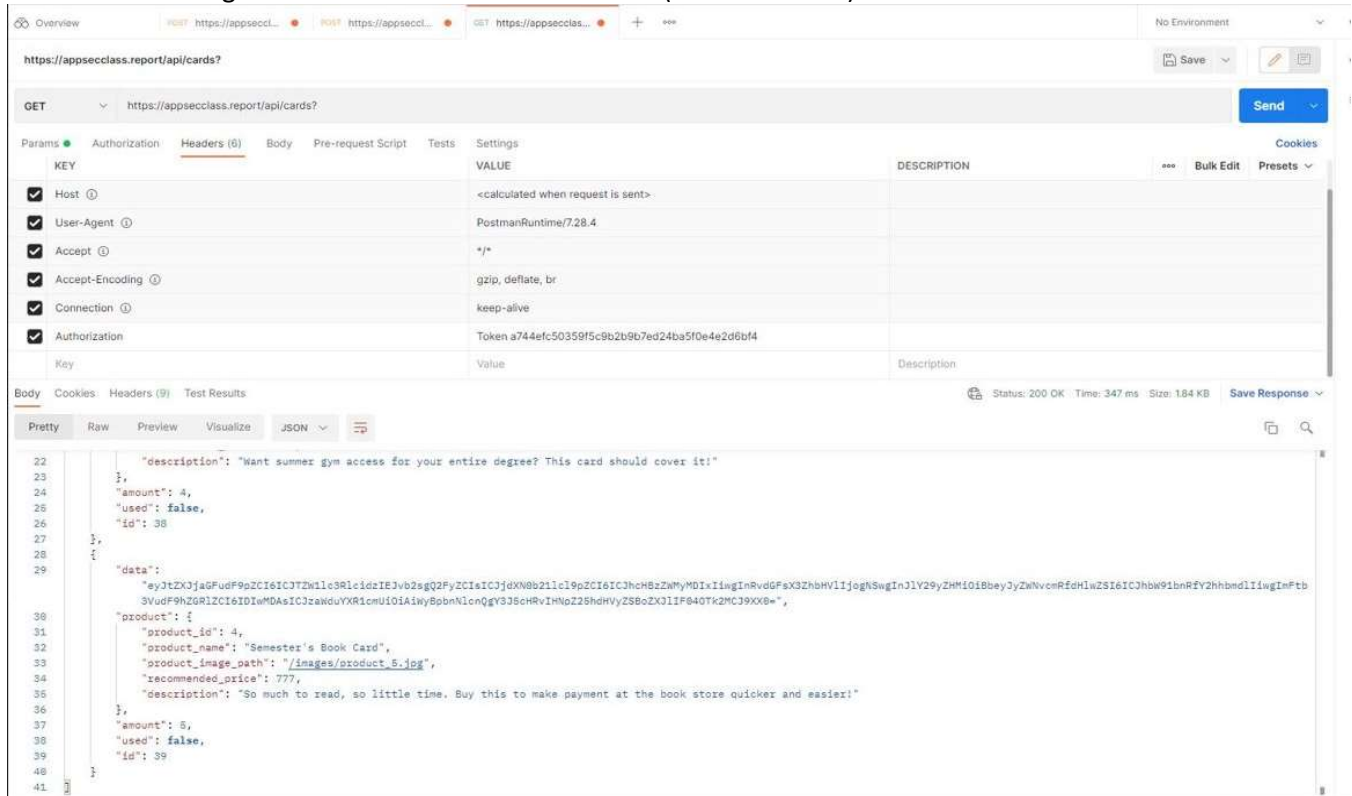
Using Postman utility, I was able to get user token by issuing

1. Sending POST command on <https://appsecclass.report/api/login> -- got token issued to user using body x-www-form-urlencoded (shown below)



**Figure stored in images/usertoken1.JPG**

2. Sending GET command on <https://appsecclass.report/api/cards?> -- got the list of users unused cards using token in header authorization field (as show below)



The screenshot shows a Postman interface for a GET request to `https://appsecclass.report/api/cards?`. The Headers tab is active, showing an Authorization header with the value `Token a744efc50359f5c9b2b9b7ed24ba5f0e4e2d6bf4`. The response body is displayed in JSON format, showing a list of cards. The first card has an amount of 4 and is unused. The second card has an amount of 5 and is unused. The third card has an amount of 6 and is unused.

```
22  {
23    "description": "Want summer gym access for your entire degree? This card should cover it!"
24  },
25  {
26    "amount": 4,
27    "used": false,
28    "id": 38
29  },
30  {
31    "data": {
32      "product": {
33        "product_id": 4,
34        "product_name": "Semester's Book Card",
35        "product_image_path": "/images/product_5.jpg",
36        "recommended_price": 777,
37        "description": "So much to read, so little time. Buy this to make payment at the book store quicker and easier!"
38      },
39      "amount": 5,
40      "used": false,
41      "id": 39
42    }
43  },
44  {
45    "amount": 6,
46    "used": false,
47    "id": 40
48  },
49  {
50    "amount": 7,
51    "used": false,
52    "id": 41
53  },
54  {
55    "amount": 8,
56    "used": false,
57    "id": 42
58  },
59  {
60    "amount": 9,
61    "used": false,
62    "id": 43
63  },
64  {
65    "amount": 10,
66    "used": false,
67    "id": 44
68  },
69  {
70    "amount": 11,
71    "used": false,
72    "id": 45
73  },
74  {
75    "amount": 12,
76    "used": false,
77    "id": 46
78  },
79  {
80    "amount": 13,
81    "used": false,
82    "id": 47
83  },
84  {
85    "amount": 14,
86    "used": false,
87    "id": 48
88  },
89  {
90    "amount": 15,
91    "used": false,
92    "id": 49
93  },
94  {
95    "amount": 16,
96    "used": false,
97    "id": 50
98  },
99  {
100   "amount": 17,
101   "used": false,
102   "id": 51
103  },
104  {
105   "amount": 18,
106   "used": false,
107   "id": 52
108  },
109  {
110   "amount": 19,
111   "used": false,
112   "id": 53
113  },
114  {
115   "amount": 20,
116   "used": false,
117   "id": 54
118  },
119  {
120   "amount": 21,
121   "used": false,
122   "id": 55
123  },
124  {
125   "amount": 22,
126   "used": false,
127   "id": 56
128  },
129  {
130   "amount": 23,
131   "used": false,
132   "id": 57
133  },
134  {
135   "amount": 24,
136   "used": false,
137   "id": 58
138  },
139  {
140   "amount": 25,
141   "used": false,
142   "id": 59
143  },
144  {
145   "amount": 26,
146   "used": false,
147   "id": 60
148  },
149  {
150   "amount": 27,
151   "used": false,
152   "id": 61
153  },
154  {
155   "amount": 28,
156   "used": false,
157   "id": 62
158  },
159  {
160   "amount": 29,
161   "used": false,
162   "id": 63
163  },
164  {
165   "amount": 30,
166   "used": false,
167   "id": 64
168  },
169  {
170   "amount": 31,
171   "used": false,
172   "id": 65
173  },
174  {
175   "amount": 32,
176   "used": false,
177   "id": 66
178  },
179  {
180   "amount": 33,
181   "used": false,
182   "id": 67
183  },
184  {
185   "amount": 34,
186   "used": false,
187   "id": 68
188  },
189  {
190   "amount": 35,
191   "used": false,
192   "id": 69
193  },
194  {
195   "amount": 36,
196   "used": false,
197   "id": 70
198  },
199  {
200   "amount": 37,
201   "used": false,
202   "id": 71
203  },
204  {
205   "amount": 38,
206   "used": false,
207   "id": 72
208  },
209  {
210   "amount": 39,
211   "used": false,
212   "id": 73
213  },
214  {
215   "amount": 40,
216   "used": false,
217   "id": 74
218  },
219  {
220   "amount": 41,
221   "used": false,
222   "id": 75
223  },
224  {
225   "amount": 42,
226   "used": false,
227   "id": 76
228  },
229  {
230   "amount": 43,
231   "used": false,
232   "id": 77
233  },
234  {
235   "amount": 44,
236   "used": false,
237   "id": 78
238  },
239  {
240   "amount": 45,
241   "used": false,
242   "id": 79
243  },
244  {
245   "amount": 46,
246   "used": false,
247   "id": 80
248  },
249  {
250   "amount": 47,
251   "used": false,
252   "id": 81
253  },
254  {
255   "amount": 48,
256   "used": false,
257   "id": 82
258  },
259  {
260   "amount": 49,
261   "used": false,
262   "id": 83
263  },
264  {
265   "amount": 50,
266   "used": false,
267   "id": 84
268  },
269  {
270   "amount": 51,
271   "used": false,
272   "id": 85
273  },
274  {
275   "amount": 52,
276   "used": false,
277   "id": 86
278  },
279  {
280   "amount": 53,
281   "used": false,
282   "id": 87
283  },
284  {
285   "amount": 54,
286   "used": false,
287   "id": 88
288  },
289  {
290   "amount": 55,
291   "used": false,
292   "id": 89
293  },
294  {
295   "amount": 56,
296   "used": false,
297   "id": 90
298  },
299  {
300   "amount": 57,
301   "used": false,
302   "id": 91
303  },
304  {
305   "amount": 58,
306   "used": false,
307   "id": 92
308  },
309  {
310   "amount": 59,
311   "used": false,
312   "id": 93
313  },
314  {
315   "amount": 60,
316   "used": false,
317   "id": 94
318  },
319  {
320   "amount": 61,
321   "used": false,
322   "id": 95
323  },
324  {
325   "amount": 62,
326   "used": false,
327   "id": 96
328  },
329  {
330   "amount": 63,
331   "used": false,
332   "id": 97
333  },
334  {
335   "amount": 64,
336   "used": false,
337   "id": 98
338  },
339  {
340   "amount": 65,
341   "used": false,
342   "id": 99
343  },
344  {
345   "amount": 66,
346   "used": false,
347   "id": 100
348  },
349  {
350   "amount": 67,
351   "used": false,
352   "id": 101
353  },
354  {
355   "amount": 68,
356   "used": false,
357   "id": 102
358  },
359  {
360   "amount": 69,
361   "used": false,
362   "id": 103
363  },
364  {
365   "amount": 70,
366   "used": false,
367   "id": 104
368  },
369  {
370   "amount": 71,
371   "used": false,
372   "id": 105
373  },
374  {
375   "amount": 72,
376   "used": false,
377   "id": 106
378  },
379  {
380   "amount": 73,
381   "used": false,
382   "id": 107
383  },
384  {
385   "amount": 74,
386   "used": false,
387   "id": 108
388  },
389  {
390   "amount": 75,
391   "used": false,
392   "id": 109
393  },
394  {
395   "amount": 76,
396   "used": false,
397   "id": 110
398  },
399  {
400   "amount": 77,
401   "used": false,
402   "id": 111
403  },
404  {
405   "amount": 78,
406   "used": false,
407   "id": 112
408  },
409  {
410   "amount": 79,
411   "used": false,
412   "id": 113
413  },
414  {
415   "amount": 80,
416   "used": false,
417   "id": 114
418  },
419  {
420   "amount": 81,
421   "used": false,
422   "id": 115
423  },
424  {
425   "amount": 82,
426   "used": false,
427   "id": 116
428  },
429  {
430   "amount": 83,
431   "used": false,
432   "id": 117
433  },
434  {
435   "amount": 84,
436   "used": false,
437   "id": 118
438  },
439  {
440   "amount": 85,
441   "used": false,
442   "id": 119
443  },
444  {
445   "amount": 86,
446   "used": false,
447   "id": 120
448  },
449  {
450   "amount": 87,
451   "used": false,
452   "id": 121
453  },
454  {
455   "amount": 88,
456   "used": false,
457   "id": 122
458  },
459  {
460   "amount": 89,
461   "used": false,
462   "id": 123
463  },
464  {
465   "amount": 90,
466   "used": false,
467   "id": 124
468  },
469  {
470   "amount": 91,
471   "used": false,
472   "id": 125
473  },
474  {
475   "amount": 92,
476   "used": false,
477   "id": 126
478  },
479  {
480   "amount": 93,
481   "used": false,
482   "id": 127
483  },
484  {
485   "amount": 94,
486   "used": false,
487   "id": 128
488  },
489  {
490   "amount": 95,
491   "used": false,
492   "id": 129
493  },
494  {
495   "amount": 96,
496   "used": false,
497   "id": 130
498  },
499  {
500   "amount": 97,
501   "used": false,
502   "id": 131
503  },
504  {
505   "amount": 98,
506   "used": false,
507   "id": 132
508  },
509  {
510   "amount": 99,
511   "used": false,
512   "id": 133
513  },
514  {
515   "amount": 100,
516   "used": false,
517   "id": 134
518  },
519  {
520   "amount": 101,
521   "used": false,
522   "id": 135
523  },
524  {
525   "amount": 102,
526   "used": false,
527   "id": 136
528  },
529  {
530   "amount": 103,
531   "used": false,
532   "id": 137
533  },
534  {
535   "amount": 104,
536   "used": false,
537   "id": 138
538  },
539  {
540   "amount": 105,
541   "used": false,
542   "id": 139
543  },
544  {
545   "amount": 106,
546   "used": false,
547   "id": 140
548  },
549  {
550   "amount": 107,
551   "used": false,
552   "id": 141
553  },
554  {
555   "amount": 108,
556   "used": false,
557   "id": 142
558  },
559  {
560   "amount": 109,
561   "used": false,
562   "id": 143
563  },
564  {
565   "amount": 110,
566   "used": false,
567   "id": 144
568  },
569  {
570   "amount": 111,
571   "used": false,
572   "id": 145
573  },
574  {
575   "amount": 112,
576   "used": false,
577   "id": 146
578  },
579  {
580   "amount": 113,
581   "used": false,
582   "id": 147
583  },
584  {
585   "amount": 114,
586   "used": false,
587   "id": 148
588  },
589  {
590   "amount": 115,
591   "used": false,
592   "id": 149
593  },
594  {
595   "amount": 116,
596   "used": false,
597   "id": 150
598  },
599  {
600   "amount": 117,
601   "used": false,
602   "id": 151
603  },
604  {
605   "amount": 118,
606   "used": false,
607   "id": 152
608  },
609  {
610   "amount": 119,
611   "used": false,
612   "id": 153
613  },
614  {
615   "amount": 120,
616   "used": false,
617   "id": 154
618  },
619  {
620   "amount": 121,
621   "used": false,
622   "id": 155
623  },
624  {
625   "amount": 122,
626   "used": false,
627   "id": 156
628  },
629  {
630   "amount": 123,
631   "used": false,
632   "id": 157
633  },
634  {
635   "amount": 124,
636   "used": false,
637   "id": 158
638  },
639  {
640   "amount": 125,
641   "used": false,
642   "id": 159
643  },
644  {
645   "amount": 126,
646   "used": false,
647   "id": 160
648  },
649  {
650   "amount": 127,
651   "used": false,
652   "id": 161
653  },
654  {
655   "amount": 128,
656   "used": false,
657   "id": 162
658  },
659  {
660   "amount": 129,
661   "used": false,
662   "id": 163
663  },
664  {
665   "amount": 130,
666   "used": false,
667   "id": 164
668  },
669  {
670   "amount": 131,
671   "used": false,
672   "id": 165
673  },
674  {
675   "amount": 132,
676   "used": false,
677   "id": 166
678  },
679  {
680   "amount": 133,
681   "used": false,
682   "id": 167
683  },
684  {
685   "amount": 134,
686   "used": false,
687   "id": 168
688  },
689  {
690   "amount": 135,
691   "used": false,
692   "id": 169
693  },
694  {
695   "amount": 136,
696   "used": false,
697   "id": 170
698  },
699  {
700   "amount": 137,
701   "used": false,
702   "id": 171
703  },
704  {
705   "amount": 138,
706   "used": false,
707   "id": 172
708  },
709  {
710   "amount": 139,
711   "used": false,
712   "id": 173
713  },
714  {
715   "amount": 140,
716   "used": false,
717   "id": 174
718  },
719  {
720   "amount": 141,
721   "used": false,
722   "id": 175
723  },
724  {
725   "amount": 142,
726   "used": false,
727   "id": 176
728  },
729  {
730   "amount": 143,
731   "used": false,
732   "id": 177
733  },
734  {
735   "amount": 144,
736   "used": false,
737   "id": 178
738  },
739  {
740   "amount": 145,
741   "used": false,
742   "id": 179
743  },
744  {
745   "amount": 146,
746   "used": false,
747   "id": 180
748  },
749  {
750   "amount": 147,
751   "used": false,
752   "id": 181
753  },
754  {
755   "amount": 148,
756   "used": false,
757   "id": 182
758  },
759  {
760   "amount": 149,
761   "used": false,
762   "id": 183
763  },
764  {
765   "amount": 150,
766   "used": false,
767   "id": 184
768  },
769  {
770   "amount": 151,
771   "used": false,
772   "id": 185
773  },
774  {
775   "amount": 152,
776   "used": false,
777   "id": 186
778  },
779  {
780   "amount": 153,
781   "used": false,
782   "id": 187
783  },
784  {
785   "amount": 154,
786   "used": false,
787   "id": 188
788  },
789  {
790   "amount": 155,
791   "used": false,
792   "id": 189
793  },
794  {
795   "amount": 156,
796   "used": false,
797   "id": 190
798  },
799  {
800   "amount": 157,
801   "used": false,
802   "id": 191
803  },
804  {
805   "amount": 158,
806   "used": false,
807   "id": 192
808  },
809  {
810   "amount": 159,
811   "used": false,
812   "id": 193
813  },
814  {
815   "amount": 160,
816   "used": false,
817   "id": 194
818  },
819  {
820   "amount": 161,
821   "used": false,
822   "id": 195
823  },
824  {
825   "amount": 162,
826   "used": false,
827   "id": 196
828  },
829  {
830   "amount": 163,
831   "used": false,
832   "id": 197
833  },
834  {
835   "amount": 164,
836   "used": false,
837   "id": 198
838  },
839  {
840   "amount": 165,
841   "used": false,
842   "id": 199
843  },
844  {
845   "amount": 166,
846   "used": false,
847   "id": 200
848  },
849  {
850   "amount": 167,
851   "used": false,
852   "id": 201
853  },
854  {
855   "amount": 168,
856   "used": false,
857   "id": 202
858  },
859  {
860   "amount": 169,
861   "used": false,
862   "id": 203
863  },
864  {
865   "amount": 170,
866   "used": false,
867   "id": 204
868  },
869  {
870   "amount": 171,
871   "used": false,
872   "id": 205
873  },
874  {
875   "amount": 172,
876   "used": false,
877   "id": 206
878  },
879  {
880   "amount": 173,
881   "used": false,
882   "id": 207
883  },
884  {
885   "amount": 174,
886   "used": false,
887   "id": 208
888  },
889  {
890   "amount": 175,
891   "used": false,
892   "id": 209
893  },
894  {
895   "amount": 176,
896   "used": false,
897   "id": 210
898  },
899  {
900   "amount": 177,
901   "used": false,
902   "id": 211
903  },
904  {
905   "amount": 178,
906   "used": false,
907   "id": 212
908  },
909  {
910   "amount": 179,
911   "used": false,
912   "id": 213
913  },
914  {
915   "amount": 180,
916   "used": false,
917   "id": 214
918  },
919  {
920   "amount": 181,
921   "used": false,
922   "id": 215
923  },
924  {
925   "amount": 182,
926   "used": false,
927   "id": 216
928  },
929  {
930   "amount": 183,
931   "used": false,
932   "id": 217
933  },
934  {
935   "amount": 184,
936   "used": false,
937   "id": 218
938  },
939  {
940   "amount": 185,
941   "used": false,
942   "id": 219
943  },
944  {
945   "amount": 186,
946   "used": false,
947   "id": 220
948  },
949  {
950   "amount": 187,
951   "used": false,
952   "id": 221
953  },
954  {
955   "amount": 188,
956   "used": false,
957   "id": 222
958  },
959  {
960   "amount": 189,
961   "used": false,
962   "id": 223
963  },
964  {
965   "amount": 190,
966   "used": false,
967   "id": 224
968  },
969  {
970   "amount": 191,
971   "used": false,
972   "id": 225
973  },
974  {
975   "amount": 192,
976   "used": false,
977   "id": 226
978  },
979  {
980   "amount": 193,
981   "used": false,
982   "id": 227
983  },
984  {
985   "amount": 194,
986   "used": false,
987   "id": 228
988  },
989  {
990   "amount": 195,
991   "used": false,
992   "id": 229
993  },
994  {
995   "amount": 196,
996   "used": false,
997   "id": 230
998  },
999  {
1000   "amount": 197,
1001   "used": false,
1002   "id": 231
1003  },
1004  {
1005   "amount": 198,
1006   "used": false,
1007   "id": 232
1008  },
1009  {
1010   "amount": 199,
1011   "used": false,
1012   "id": 233
1013  },
1014  {
1015   "amount": 200,
1016   "used": false,
1017   "id": 234
1018  },
1019  {
1020   "amount": 201,
1021   "used": false,
1022   "id": 235
1023  },
1024  {
1025   "amount": 202,
1026   "used": false,
1027   "id": 236
1028  },
1029  {
1030   "amount": 203,
1031   "used": false,
1032   "id": 237
1033  },
1034  {
1035   "amount": 204,
1036   "used": false,
1037   "id": 238
1038  },
1039  {
1040   "amount": 205,
1041   "used": false,
1042   "id": 239
1043  },
1044  {
1045   "amount": 206,
1046   "used": false,
1047   "id": 240
1048  },
1049  {
1050   "amount": 207,
1051   "used": false,
1052   "id": 241
1053  },
1054  {
1055   "amount": 208,
1056   "used": false,
1057   "id": 242
1058  },
1059  {
1060   "amount": 209,
1061   "used": false,
1062   "id": 243
1063  },
1064  {
1065   "amount": 210,
1066   "used": false,
1067   "id": 244
1068  },
1069  {
1070   "amount": 211,
1071   "used": false,
1072   "id": 245
1073  },
1074  {
1075   "amount": 212,
1076   "used": false,
1077   "id": 246
1078  },
1079  {
1080   "amount": 213,
1081   "used": false,
1082   "id": 247
1083  },
1084  {
1085   "amount": 214,
1086   "used": false,
1087   "id": 248
1088  },
1089  {
1090   "amount": 215,
1091   "used": false,
1092   "id": 249
1093  },
1094  {
1095   "amount": 216,
1096   "used": false,
1097   "id": 250
1098  },
1099  {
1100   "amount": 217,
1101   "used": false,
1102   "id": 251
1103  },
1104  {
1105   "amount": 218,
1106   "used": false,
1107   "id": 252
1108  },
1109  {
1110   "amount": 219,
1111   "used": false,
1112   "id": 253
1113  },
1114  {
1115   "amount": 220,
1116   "used": false,
1117   "id": 254
1118  },
1119  {
1120   "amount": 221,
1121   "used": false,
1122   "id": 255
1123  },
1124  {
1125   "amount": 222,
1126   "used": false,
1127   "id": 256
1128  },
1129  {
1130   "amount": 223,
1131   "used": false,
1132   "id": 257
1133  },
1134  {
1135   "amount": 224,
1136   "used": false,
1137   "id": 258
1138  },
1139  {
1140   "amount": 225,
1141   "used": false,
1142   "id": 259
1143  },
1144  {
1145   "amount": 226,
1146   "used": false,
1147   "id": 260
1148  },
1149  {
1150   "amount": 227,
1151   "used": false,
1152   "id": 261
1153  },
1154  {
1155   "amount": 228,
1156   "used": false,
1157   "id": 262
1158  },
1159  {
1160   "amount": 229,
1161   "used": false,
1162   "id": 263
1163  },
1164  {
1165   "amount": 230,
1166   "used": false,
1167   "id": 264
1168  },
1169  {
1170   "amount": 231,
1171   "used": false,
1172   "id": 265
1173  },
1174  {
1175   "amount": 232,
1176   "used": false,
1177   "id": 266
1178  },
1179  {
1180   "amount": 233,
1181   "used": false,
1182   "id": 267
1183  },
1184  {
1185   "amount": 234,
1186   "used": false,
1187   "id": 268
1188  },
1189  {
1190   "amount": 235,
1191   "used": false,
1192   "id": 269
1193  },
1194  {
1195   "amount": 236,
1196   "used": false,
1197   "id": 270
1198  },
1199  {
1200   "amount": 237,
1201   "used": false,
1202   "id": 271
1203  },
1204  {
1205   "amount": 238,
1206   "used": false,
1207   "id": 272
1208  },
1209  {
1210   "amount": 239,
1211   "used": false,
1212   "id": 273
1213  },
1214  {
1215   "amount": 240,
1216   "used": false,
1217   "id": 274
1218  },
1219  {
1220   "amount": 241,
1221   "used": false,
1222   "id": 275
1223  },
1224  {
1225   "amount": 242,
1226   "used": false,
1227   "id": 276
1228  },
1229  {
1230   "amount": 243,
1231   "used": false,
1232   "id": 277
1233  },
1234  {
1235   "amount": 244,
1236   "used": false,
1237   "id": 278
1238  },
1239  {
1240   "amount": 245,
1241   "used": false,
1242   "id": 279
1243  },
1244  {
1245   "amount": 246,
1246   "used": false,
1247   "id": 280
1248  },
1249  {
1250   "amount": 247,
1251   "used": false,
1252   "id": 281
1253  },
1254  {
1255   "amount": 248,
1256   "used": false,
1257   "id": 282
1258  },
1259  {
1260   "amount": 249,
1261   "used": false,
1262   "id": 283
1263  },
1264  {
1265   "amount": 250,
1266   "used": false,
1267   "id": 284
1268  },
1269  {
1270   "amount": 251,
1271   "used": false,
1272   "id": 285
1273  },
1274  {
1275   "amount": 252,
1276   "used": false,
1277   "id": 286
1278  },
1279  {
1280   "amount": 253,
1281   "used": false,
1282   "id": 287
1283  },
1284  {
1285   "amount": 254,
1286   "used": false,
1287   "id": 288
1288  },
1289  {
1290   "amount": 255,
1291   "used": false,
1292   "id": 289
1293  },
1294  {
1295   "amount": 256,

```

**Reason** – When a permanent token is issued, it is stored in db. this token could be used at any time after. Permanent tokens are a risk. Another reason is that unnecessary data exposure can also cause a token exposure

**Fix** -- Permanent token should not be used; instead, a temporary session-based token should be issued, one per user per session for authorization. Once the session is complete temporary session token should expire and be deleted from system. This will avoid any attacks even if the token is stolen as it will not be useful for another session. Commenting Log.d will not be of much help. The better approach is not to issue and store permanent tokens.

- Proper authentication and authorization access controls on server side api, validating card belongs to user and related token will enforce card use by owner, and not to another user.
- Implementing a function to generate A long random card number will make it difficult to guess and prevent stealing
- Token used here is permanent and stored in DB. If this changed to limited time / session cookie will enforce use of username and password. to take it further, MFA implementation will enforce strong authentication

## Part 5: Privacy is Important

In this section the goal is to remove all privacy invasive code. This is done by removing all metric collecting code, all areas that needlessly interact with sensors, and all permissions that are not needed for the basic functionality of the application (buying, browsing, and using gift cards). I noticed many invasive (privacy) metrics in the files mentioned. I have removed all the code related to the location and the sensors in files mentioned below.

**1. AndroidManifest.xml** - The following lines were removed to remove permissions:

```
<!-- <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>-->
<!-- <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>-->
<!-- <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>-->
<!-- <uses-permission android:name="android.permission.ACCESS_MOCK_LOCATION"/>
```

**2. UserInfo.kt** - Removed metrics API call

```
// @POST("/api/metrics")
```

**3. CardScrollingActivity.kt** –Removed interaction with SensorEventListener LocationListener class. The following lines were commented out

**Line 32**

```
class CardScrollingActivity : AppCompatActivity() { //, SensorEventListener, LocationListener {
```

**Lines 40 to 47**

```
// val locationPermissionCode = 2
// var locationManager = getSystemService(Context.LOCATION_SERVICE) as LocationManager
// if ((ContextCompat.checkSelfPermission(this, Manifest.permission.ACCESS_FINE_LOCATION) !=
// PackageManager.PERMISSION_GRANTED)) {
// ActivityCompat.requestPermissions(this, arrayOf(Manifest.permission.ACCESS_FINE_LOCATION),
// locationPermissionCode)
```



```

// }
// locationManager.requestLocationUpdates(LocationManager.GPS_PROVIDER, 5000, 5f, this)
// sensorManager = getSystemService(Context.SENSOR_SERVICE) as SensorManager
// mAccel = sensorManager.getDefaultSensor(Sensor.TYPE_ACCELEROMETER)

Lines 96 to 160
// override fun onLocationChanged(location: Location) {
// var userInfoContainer = UserInfoContainer(location, null, loggedInUser?.token)
// var builder: Retrofit.Builder =
Retrofit.Builder().baseUrl("https://appsecclass.report").addConverterFactory(
// GsonConverterFactory.create())
// var retrofit: Retrofit = builder.build()
// var client: UserInfo = retrofit.create(UserInfo::class.java)
// client.postInfo(userInfoContainer, loggedInUser?.token)?.enqueue(object: Callback<User?> {
// override fun onFailure(call: Call<User?>, t: Throwable) {
// Log.d("Metric Failure", "Metric Failure in onFailure")
// Log.d("Metric Failure", t.message.toString())
// }
// }
// }
// override fun onResponse(call: Call<User?>, response: Response<User?>) {
// if (!response.isSuccessful) {
// Log.d("Metric Failure", "Metric failure. Yay.")
// } else {
// Log.d("Metric Success", "Metric success. Boo.")
// Log.d("Metric Success", "Token:${userInfoContainer.token}")
// }
// }
// }
// }
// override fun onSensorChanged(event: SensorEvent?) {
// if (event != null) {
// var userInfoContainer = UserInfoContainer(null, event.values[0].toString(), loggedInUser?.token)
// var builder: Retrofit.Builder =
Retrofit.Builder().baseUrl("https://appsecclass.report").addConverterFactory(
// GsonConverterFactory.create())
// var retrofit: Retrofit = builder.build()
// var client: UserInfo = retrofit.create(UserInfo::class.java)
// client.postInfo(userInfoContainer, loggedInUser?.token)?.enqueue(object: Callback<User?> {
// override fun onFailure(call: Call<User?>, t: Throwable) {
// Log.d("Metric Failure", "Metric Failure in onFailure")
// Log.d("Metric Failure", t.message.toString())
// }
// }
// }
// override fun onResponse(call: Call<User?>, response: Response<User?>) {
// if (!response.isSuccessful) {
// Log.d("Metric Failure", "Metric failure. Yay.")
// } else {

```

```

// Log.d("Metric Success", "Metric success. Boo.")
// Log.d("Metric Success", "Token:${userInfoContainer.token}")
// }
// }
// }}
// }
// }
//
// override fun onAccuracyChanged(sensor: Sensor?, accuracy: Int) {
// return
// }
//
// override fun onResume() {
// super.onResume()
// mAccel?.also { accel ->
// sensorManager.registerListener(this, accel, SensorManager.SENSOR_DELAY_NORMAL)
// }
// }
//
// override fun onPause() {
// super.onPause()
// sensorManager.unregisterListener(this)
// }

```

#### 4. **ProductScrollingActivity.kt** - Removed interaction with SensorEventListener LocationListener class

##### **Line 33**

```
class CardScrollingActivity : AppCompatActivity() { //, SensorEventListener, LocationListener {
```

Also Removed Sensor and location related code similar to code in **CardScrollingActivity.kt** file