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

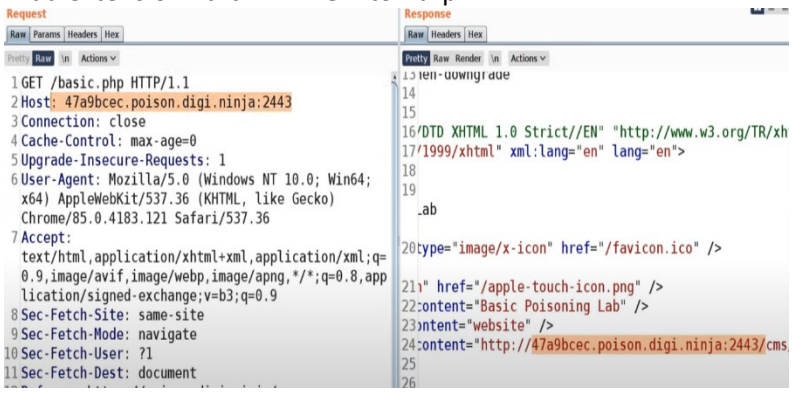


Fig: Observe the host and meta-data content are same.

- Right click and click on "Guess Header"

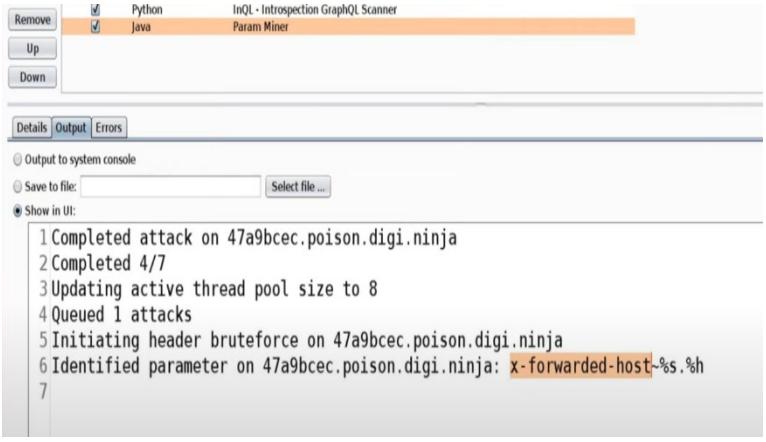


Fig : Parameter identified is x-forwarded-host

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

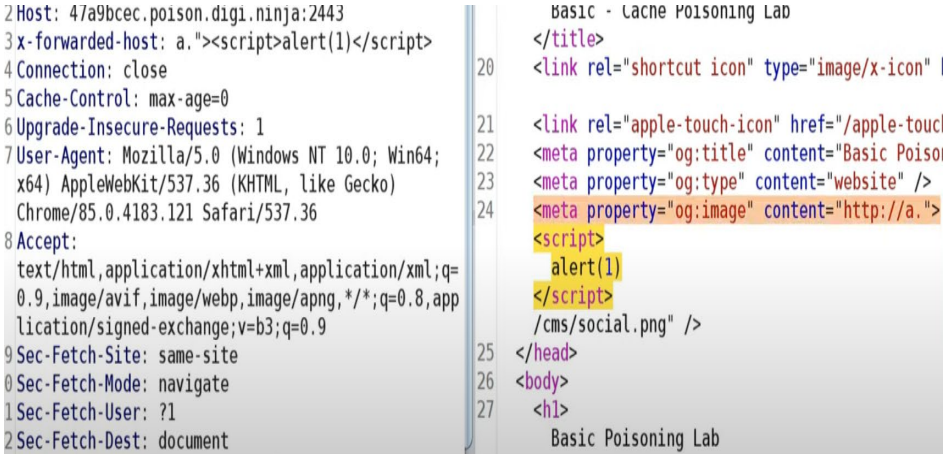
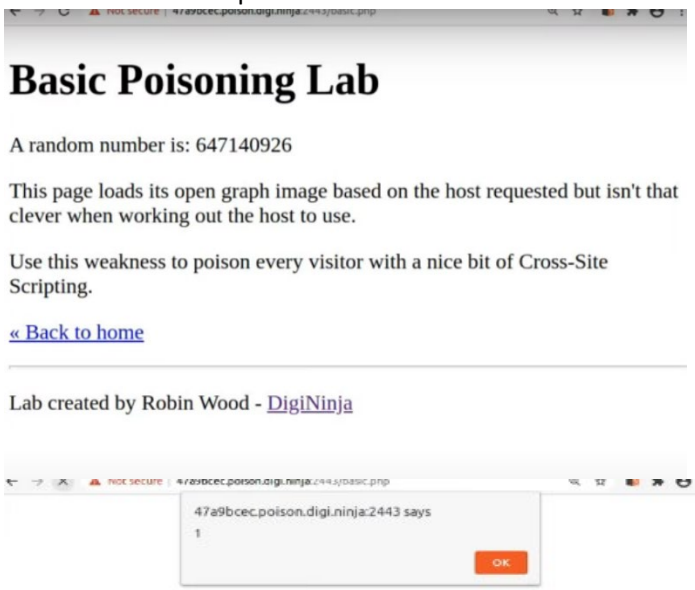


Fig: Injected payload is observed in the response.

- Turn off the Intercept and refresh the lab



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

Thank You. 😊