ClickJacking

Notes

Clickjacking
is a technique, also known as User Interface (UI) redressing, where an attacker tricks a victim into clicking on a resource that is different from what they actually intend to click on

A necessary condition for this purpose is that the target page can be included through an iframe element inside any HTML pages.

```
<html>
   <body>
<frame src="[TargetPage]"> </frame> <body>
</html>
```

POC can be done with burp clickbandit

Mitigation:

1- The old way (using JS):
```
<script>
        if(top != window) {
        top.location = window.location
        }
</script>
```
This protection is weak at best, simply because the top level window (the one which the iframe tried to change its location) could prevent this change.

2- The new way (using Headers):
X-Frame-Options header : <meta http-equiv="X-Frame-Options" content="deny">
sent over HTTP web server responses to prevent a
document from being shown inside an iframe.

Cursorjacking is a clickjacking technique that consists of using a custom cursor icon to change the actual position of the pointer, tricking users into clicking on something other than what they intended to click on.

DOS Greedy:
In the case of Greedy Pages, the attacker performs HTTP requests to each page available on the target site (any script, image, etc.) and analyzes the response time of each request. Requests appearing to take a long time are marked as critical requests and will be used to perform new requests.

In open source web applications, resource-hogs like scripts running large SQL queries are well known.
An attacker can use these pages to perform many requests with the goal of wearing down the web server resources and grinding the site to a halt.