Tabnabbing

> Reverse tabnabbing is an attack where a page linked from the target page is able to rewrite that page, for example to replace it with a phishing site. As the user was originally on the correct page they are less likely to notice that it has been changed to a phishing site, especially if the site looks the same as the target. If the user authenticates to this new page then their credentials (or other sensitive data) are sent to the phishing site rather than the legitimate one.

Summary

Tools

- Discover Reverse Tabnabbing - Burp Extension

More information about the vulnerability

When tabnabbing, the attacker searches for links that are inserted into the website and are under his control. Such links may be contained in a forum post, for example. Once he has found this kind of functionality, it checks that the link's `rel` attribute does not contain the value `noopener` and the target attribute contains the value `_blank`. If this is the case, the website is vulnerable to tabnabbing.

How to exploit

```
1. Attacker posts a link to a website under his control that contains the following
JS code: window.opener.location = "http://evil.com"
2. He tricks the victim into visiting the link, which is opened in the browser in a
new tab.
3. At the same time the JS code is executed and the background tab is redirected to
the website evil.com, which is most likely a phishing website.
4. If the victim opens the background tab again and doesn't look at the address bar,
it may happen that he thinks he is logged out, because a login page appears, for
example.
5. The victim tries to log on again and the attacker receives the credentials
```

How to hunt for it

As already mentioned, you have to search for the following link formats:

```
<a href="..." target="_blank" rel="" />
or
<a href="..." target="_blank" />
```

References

- Reverse Tabnabbing - OWASP, 20.10.20
- Tabnabbing - Wikipedia, 20.10.20