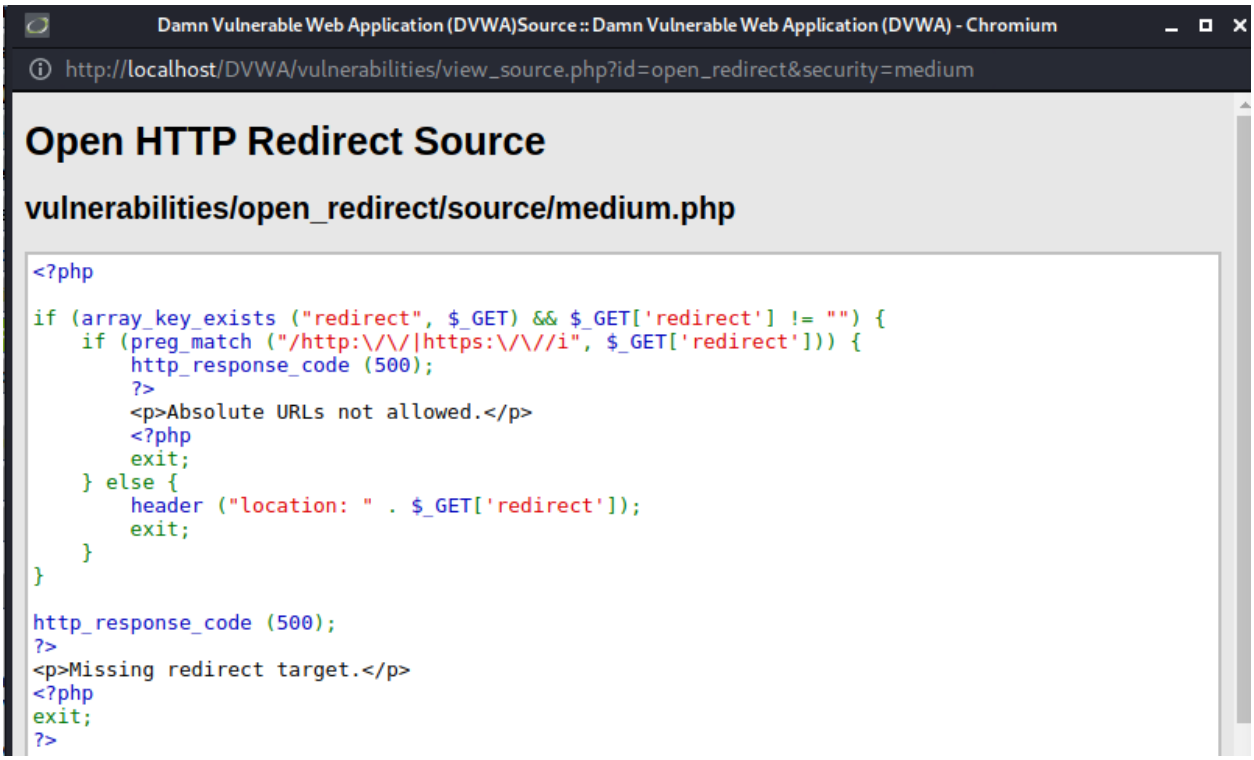
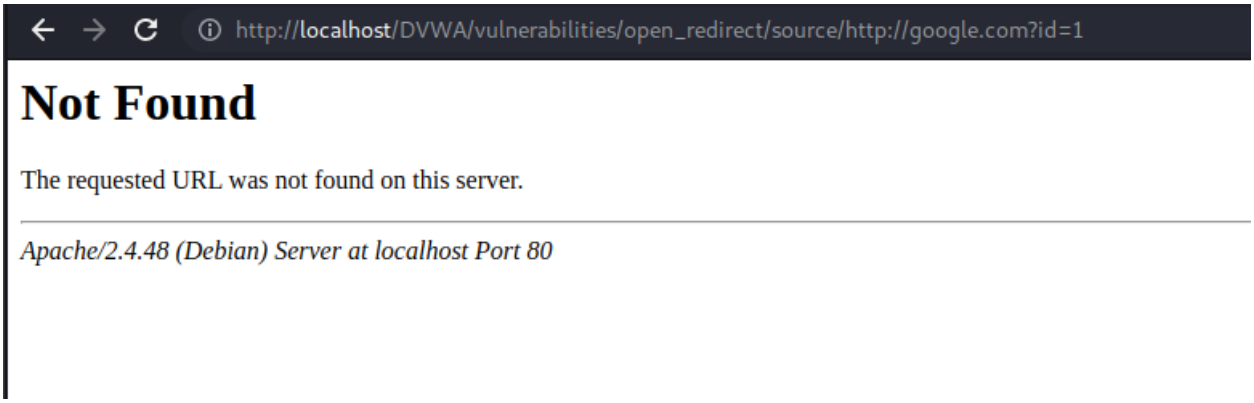
The goal is to use the address field to redirect from the website to another website. The source code blocks redirections and ‘http’, ‘https’, so without burpsuite on medium level it will not work.

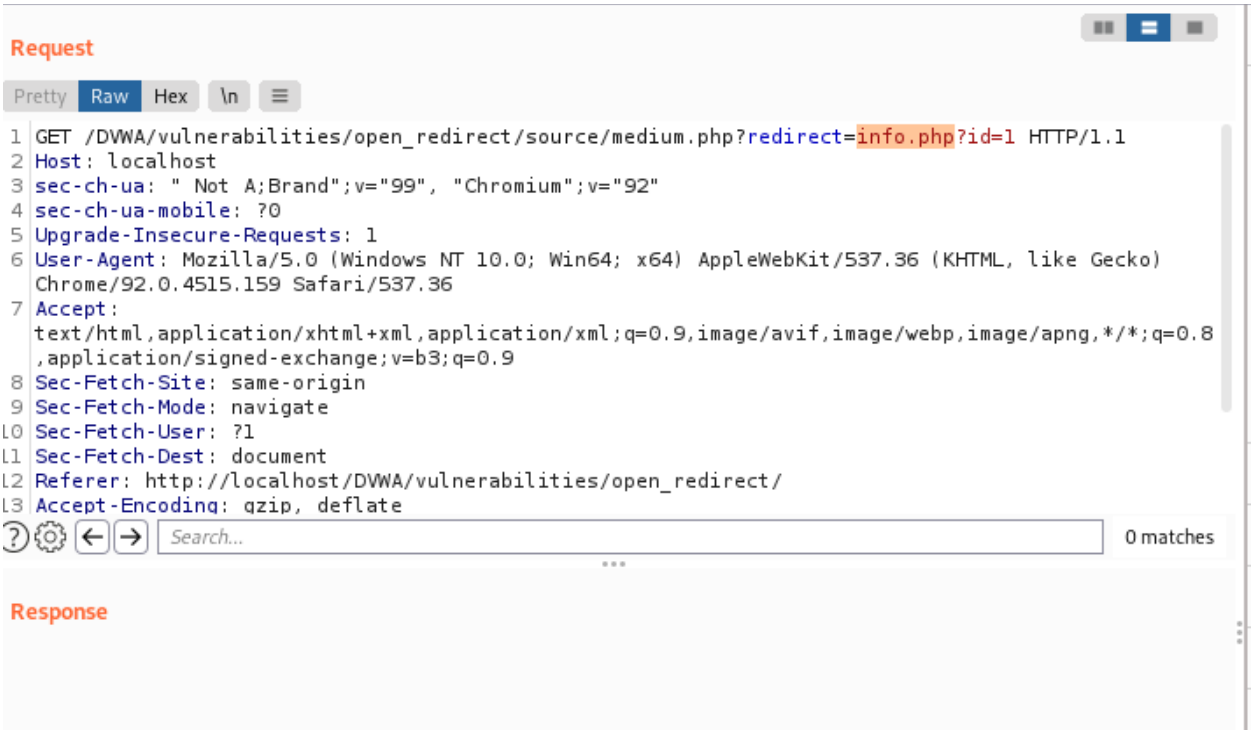




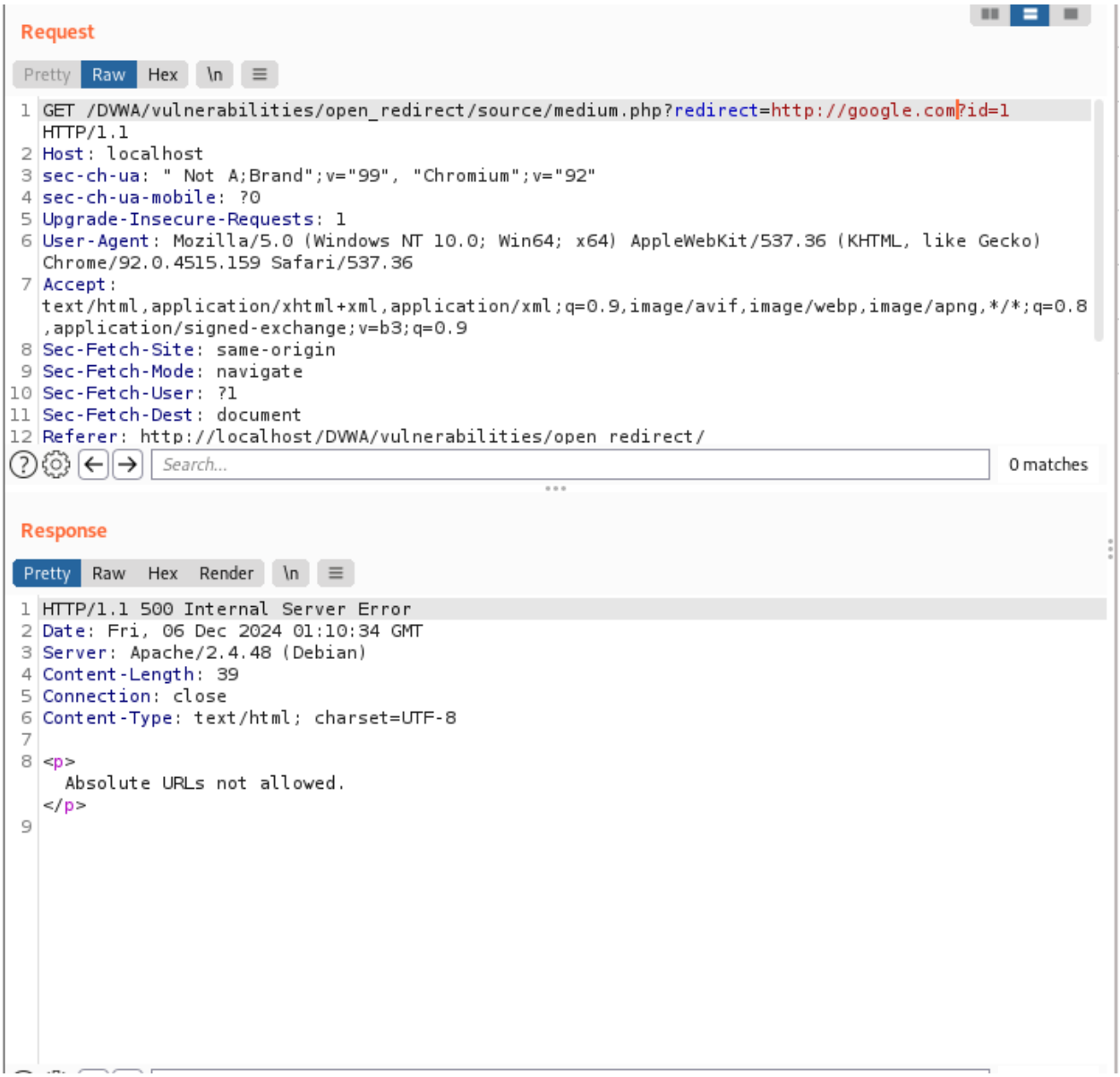
So, now i will intercept the traffic using burpsuite and change the code to redirect to the google.com website from dvwa.

```
Pretty Raw Hex \n ≡
1 GET /DVWA/vulnerabilities/open_redirect/source/medium.php?redirect=info.php?id=1 HTTP/1.1
2 Host: localhost
3 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
4 sec-ch-ua-mobile: ?0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
  3;q=0.9
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Referer: http://localhost/DVWA/vulnerabilities/open_redirect/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15 Cookie: PHPSESSID=mltqnv2jg8ri6a0b0gl14s2pv9; security=medium
16 Connection: close
17
18
```

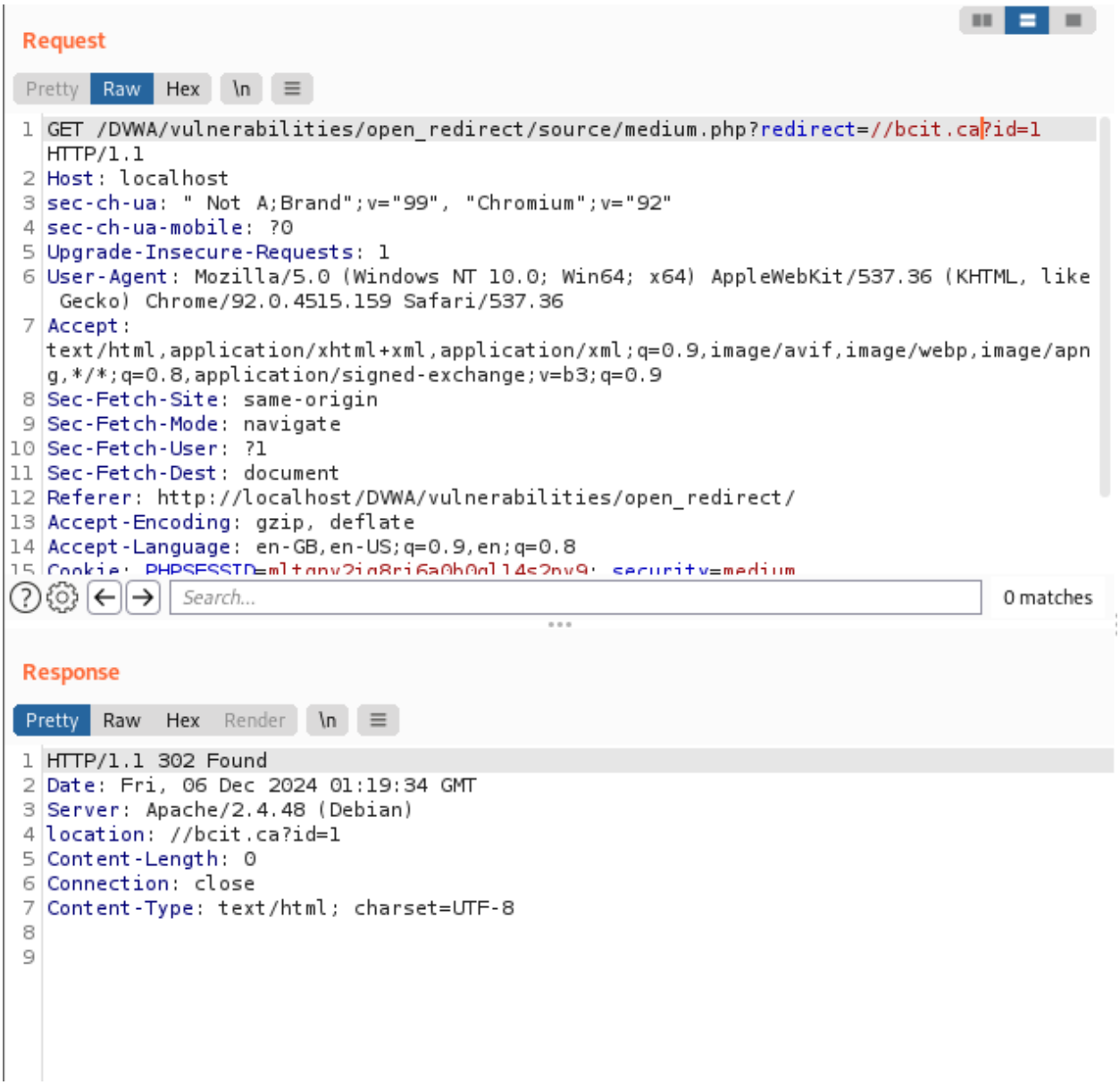
On line 1 we can see redirect field where it has info.php. Which redirect to the Quote 1 and has ID 1. we will change info.php to another URL. Firstly i have used http://google.com. It will fail becase of the security level that blocks the redirection of http and https.



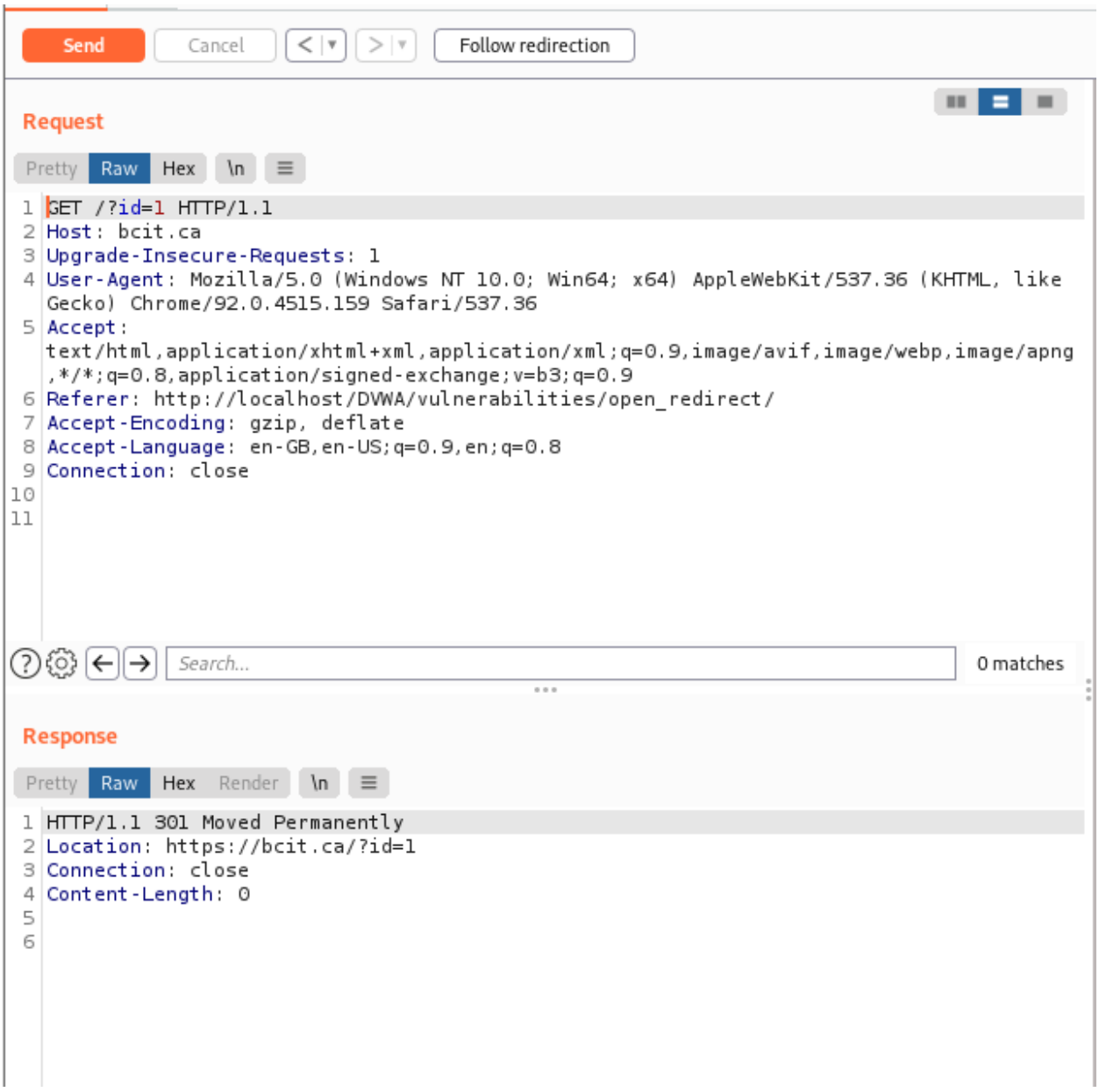
Below you can see that it didnt work and we got 500 error and message ‘Absolute URLs not allowed’.



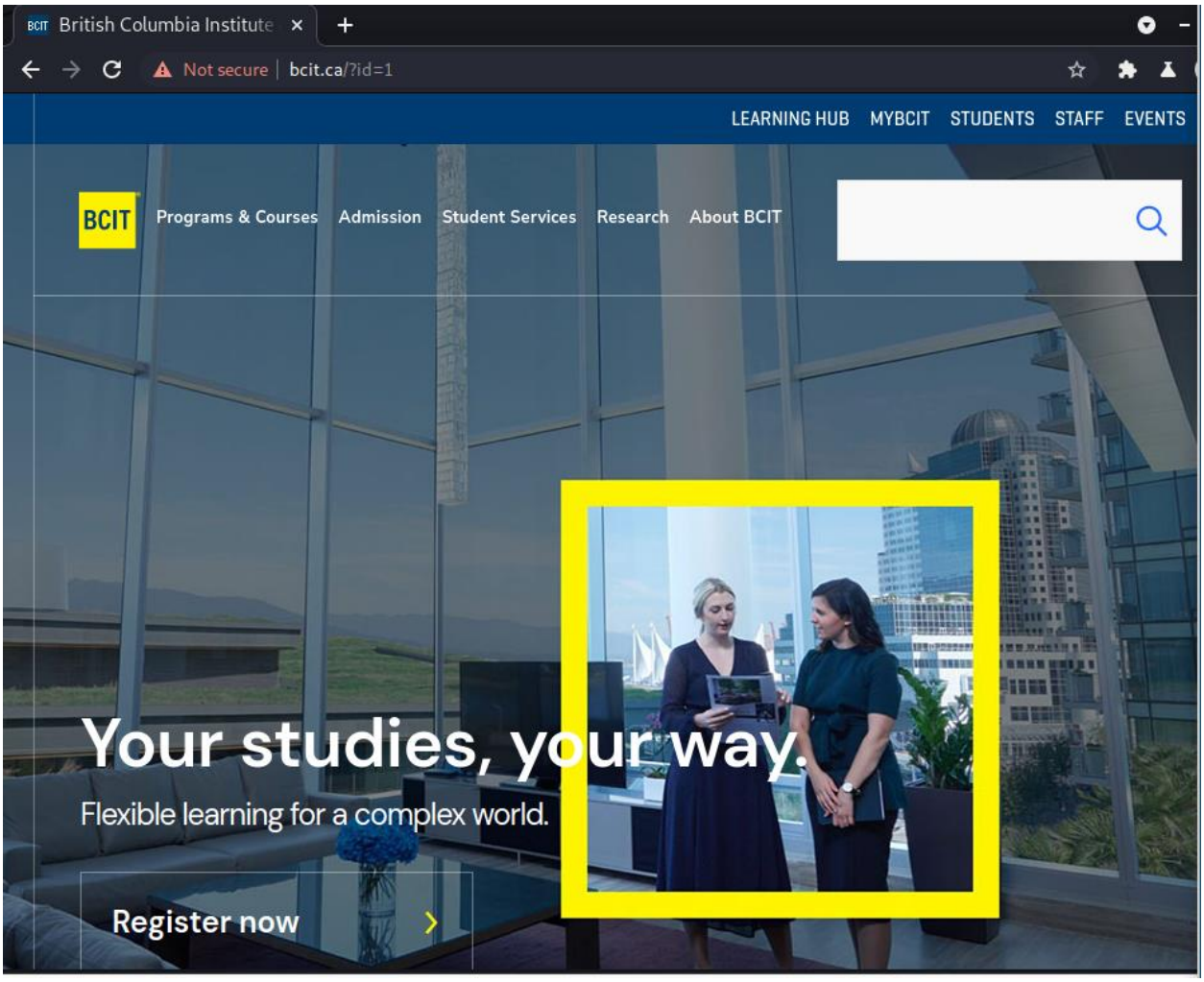
After that i have tried ‘bcit.ca’ and it worked.



Then i press follow redirection.



Proxy again and change the address there. And forward the request. And we got redirected to the bcit.ca.


British Columbia Institute
Not secure | bcit.ca/?id=1
LEARNING HUB
MYBCIT
STUDENTS
STAFF
EVENTS
BCIT
Programs & Courses
Admission
Student Services
Research
About BCIT
Your studies, your way.
Flexible learning for a complex world.
Register now