**Cybersecurity 401**

**Module 8 - Web Application Security**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## **Lab 36 - XSS with w3af, DVWA**

## 

**| Rodrigo Brasil 01/2024 |**

### 

### **Part 1: Staging**

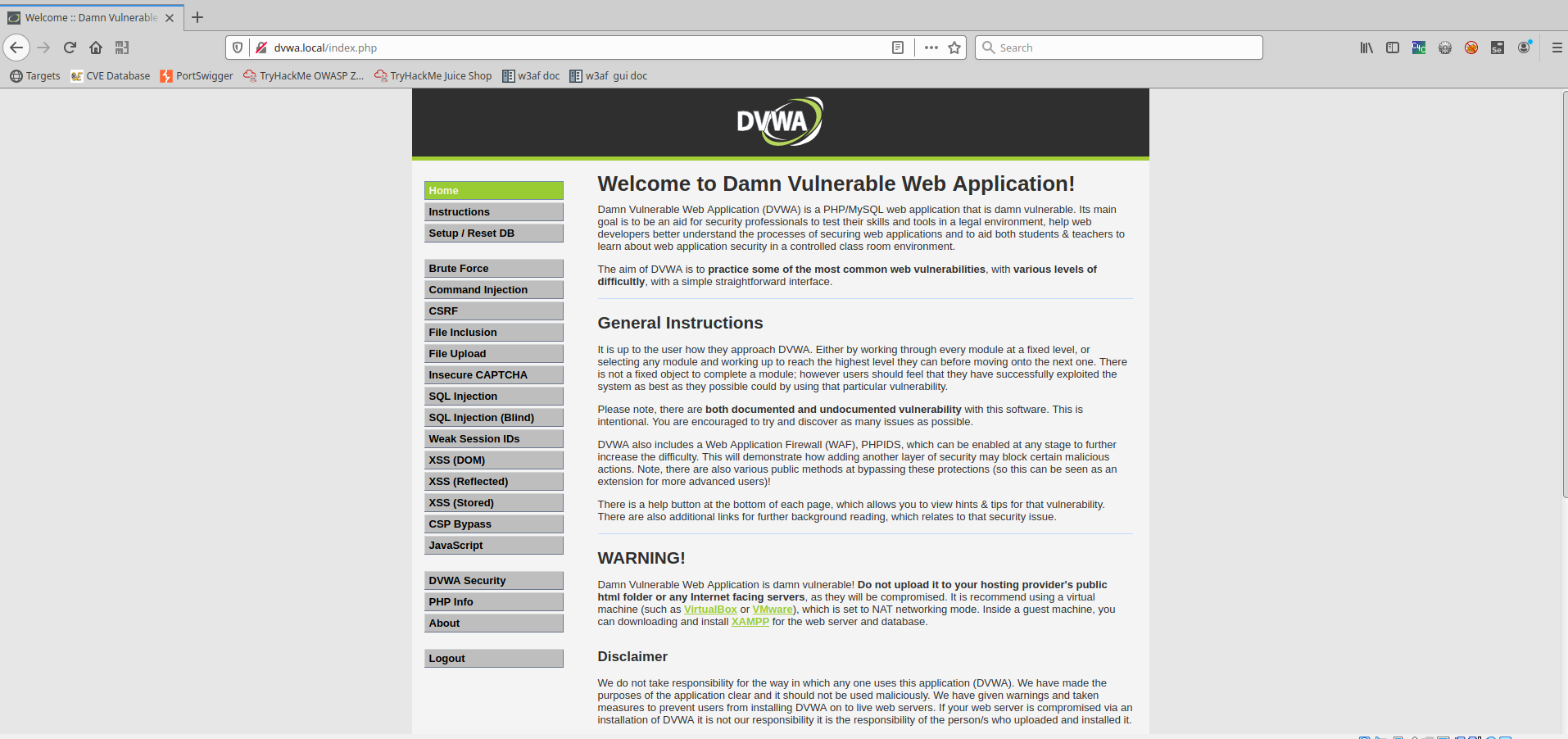
This lab requires Web Security Dojo OVA.

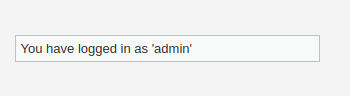


### 

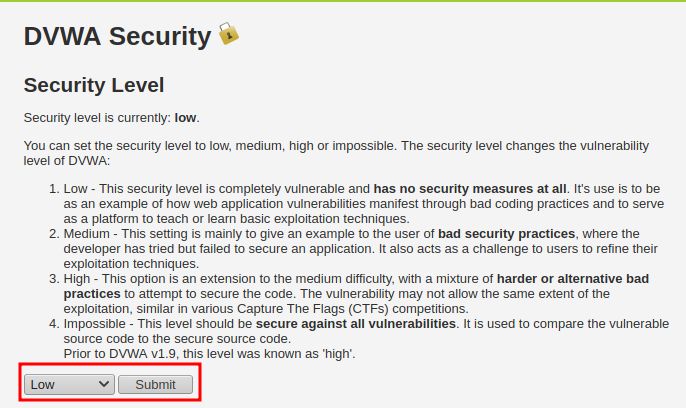
### **Part 2: XSS on DVWA**

Login to DVWA as the administrator. For each successful outcome achieved, include the string you typed into the field and a screenshot of the outcome.

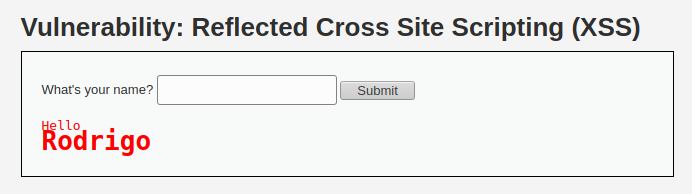




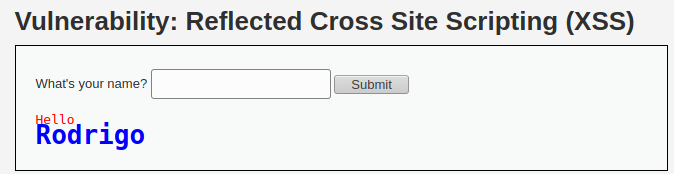
* Set DVWA Security to “Low”



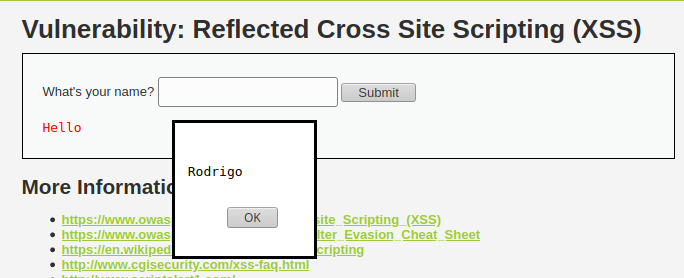
* Perform the following XSS (Reflected) exploits:
  + Have the site return your name as a larger font



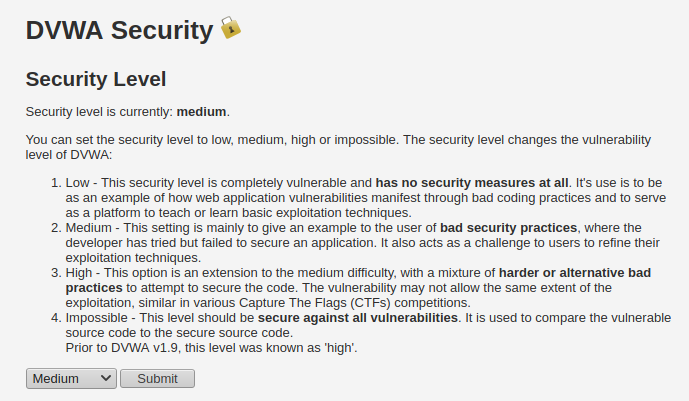
* + Have the site return your name in a different color



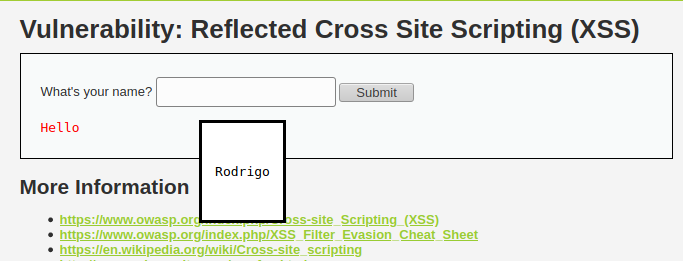
* + Have the site return your name in a popup box



* Set DVWA Security to “Medium”



* Perform the following XSS (Reflected) exploits:
  + Have the site return your name in a popup box  
    *Hint: How do you think the site is detecting your script command? Perhaps its defenses are not as “sensitive” as they seem!*

**

*<dialog open> <p>Rodrigo</p> </form> </dialog>*

* + Have the site return the session cookie in a popup box  
    *Hint: How did you get a popup box to appear last time?*

*<dialog open>*

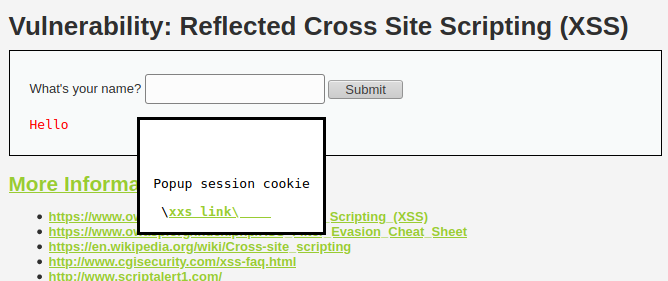
*<form>*

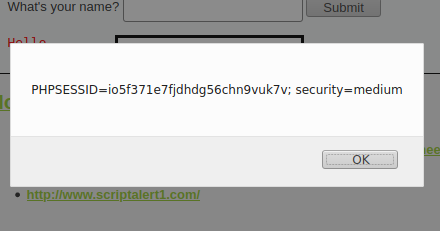
*<p>Popup session cookie</p>*

*\<a onmouseover="alert(document.cookie)"\>xxs link\</a\>*

*</form>*

*</dialog>*

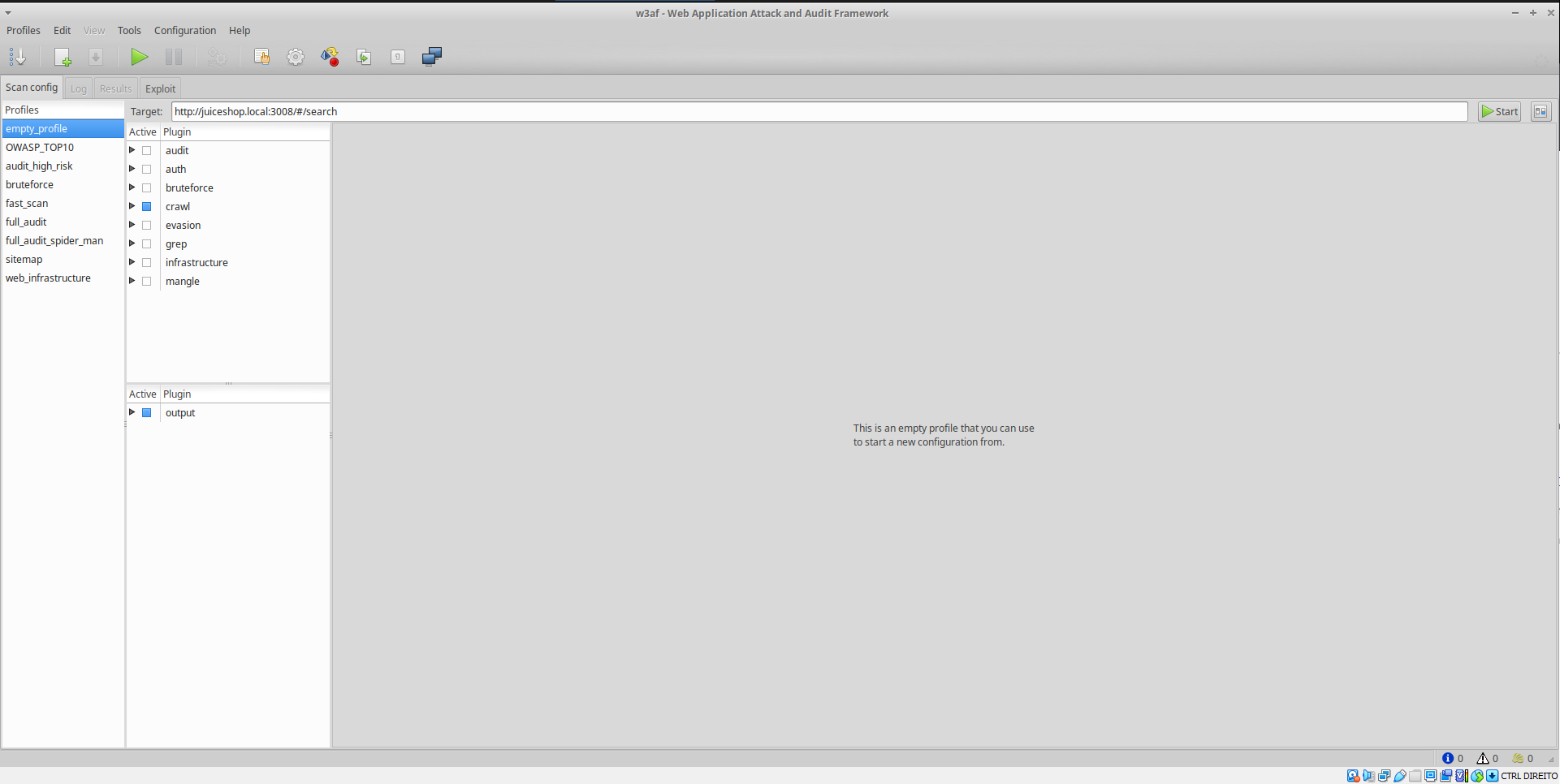
**

**

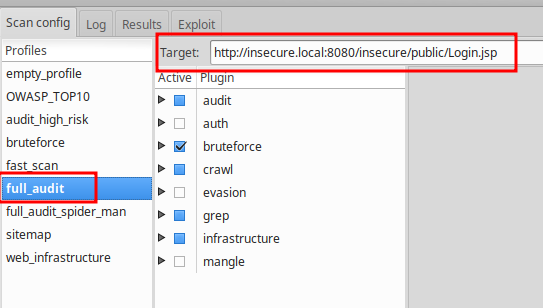
### **Part 3: Evaluating InsecureWebApp with w3af**

In this next part we will scan InsecureWebApp with w3af.

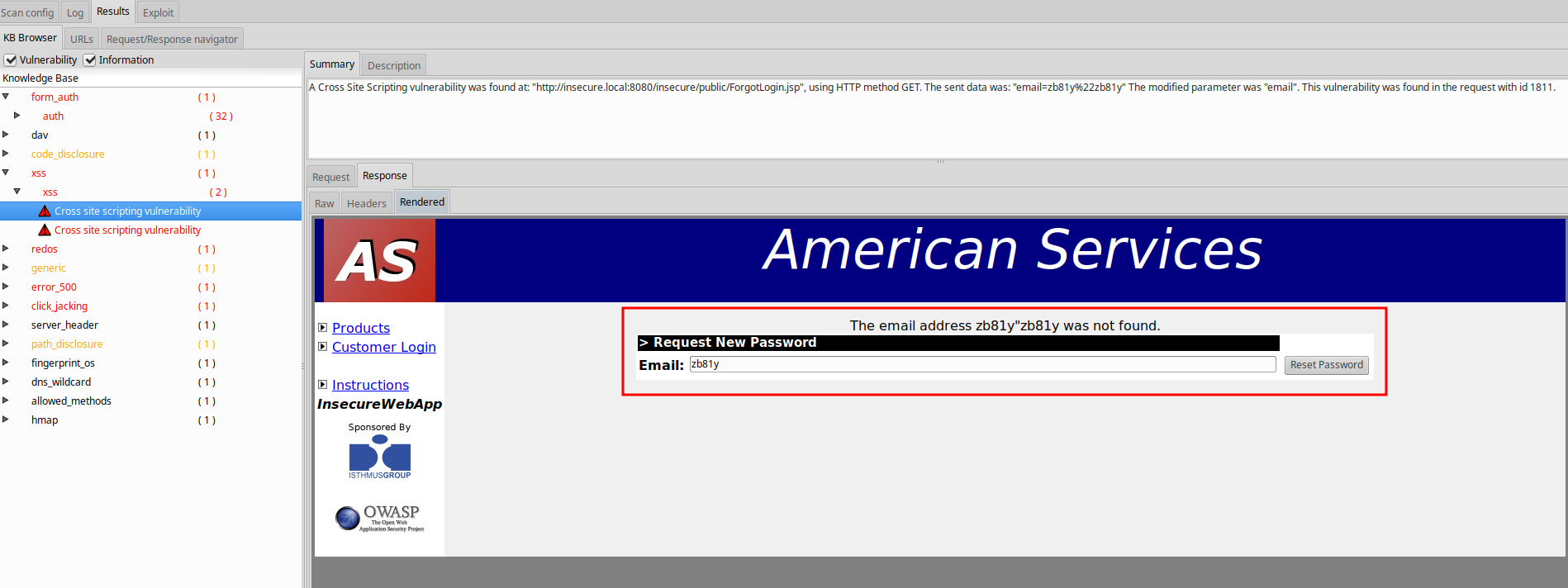
* Launch w3af (GUI version)



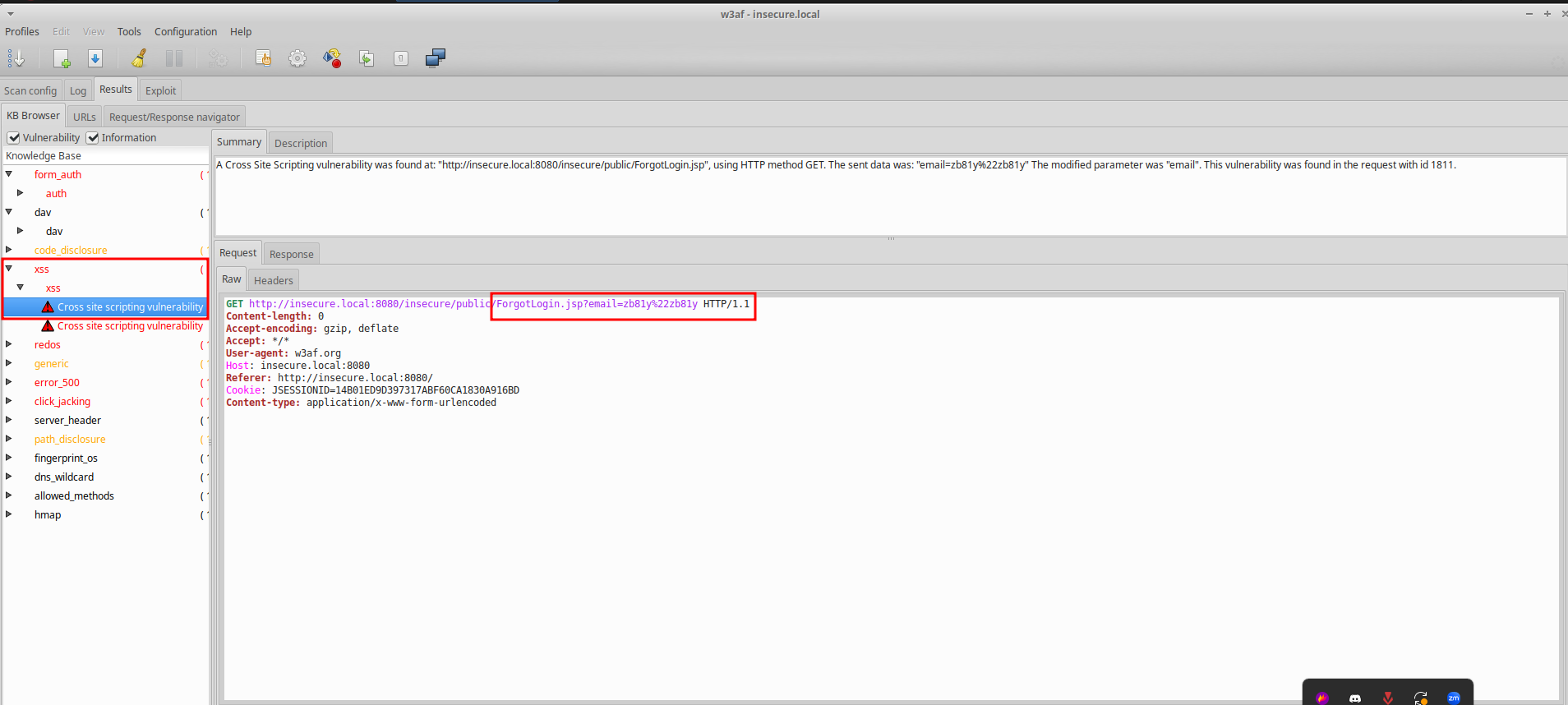
* Scan <http://insecure.local:8080/insecure/public/Login.jsp>



* Include a screenshot of the rendered response of the XSS vulnerability as discovered in w3af GUI that is associated with the “Forgot Login” page



* Include a screenshot of the results of the web crawler.



For the discovered XSS vulnerability, document in your submission:

* Name of the vulnerability
* XSS (Cross site scripting)
* Date of the discovery
* 16 january 2024
* Score based on CVE (Common Vulnerabilities and Exposures) databases
* A detailed description of the vulnerability
* A detailed description of the affected systems
* Details of the process to correct the vulnerability

### 

### **Part 4: Reporting**

Answer the below prompts in your own words:

* What is XSS, and why is it a security threat?
* XSS or cross site scripting is a website vulnerability that occurs when an application includes untrusted data on a web page. It is a security threat because this allows an attacker to inject malicious scripts into web pages viewed by other users which can lead to stolen login credentials or personal data.
* What is a session cookie?
* A session cookie is a piece of temporary data, Its primary purpose is to maintain the state of a user's interaction with the website across multiple requests and responses. They are temporary and are supposed to be discarded after a user closes the browser.
* How can a session cookie be abused by an attacker?
* It can be used by an attacker to act like a certain user like an admin for exemple.