

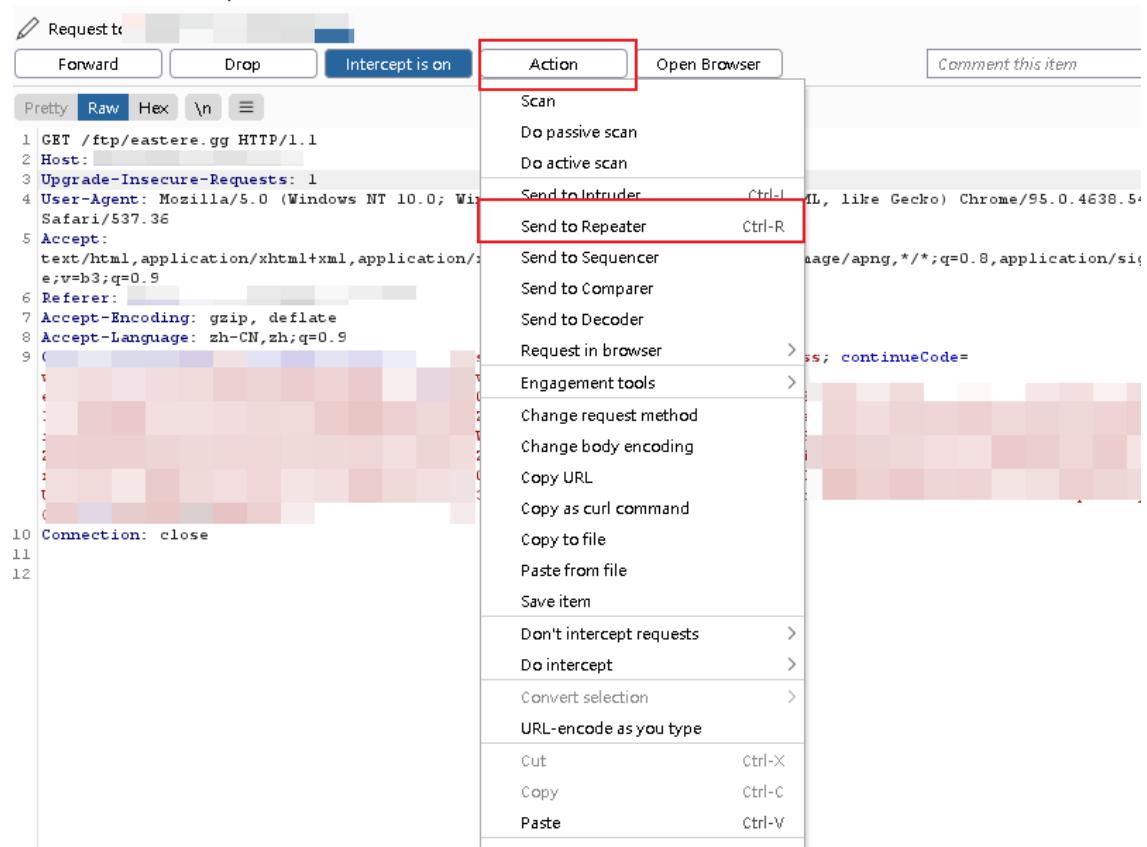
Decoder功能实战

1. 访问ip:3000/ftp, 利用Burp的Proxy抓取eastere.gg文件的数据包

The screenshot shows the Burp Suite web proxy interface. The address bar displays `ip:3000/ftp`. The file list under `~/ftp` includes `eastere.gg`, which is highlighted with a red box. Below the file list, the 'Request to' tab is active, showing the raw HTTP request. The request is a GET request to `/ftp/eastere.gg` with various headers including `Host`, `Upgrade-Insecure-Requests`, `User-Agent`, `Accept`, `Referer`, `Accept-Encoding`, and `Accept-Language`. The request body is redacted with a large red box.

```
1 GET /ftp/eastere.gg HTTP/1.1
2 Host:
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Referer:
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9
0 Connection: close
1
2
```

2. 将数据包发送到Repeater



3. 利用数据截断访问eastere.gg文件



4. 发送数据包, 查看响应

The screenshot shows the 'Response' tab in a web browser's developer tools. The response is an HTTP 200 OK with the following headers:

- Access-Control-Allow-Origin: *
- X-Content-Type-Options: nosniff
- X-Frame-Options: SAMEORIGIN
- Feature-Policy: payment 'self'
- Accept-Ranges: bytes
- Cache-Control: public, max-age=0
- Last-Modified: Tue, 08 Feb 2022 22:37:56 GMT
- ETag: W/"144-17edb7c7da0"
- Content-Type: application/octet-stream
- Content-Length: 324
- Date: Fri, 18 Mar 2022 09:54:25 GMT
- Connection: close

The body of the response contains the following text:

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 Accept-Ranges: bytes
7 Cache-Control: public, max-age=0
8 Last-Modified: Tue, 08 Feb 2022 22:37:56 GMT
9 ETag: W/"144-17edb7c7da0"
10 Content-Type: application/octet-stream
11 Content-Length: 324
12 Date: Fri, 18 Mar 2022 09:54:25 GMT
13 Connection: close
14
15 "Congratulations, you found the easter egg!"
16 - The incredibly funny developers
17
18 ...
19 ...
20 ...
21 ...
22 ...
23
24 Oh' wait, this isn't an easter egg at all! It's just a
25 boring text file! The real easter egg can be found here:
26 L2dlci9xcmlmL25lci9mYi9zaGFhYmZ3JlL3J0dA==
27
28 Good luck, egg hunter!
```

5. 复制加密语句到Decoder, 以Base64方式解密

The screenshot shows a Base64 decoder tool. The input field contains the Base64 string:

```
L2dlci9xcmlmL25lci9mYi9zaGFhYmZ3JlL3J0dA==
```

The 'Decode as ...' dropdown menu is open, showing the following options:

- Plain
- URL
- HTML
- Base64
- ASCII hex
- Hex
- Octal
- Binary
- Gzip

The 'Base64' option is selected. The output field shows the decoded result:

```
/gur/qrif/ner/fb/shaal/gurl/uvq/na/rnfgre/rtt/jvquva/gur/rnfgre/rtt
```

6. 将解密结果用ROT13解

密, /the/devs/are/sp/funny/they/hid/an/easter/egg/within/the/easter/egg, 访问目录完成

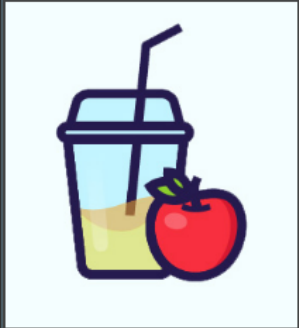
JS

OWASP Juice Shop

Account

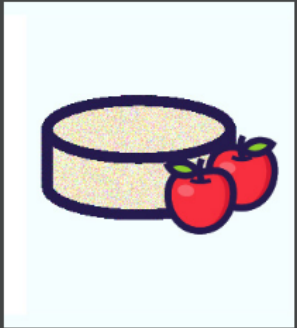
You successfully solved a challenge: Easter Egg (Find the hidden easter egg.)

All Products



Apple Juice
(1000ml)
1.99¥

Add to Basket



Apple Pom
0.89¥

Add to Basket