* App uses cache but it is not validating properly. (.js, .css, ...)

backgrounds:

→ web application uses proxy server, load balancer, CDN networks (وقت الاستجابة) or maybe other services to reduce its latency towards users.

but it is not validating.

target.com/profile.php/attack.js

They may cache the url under their cache directory.

→ if someone visit the link I will get his infos.

* exploitation:

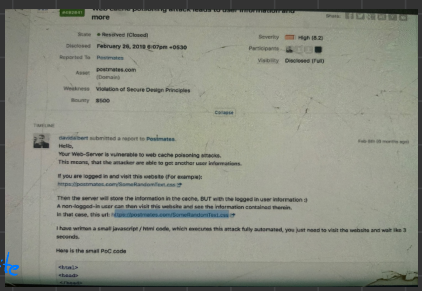
```
1  Exploitation Way
2
3  step1. victim to open malacious crafted link
4
5  target.com/mydetailes/malacious.mp3
6
7  application may ignore malacious.mp3
8
9  part of the url , the victim profile is loaded
10
11 step 2. attacker sends a GET request for the cached pages
12
13 target.com/mydeatils/malacious.mp3
14                                    I added it
```

→ if content is displayed as target.com/mydetails and the cache is saving the page, so open the url target.com/mydetails/mymalicious.mp3 in private window and see if content of cache is displayed, it is vulnerable.

→ if you can't get sensitive data, vulnerabe means nothing

* Automation tools

1. Copy as python-requests extender in Burpsuite
2. web cache python file.



Steps to exploit:

1. login into the target website
2. get your profile url and spider it with burpsuite
3. you can spider what you think it is sensitive.
4. Send any url to repeat + copy as request
5. Copy cookie + header value + paste it in python file.
6. Now you need urls, so go target → sitemap and choose a directory + copy url in this branch.

7. Save url in a text file (see that url has / at the end.

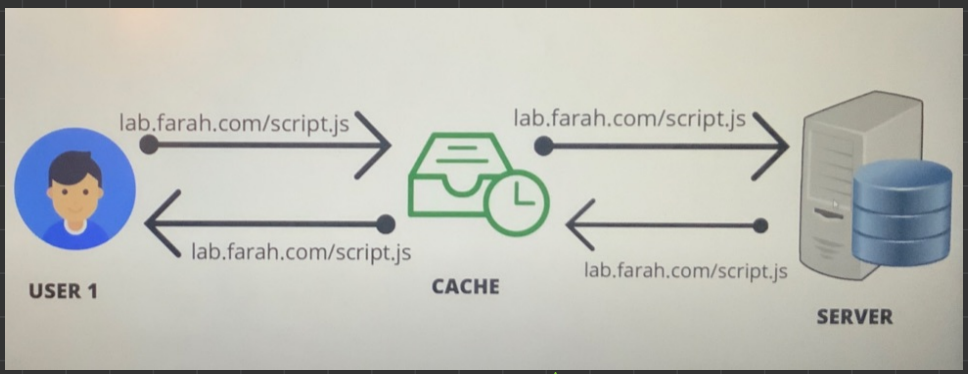
8. run → python webcache.py urls.txt

↳ status code should be 200, if you see possible cache

open new private window and paste url

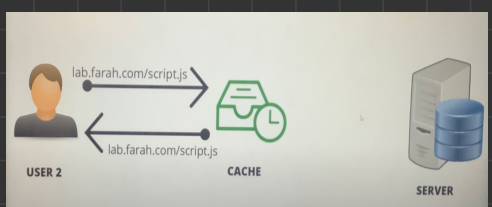
if you get the profile and edit it, it is vulnerability

What is a cache ?



developer configure web cach functionality to their application which store files that are frequently request by user, so when a user request one of those files, it is self directly from the cach and there is no need for server to deal with requests over and over again.

→This help introducing load on server and help users to get their content faster.



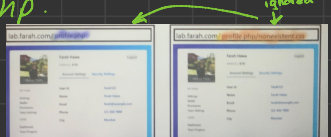
What files are cached ?

public and static files, do not contain any sensitive infos.

Files cached	Files not cached
stylesheets.css	profile.php
scripts.js	wallet.php
image.png	orders.php

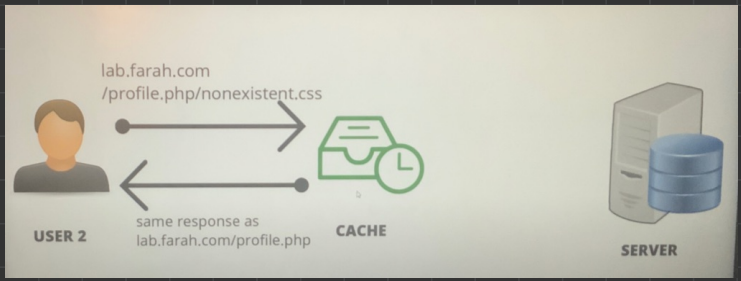
What happen if we request a non existing file cach from the server

It could be possible that non-existing file in ignored and the response that it returned is profile.php.



The Bug

What happen?.
the cache sees that the .css at the end and caches it, because of its configuration, while the content of url contain Senstive data



exploitation conditions

- Condition 1: When accessing a path like lab.farah.com/profile.php/nonexistent.css, the response returned should be for lab.farah.com/profile.php
- Condition 2: The caching functionality should be configured to cache/not cache files based on their extensions.