**ASSESSMENT**

**DHAREKA S. – 727623BSC029**

**TARGET SITE:** [**http://python.testvicti.com**](http://python.testvicti.com)

**SCOPE:**

**Authentication**

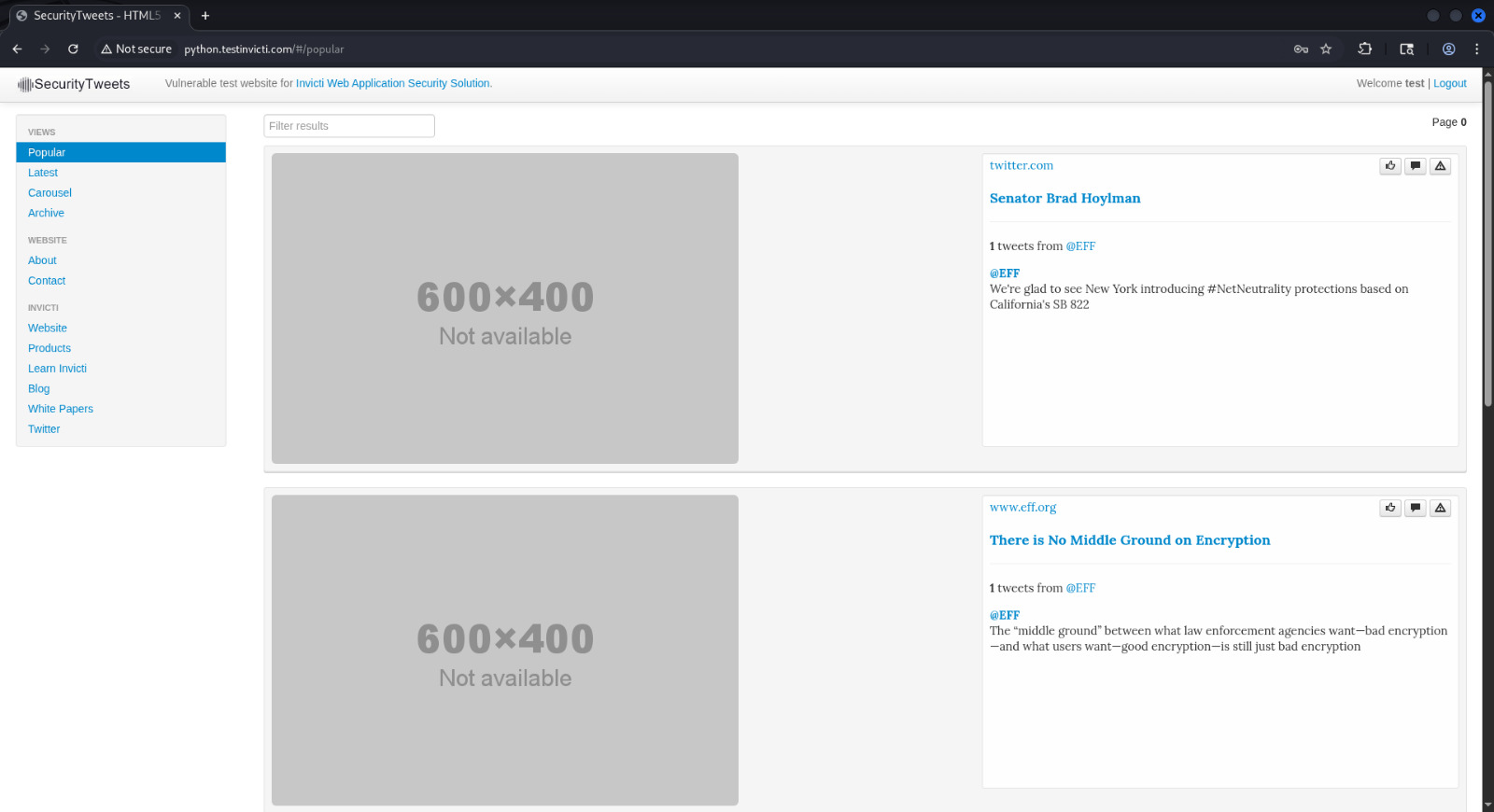
**Authorization**

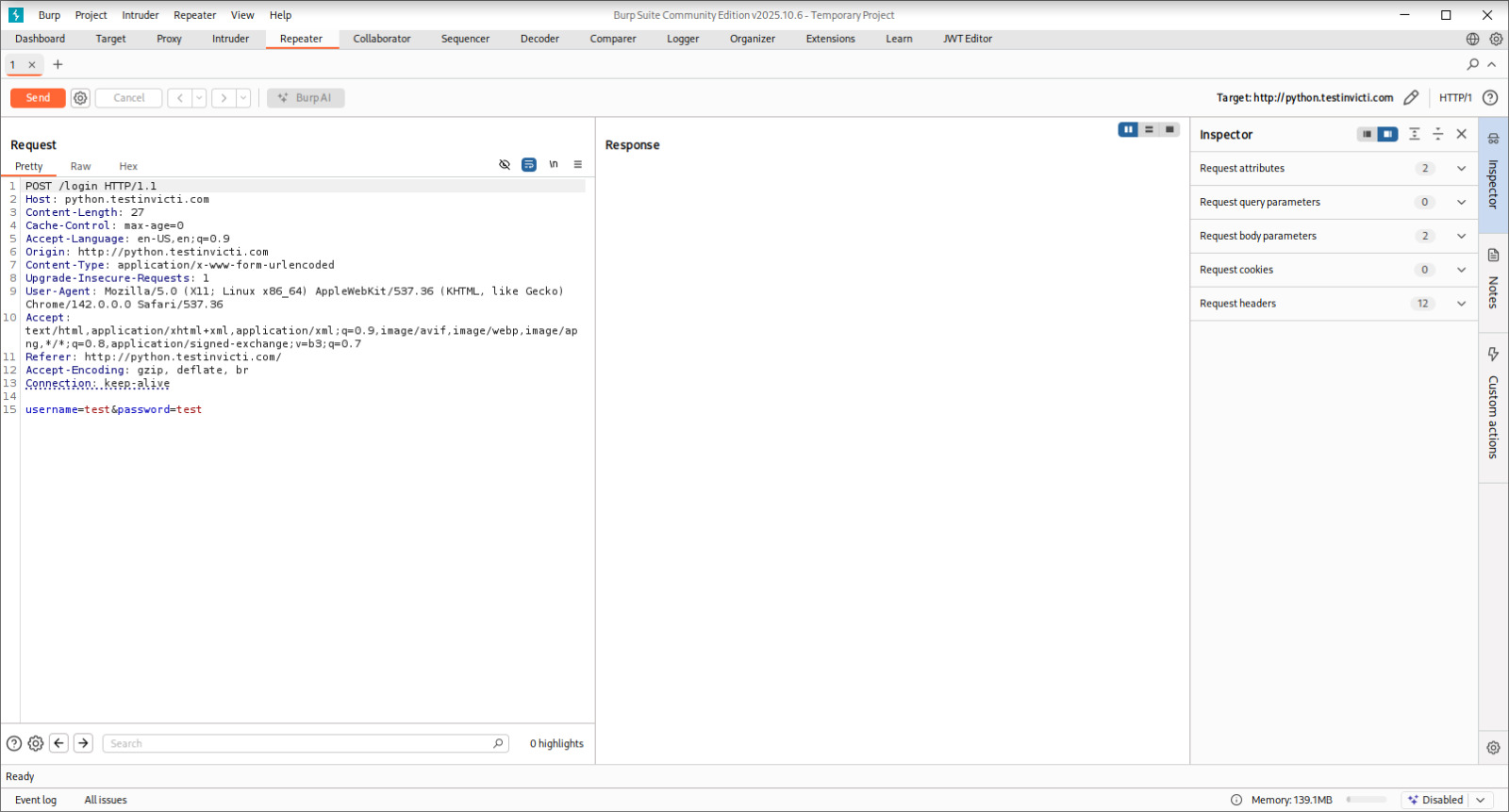
**Cross site Scripting XSS**

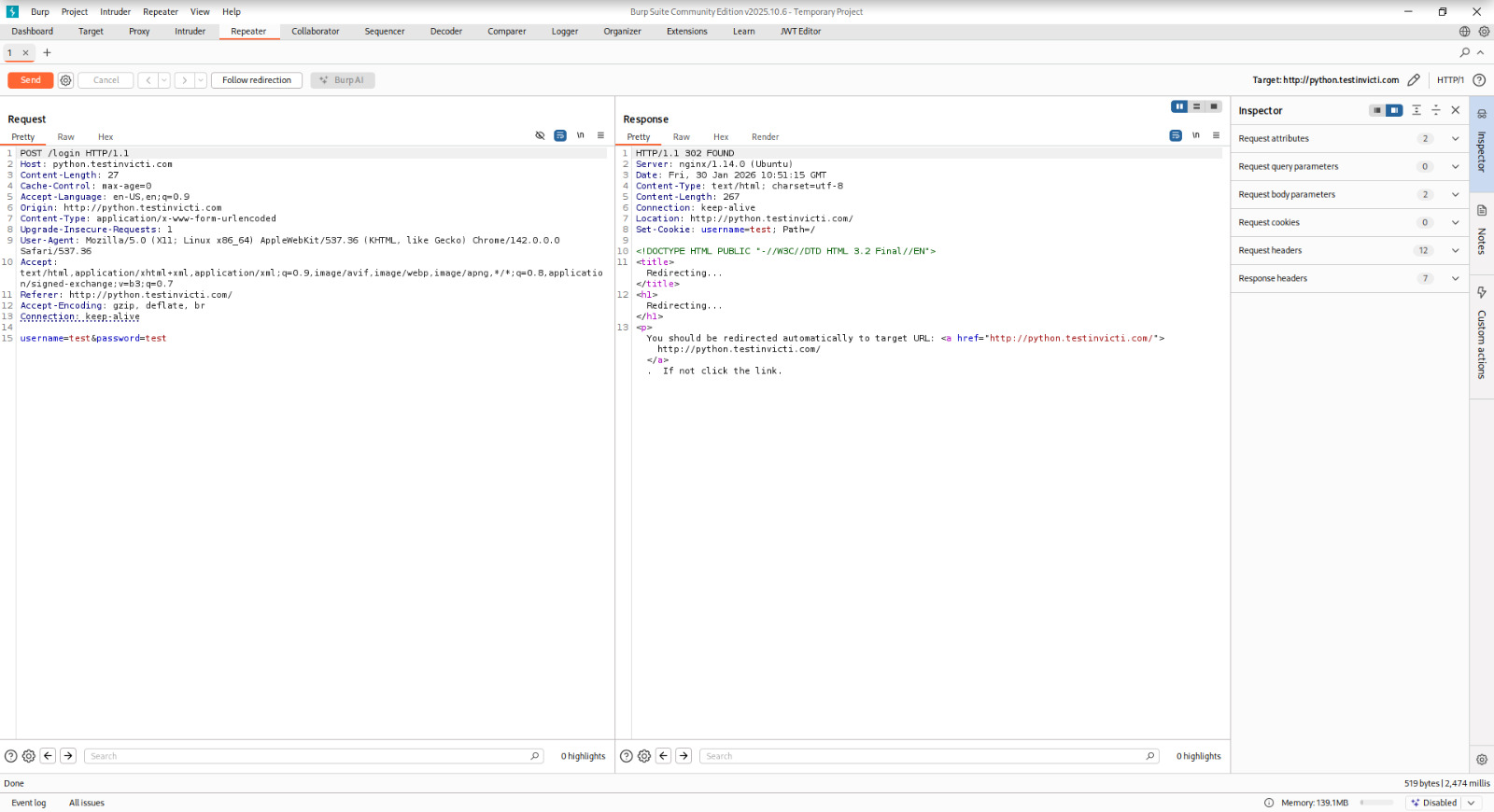
**SQL Injection**

**AUTHENTICATION:**

**1.WEAK PASSWORD POLICY**

****

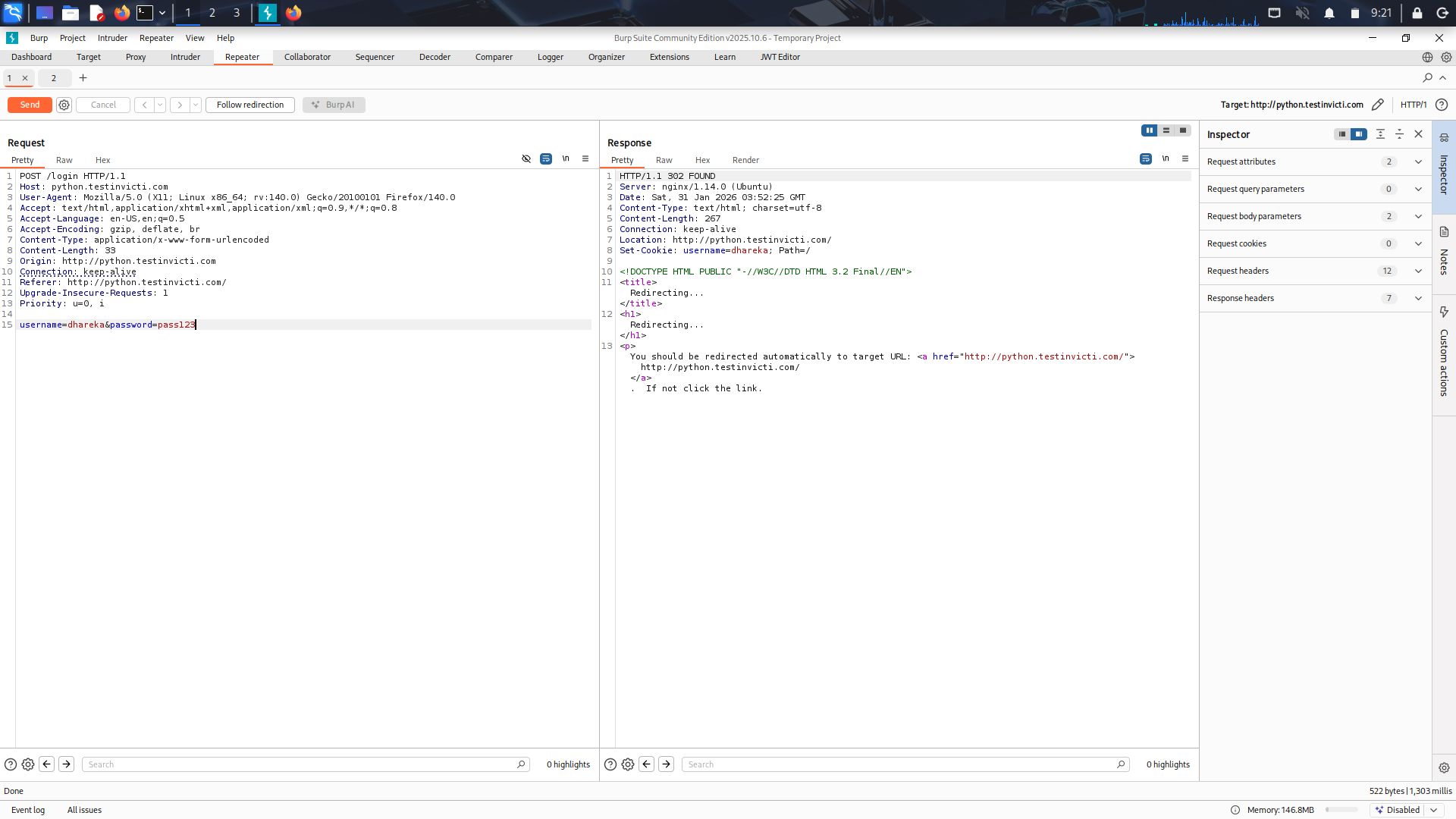
****

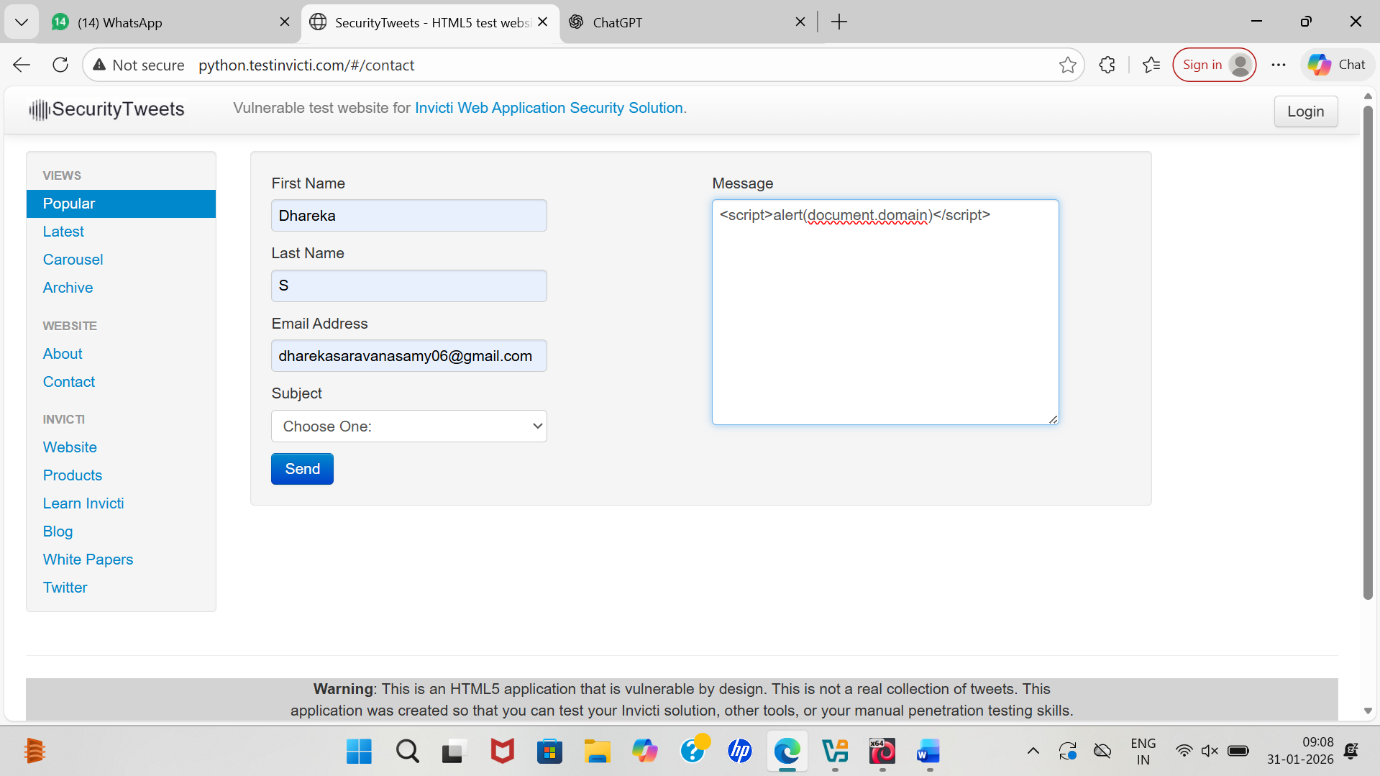
****

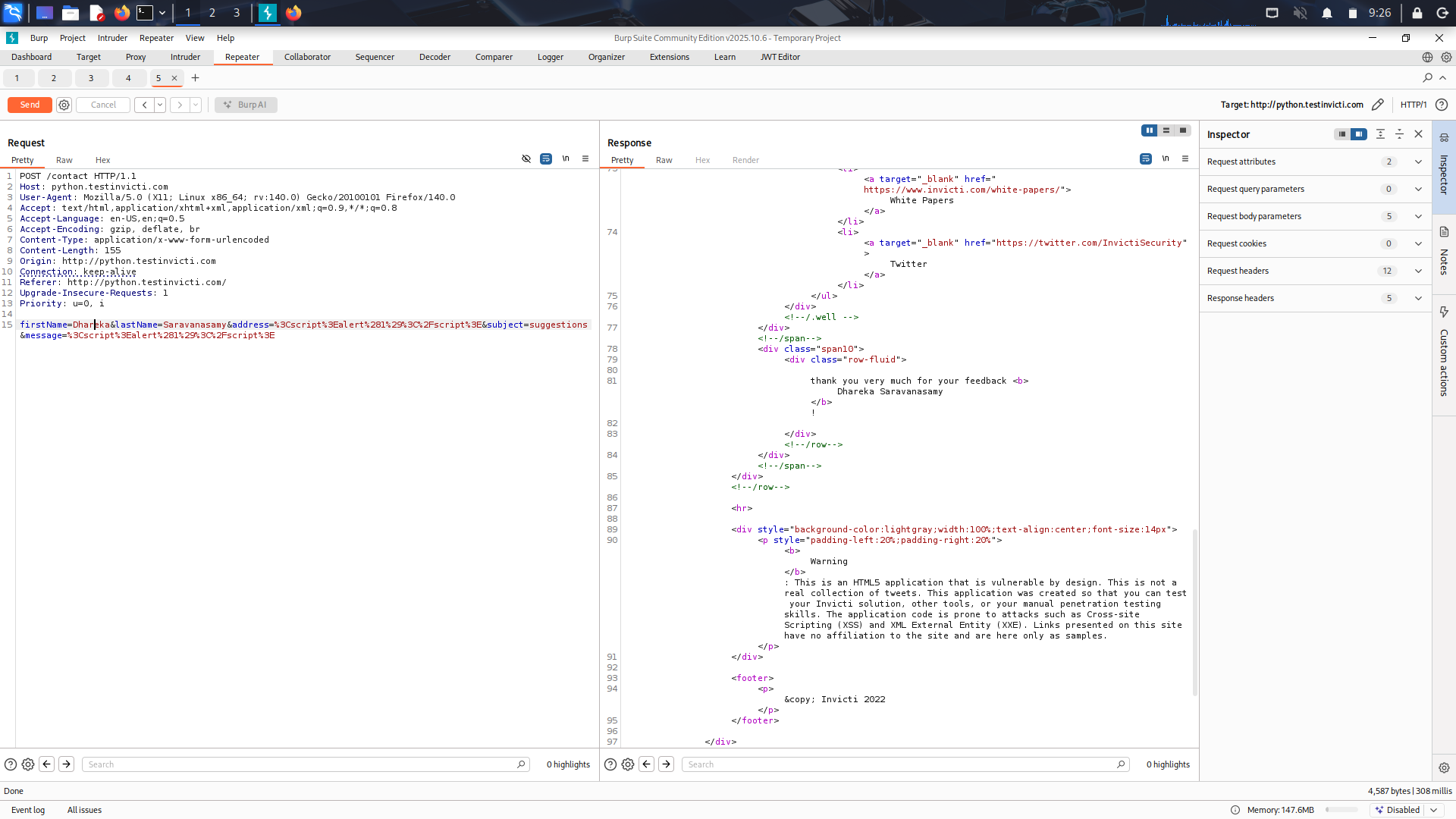
A login request with password=123456 resulted in a successful authentication.

The server responded with HTTP 302 and issued a session cookie.

**2. Input Feields are in String format so XSS scripts are not posible**

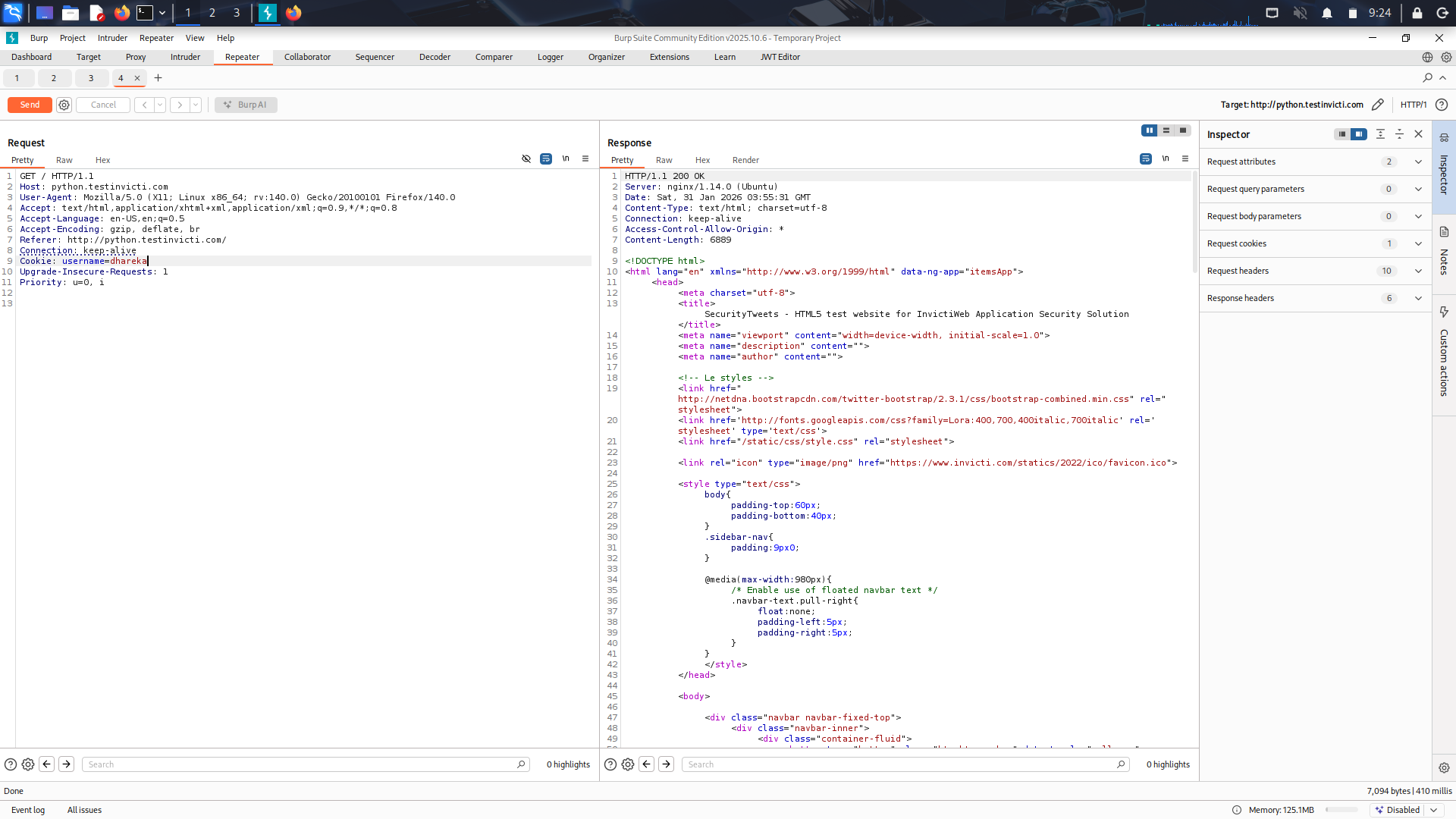
****

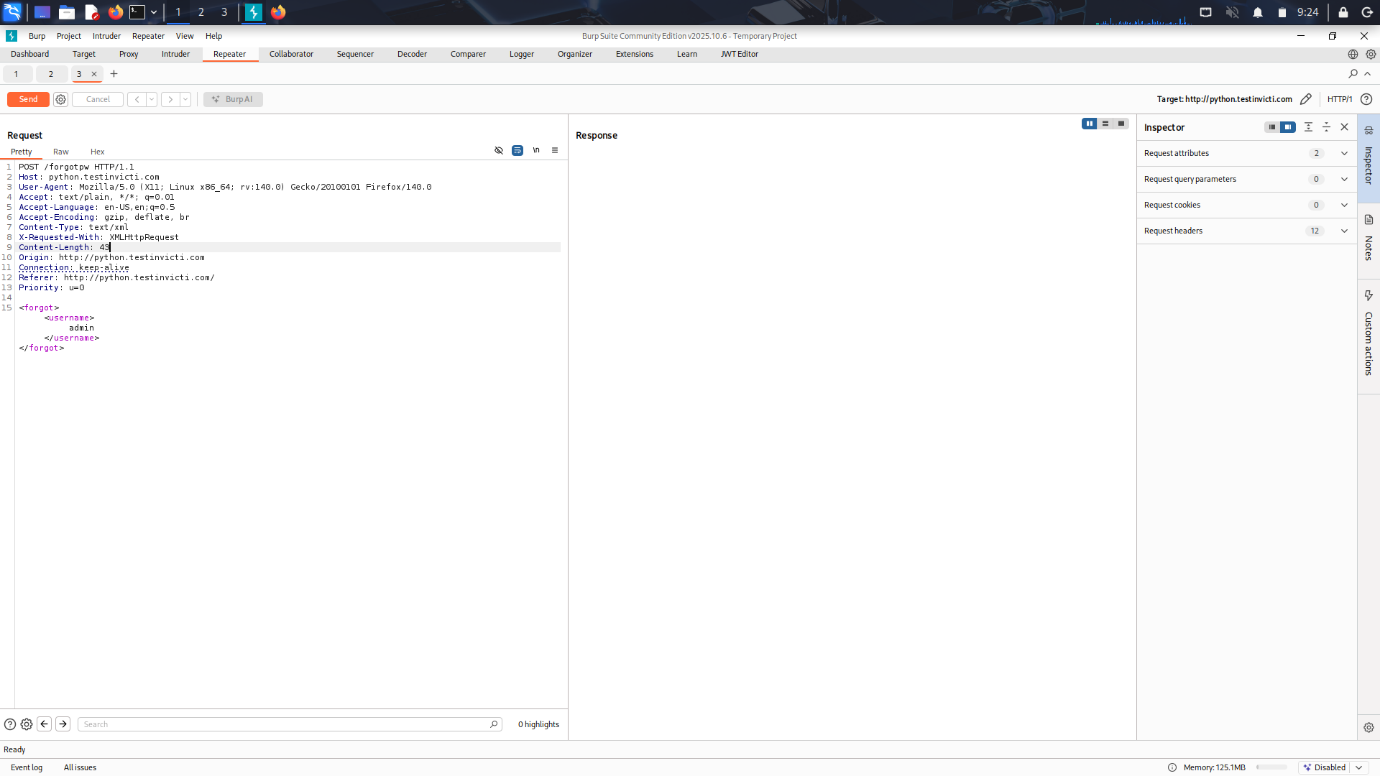
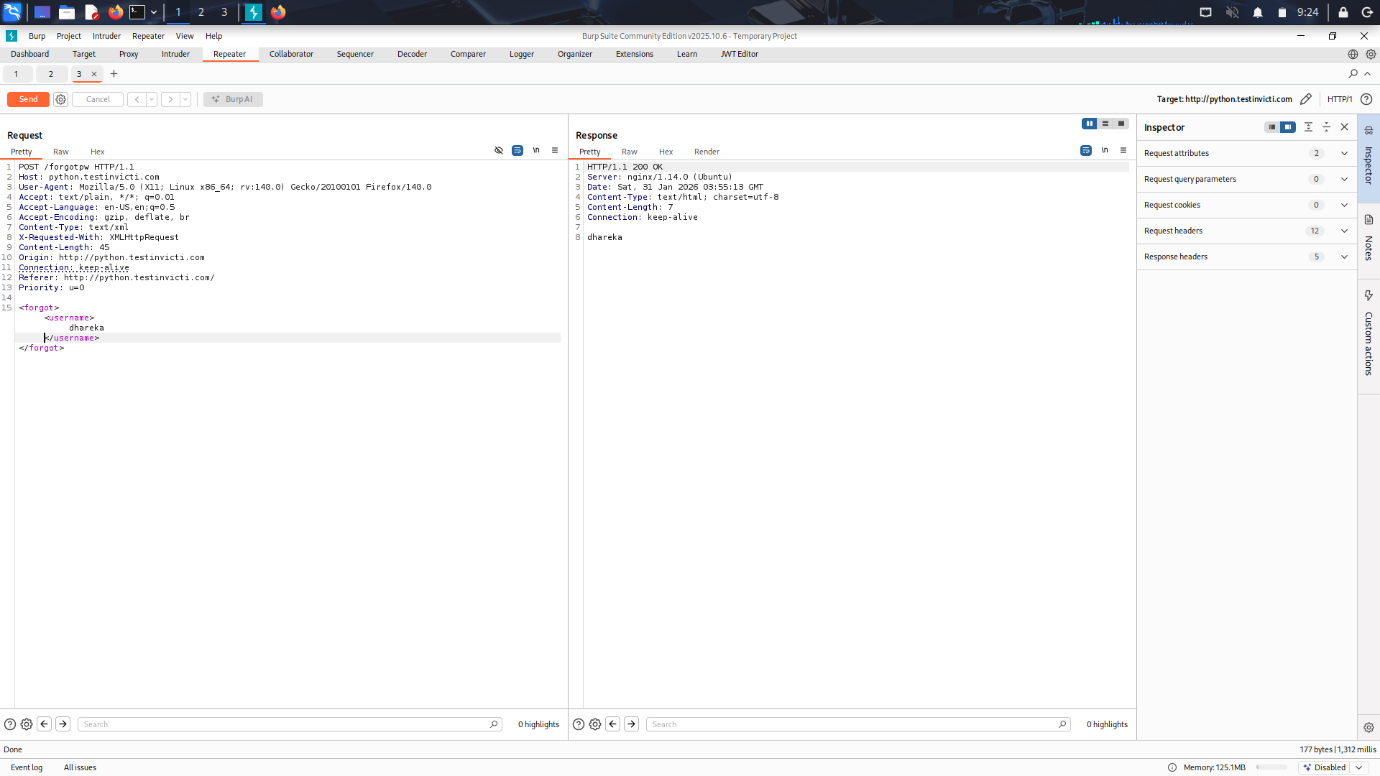
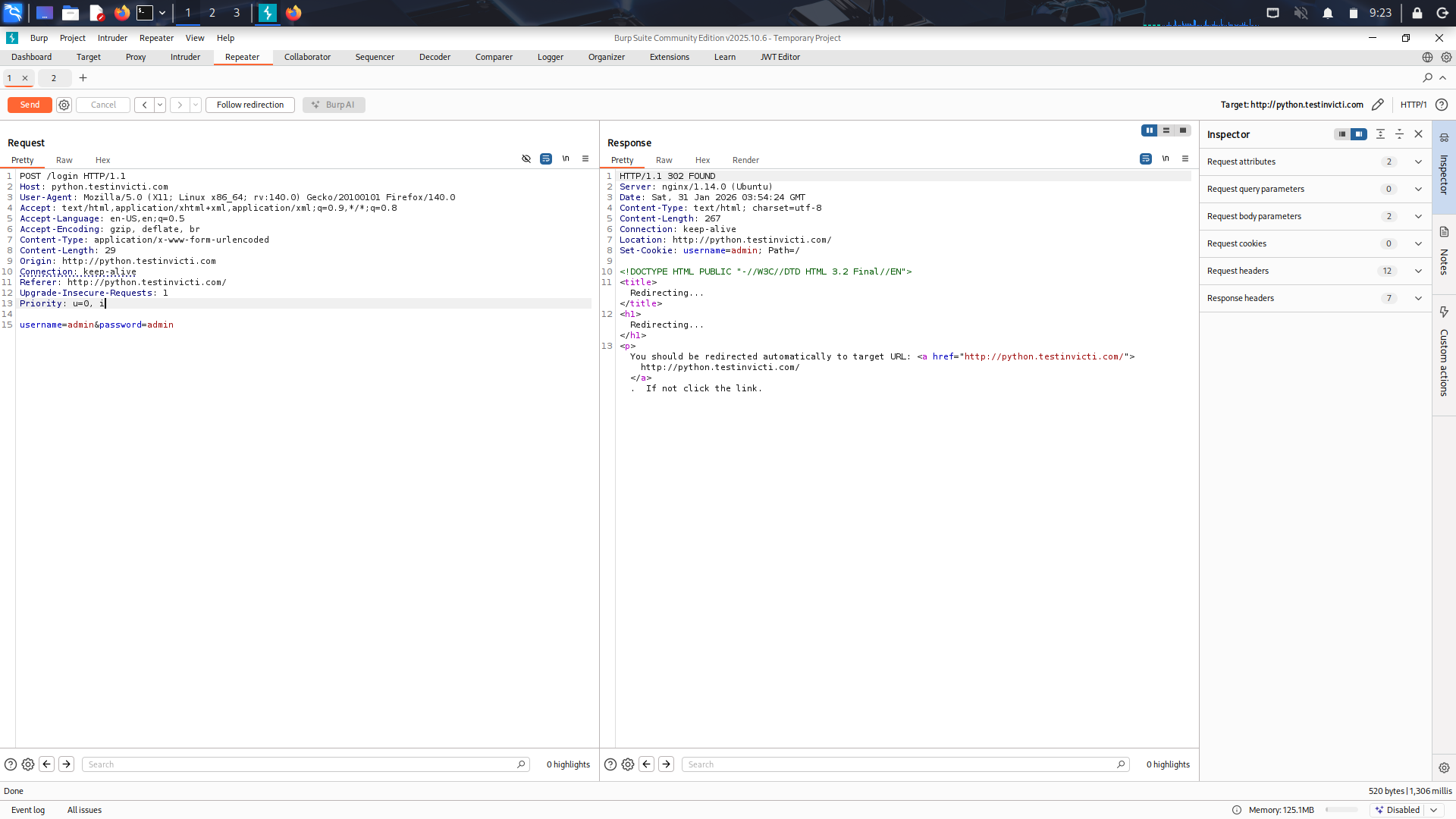
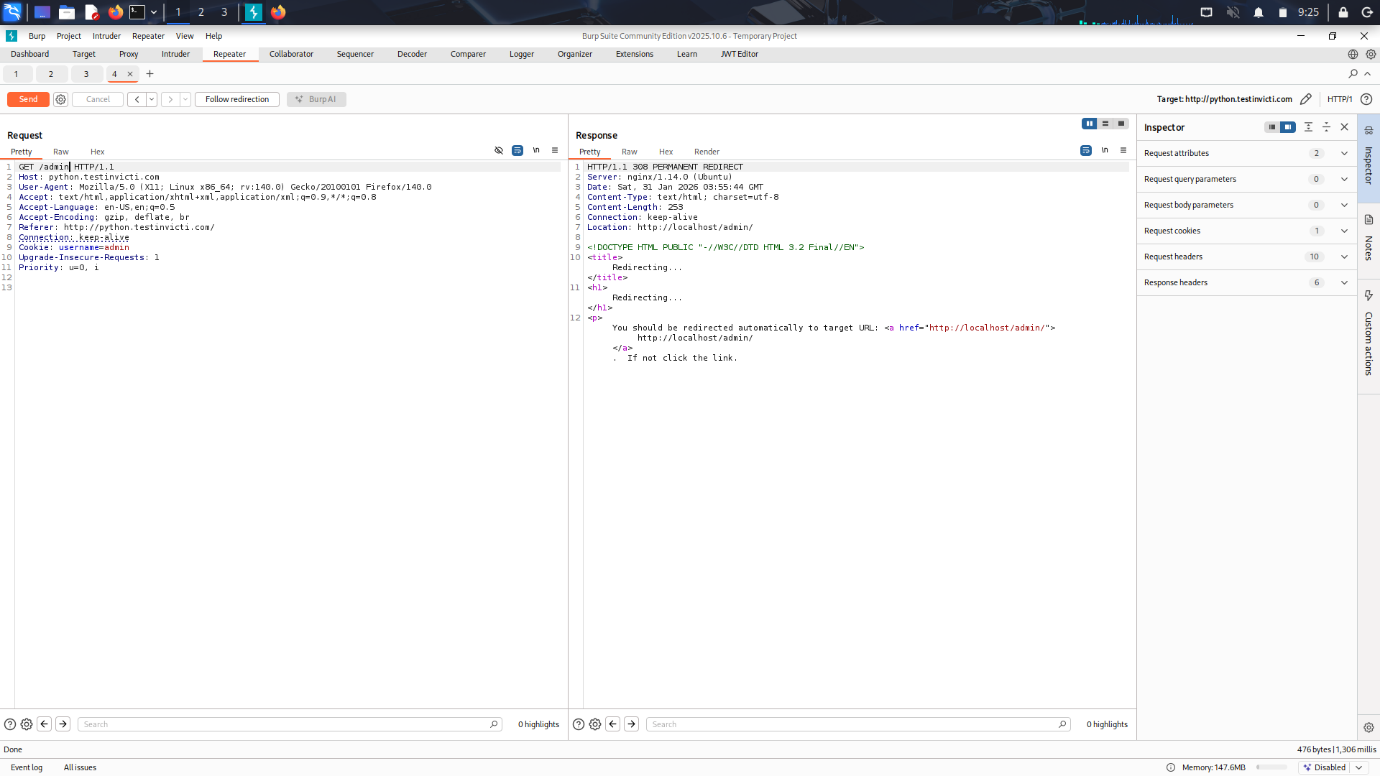
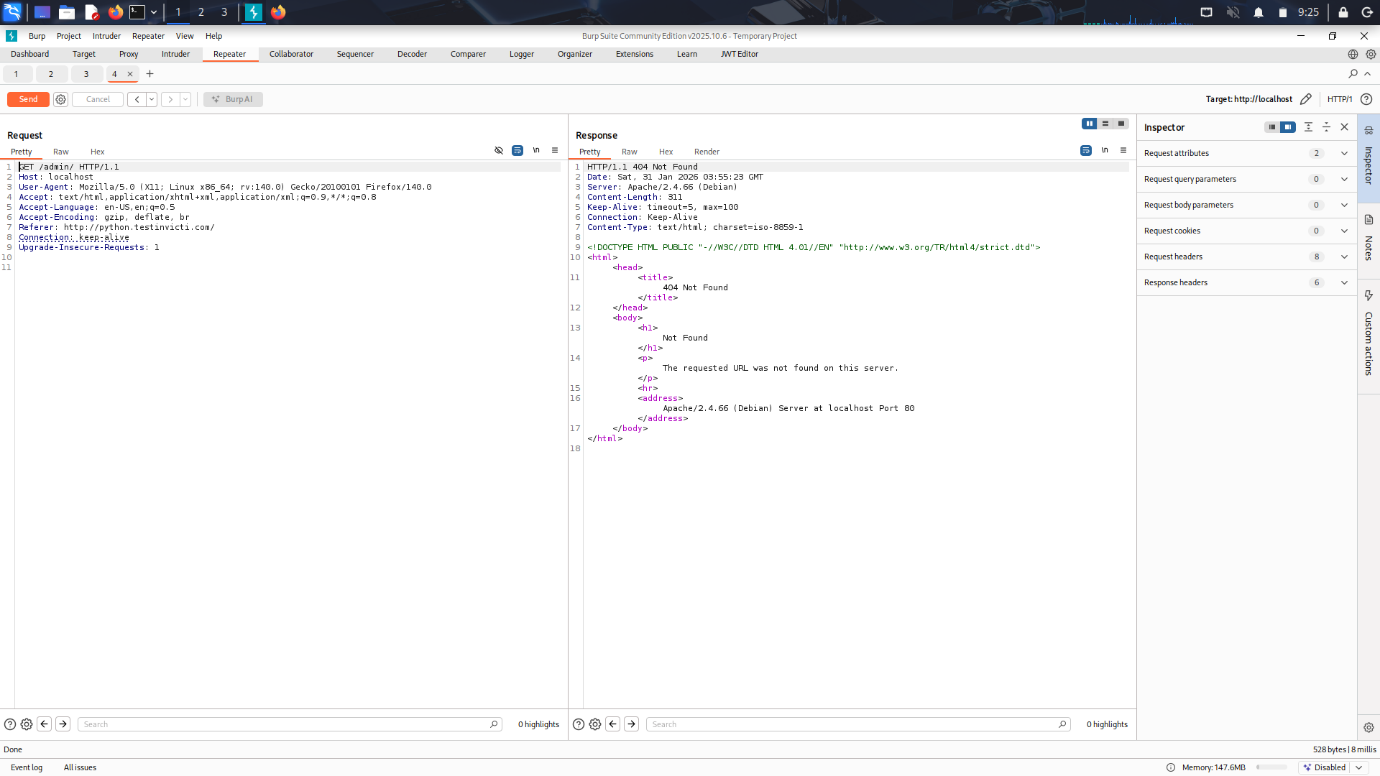
**3.Broken object access**

****

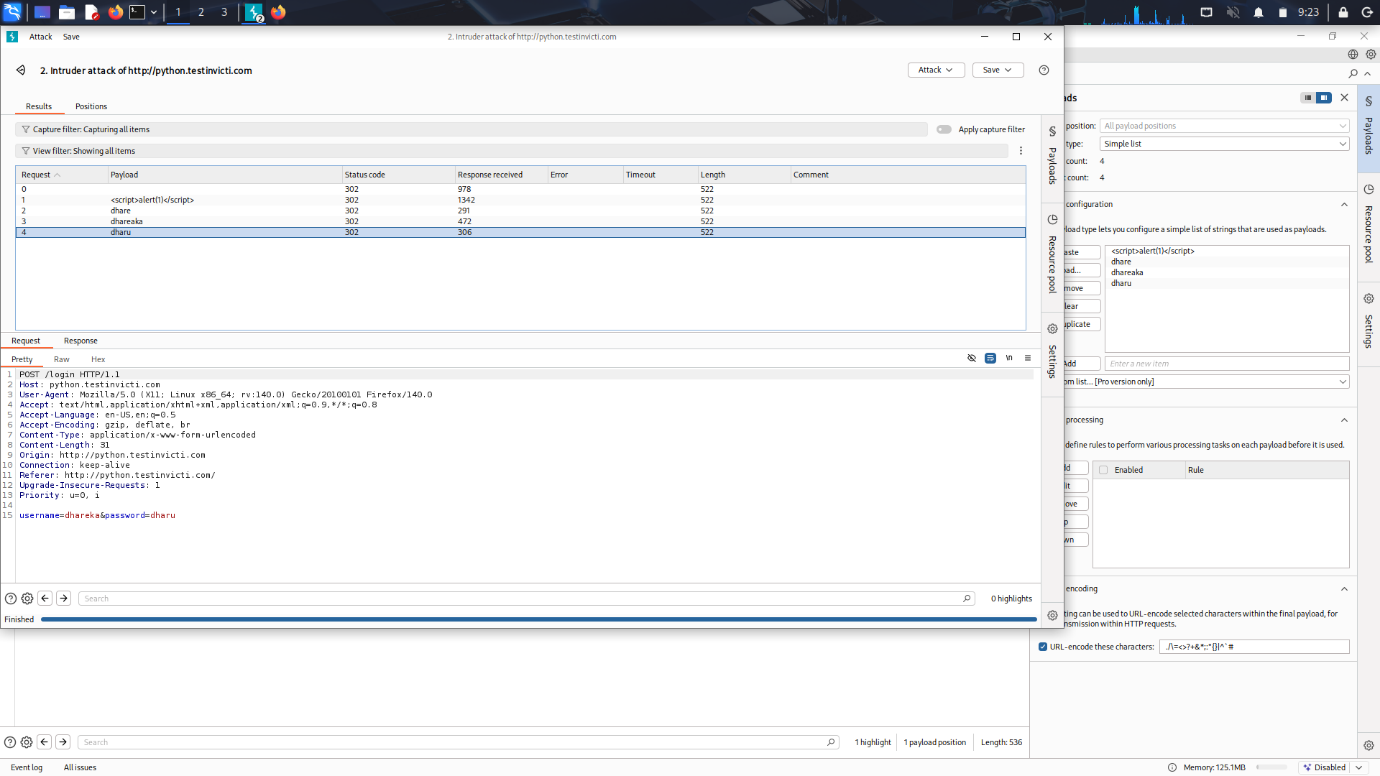
**4.FORGET PASSWORD – RATE LIMITING :**

**Authorization:**

****

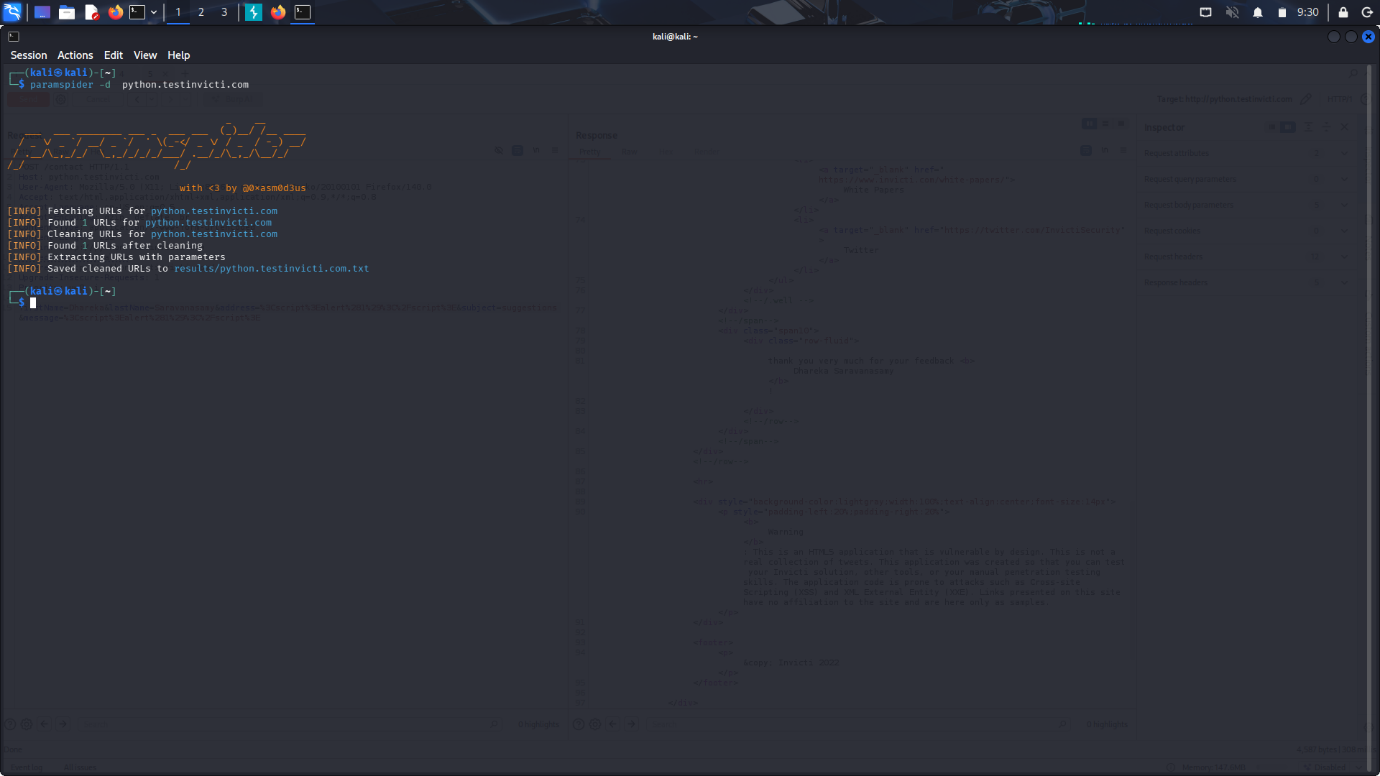
**1.Vertical privilege escalation:**

**2.Horizontal privilege escalation:**

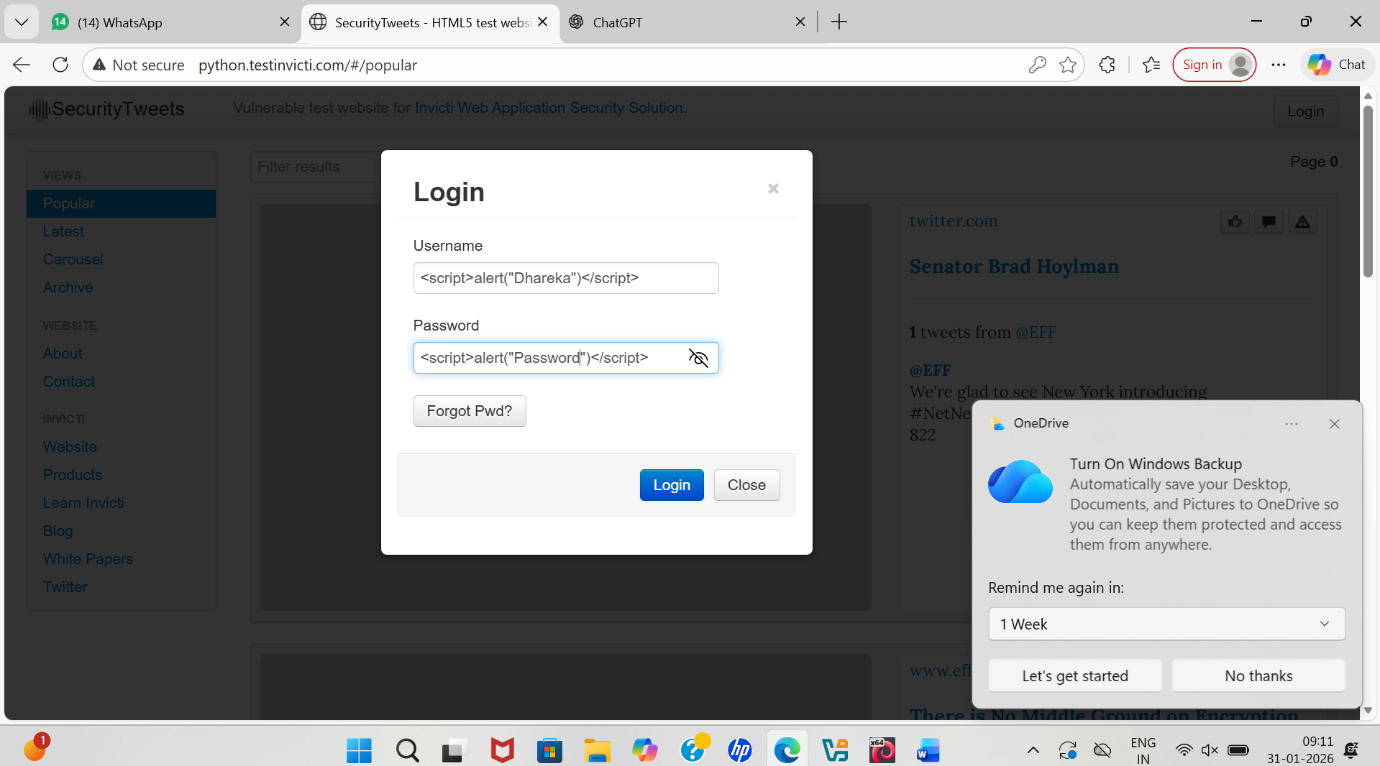
****

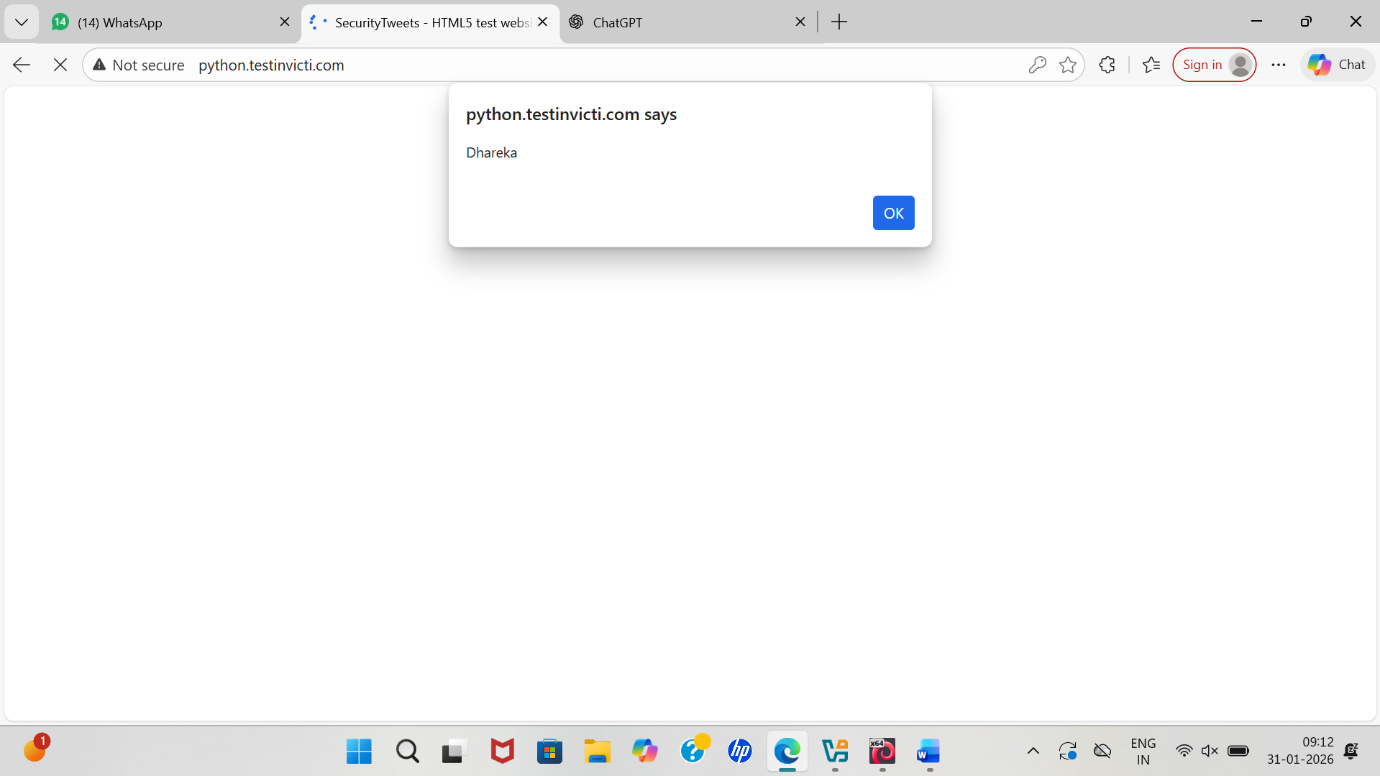
**Cross Site Scripting(XSS):**

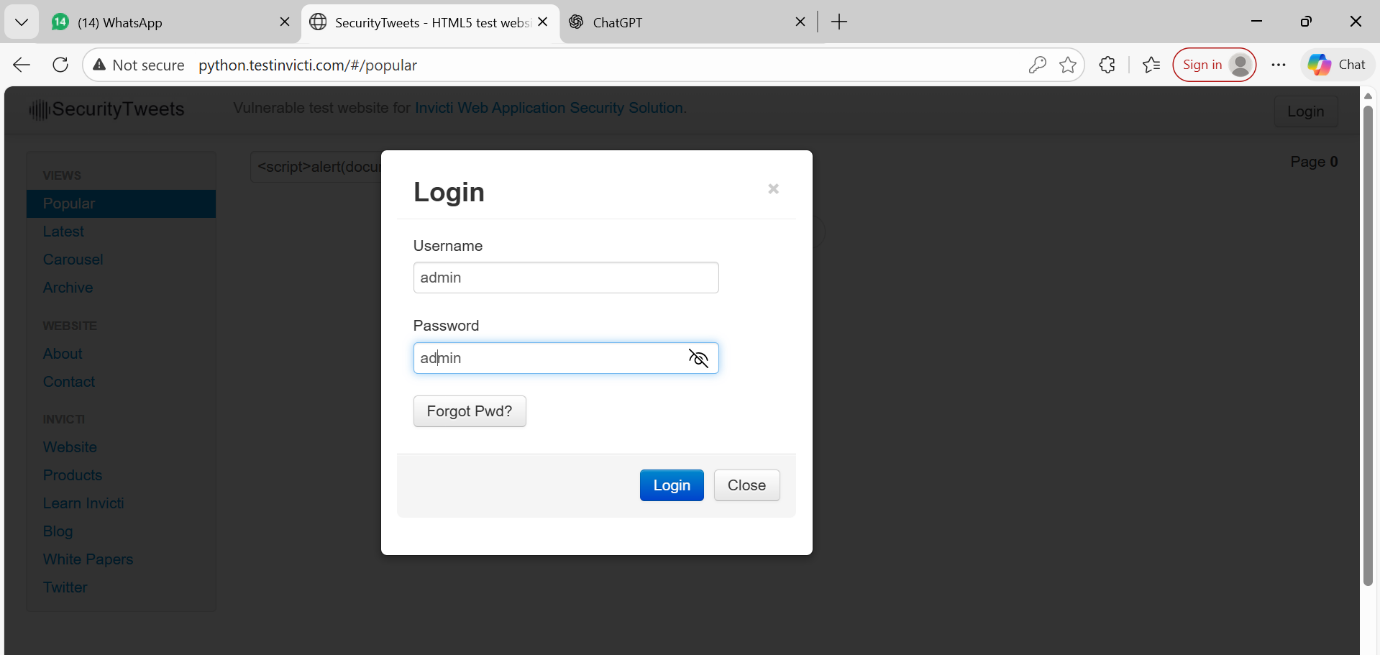
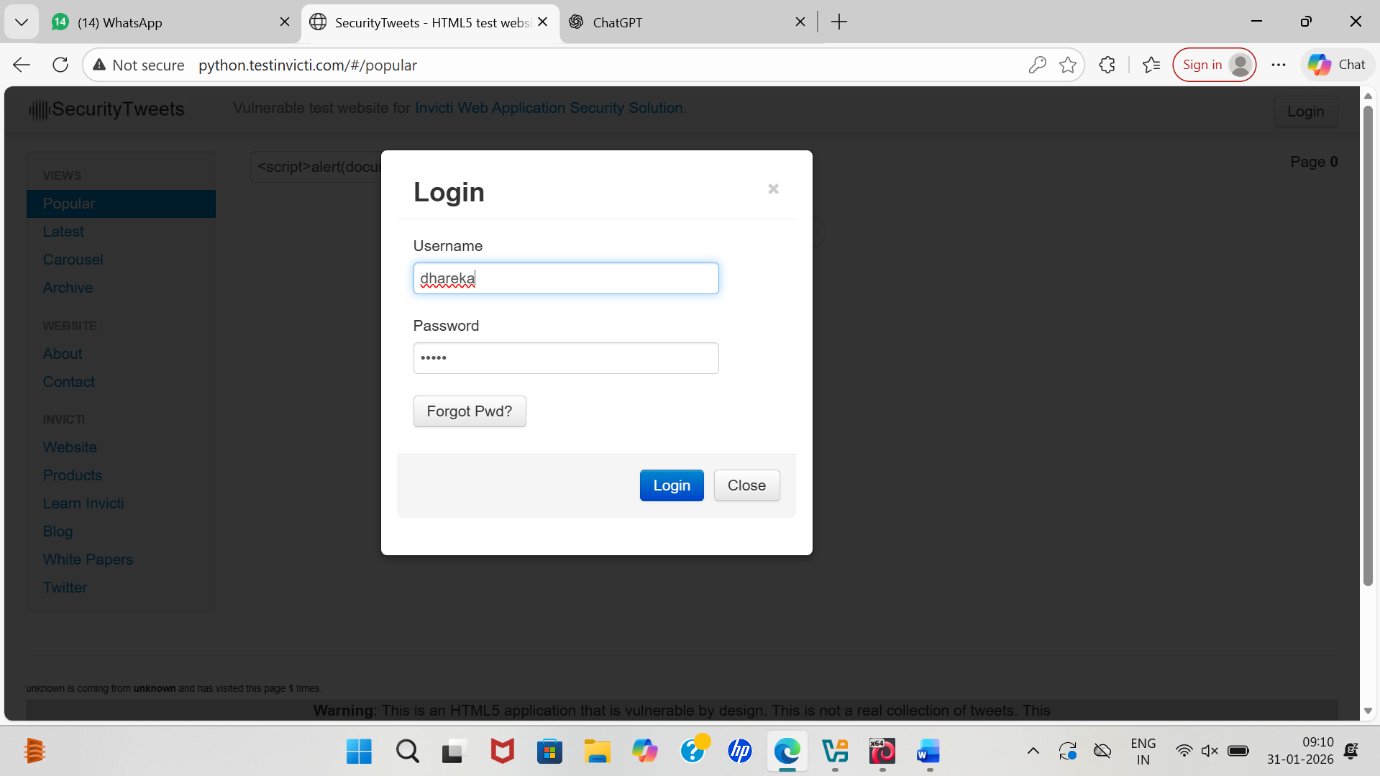
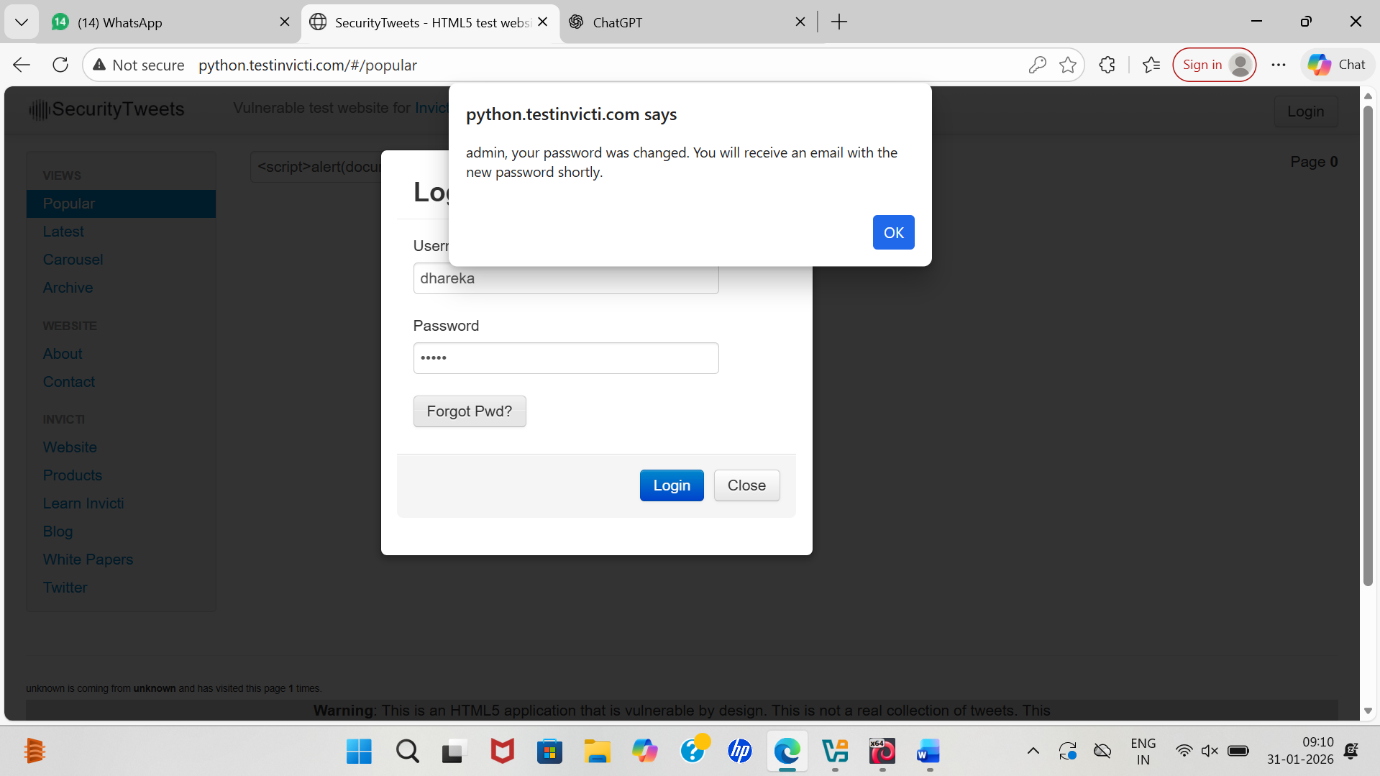
**1.Checking all sites with parameters**

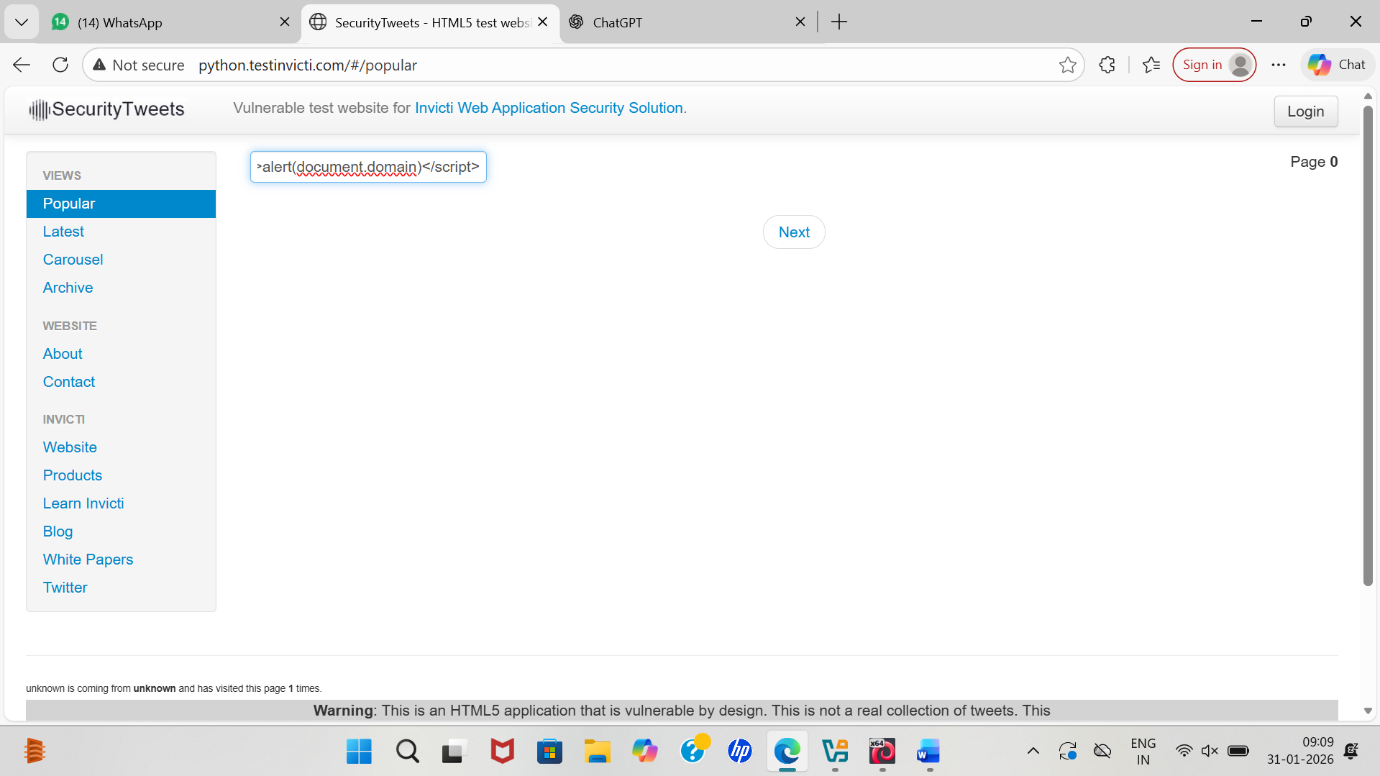
****

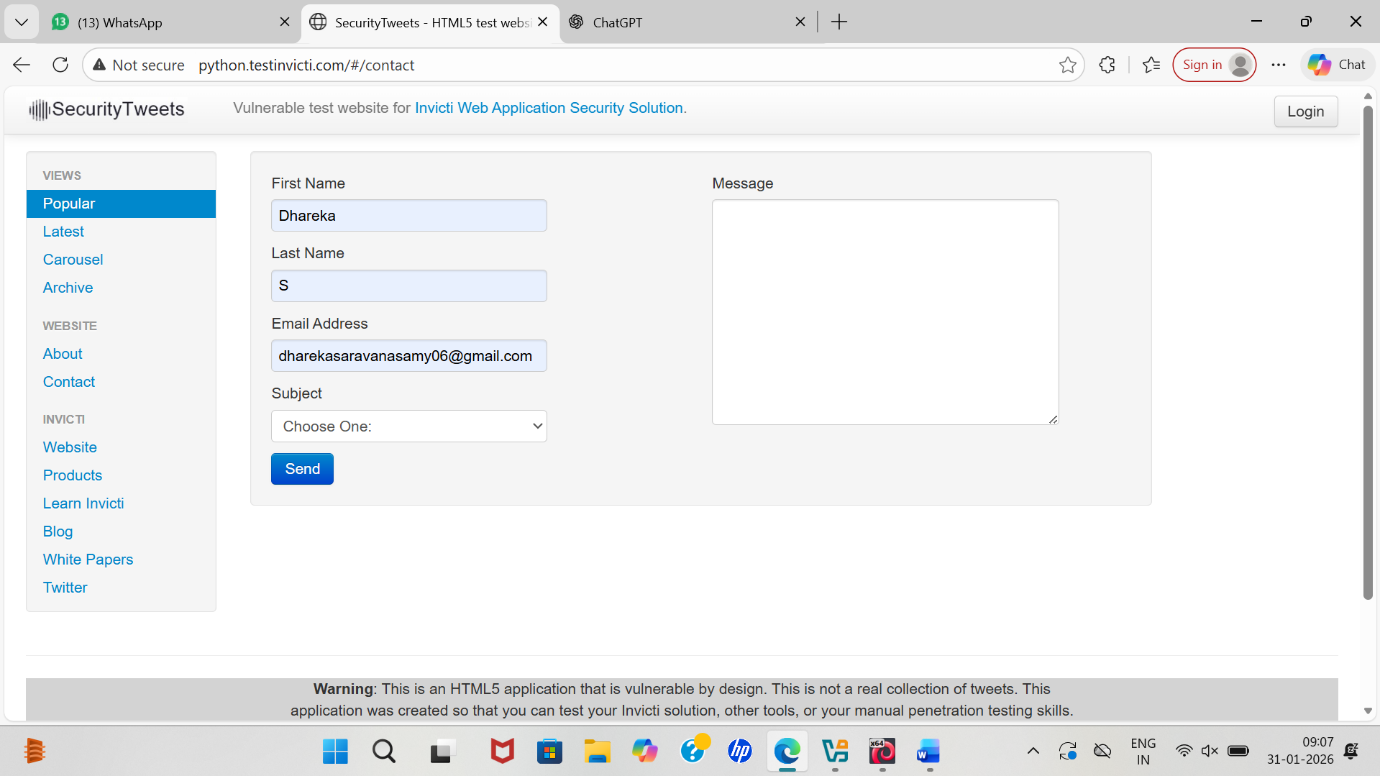
**2.XSS scripts are working in username Fields:**

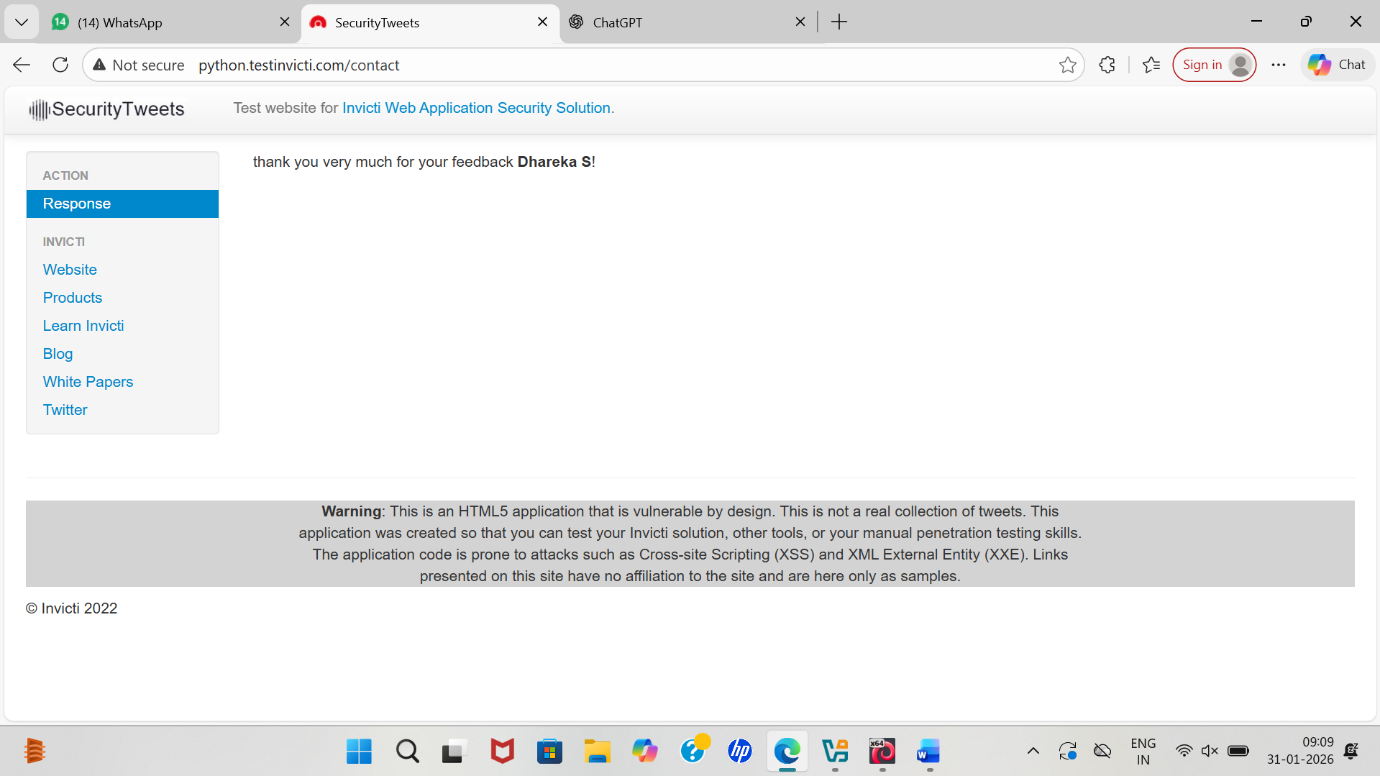
**<script>alert(document.domain)</script>**

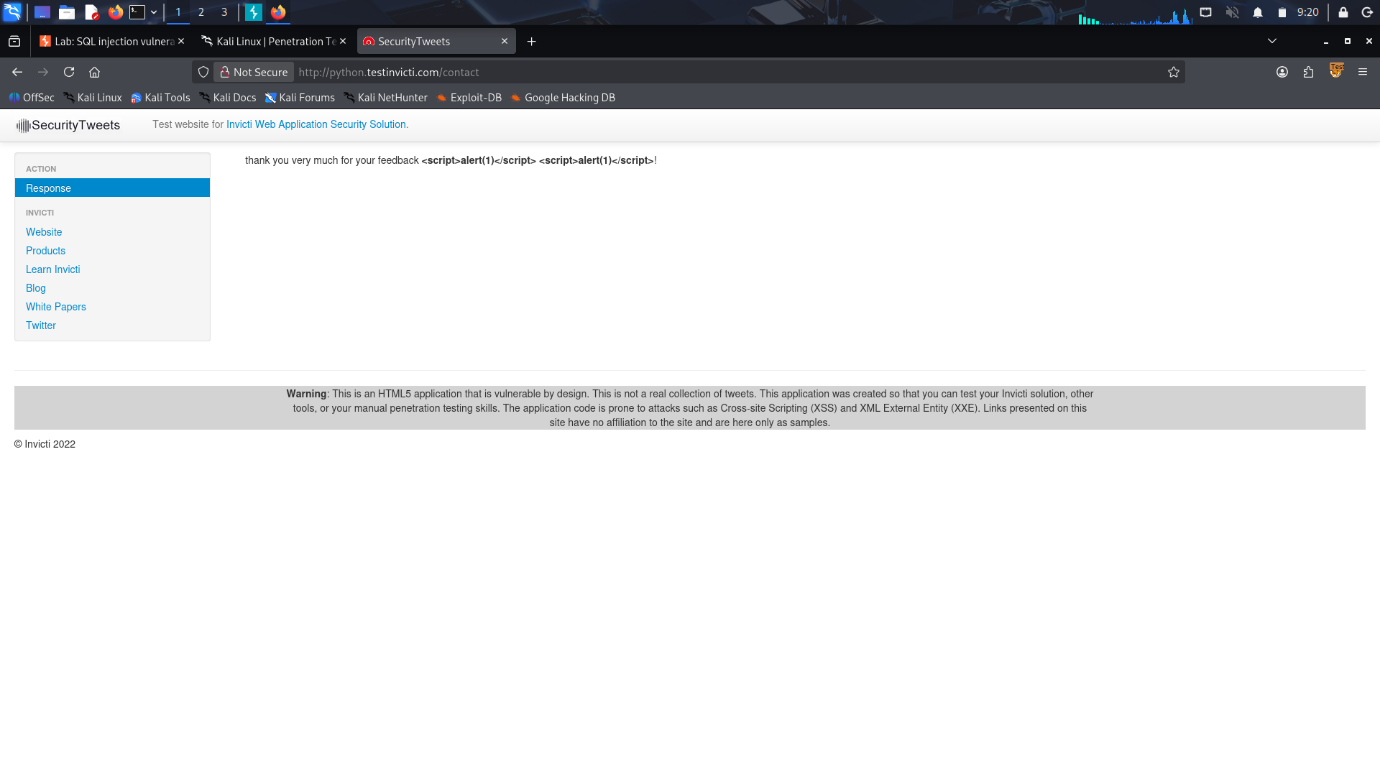
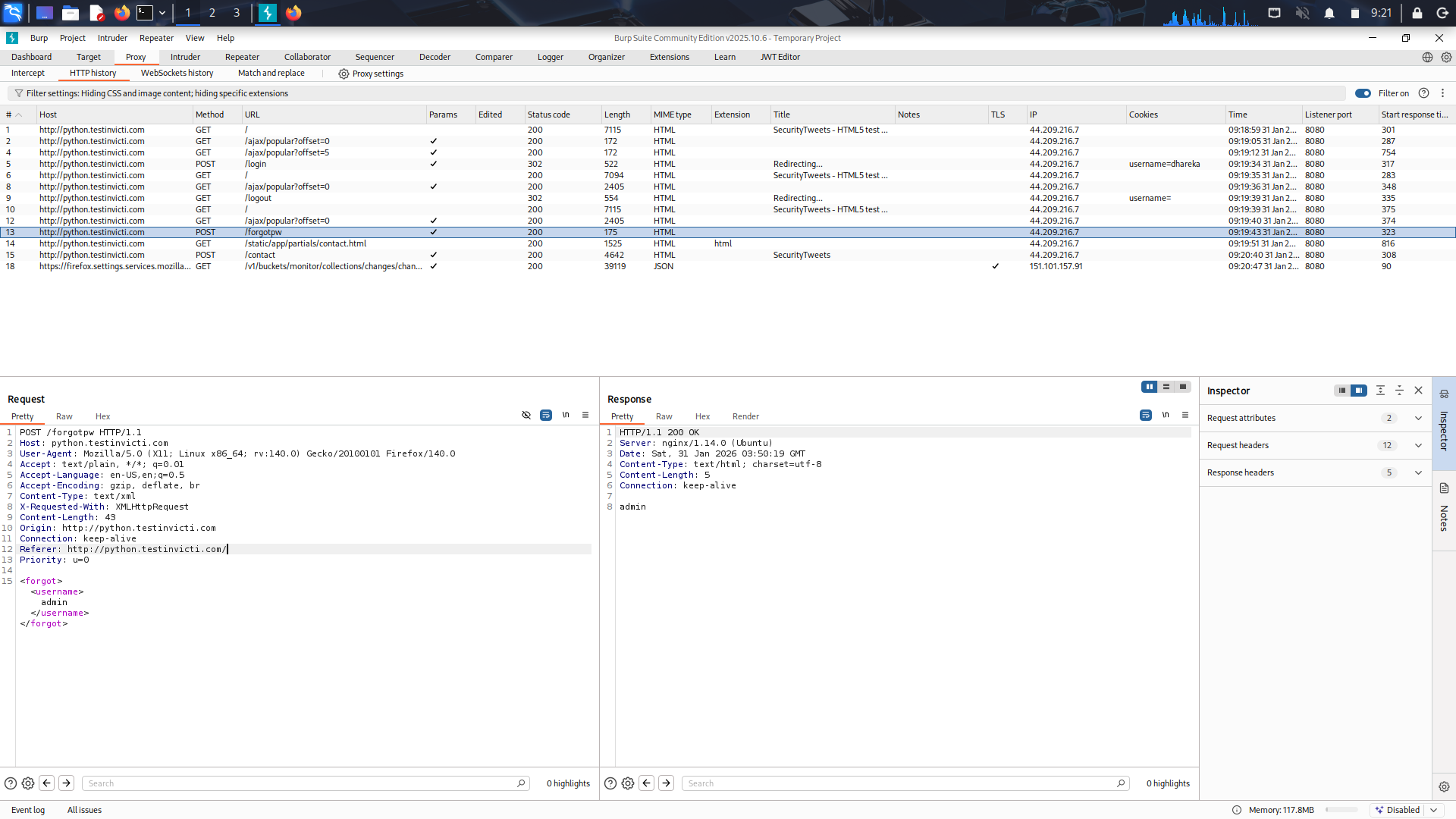
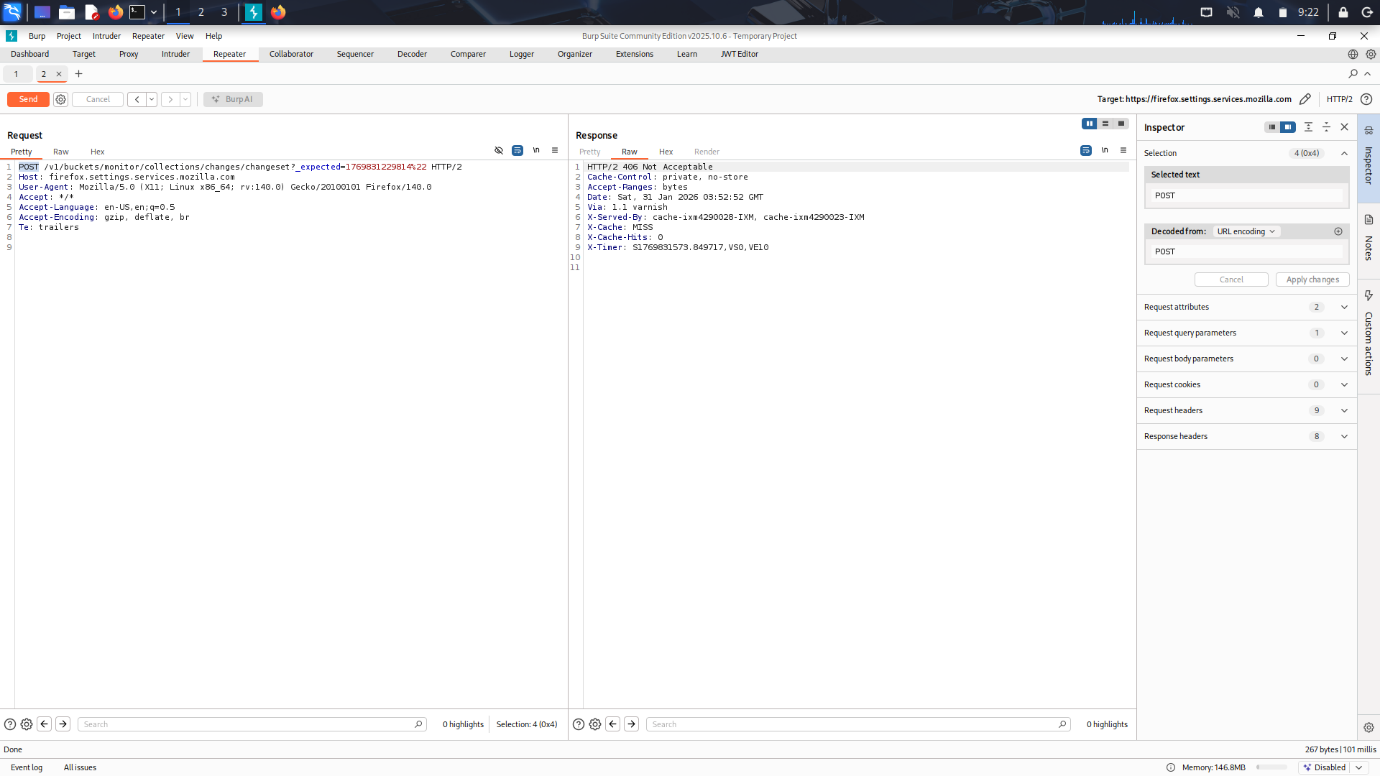
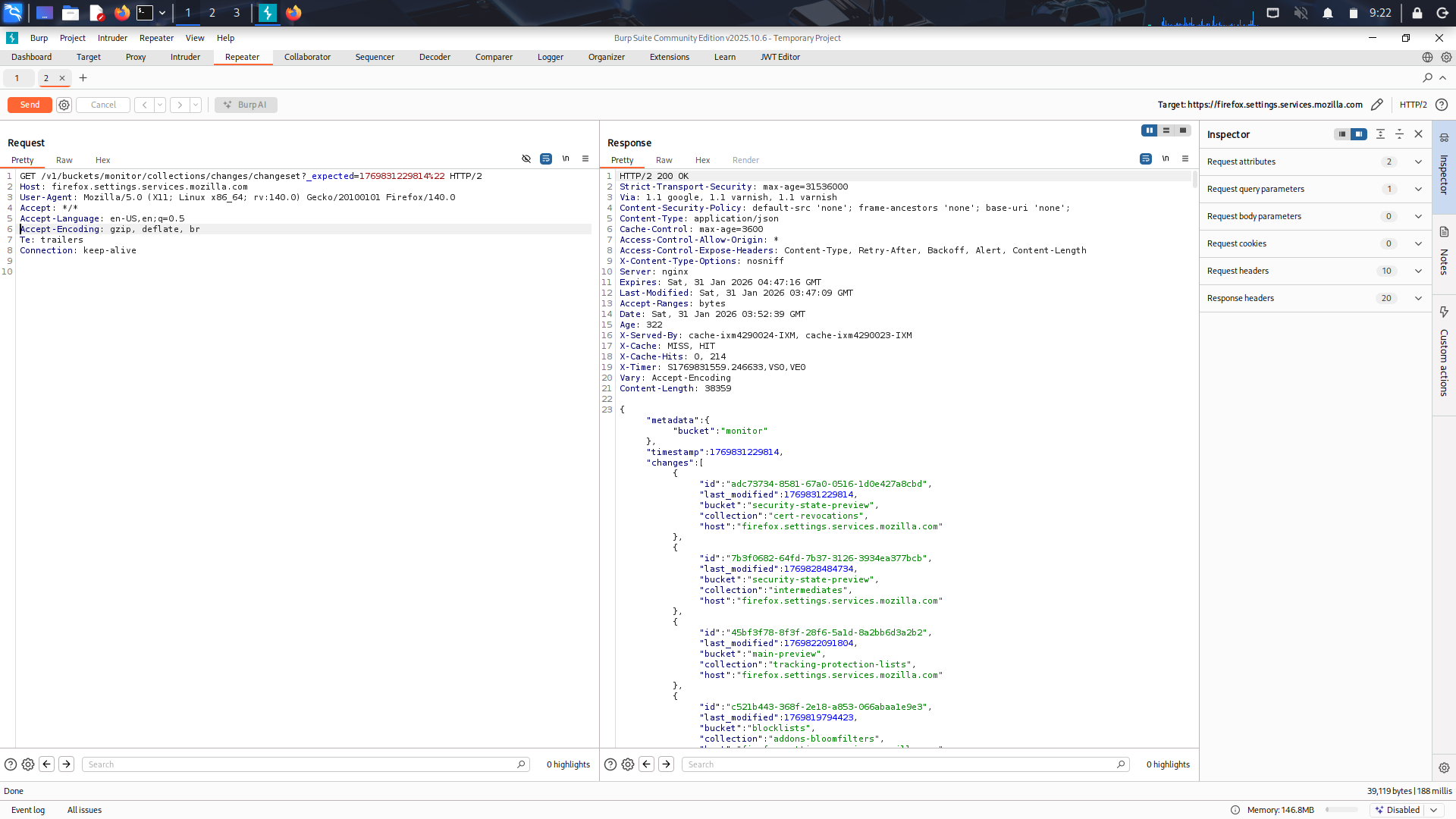
****

****

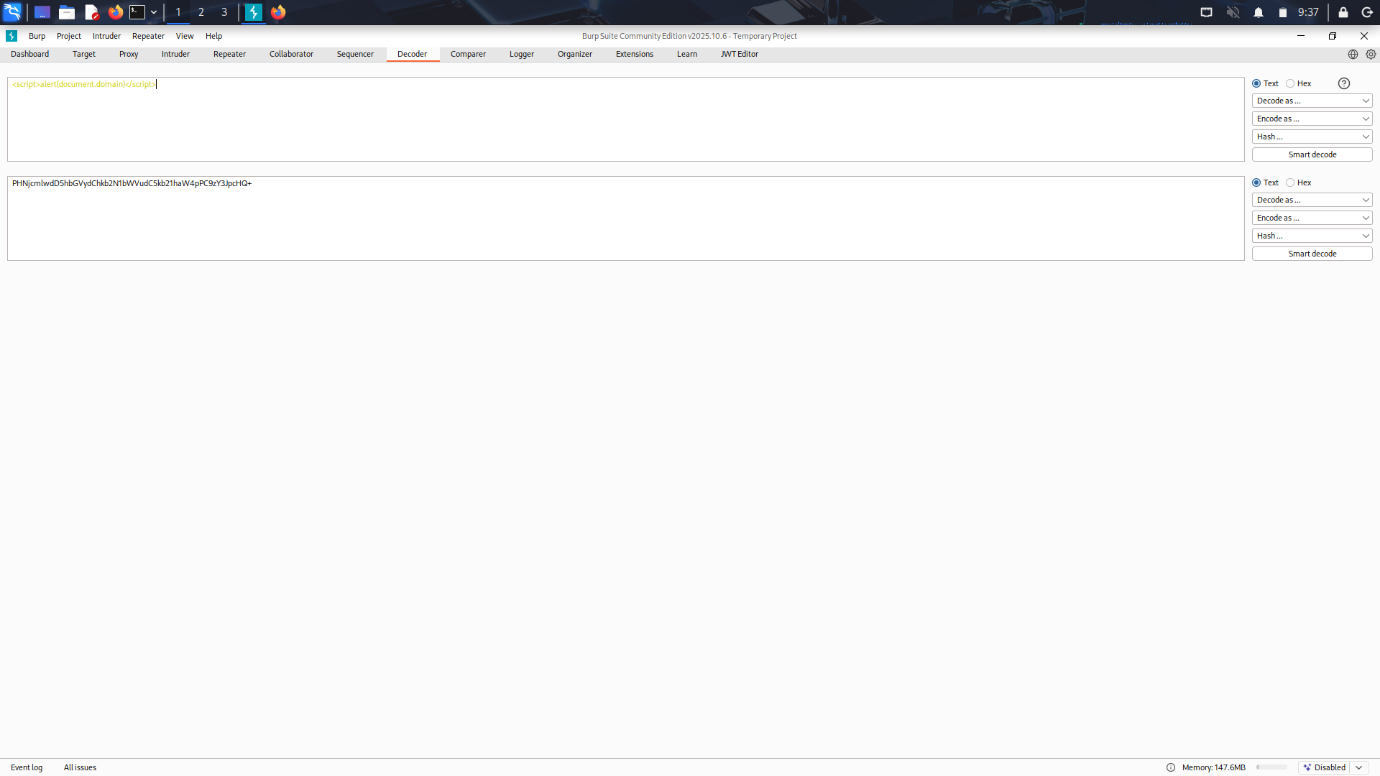
**3.Checking all the parameters with XSS Scripts:**

****

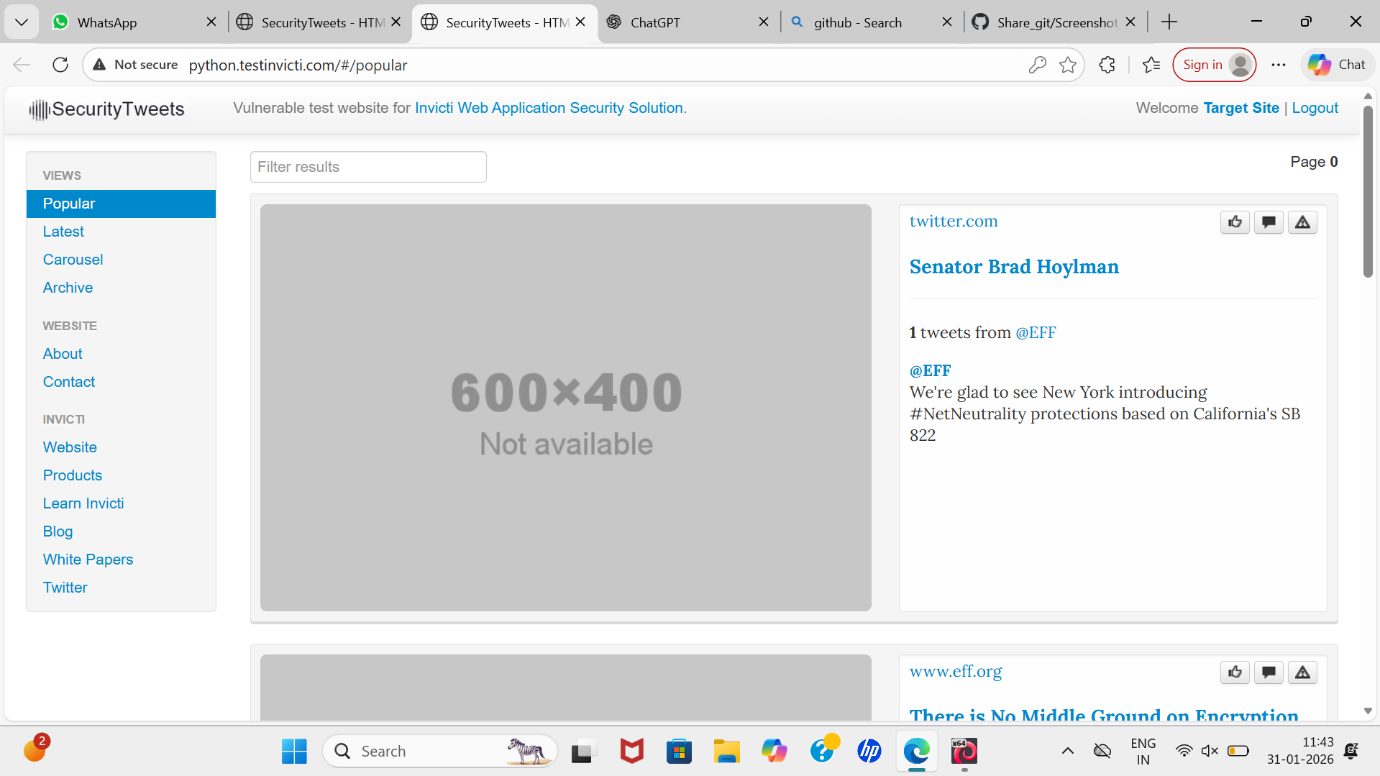
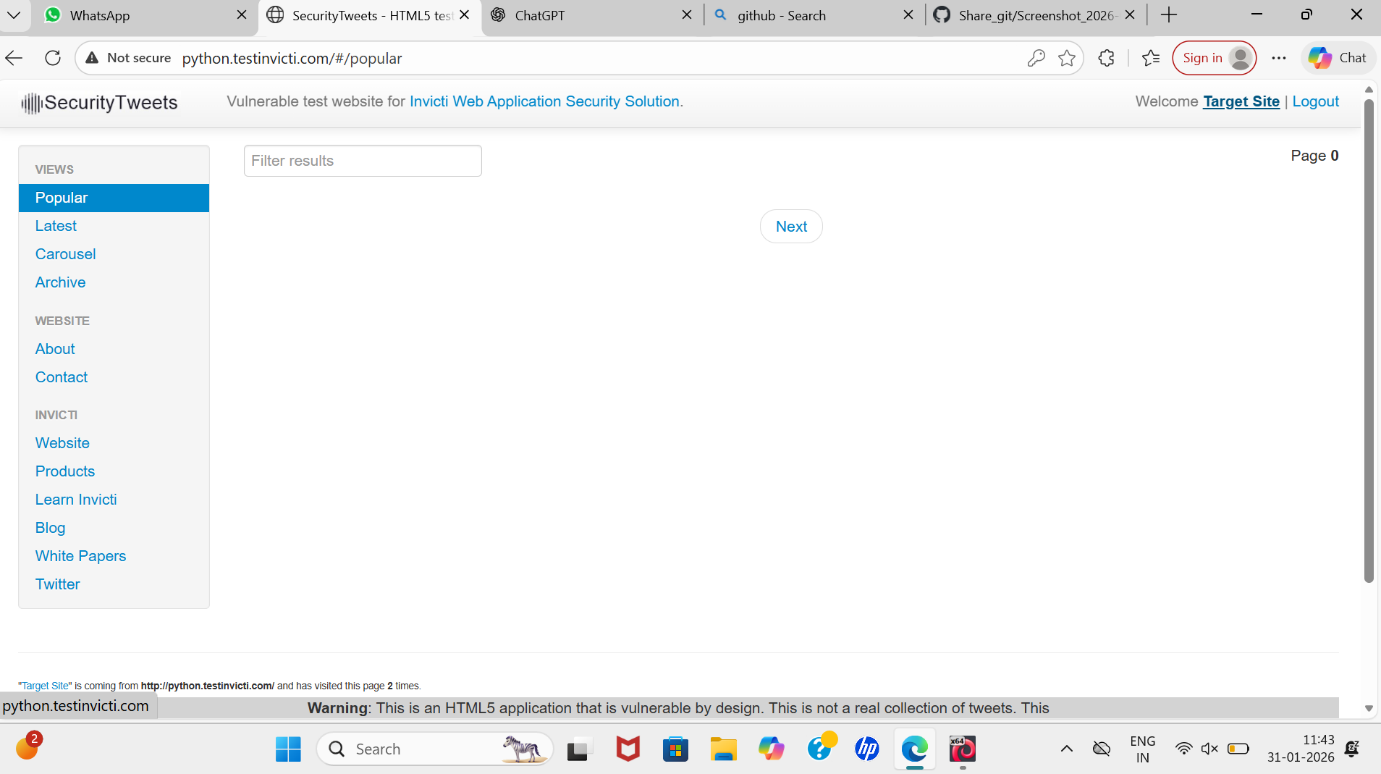
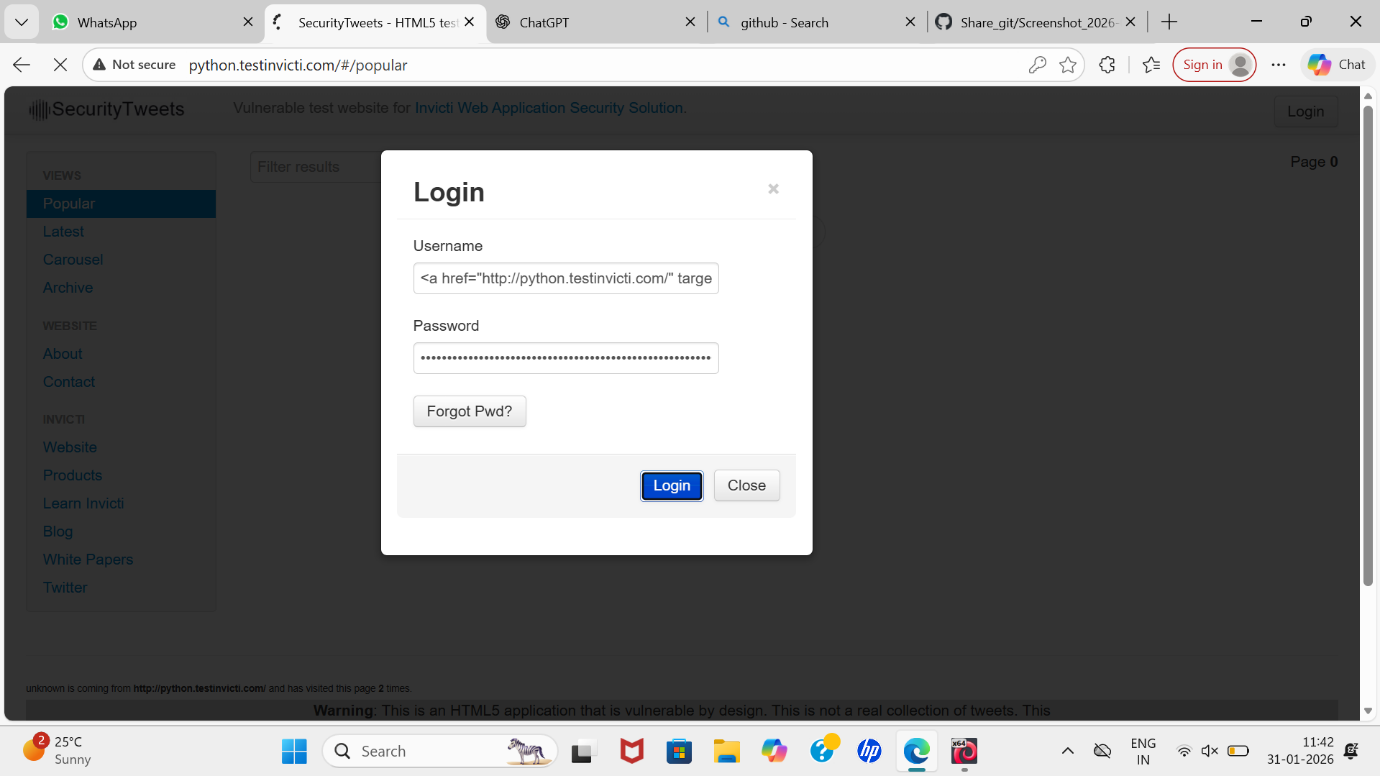
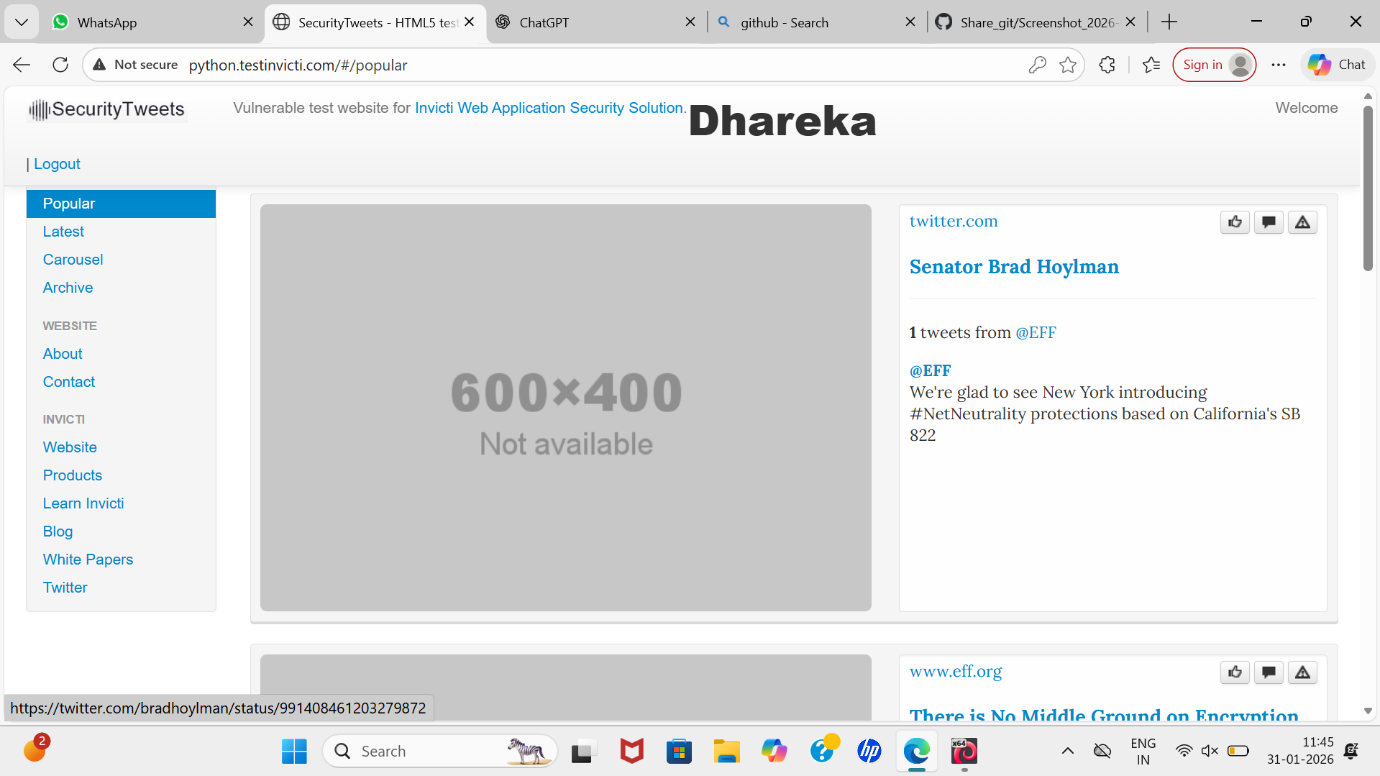
****

**4.Changing Get method To Post Method:**

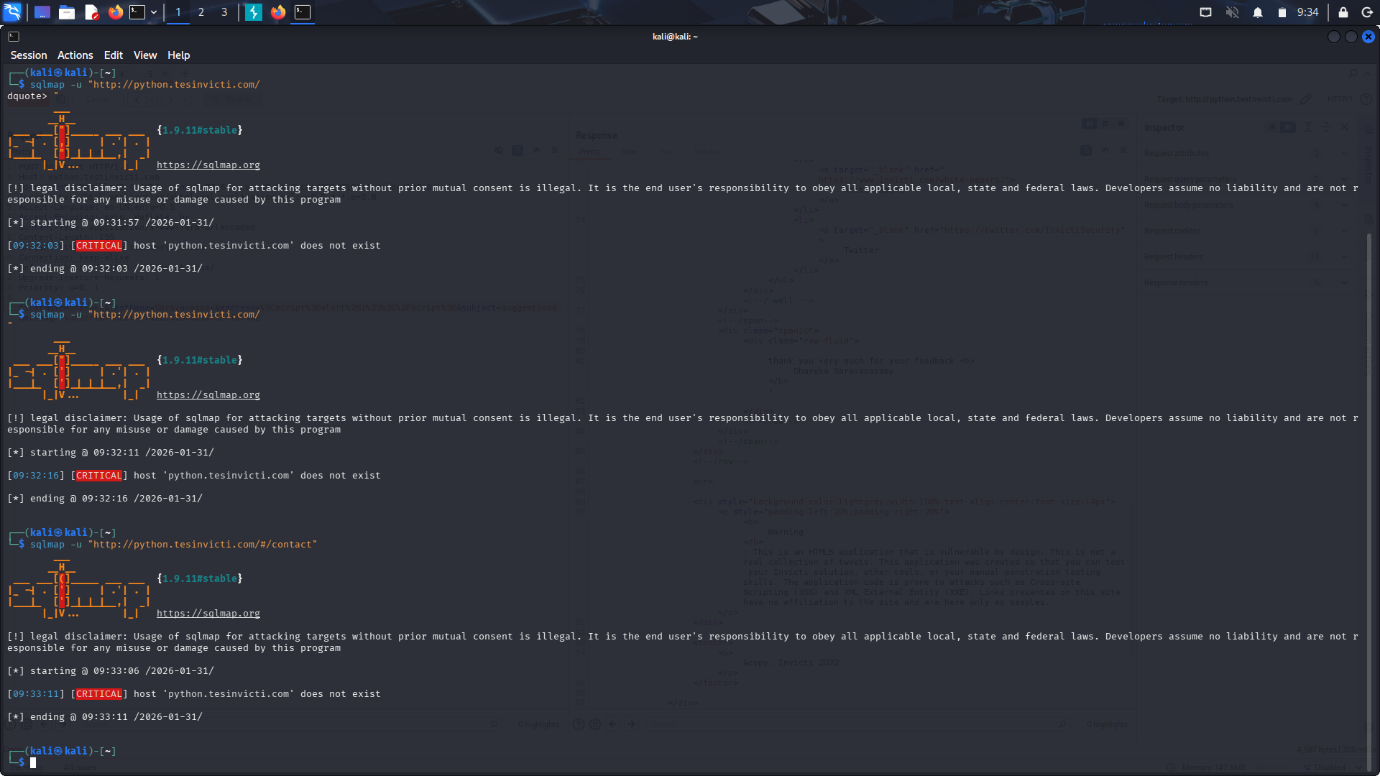
**5,URL encoding with XSS Scripts:**

****

**6.Hyperlink & HTML Tags in parameter: **

****

**SQLMAP is not possible in this website:**

****