Reverse Tab Nabbing

By Asia Erickson

ENTER

01
02
03
04

What is Reverse Tab Nabbing?

When an attacker gains control over the href attribute of an ‘<a>’ tag with attributes **target=“_blank”** and **rel=“opener”**:

- The attacker can redirect the victim to a malicious website by changing the href attribute
- They can exploit the rel=“opener” attribute and gain control over the original page through window.opener in Javascript
- Even without rel=“opener,” of the page uses target=“_blank” without rel=“noopener,” it is still vulnerable

Why is this bad?

01

02

03

04

Redirection

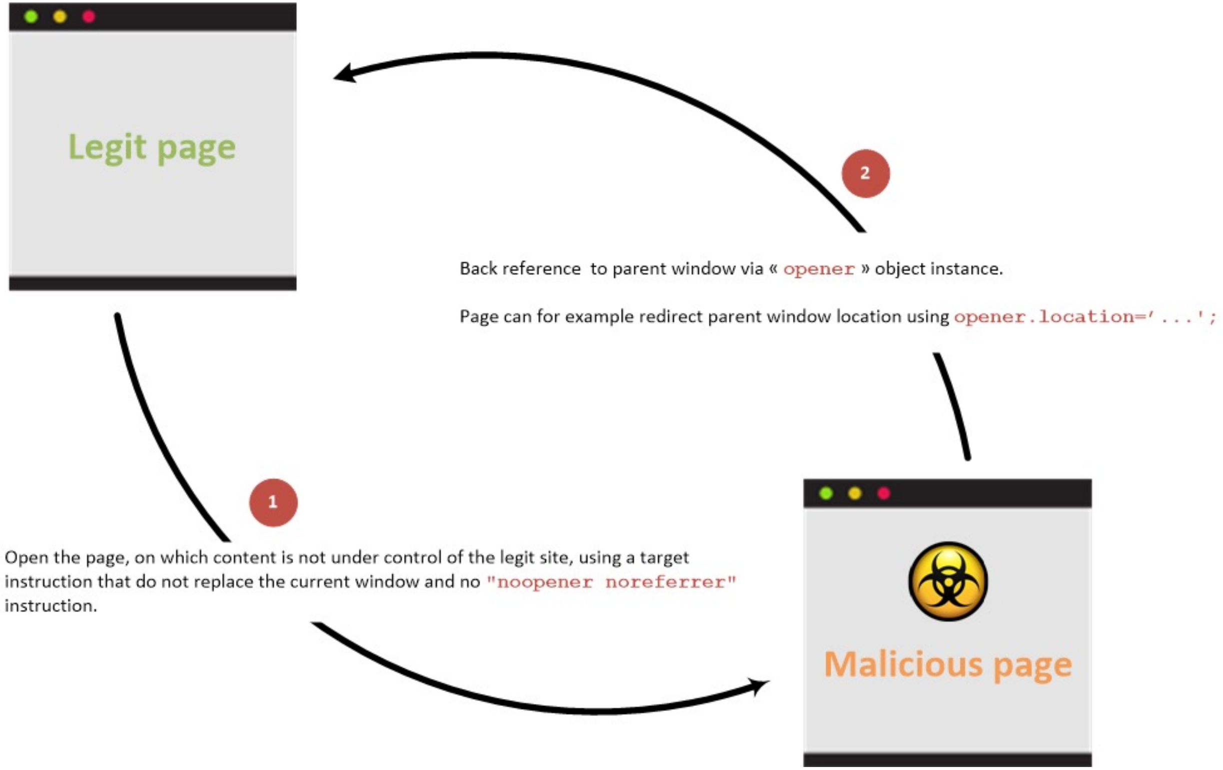
This can allow the attacker to redirect the victim to a fake website using hyperlinks

Extraction

The attacker can extract sensitive information such as logins

01
02
03
04

Website Vulnerable to Tab Nabbing



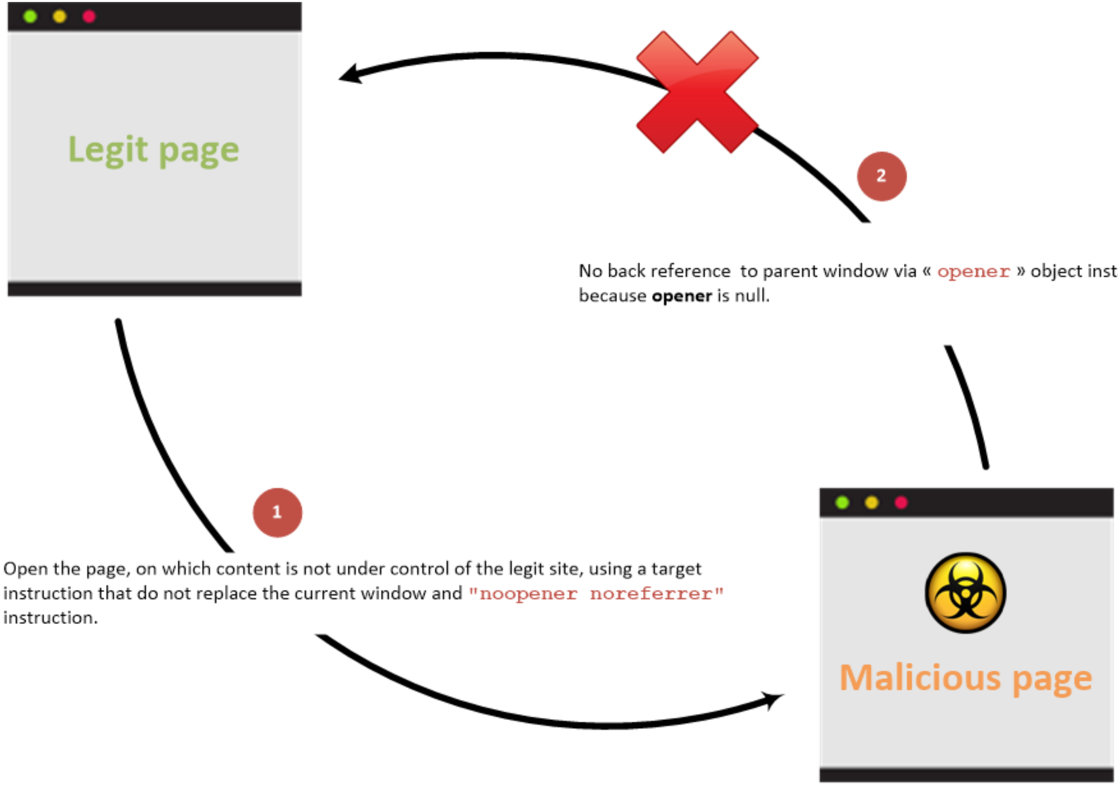
Back reference to parent window via « opener » object instance.

Page can for example redirect parent window location using `opener.location='...';`

Open the page, on which content is not under control of the legit site, using a target instruction that do not replace the current window and no `"noopener noreferrer"` instruction.

01
02
03
04

Not Vulnerable to Tab Nabbing



No back reference to parent window via « opener » object instance because **opener** is null.

Open the page, on which content is not under control of the legit site, using a target instruction that do not replace the current window and "noopener noreferrer" instruction.

01
02
03
04

Demo!

We're going to look at a vulnerable code and then the fix!

01
02
03
04

Basic Example from HackTricks

vulnerable.html

```
<!DOCTYPE html>
<html>
<body>
<h1>Victim Site</h1>
<a href="http://127.0.0.1:8000/malicious.html" target="_blank" rel="opener">Controlled by the attacker</a>
</body>
</html>
```

Basic Example from HackTricks Cont.

malicious.html

```
<!DOCTYPE html>
<html>
 <body>
  <script>
  window.opener.location = "http://127.0.0.1:8000/malicious_redir.html";
  </script>
 </body>
</html>
```

malicious_redir.html

```
<!DOCTYPE html>
<html>
<body>
<h1>New Malicious Site</h1>
</body>
</html>
```

01

02

03

04

01
02
03
04

Burp Tool

“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. 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. Because of this I created the Discovering Reverse Tabnabbing, that is a Burp extension written in Python which helps to locate HTML links that use the target="_blank" attribute, omitting the rel="noopener" attribute.

(requires Burp Suite Professional)

Resources

Hacktricks

https://book.hacktricks.xyz/pentesting-web/reverse-tab-nabbing

OWASP

https://owasp.org/www-community/attacks/Reverse_Tabnabbing

OWASP Cheat Sheets

https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html#tabnabbing

01
02
03
04

01
02
03
04

Thank you!

Questions?