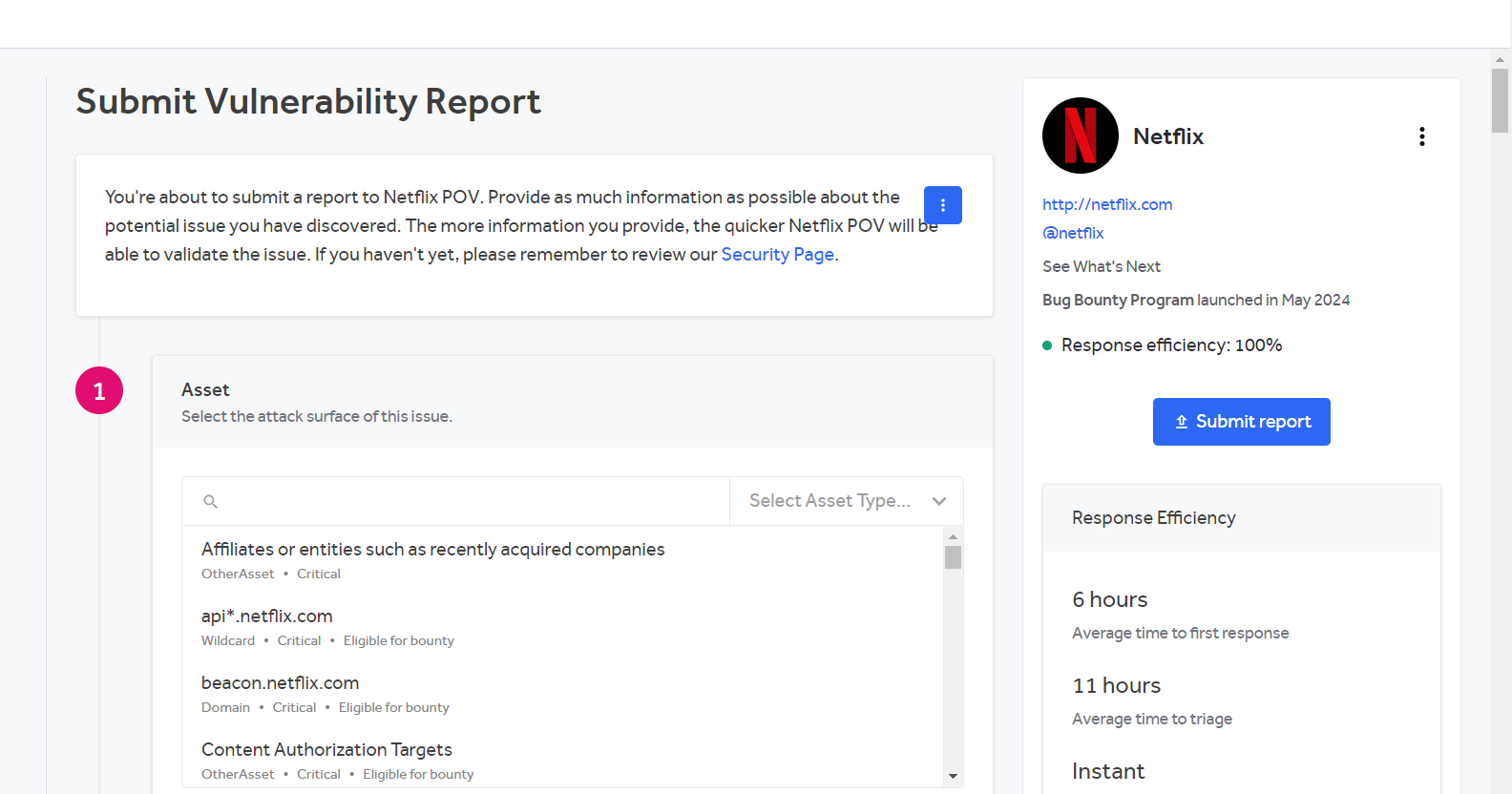
PROBLEM 01:



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

PROBLEM 02:

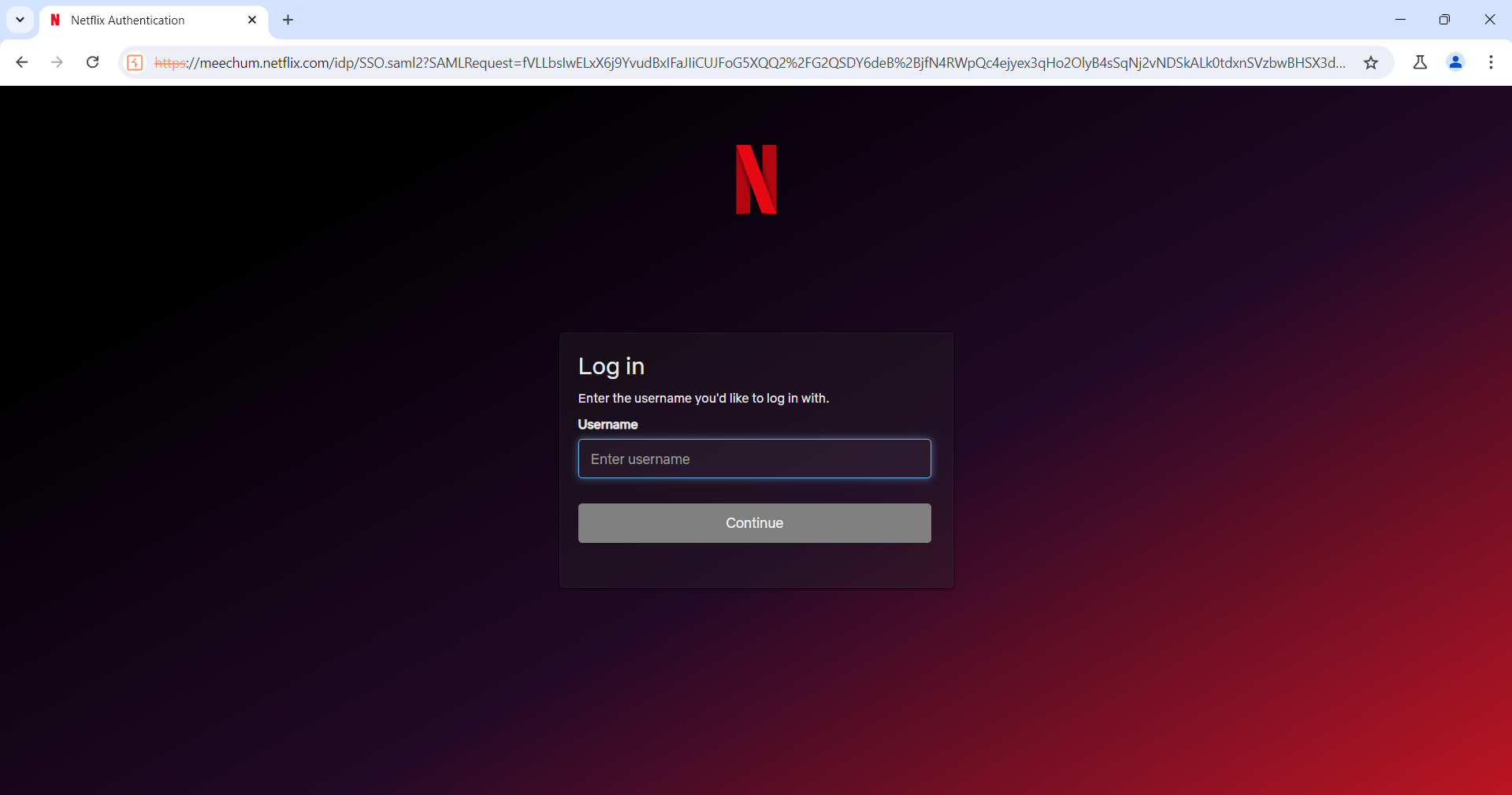
**Summary:**

The vulnerability involves exploiting identified subdomains and sites using Burp Suite. After mapping all the live subdomains of Netflix, Burp Suite was used to test for common web vulnerabilities. This allowed the attacker to manipulate requests, intercept traffic, and identify weaknesses that could lead to unauthorized access or data breaches.

**Steps To Reproduce:**

1. **Identify Target Subdomains:**
   * Use the previously gathered list of live subdomains from Subfinder, Assetfinder, and HTTPX.
   * Focus on the subdomains that returned HTTP status codes 301 and 200.
2. **Set Up Burp Suite:**
   * Open Burp Suite and configure the browser to route traffic through Burp's proxy.
   * Load the identified subdomains in the browser, allowing Burp Suite to intercept the traffic.
3. **Analyze and Manipulate Requests:**
   * Use Burp Suite's features like "Repeater" and "Intruder" to manipulate and send crafted requests to the target sites.
   * Test for common vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and other potential weaknesses.
4. **Identify Vulnerabilities:**
   * Review the responses in Burp Suite to identify any signs of vulnerability, such as unsanitized input fields, improper redirects, or error messages revealing sensitive information.

**Supporting Material/References:**

****

**A screenshot of a computer screen

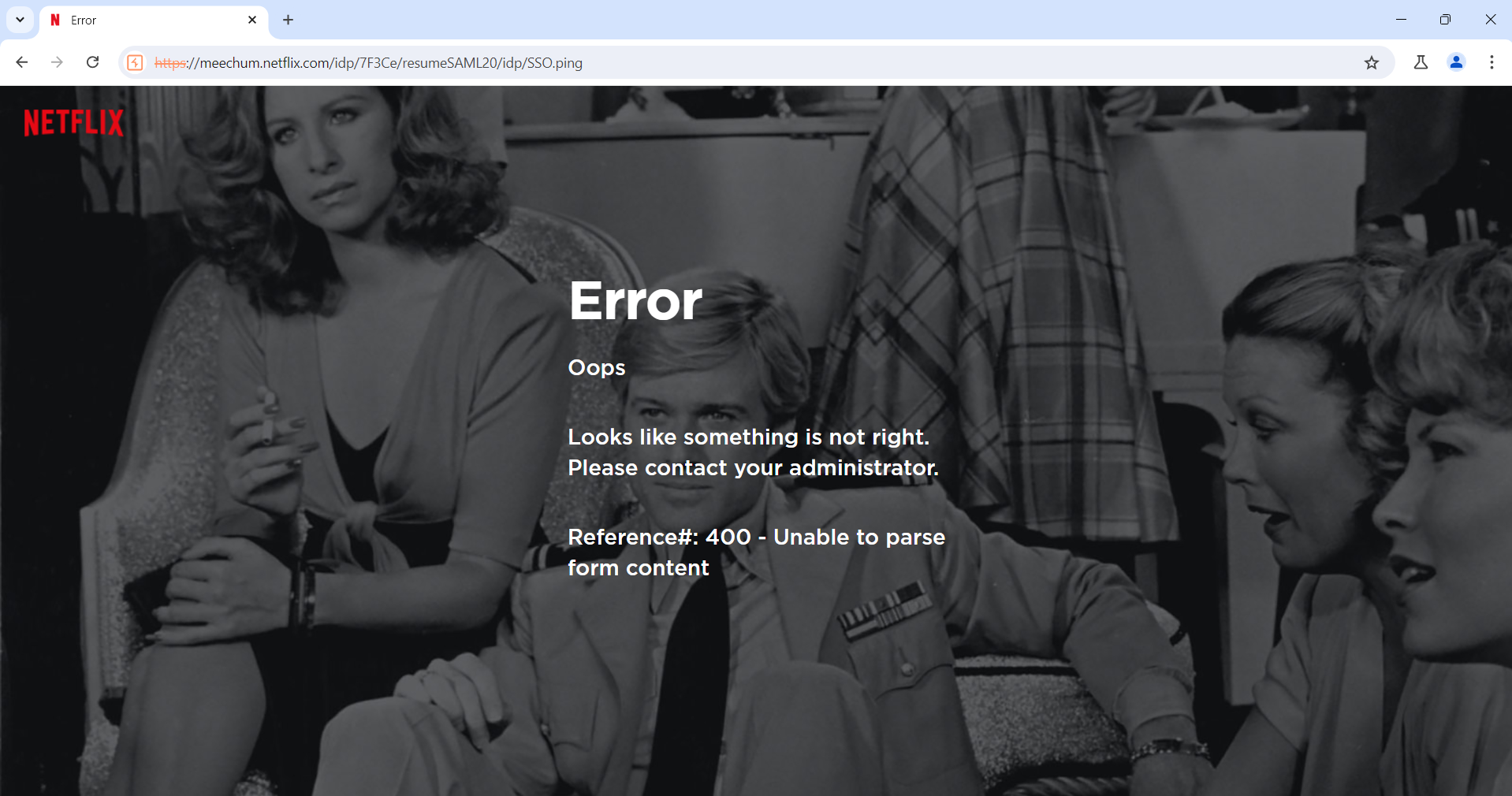
Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**A screen shot of a computer program

Description automatically generated**

****

**Impact:**

The use of Burp Suite to attack vulnerable subdomains can lead to significant security risks:

**Security Impact:**

* **Unauthorized Access:** By exploiting vulnerabilities, an attacker could gain unauthorized access to sensitive data or administrative functionalities.
* **Data Breach:** Successful attacks could result in the exposure of user data, confidential information, or intellectual property.
* **Service Disruption:** Manipulating requests could lead to denial-of-service conditions or other disruptions in service availability.
* **Escalation of Attacks:** Initial exploitation could be used as a foothold to launch more severe attacks against the broader infrastructure.