XSS

CROSS-SITE SCRIPTING

Types

- Stored XSS (persistent, or type-2)
- Reflected XSS (non-persistent, or type-1)
- DOM-base (type-0)

Stored XSS (persistent, or type-2)

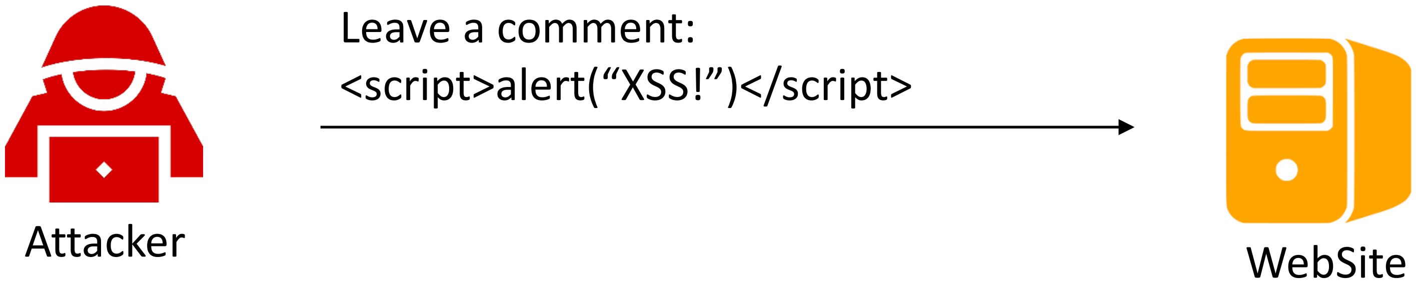
Stored XSS (persistent, or type-2)

Stored XSS (persistent, or type-2)

Attacker

WebSite

Stored XSS (persistent, or type-2)

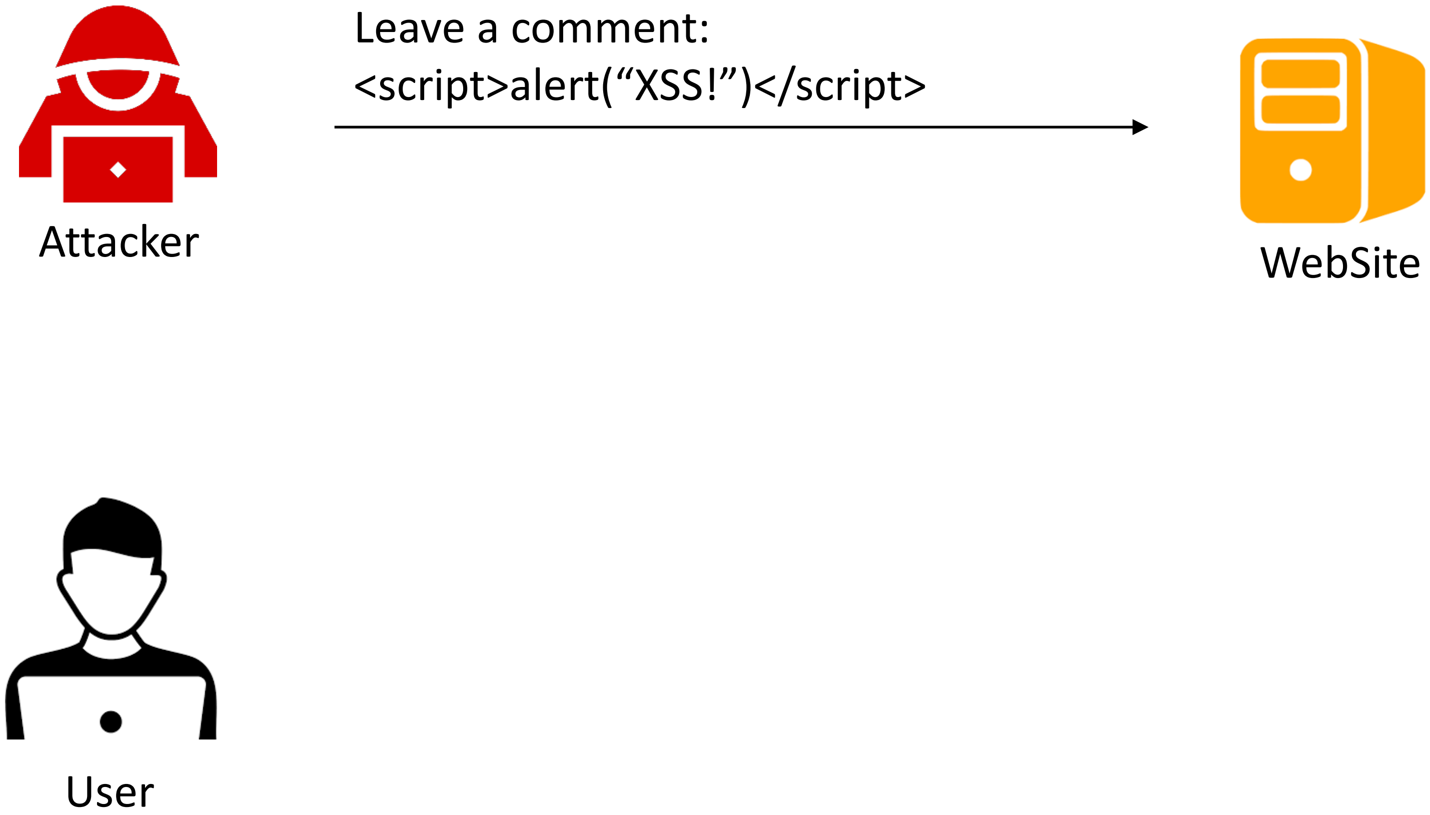


Attacker

Leave a comment:
<script>alert(“XSS!”)</script>

WebSite

Stored XSS (persistent, or type-2)



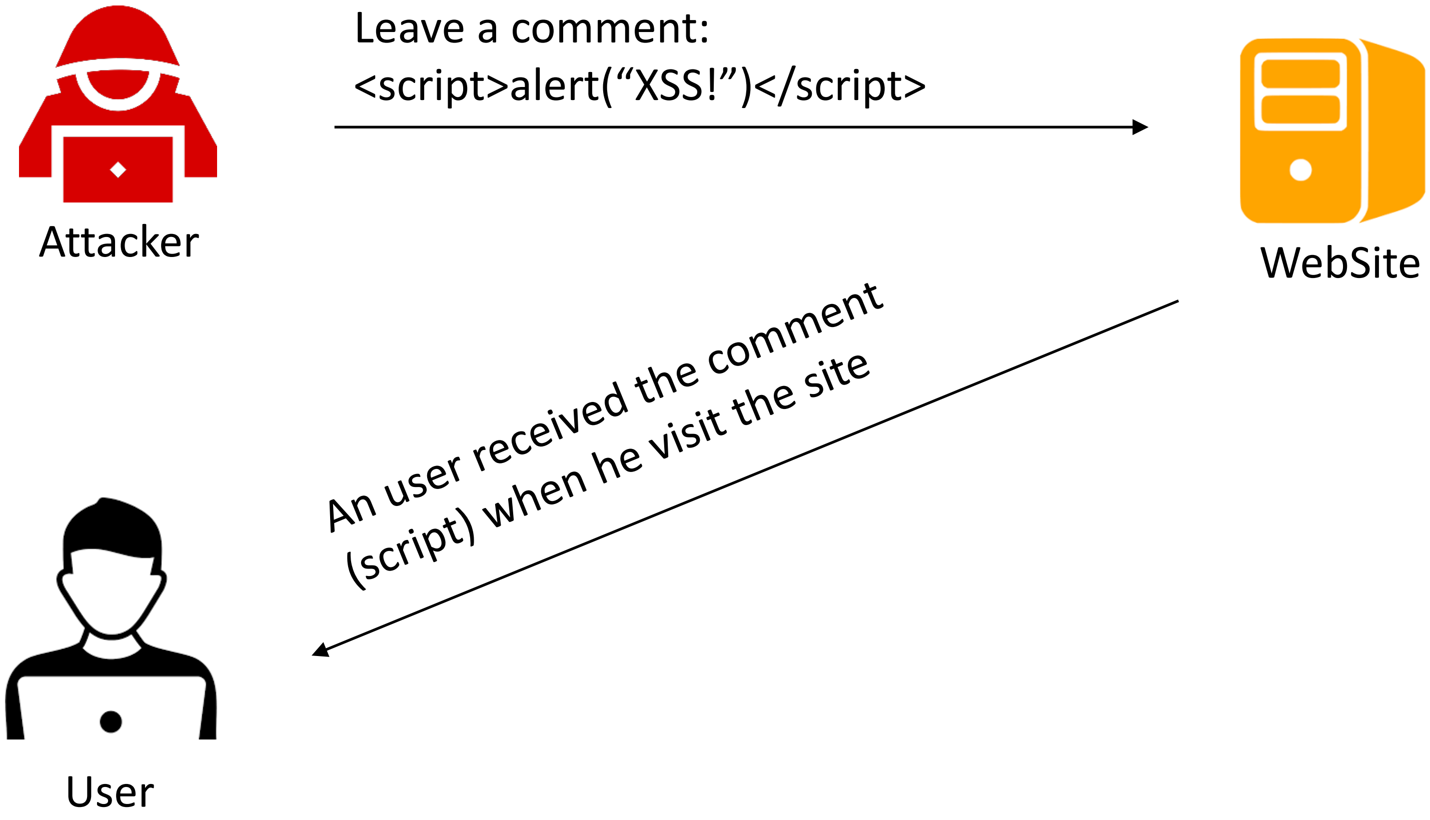
Attacker

Leave a comment:
<script>alert(“XSS!”)</script>

WebSite

User

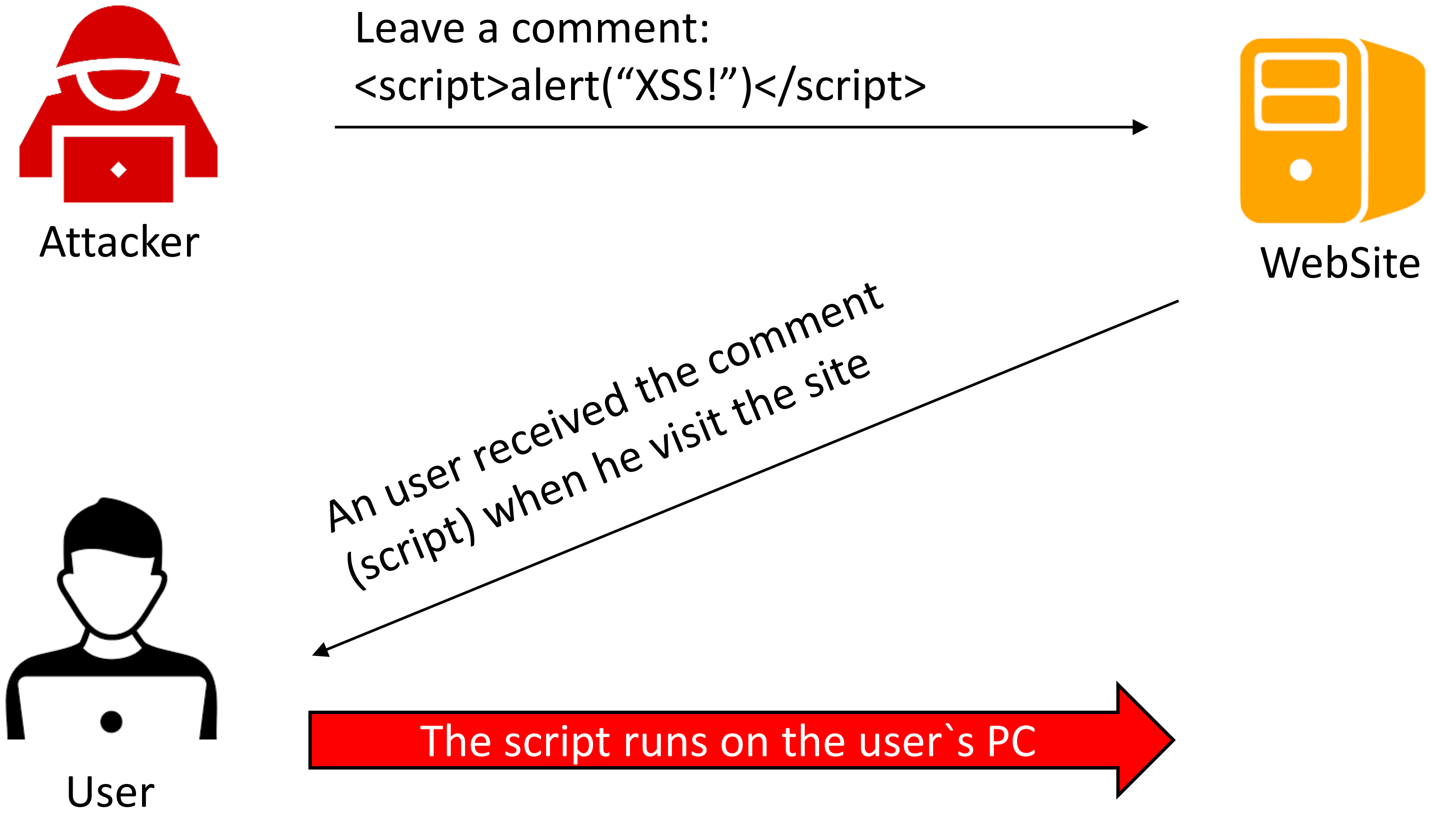
Stored XSS (persistent, or type-2)



Leave a comment:
<script>alert(“XSS!”)</script>

An user received the comment (script) when he visit the site

Stored XSS (persistent, or type-2)



Attacker

Leave a comment:
<script>alert(“XSS!”)</script>

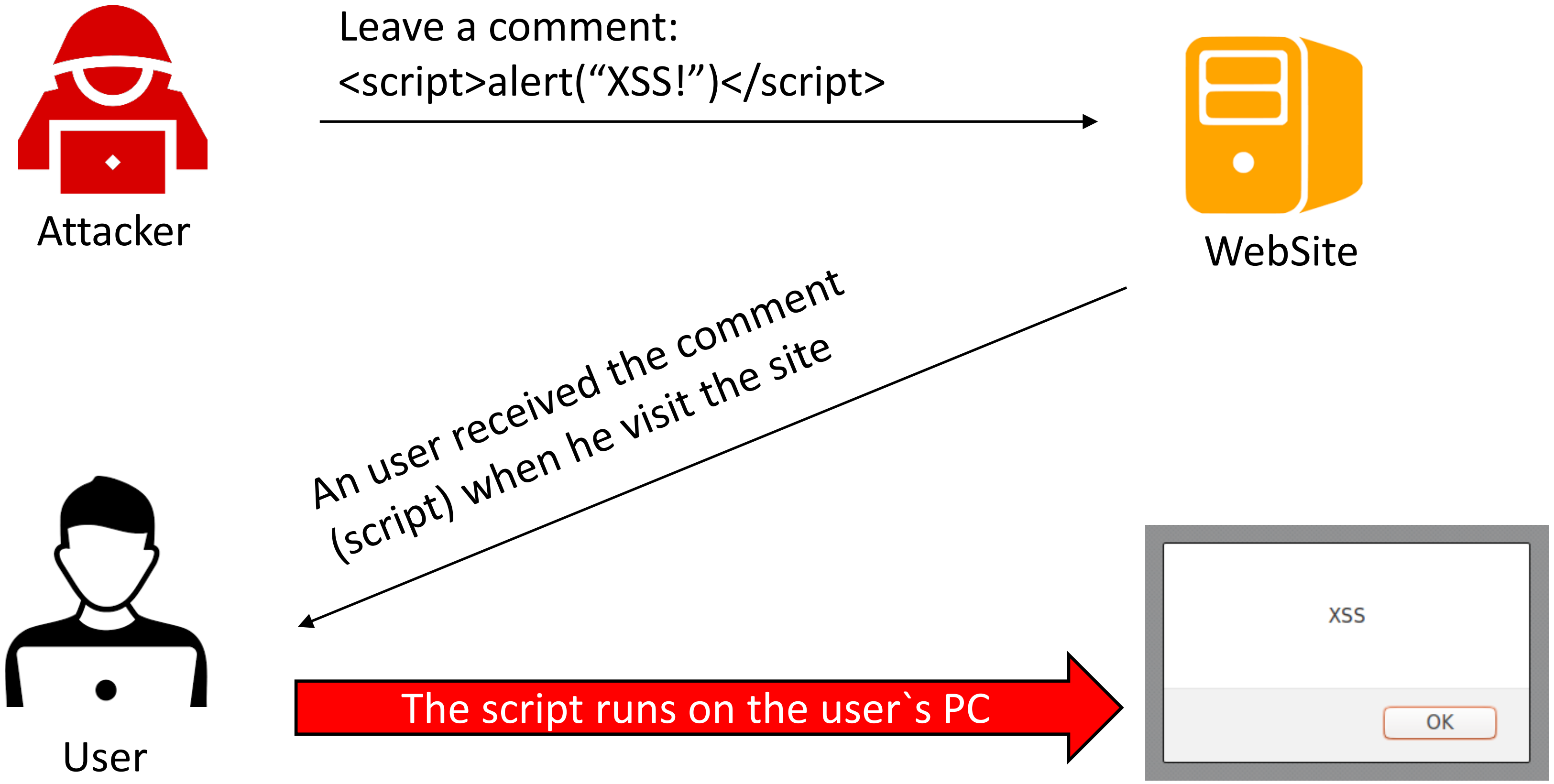
WebSite

An user received the comment
(script) when he visit the site

User

The script runs on the user`s PC

Stored XSS (persistent, or type-2)

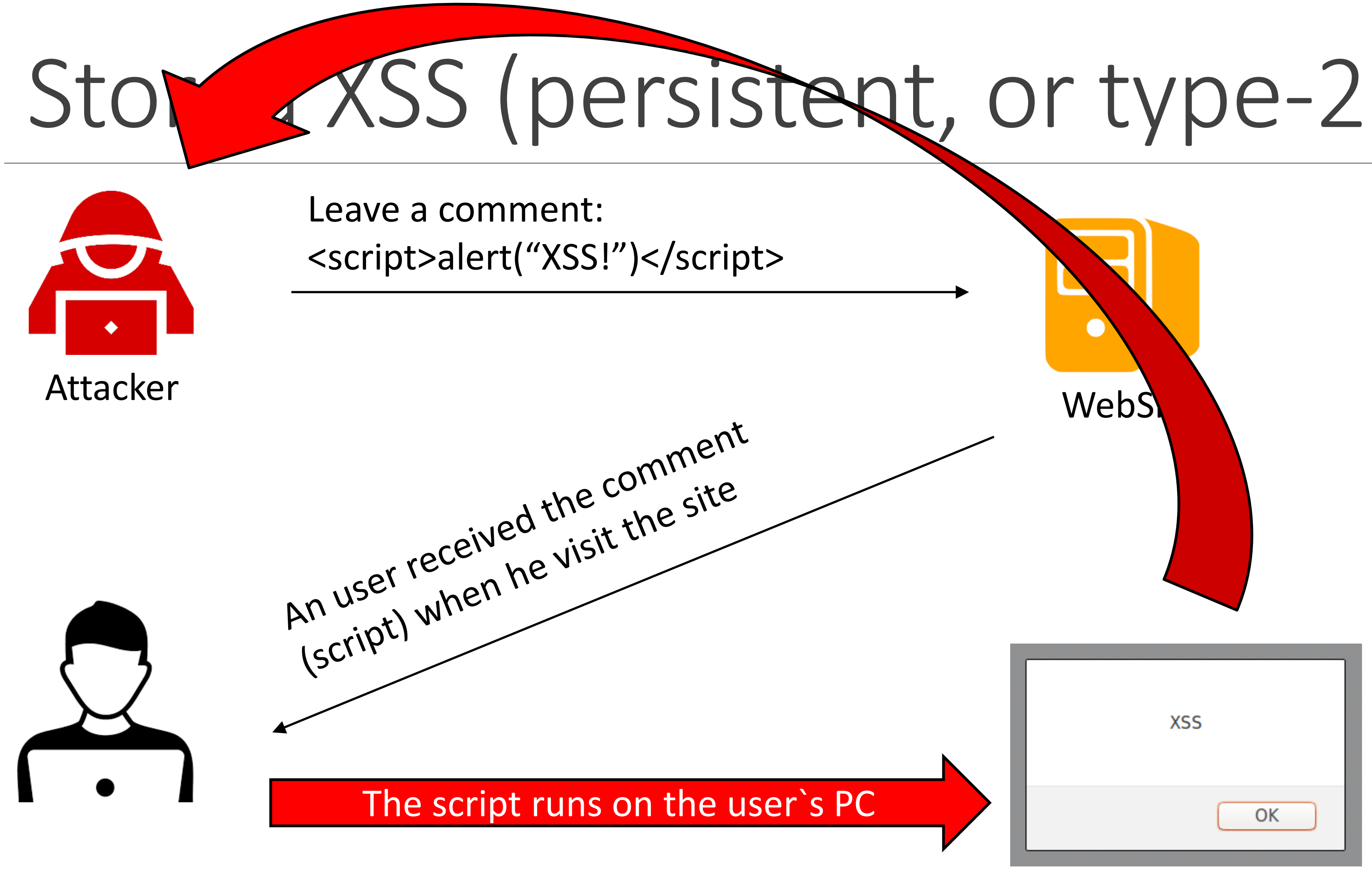


Leave a comment:
<script>alert(“XSS!”)</script>

An user received the comment (script) when he visit the site

The script runs on the user`s PC

Stored XSS (persistent, or type-2)



The script can send sensitive information to the user (like cookies, sessionid etc)

Leave a comment:
<script>alert(“XSS!”)</script>

An user received the comment (script) when he visit the site

The script runs on the user`s PC

Reflected XSS (non-persistent, type-1)

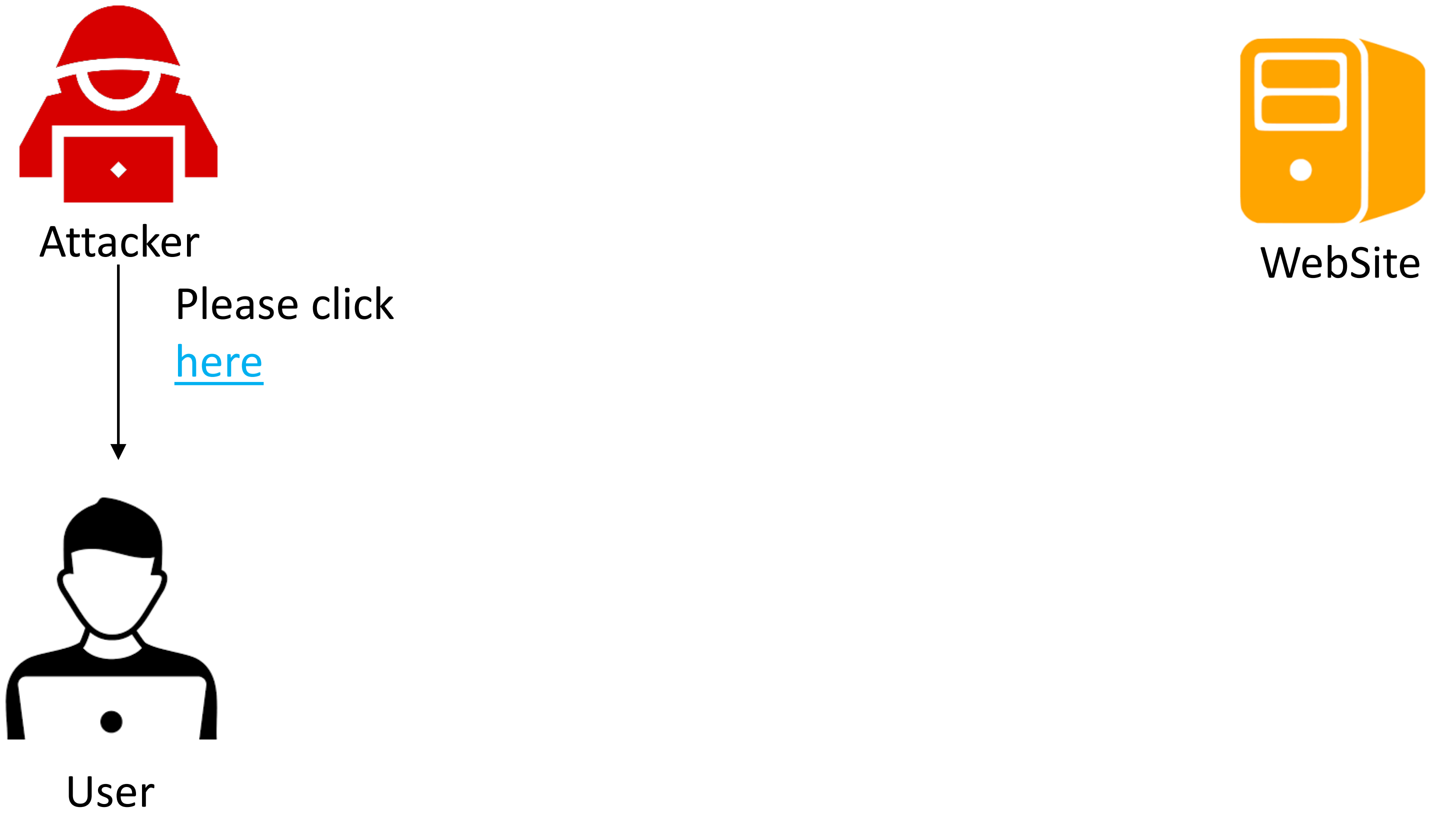
Reflected XSS (non-persistent, type-1)

Attacker

WebSite

User

Reflected XSS (non-persistent, type-1)



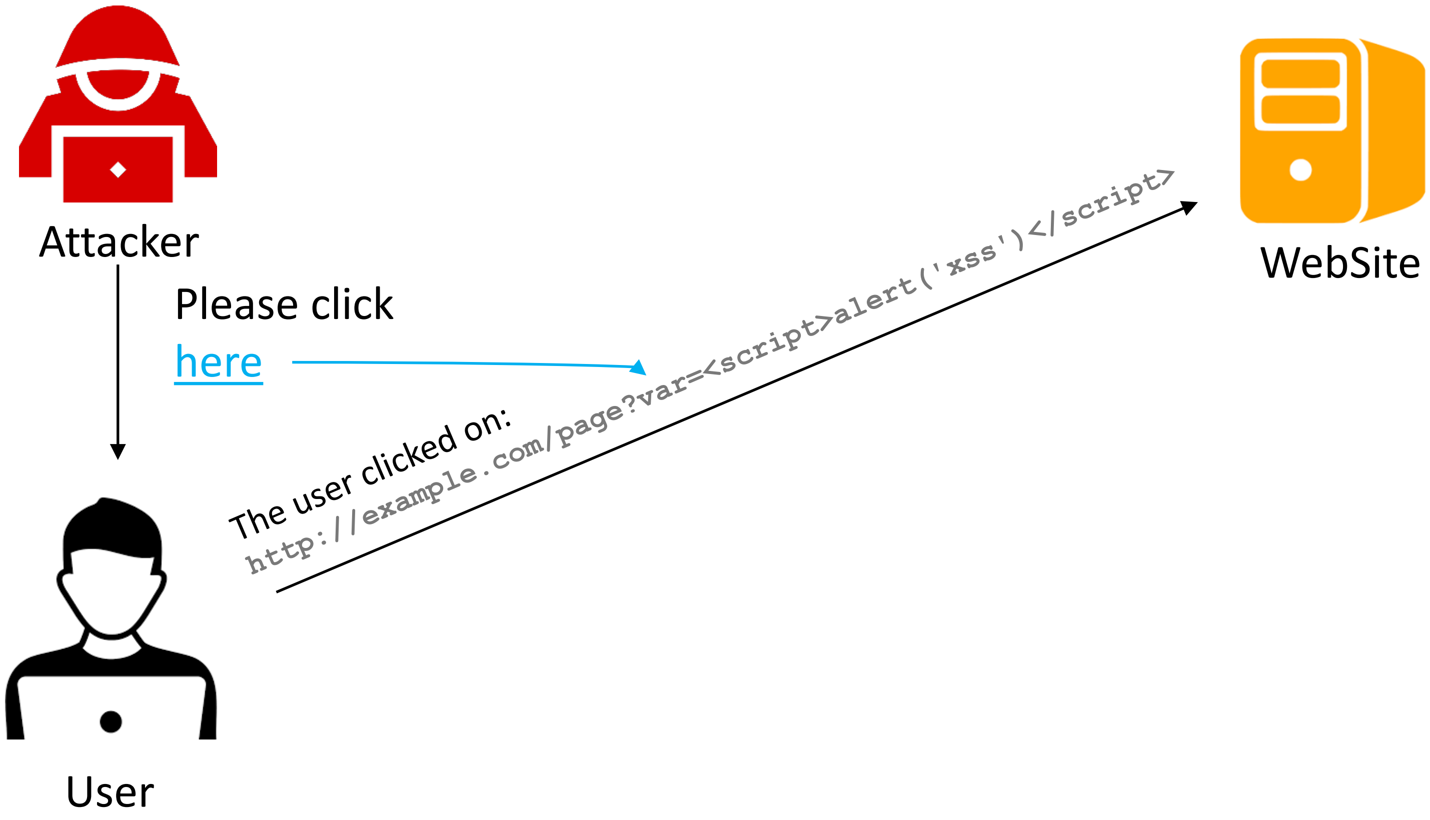
Attacker

Please click here

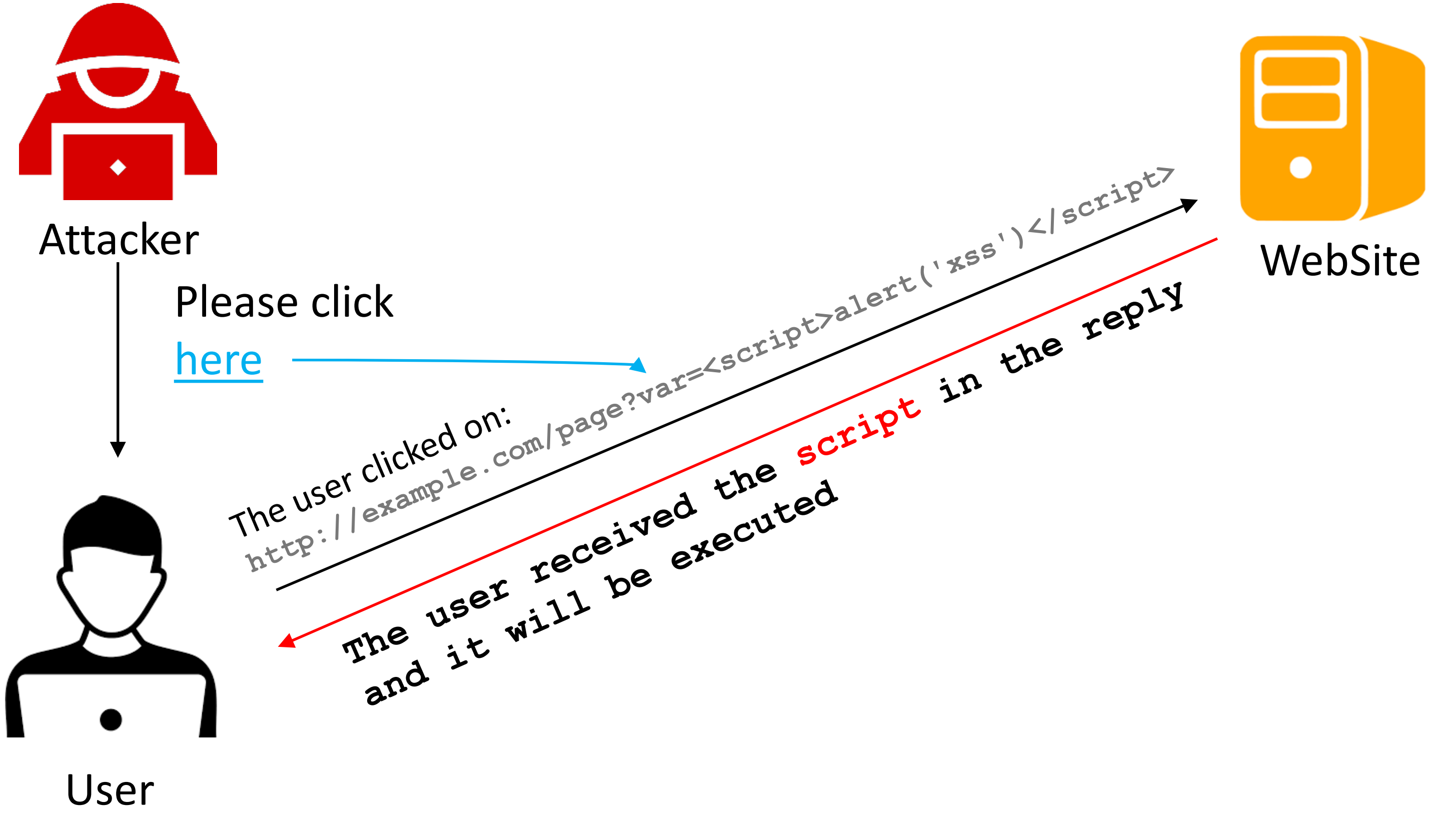
User

WebSite

Reflected XSS (non-persistent, type-1)



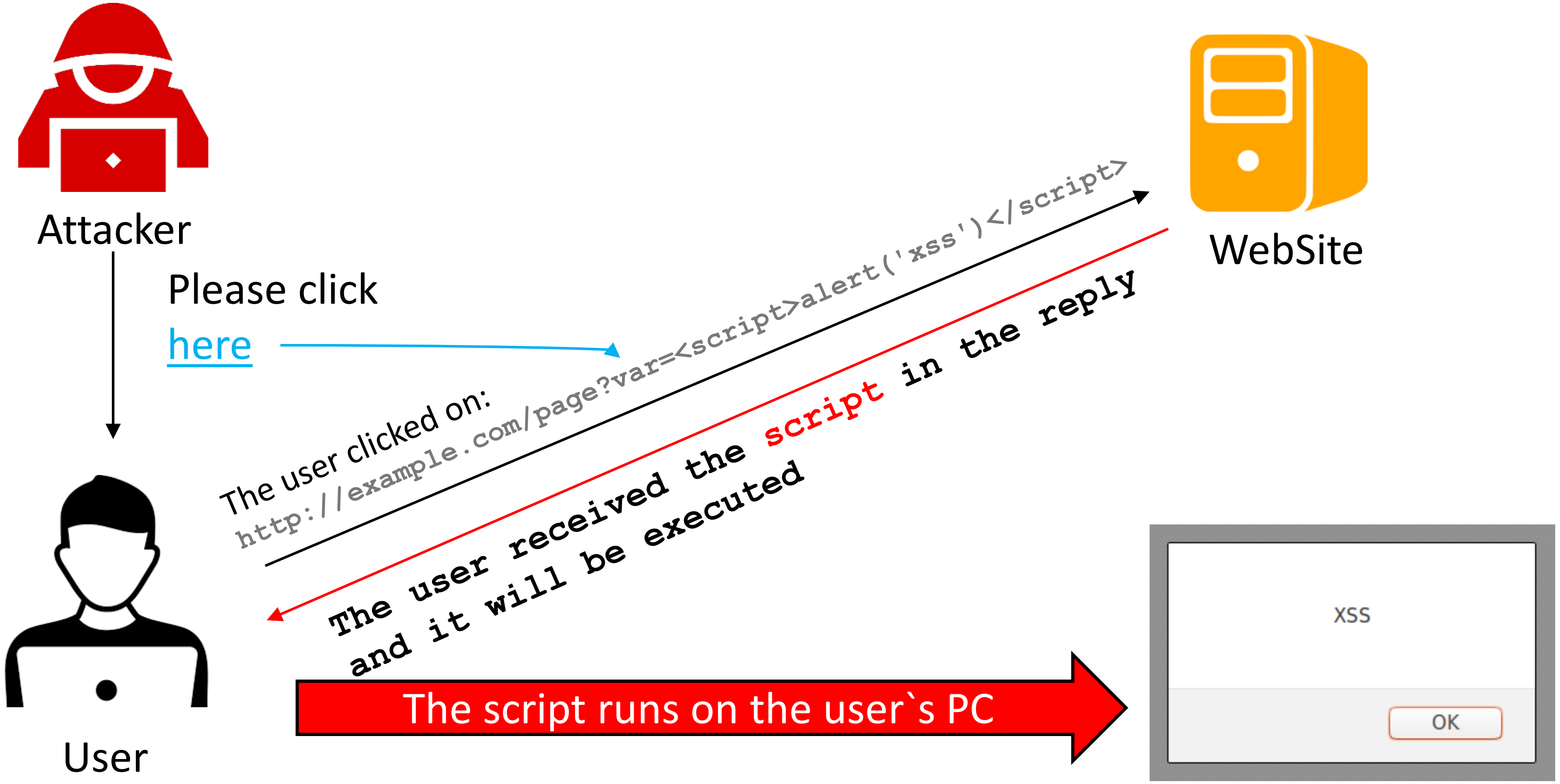
Reflected XSS (non-persistent, type-1)



The user clicked on:
`http://example.com/page?var=<script>alert('xss')</script>`

The user received the script in the reply and it will be executed

Reflected XSS (non-persistent, type-1)



Attacker

Please click here

The user clicked on:
`http://example.com/page?var=<script>alert('xss')</script>`

WebSite

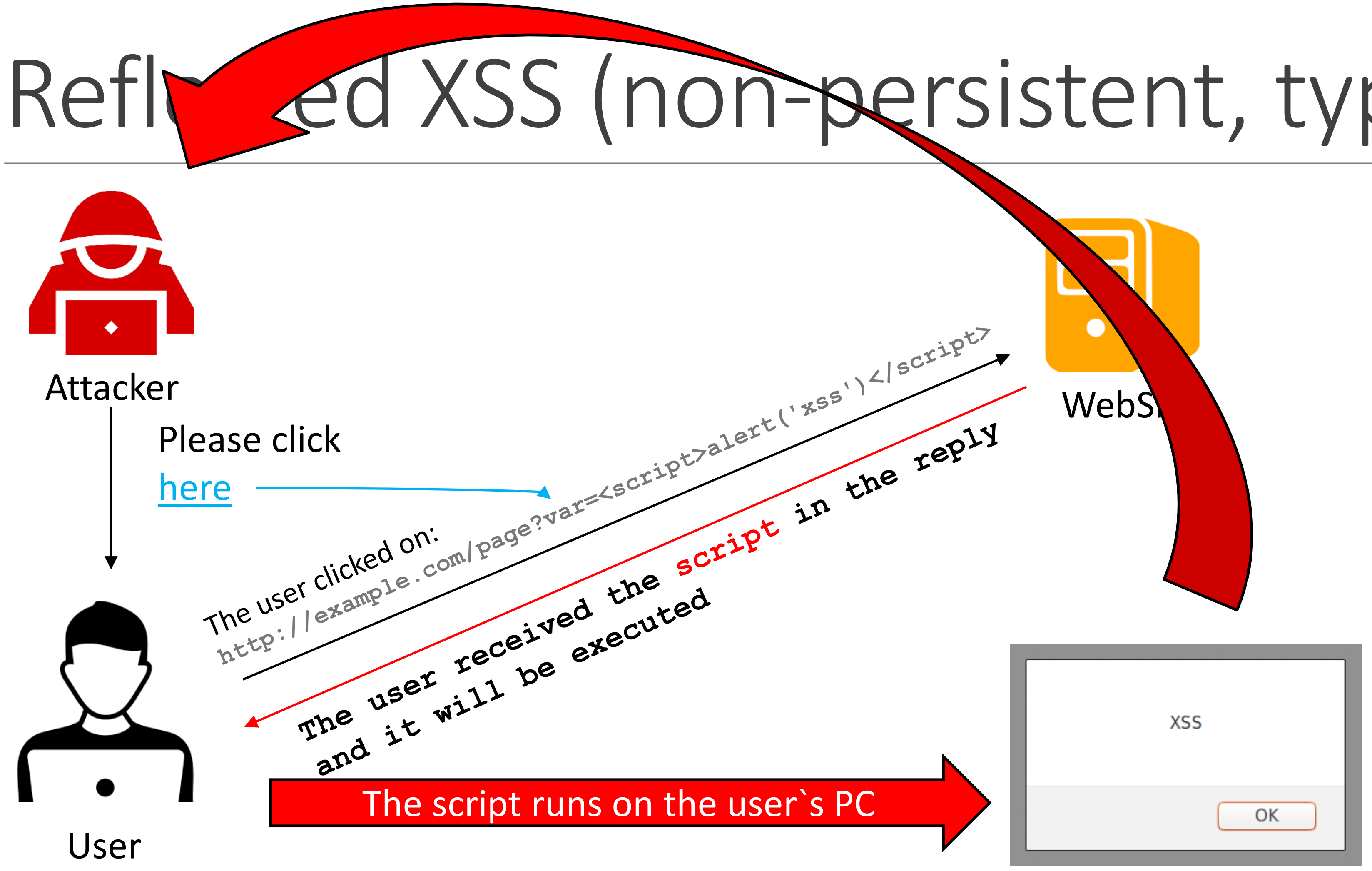
The user received the script in the reply and it will be executed

User

The script runs on the user`s PC

The script can send sensitive information to the user (like cookies, sessionid etc)

Reflected XSS (non-persistent, type-1)



The user clicked on:
`http://example.com/page?var=<script>alert('xss')</script>`

The user received the script in the reply and it will be executed

The script runs on the user`s PC

DOM-based XSS (type-0)

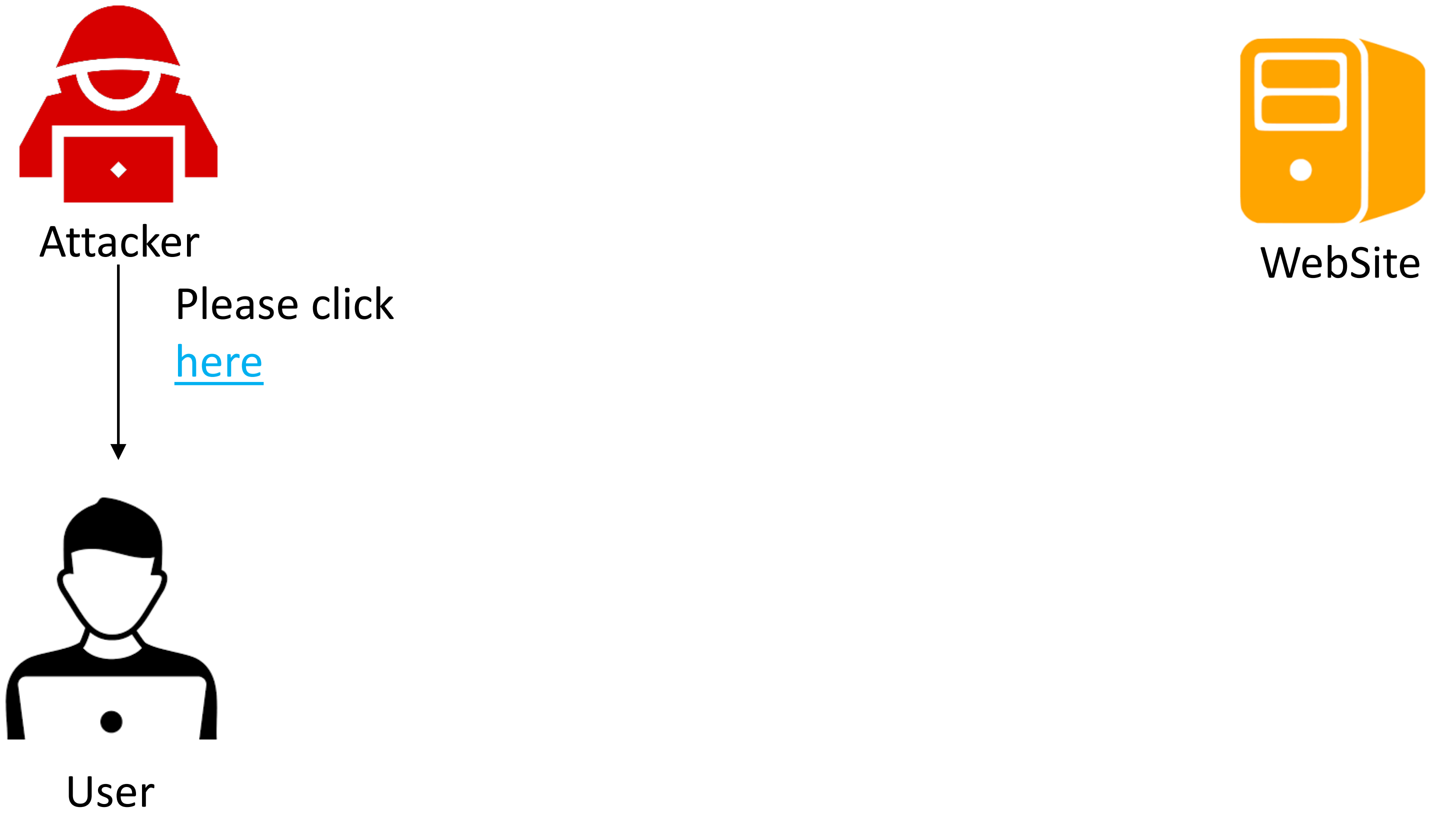
DOM-based XSS (type-0)

Attacker

WebSite

User

DOM-based XSS (type-0)



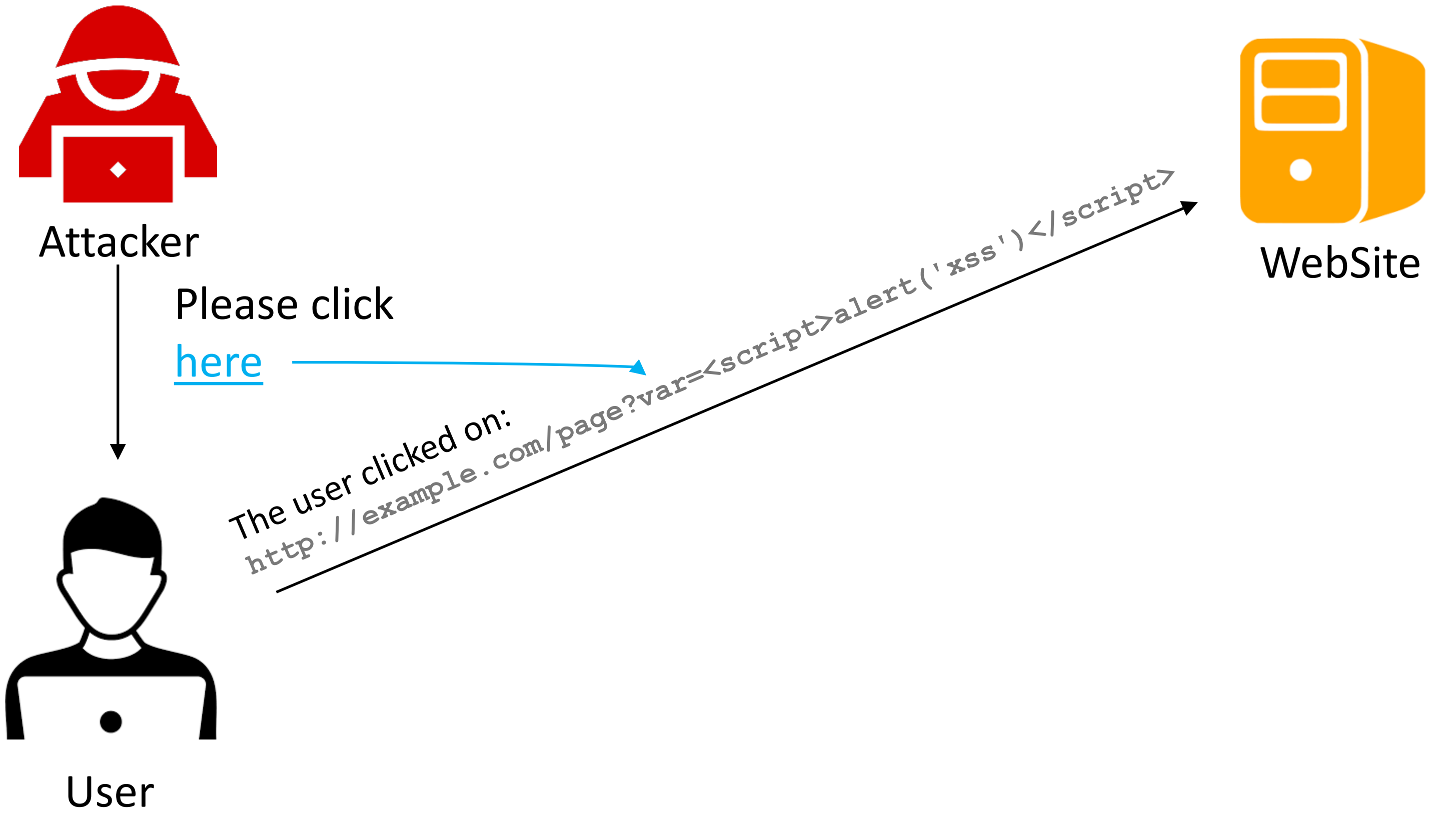
Attacker

Please click here

User

WebSite

DOM-based XSS (type-0)



Attacker

Please click

here

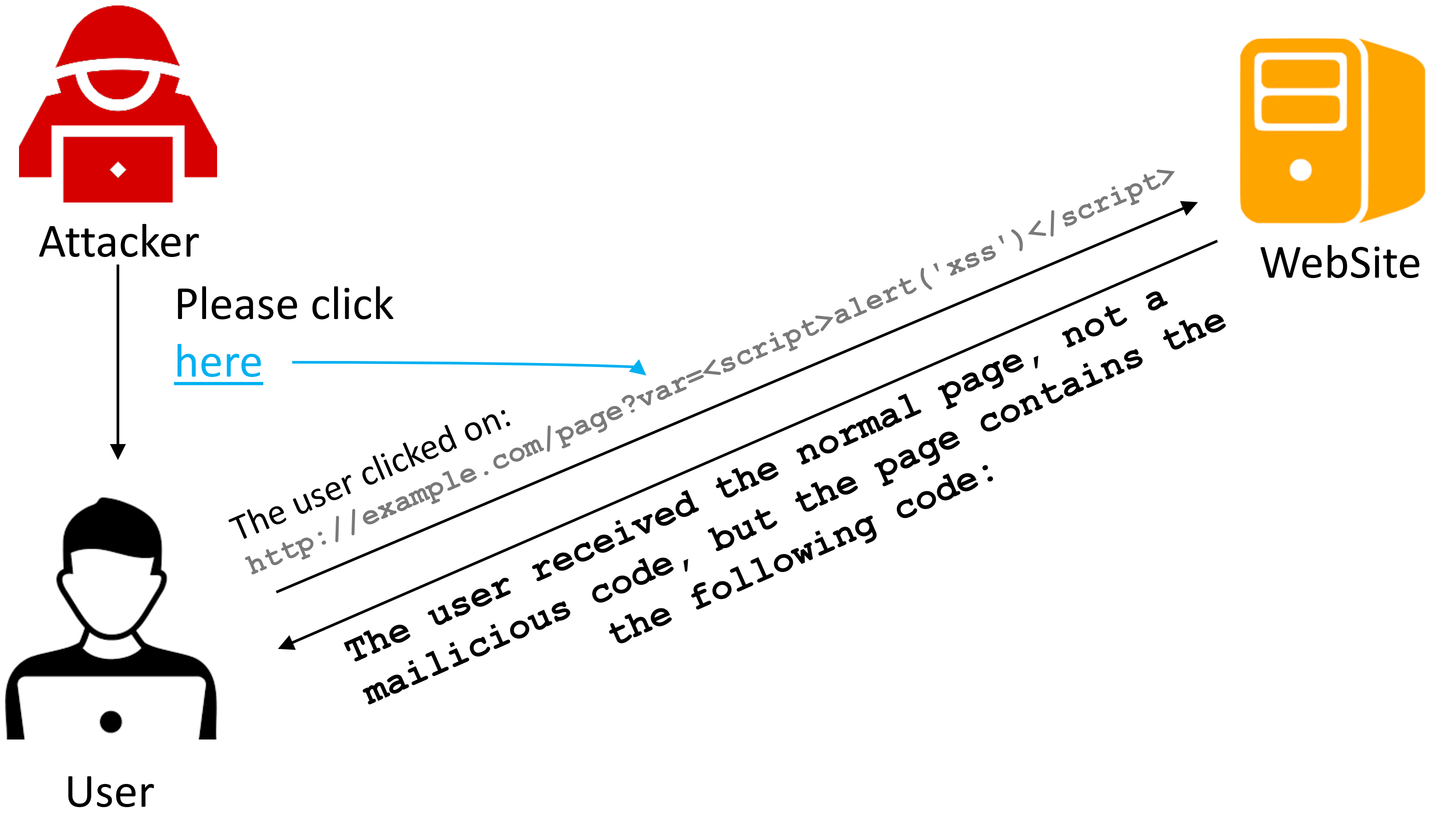
The user clicked on:

`http://example.com/page?var=<script>alert('xss')</script>`

WebSite

User

DOM-based XSS (type-0)



Attacker

Please click here

The user clicked on:

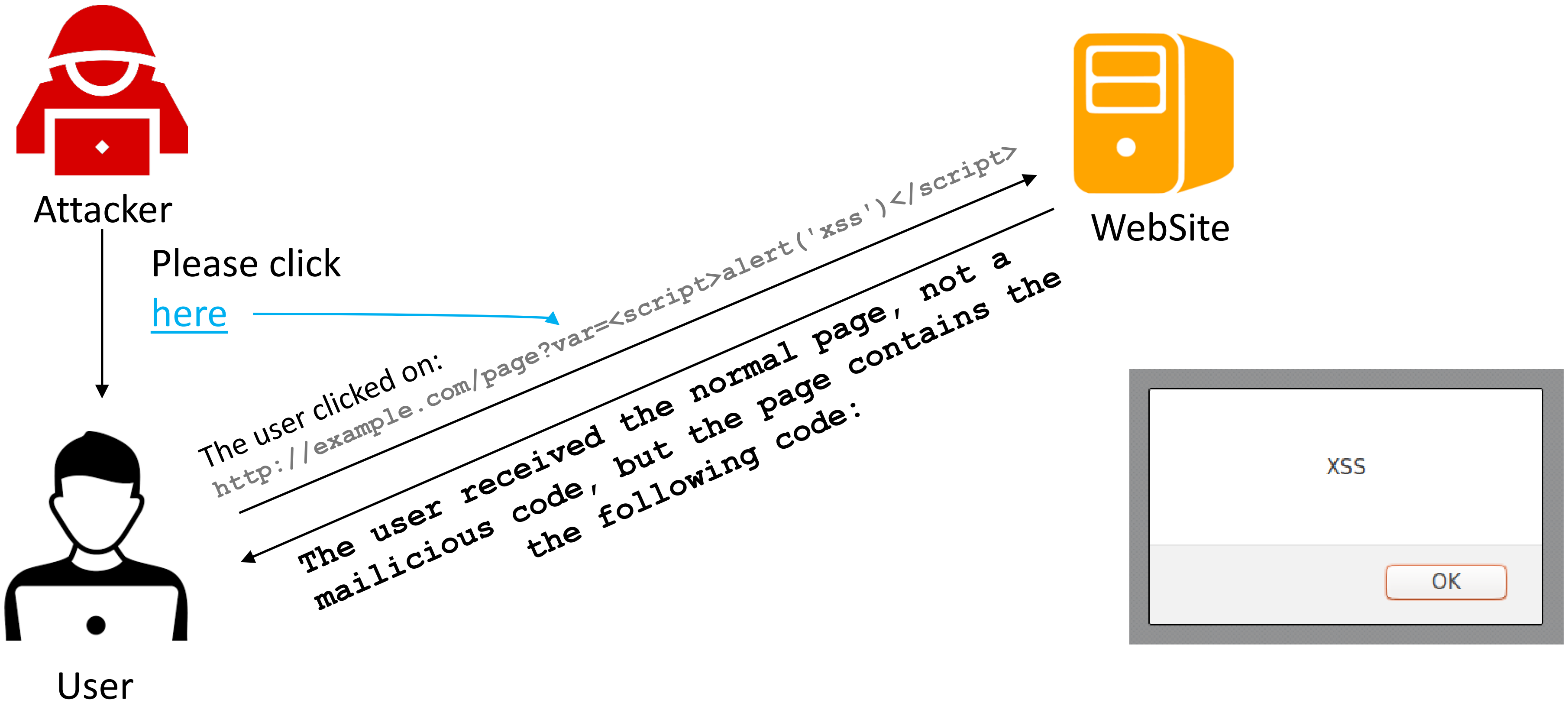
`http://example.com/page?var=<script>alert('xss')</script>`

WebSite

`The user received the normal page, not a mailicious code, but the page contains the the following code:`

User

DOM-based XSS (type-0)

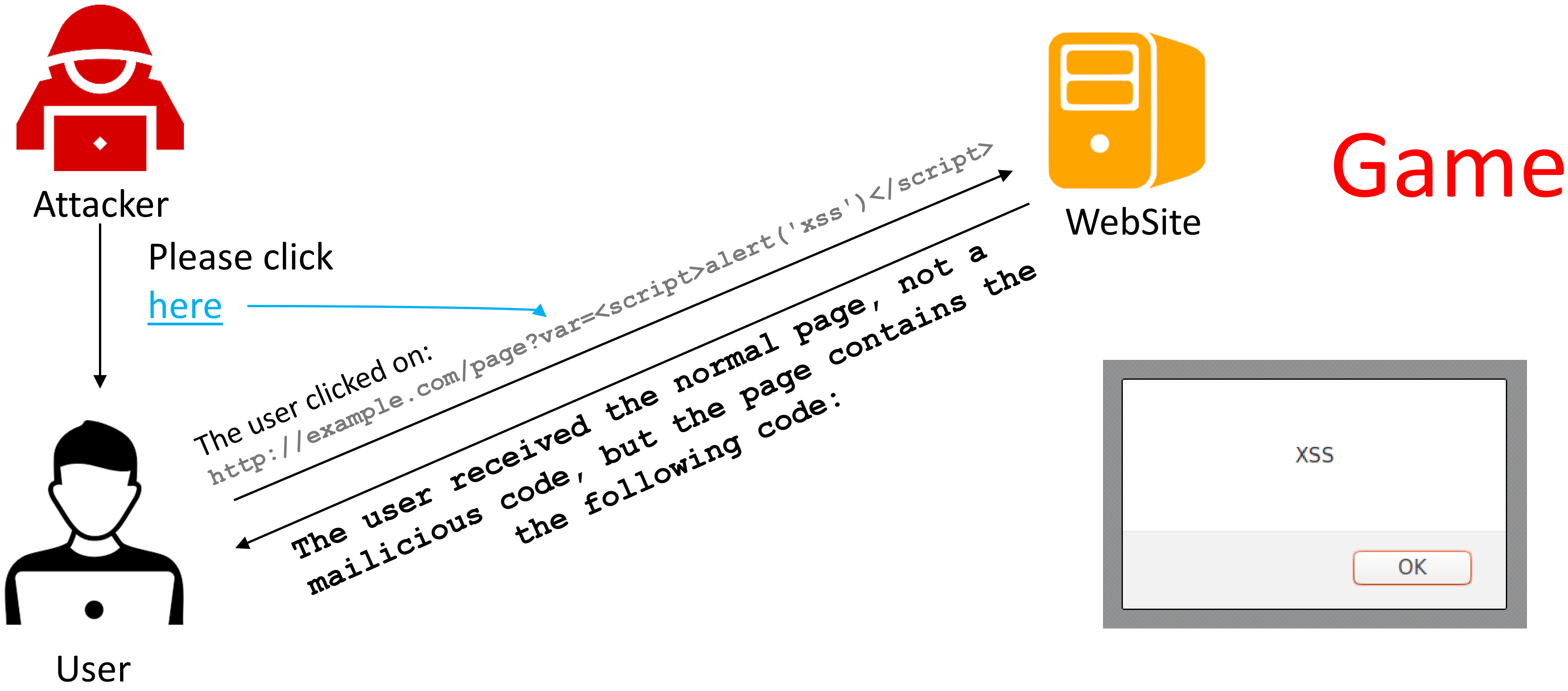


The user clicked on:
http://example.com/page?var=<script>alert('xss')</script>

The user received the normal page, not a mailicious code, but the page contains the the following code:

```
var pos=document.URL.indexOf("var=")+4;
document.write(document.URL.substring(pos,document.URL.length));
```

DOM-based XSS (type-0)


Attacker
Please click
here
The user clicked on:
http://example.com/page?var=<script>alert('xss')</script>
WebSite
The user received the normal page, not a mailicious code, but the page contains the the following code:
XSS
OK
User

Game Over

```
var pos=document.URL.indexOf("var=")+4;
document.write(document.URL.substring(pos,document.URL.length));
```