**DAY 36**

URL/open redirection vulnerability:

🡪search for url encodings

%3A :

%2F /

%3F ?

%3D =

%26 &

The redirection with site for some resource or from one website to another website is called URL redirection.

What is URL redirection?

URL redirect (also referred as URL forwarding) is a technique which is used to redirect your domain’s visitors to a different URL. You can forward your domain name to any websites, webpage etc. which is available online.

Redirection use status codes defined within the HTTP protocols.

Based on this, URL forwarding may be of the following types:

301-permanent

302-temporary

URL frame (masked redirect)

🡪search for redirect types

HTTP response codes:

1xx informational

2xx success

3xx redirection

4xx server error

Httpstatuses.com

Impact:

Case-1:

URL redirection

Can lead to account take over.

Note: If the url redirections with authentication token

Case-2:

This can lead to phishing attack by attackers

github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Open%20Redirect

Google dork:

Inurl:?redir= site: