

A7 :

2) yes

[procedure :

1. copy paste the url in 2 different tab

2.web developer – console and paste alert(document.cookie);[do on both tab]

3.note the pop up of both

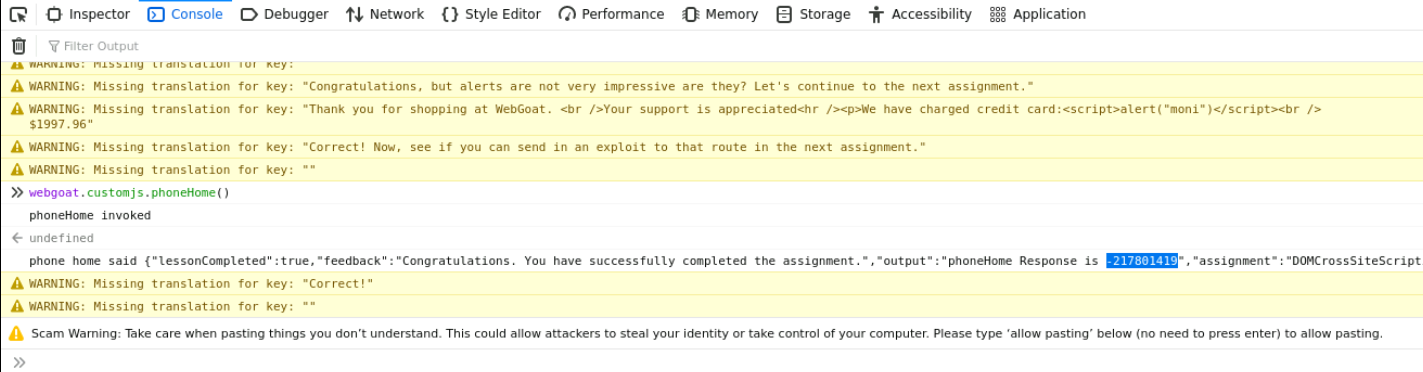
4. compare both , same – yes]

3)<script>alert(“moni”)</script>

start.mvc#test/

11) go to more tools - webdeveloper - console - type webgoat.customjs.phonehome()

then you will note the code



Solution 4: No because the browser trusts the website if it is acknowledged trusted, then the browser does not know that the script is malicious.

Solution 3: The data is included in dynamic content that is sent to a web user without being validated for malicious content.

Solution 1: The script is permanently stored on the server and the victim gets the malicious script when requesting information from the server.

Solution 2: They reflect the injected script off the web server. That occurs when input sent to the web server is part of the request.

Solution 4: No there are many other ways. Like HTML, Flash or any other type of code that the browser executes.

A5

2]

2. **Users,Config**

[procedure:

Right click on log out button

Click on inspect element.

In inspector , you will find answer ]

3. **PdnwzIsKQJ+kHloFkNyfki9qD7MZ9cxHdHizBk3gWL0=**

visit <http://localhost:8080/users>

Then open burp suite

Turn on proxy on foxyproxy

In burpsuite , webgost/user ,right click – send to repeaters

In repeaters, add

Content – Type : application/json

Press send

Copy the hash value

[Procedure link : https://pvxs.medium.com/webgoat-missing-function-level-access-control-2-3-5a1dcd2c4621]

1]

2. tom,cat

3.userId,role

4.WebGoat/IDOR/profile/2342384

5. visit <http://localhost:8080/WebGoat/IDOR/profile/2342384>

Change the last list until it becomes 2342388

The lesson automatically turned green

A4

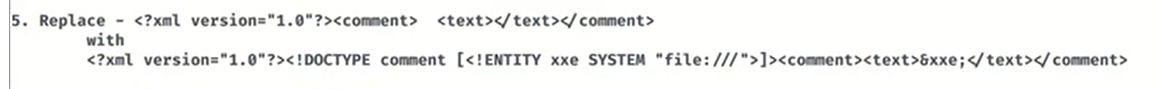
4.

1.Burp suite

2.3Proxy setting

3.Click submit

4.Select Webgoat/xxe/ submit and send to repeater



<?xml version="1.0"?>

<!DOCTYPE comment [<!ENTITY xxe SYSTEM "file:///">]>

<comment> <text>&xxe;</text></comment>

Send

7.

Same as 1 to 4

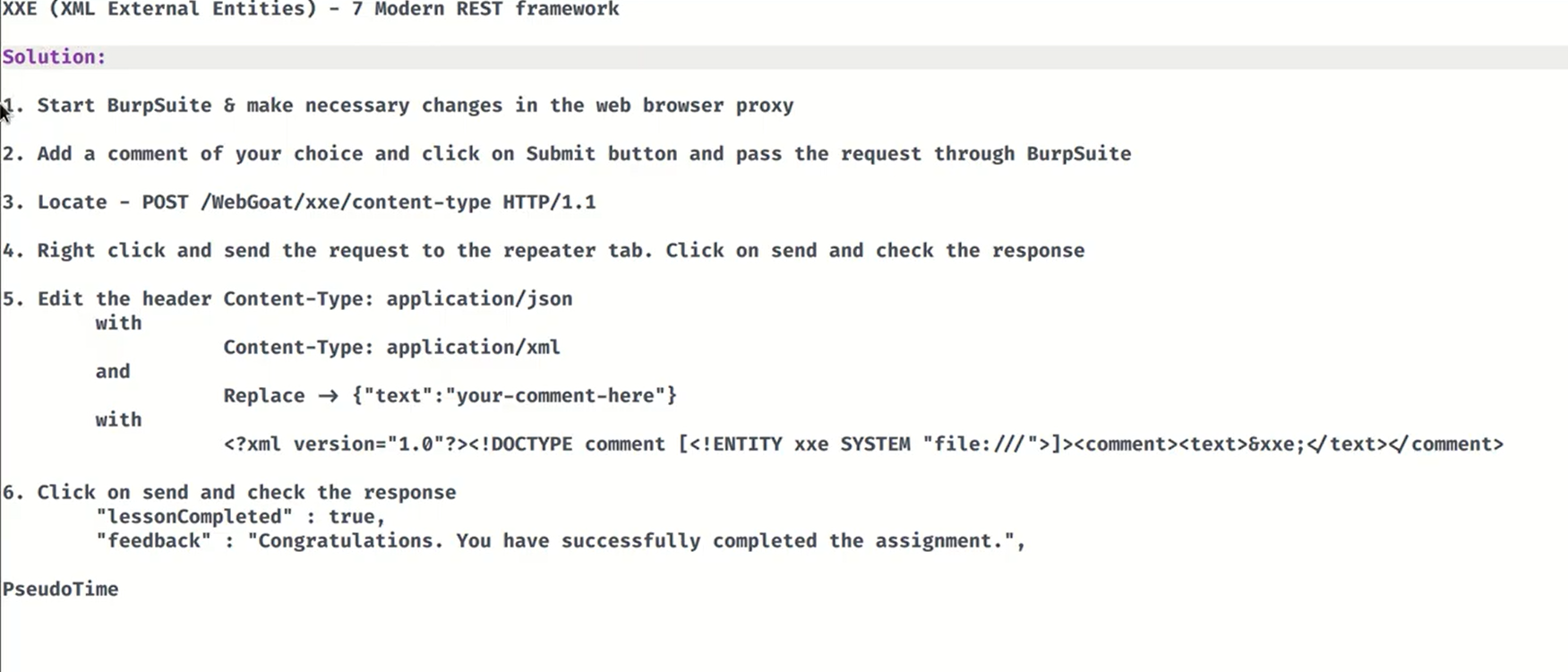
Replace

/json with /xml

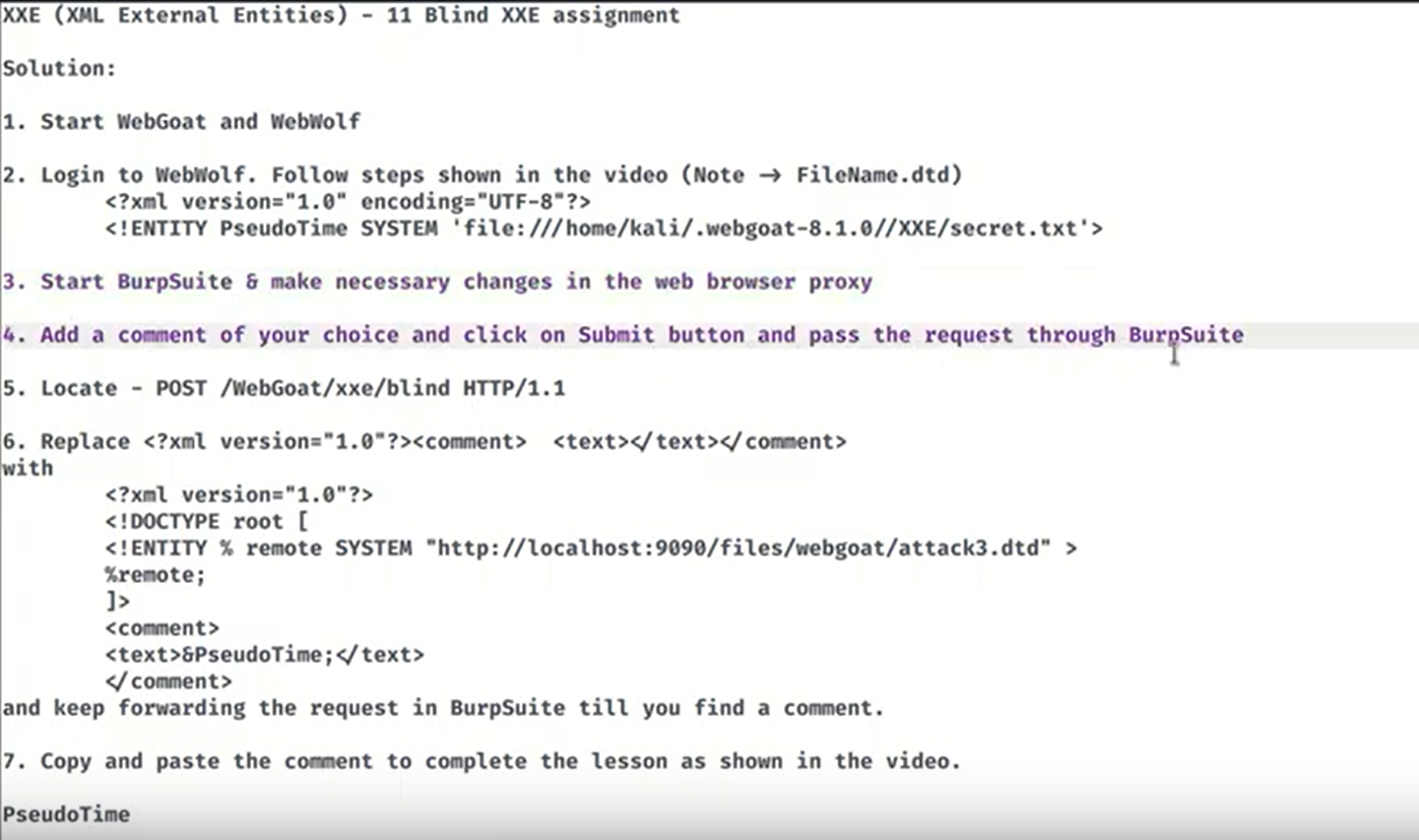
Replace {“text”:”your -comment”} with <?xml version="1.0"?>

<!DOCTYPE comment [<!ENTITY xxe SYSTEM "file:///">]>

<comment> <text>&xxe;</text></comment>

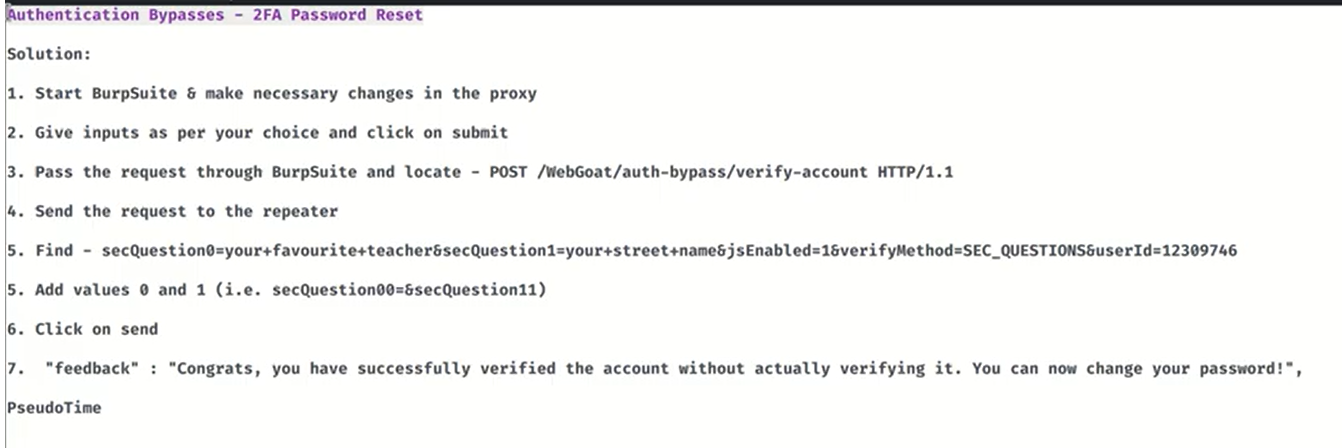


11.



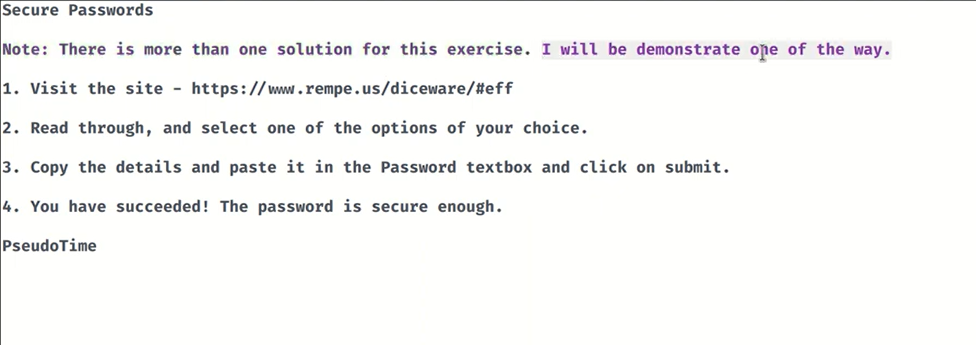
A2:

1.2. 2fa password:

****

**4.3 secure pwd :**

**Ans : requisite pry aftermost unmanned matted refute**

****

**3. password reset**

**2. forgot password**

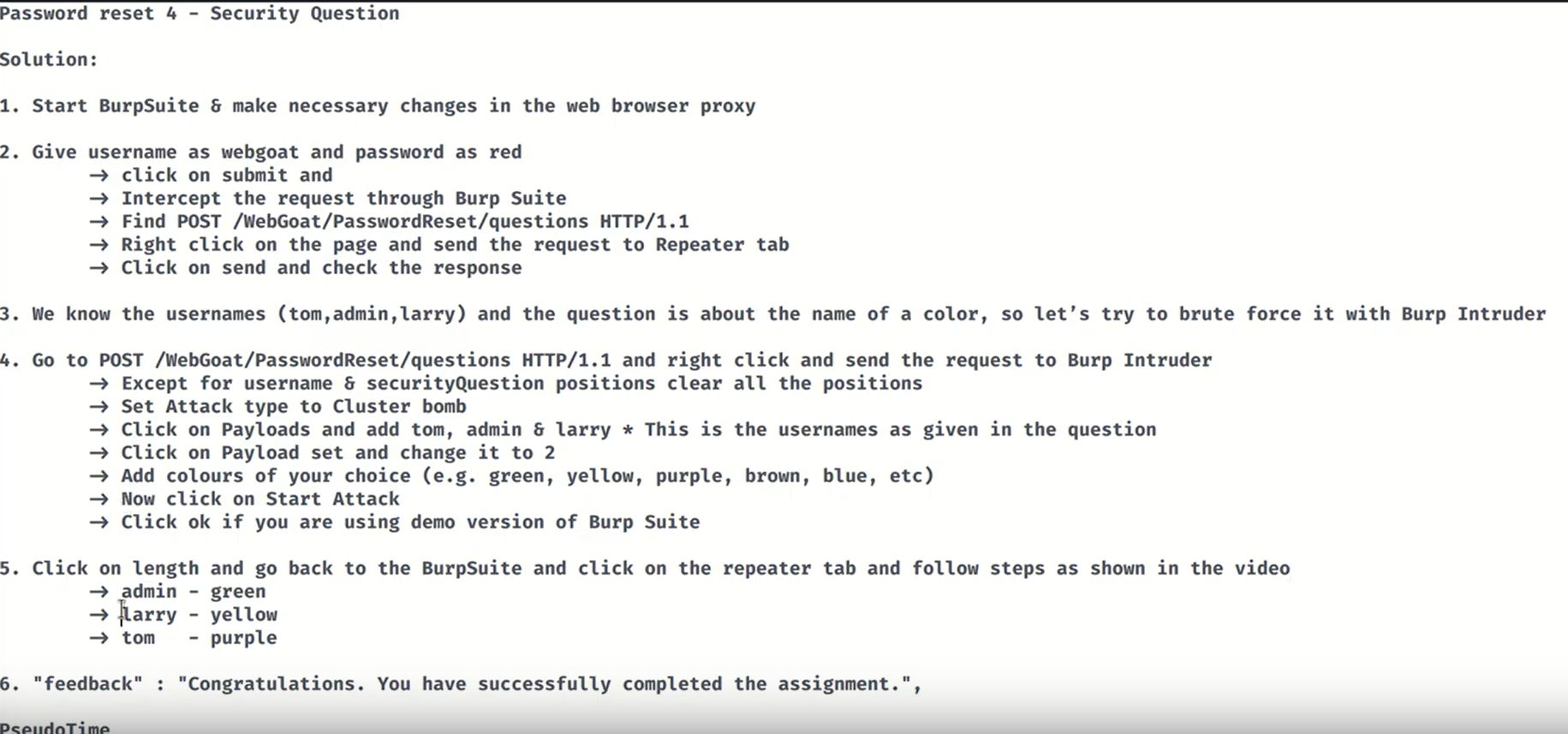
[**Username@webgoat.org**](mailto:Username@webgoat.org)

**Mail sent to webwolf with password**

**Back to account access , type email and password**

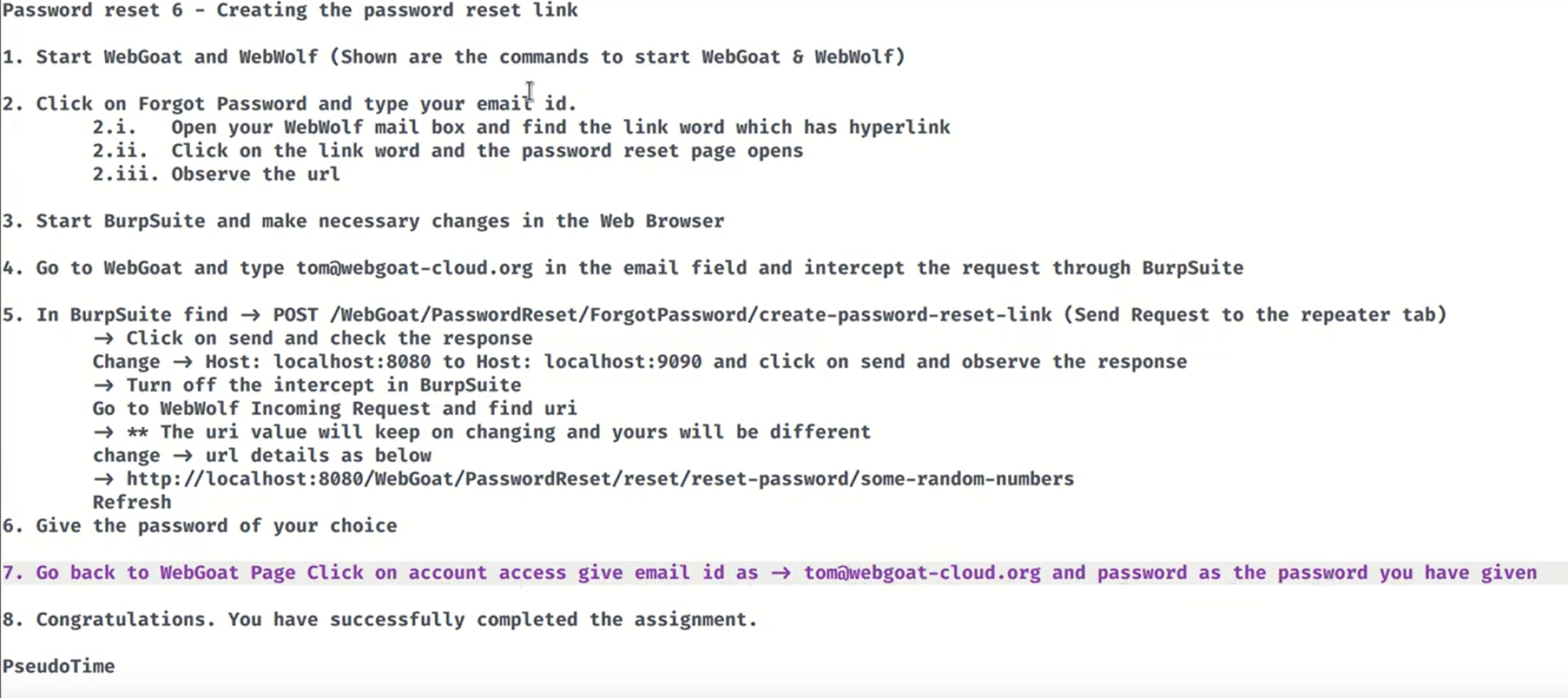
**4.**

**Larry,yellow**

****

**5. just press check**

**Or else select ‘what is fav color ‘ and then press check**

**6.** ****

2.JWT token

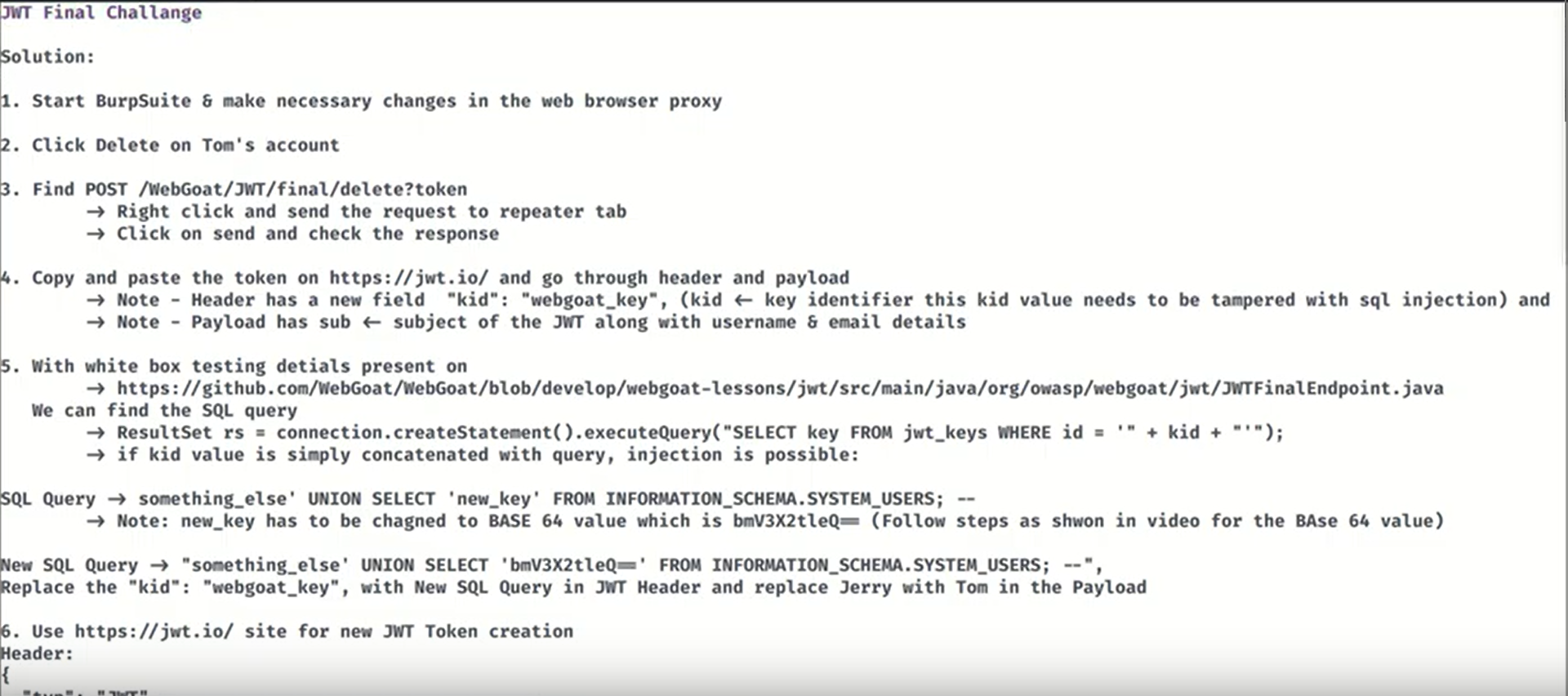
3.user

7. line 12

Line 9

Balance : 5,8,10

11.

****

**Graphical user interface, text, application, email

Description automatically generated**