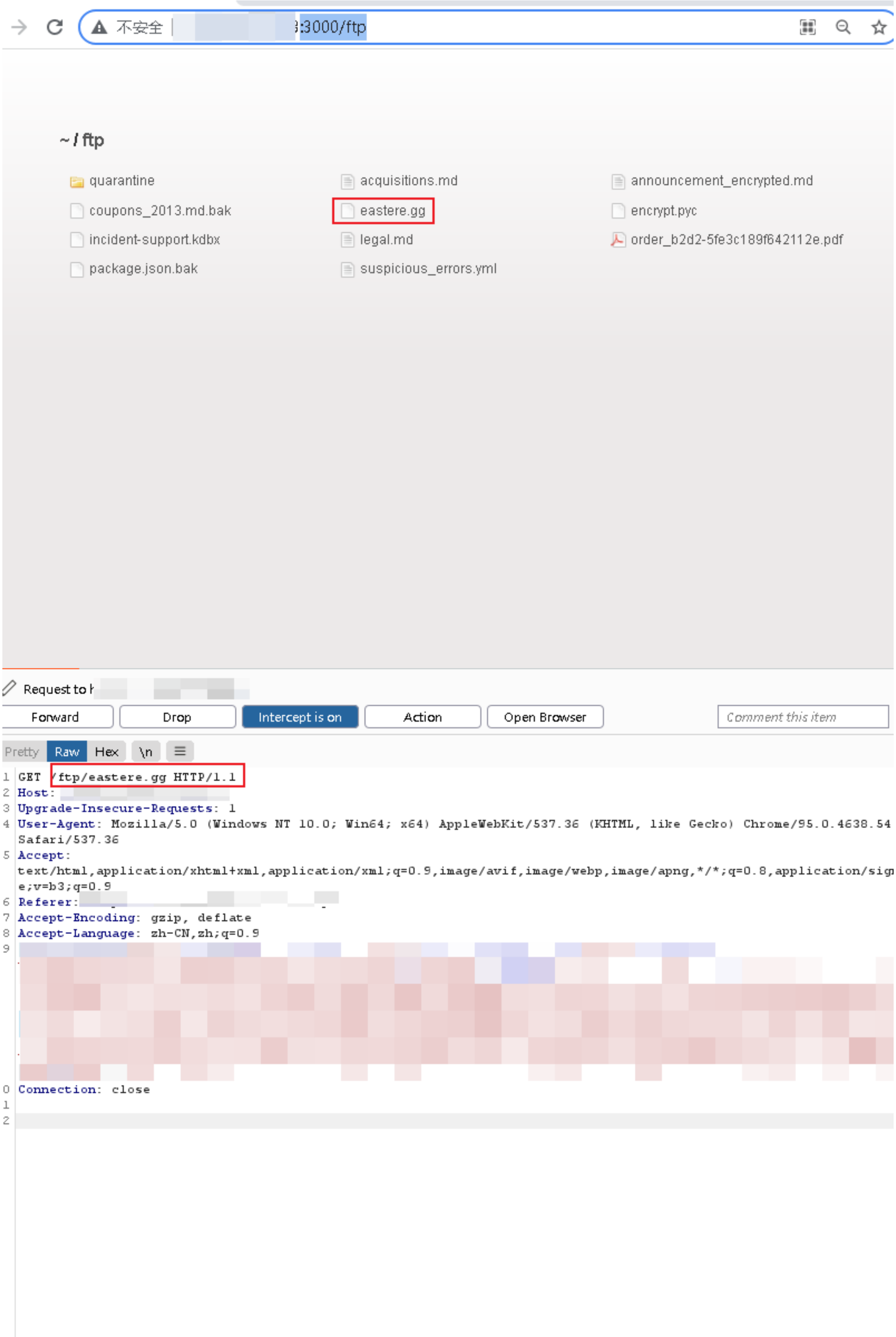
Decoder功能实战

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

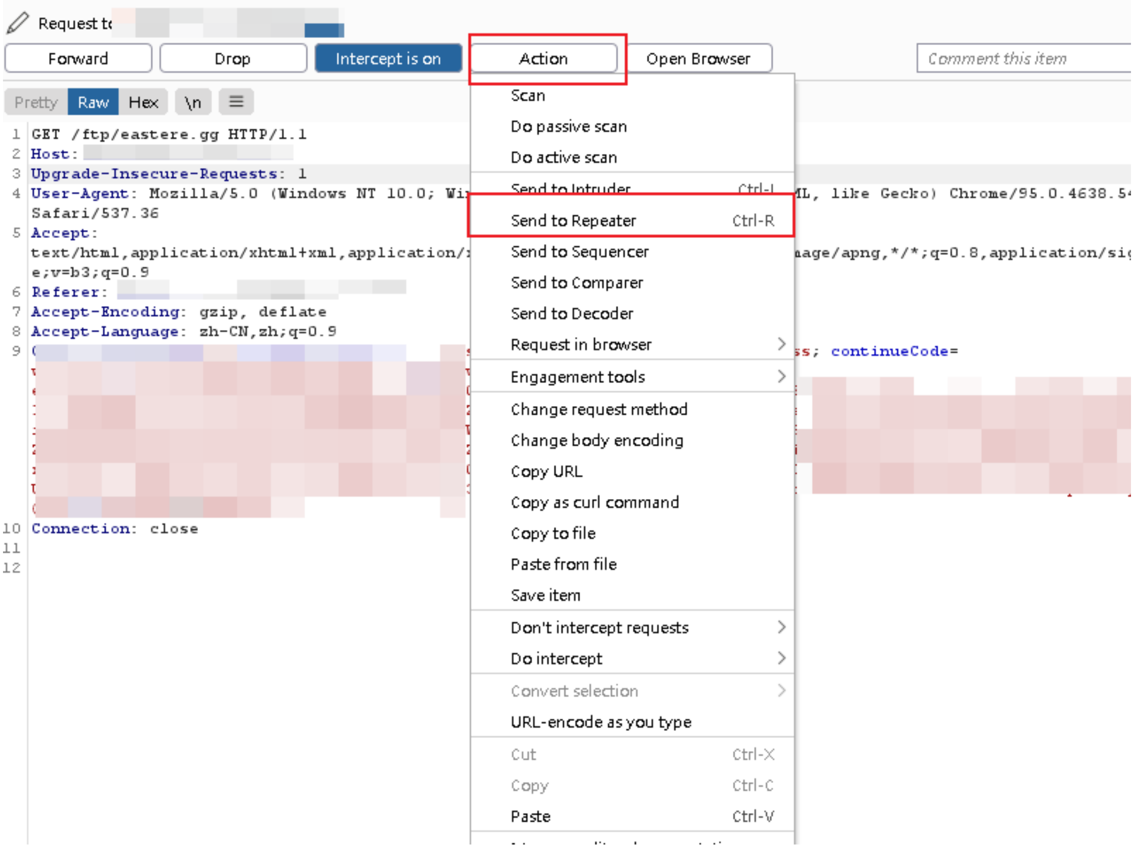


~ / ftp

quarantine
acquisitions.md
announcement_encrypted.md
coupons_2013.md.bak
eastere.gg
encrypt.pyc
incident-support.kdbx
legal.md
order_b2d2-5fe3c189f642112e.pdf
package.json.bak
suspicious_errors.yml

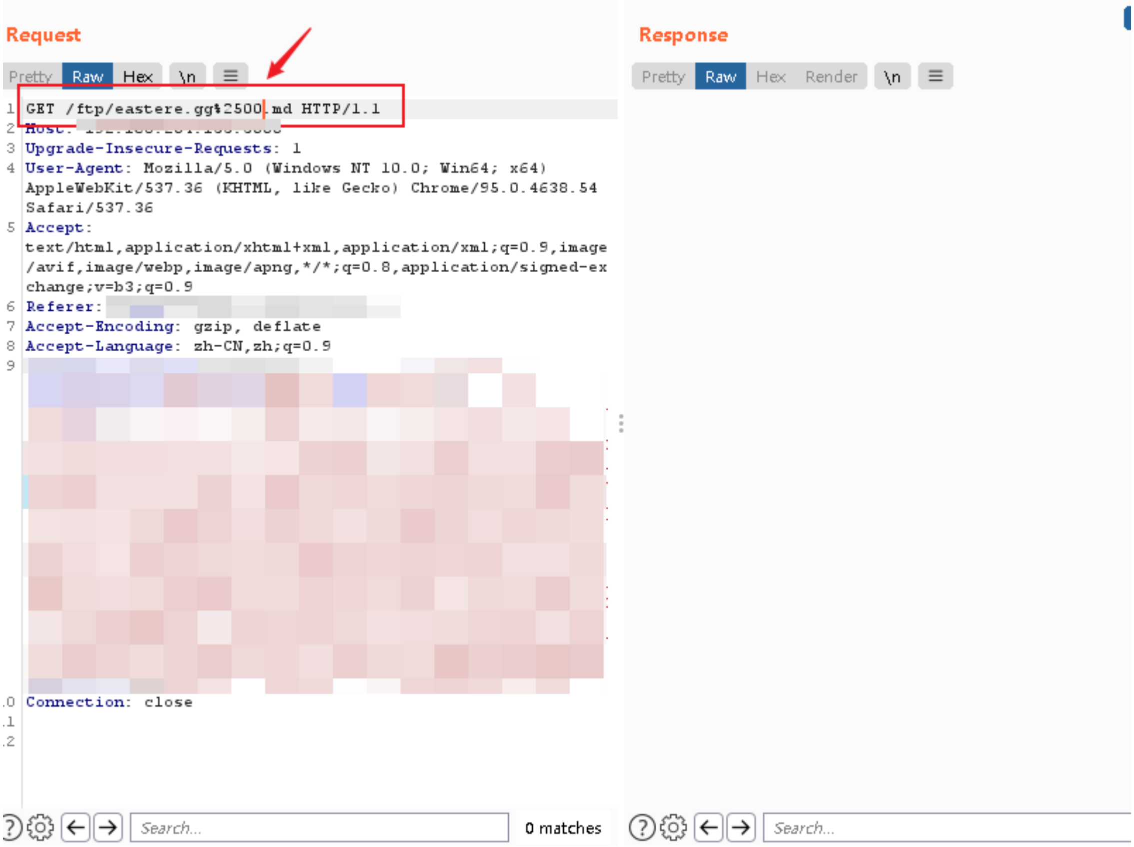
```
GET /ftp/eastere.gg HTTP/1.1
Host: [redacted]
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig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

```

2. 将数据包发送到Repeater



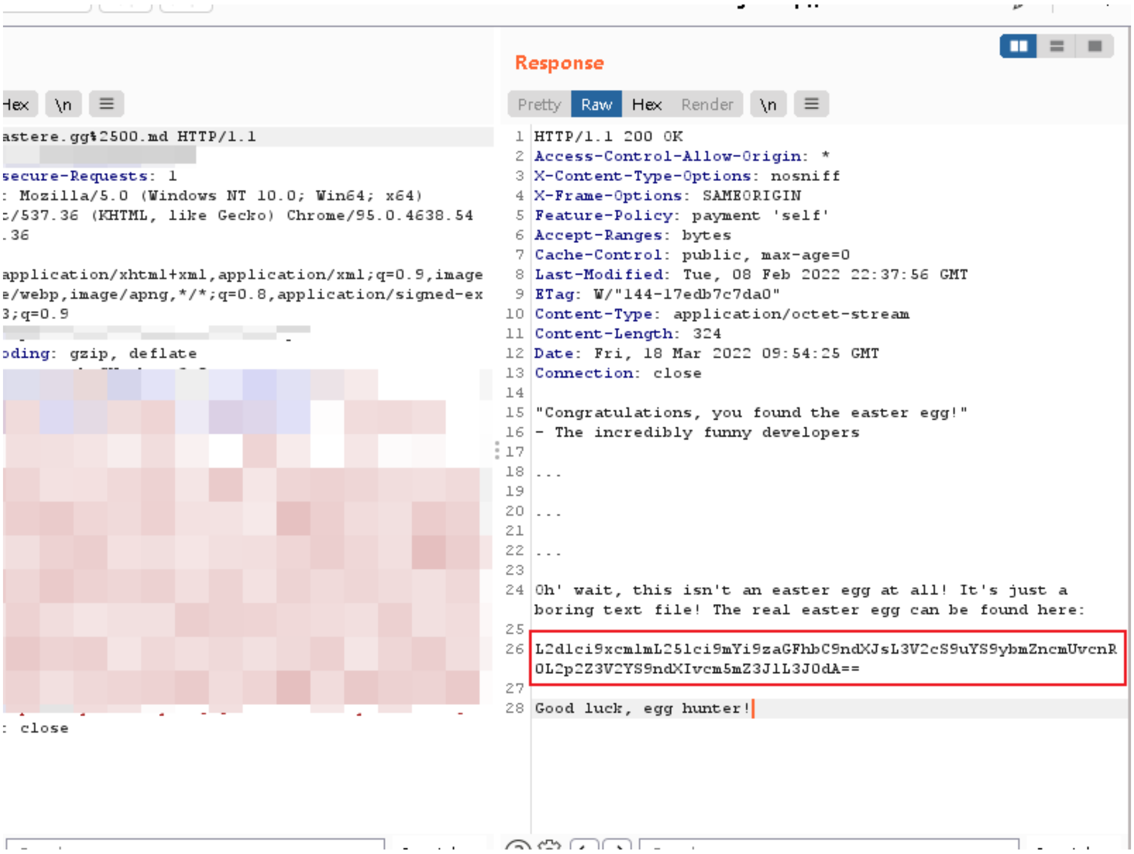
```
GET /ftp/eastere.gg HTTP/1.1
Host: [redacted]
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Wi                              ML, like Gecko) Chrome/95.0.4638.54
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/i                             mage/apng,*/*;q=0.8,application/sig
e;v=b3;q=0.9
Referer: [redacted]
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
[redacted]                                                                ss; continueCode=
Connection: close
```

3. 利用数据截断访问eastere.gg文件



```
GET /ftp/eastere.gg%2500.md HTTP/1.1
Host: [redacted]
Upgrade-Insecure-Requests: 1
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.9
Referer: [redacted]
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
[redacted]
Connection: close
```

4. 发送数据包，查看响应

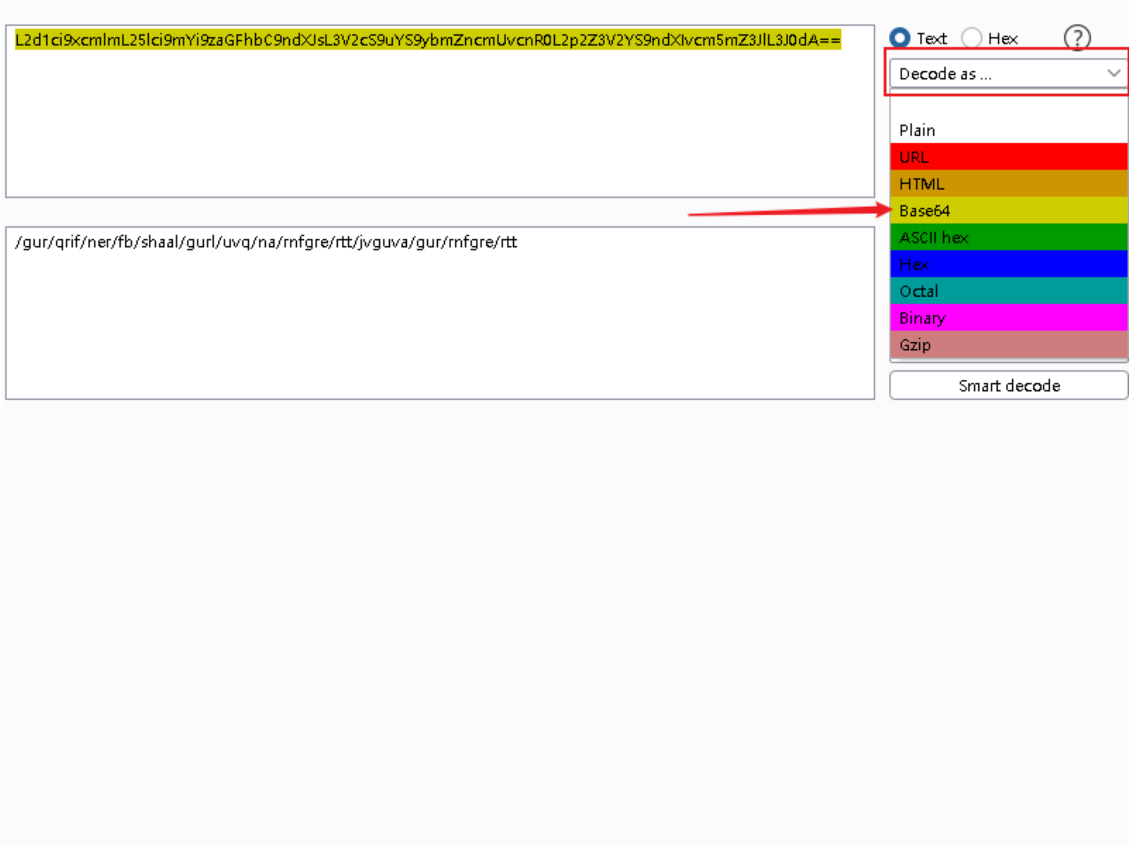


```
astere.gg%2500.md HTTP/1.1
[redacted]
secure-Requests: 1
: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
:/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54
.36

application/xhtml+xml,application/xml;q=0.9,image
e/webp,image/apng,*/*;q=0.8,application/signed-ex
3;q=0.9
[redacted]
oding: gzip, deflate
[redacted]
: close
```

Response

```
HTTP/1.1 200 OK
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

"Congratulations, you found the easter egg!"
- The incredibly funny developers

...

...

...

Oh' wait, this isn't an easter egg at all! It's just a
boring text file! The real easter egg can be found here:

L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR
0L2p2Z3V2YS9ndXIvcm5mZ3JlL3J0dA==

Good luck, egg hunter!
```

5. 复制加密语句到Decoder，以Base64方式解密

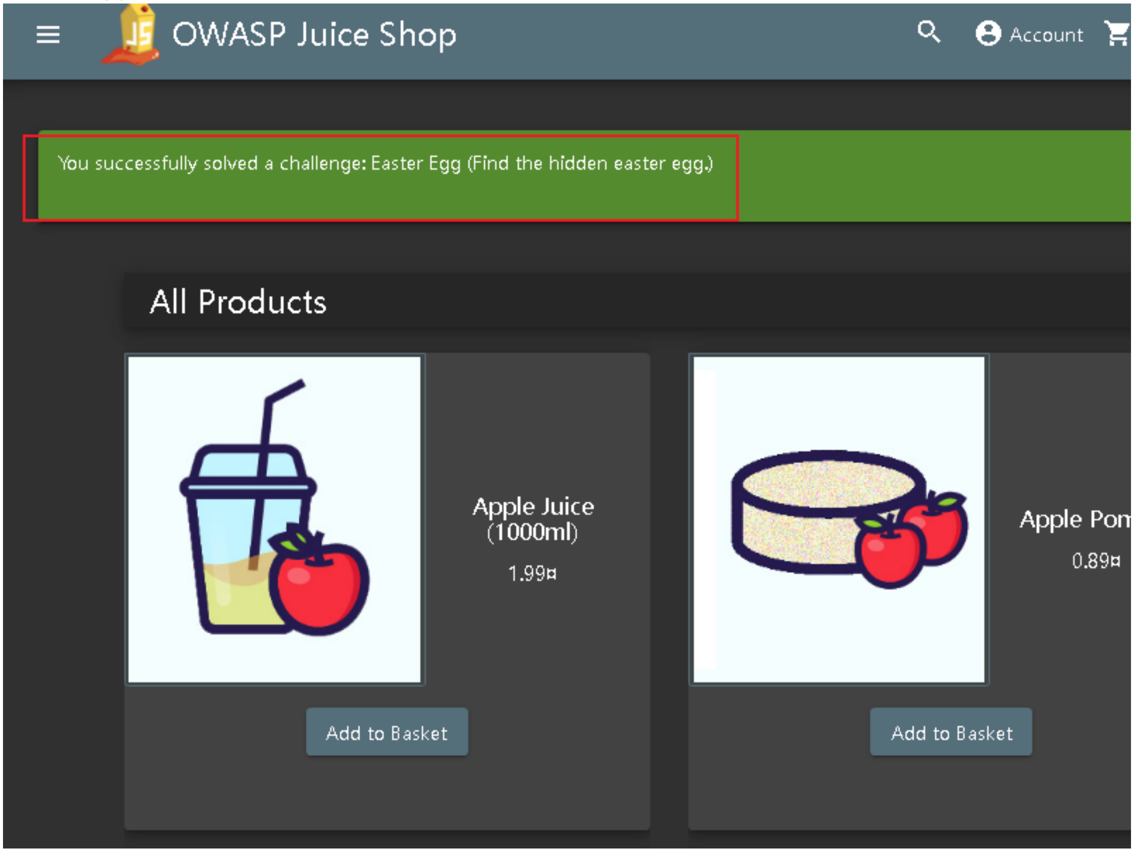


```
L2d1ci9xcmlmL25lci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmZncmUvcnR0L2p2Z3V2YS9ndXIvcm5mZ3JlL3J0dA==
```

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

Easter egg挑战



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