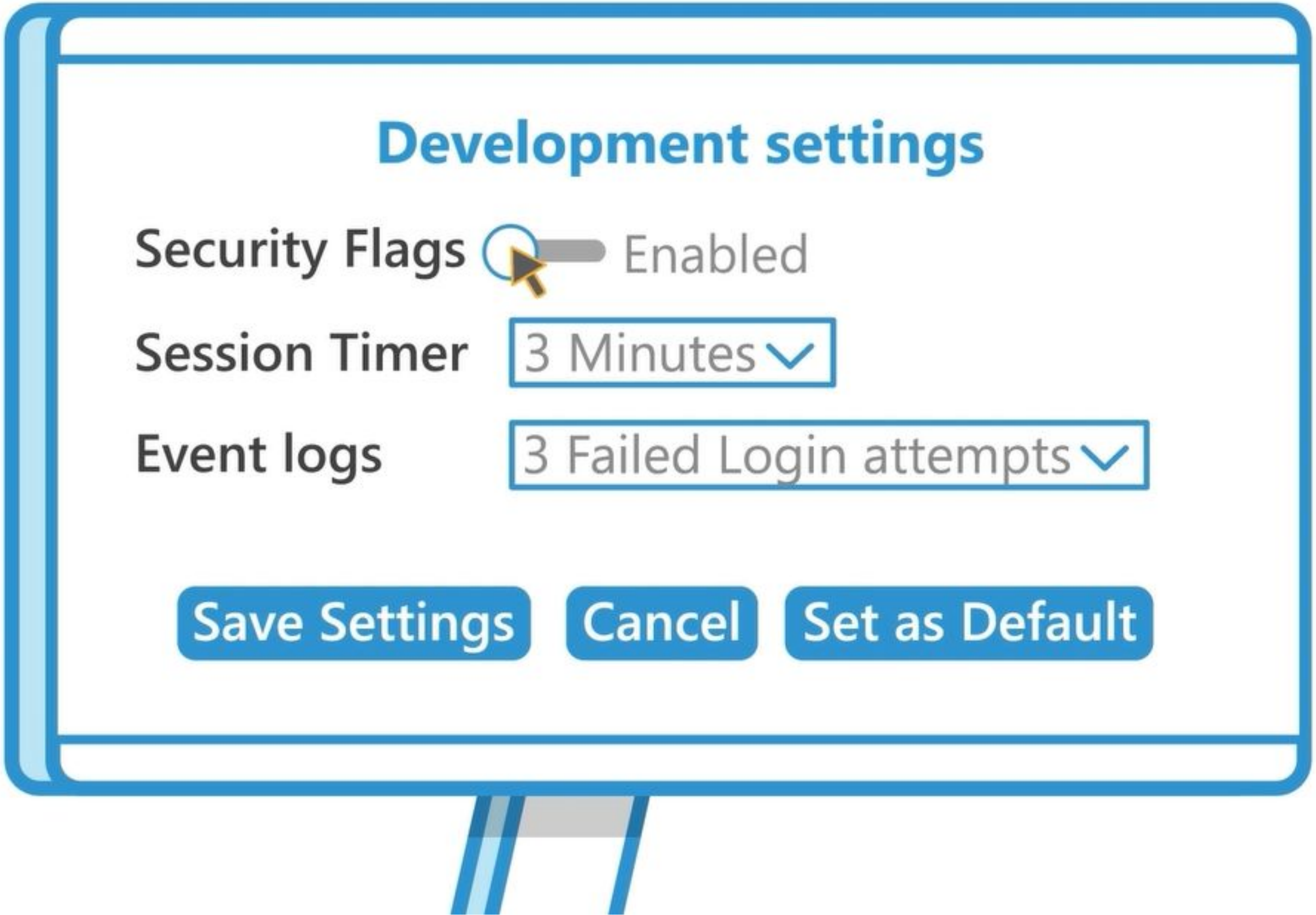
SECURE CODE WARRIOR®

DISABLED SECURITY FEATURES

WHAT DO WE MEAN BY DISABLED SECURITY FEATURES?

Disabled Security Features is a vulnerability where features that can help protect against hackers have been deactivated.



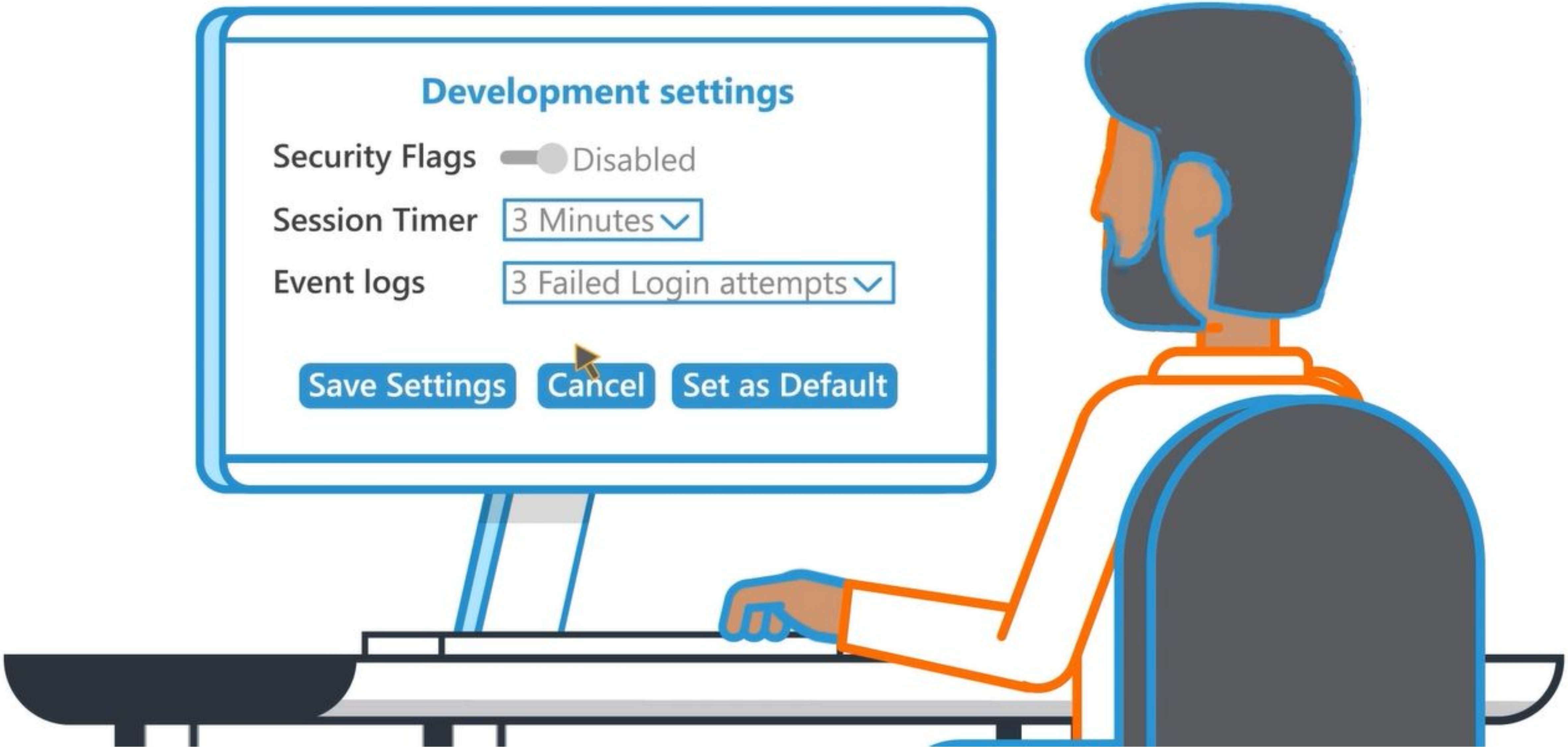
Development settings

Security Flags ○ Enabled

Session Timer 3 Minutes

Event logs 3 Failed Login attempts

Security features may have been disabled for operational reasons or they may be simply disabled by default.



Development settings

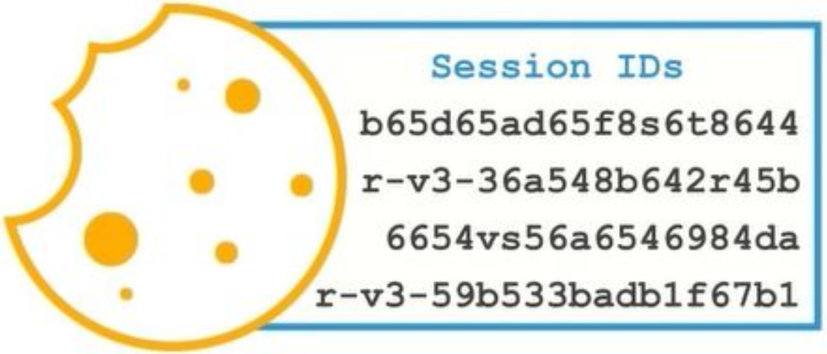
Security Flags Disabled

Session Timer 3 Minutes

Event logs 3 Failed Login attempts

LET'S LOOK AT AN EXAMPLE

A popular web application is storing the session ID in a cookie.



Session IDs

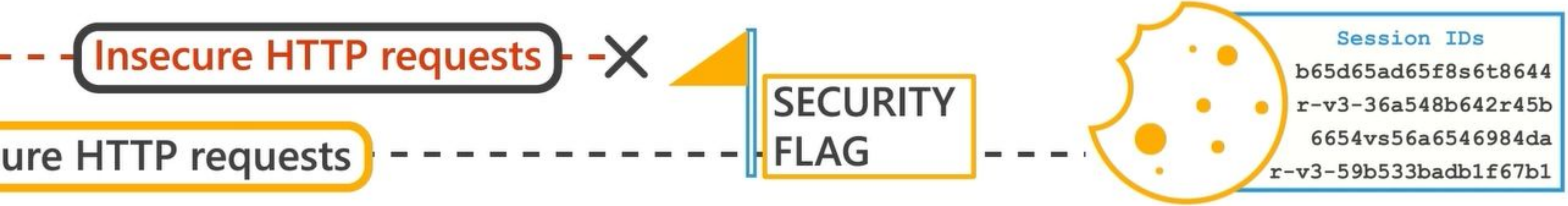
b65d65ad65f8s6t8644

r-v3-36a548b642r45b

6654vs56a6546984da

r-v3-59b533badb1f67b1

Despite being securely generated,



Insecure HTTP requests

ure HTTP requests

SECURITY FLAG

Session IDs

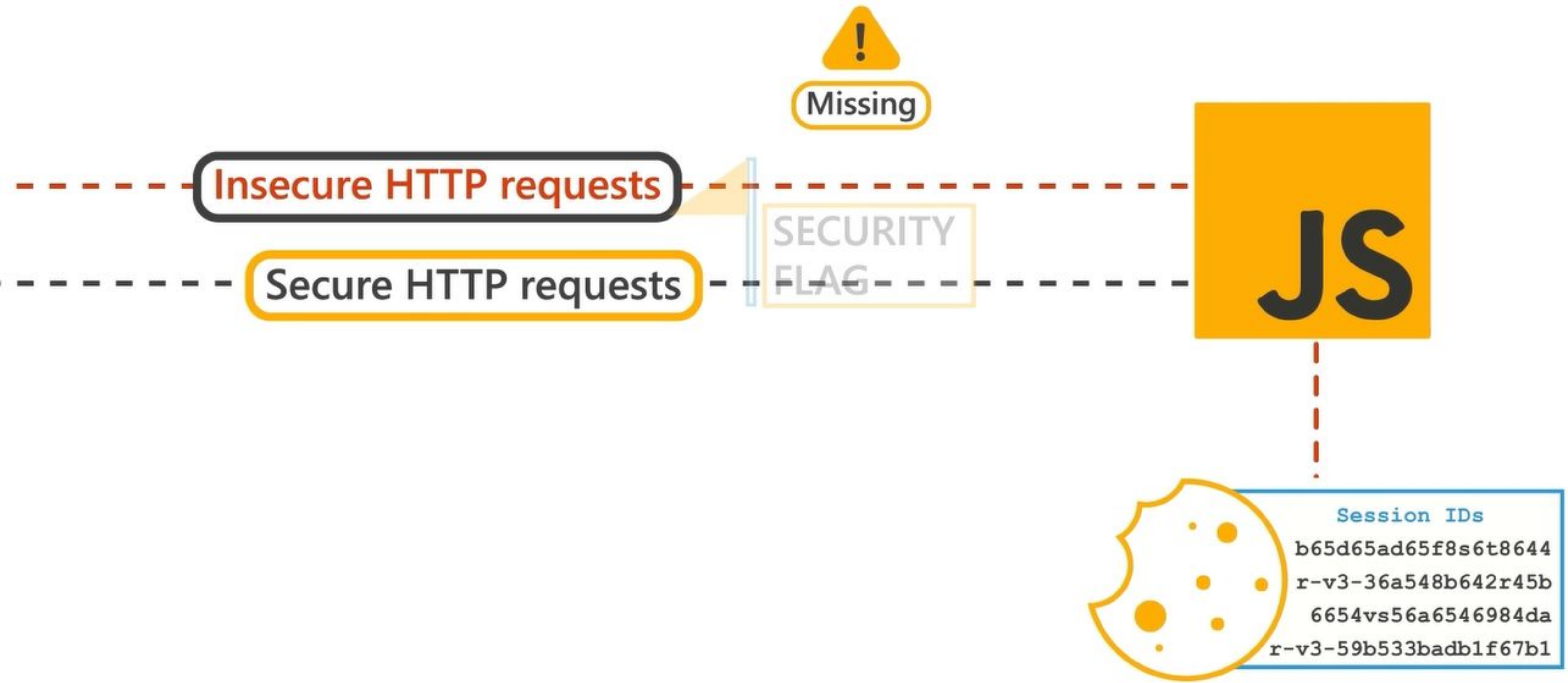
b65d65ad65f8s6t8644

r-v3-36a548b642r45b

6654vs56a6546984da

r-v3-59b533badb1f67b1

the cookie is missing the flags that restrict it to secure HTTP requests



Missing

Insecure HTTP requests

Secure HTTP requests

SECURITY FLAG

JS

Session IDs

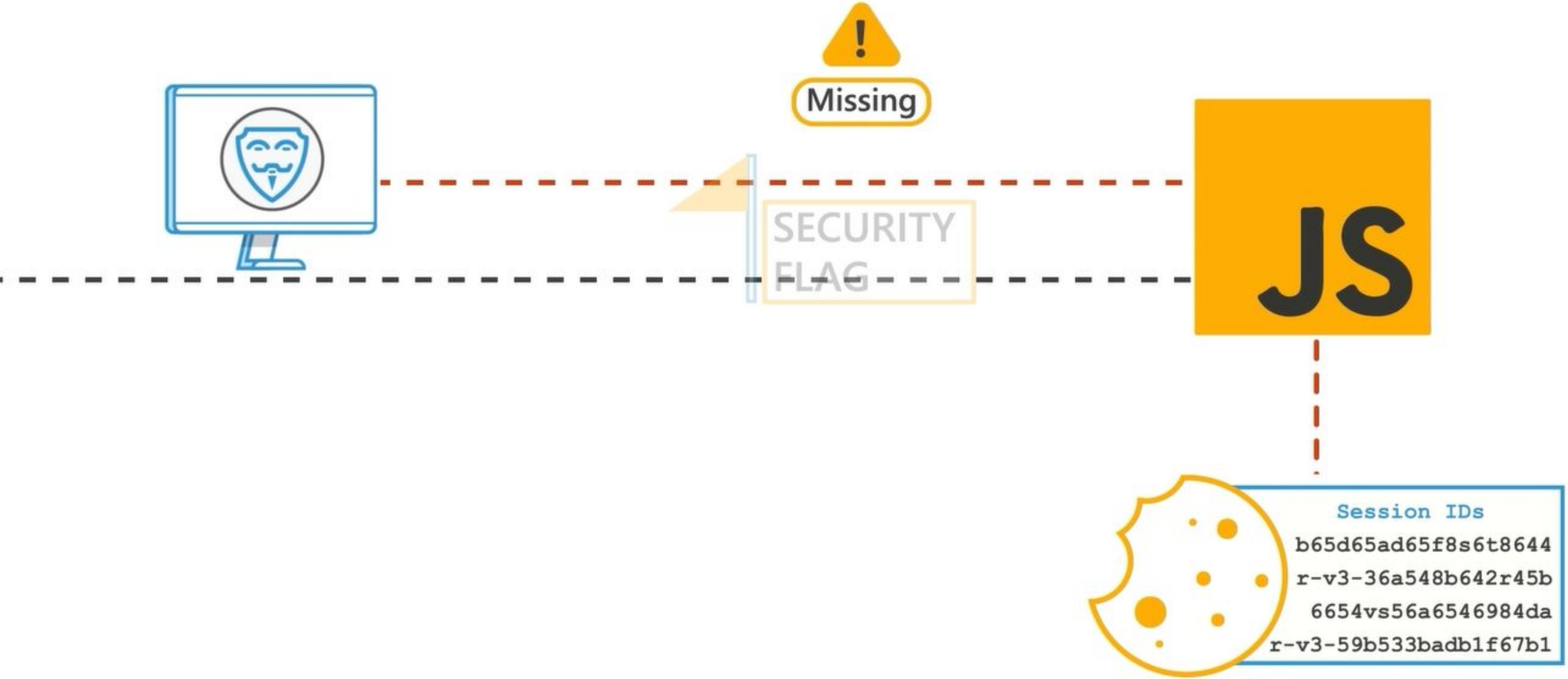
b65d65ad65f8s6t8644

r-v3-36a548b642r45b

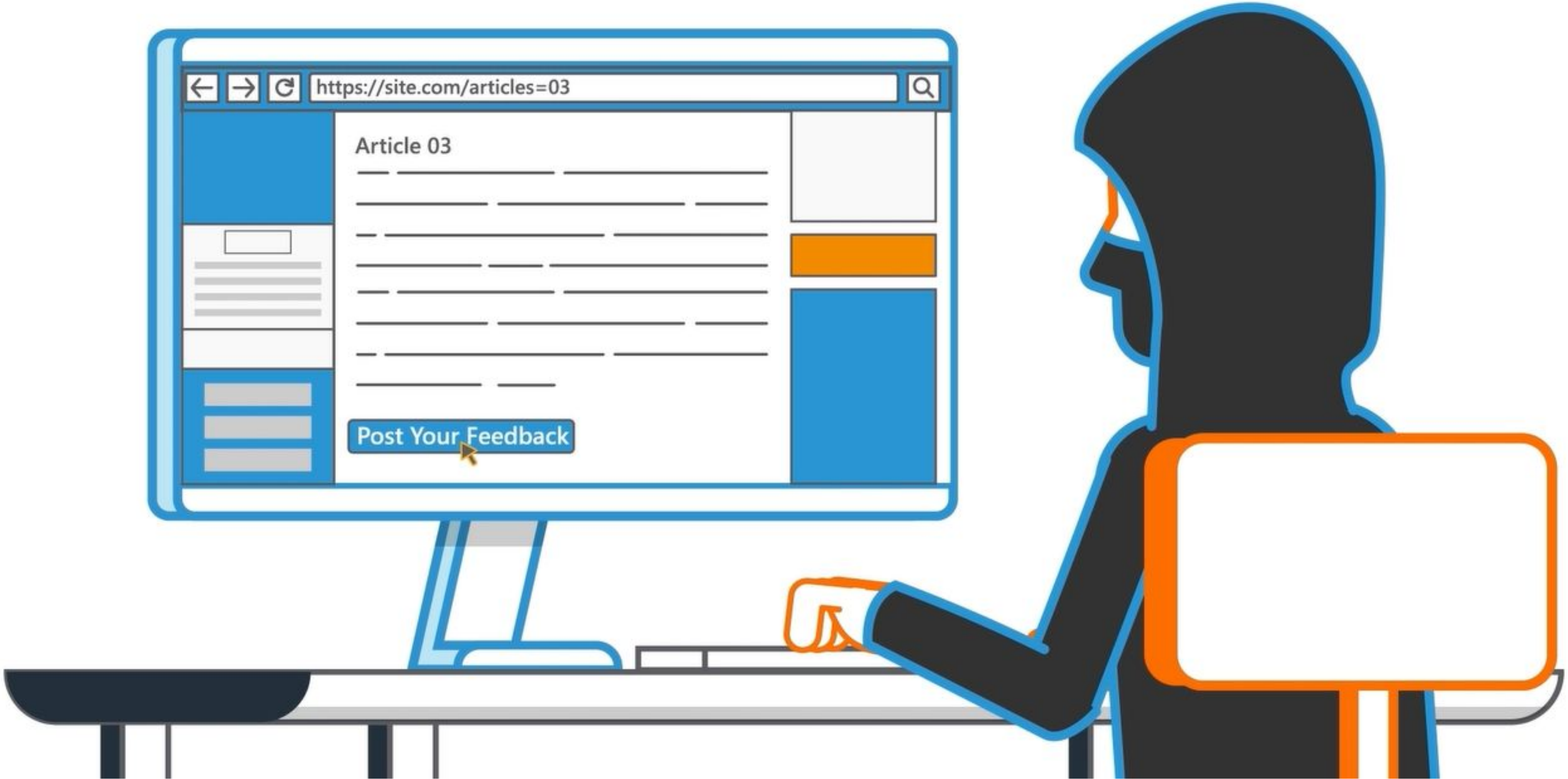
6654vs56a6546984da

r-v3-59b533badb1f67b1

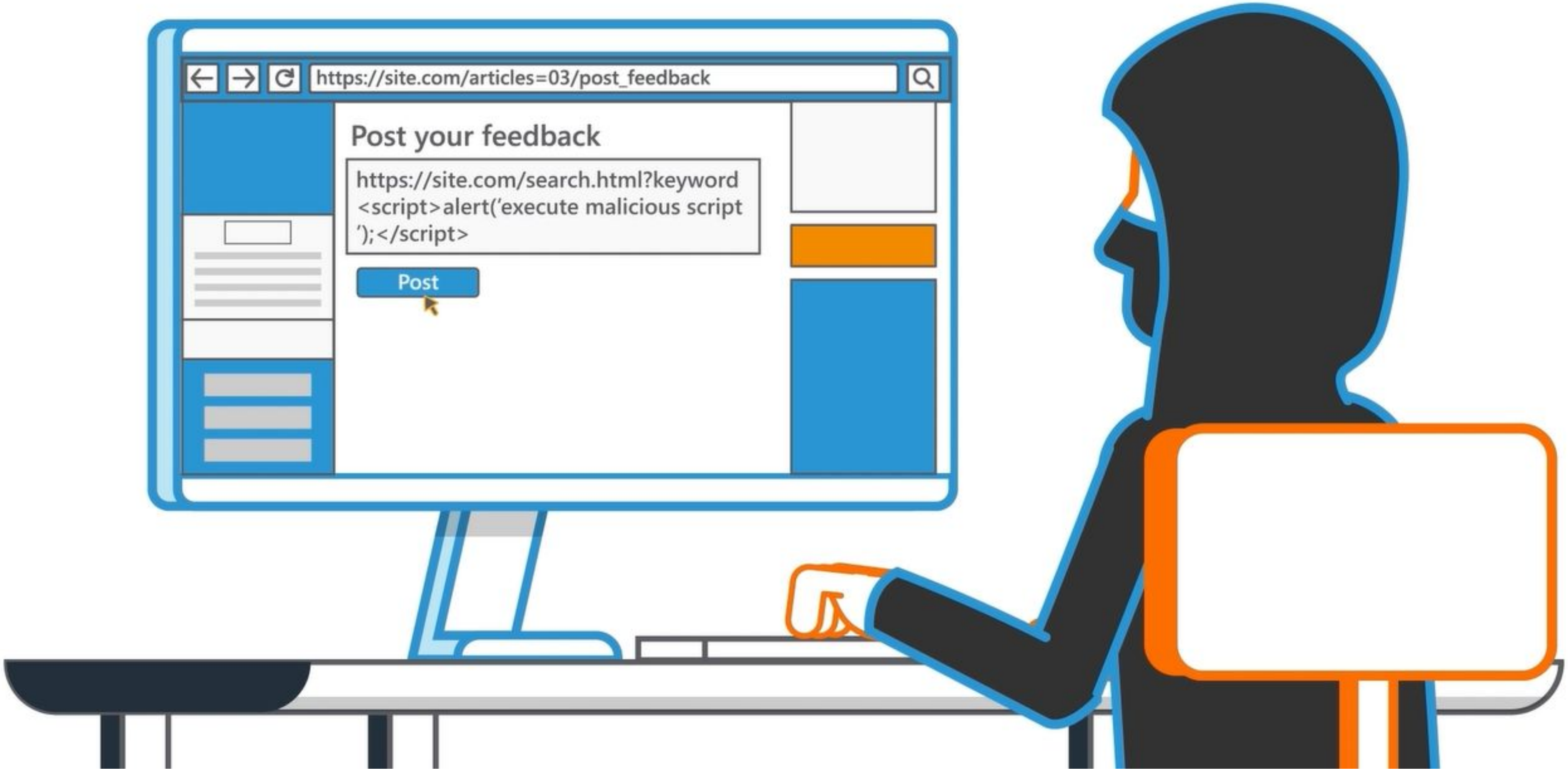
and prevent it from being accessed by browser scripts.



A hacker manages to find a vulnerable field in the site's feedback form



and injects some malicious scripts to run in the browser. This compromise is already bad.



```
https://site.com/search.html?keyword
<script>alert(‘execute malicious script
’);</script>
```

But to make matters worse, the scripts are also made to read the session cookie,

Session IDs
b65d65ad65f8s6t8644
r-v3-36a548b642r45b
6654vs56a6546984da
r-v3-59b533ba

transmitting its data to the hacker.

Session IDs

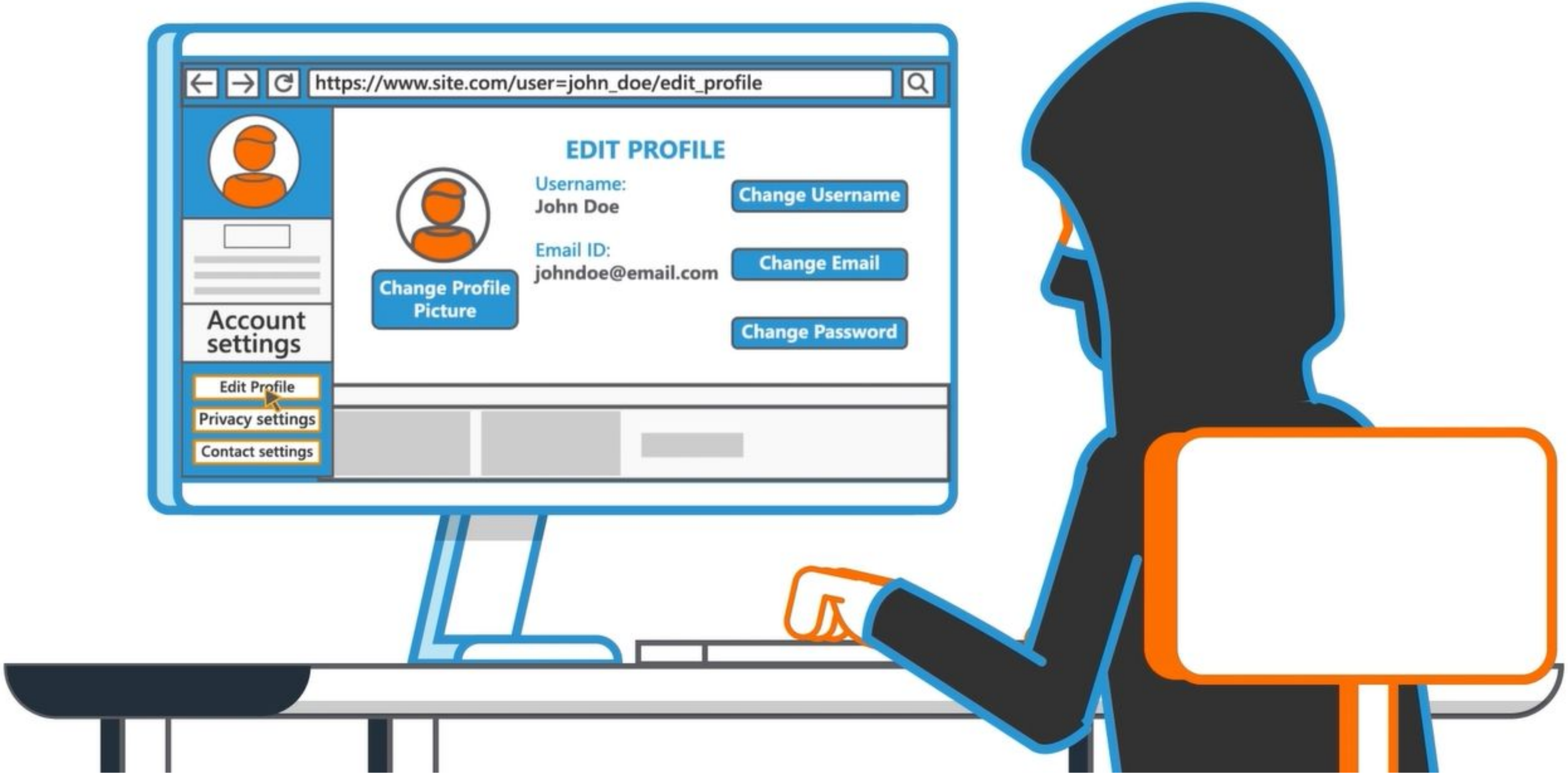
b65d65ad65f8s6t8644

r-v3-36a548b642r45b

6654vs56a6546984da

r-v3-59b533badb1f67b1

The hacker can now use the captured cookie data to pretend to be any of the users from the site,



stealing account details and performing actions as those users.

...w.site.com/user=john_doe/profile_settings/change_password
CHANGE PASSWORD
Enter new password: *******
Re-enter new password: *******
Done
settings
Edit P
ttings
HACKED!

To avoid attacks relating to Disabled Security Features

- It’s recommended to verify that all relevant restrictions are enabled.
- Additionally, developers should ensure that, where features need to be disabled, the data is coupled with extra checks to help prevent manipulation by hackers.

Congratulations, you have now completed this module!

SECURE
CODE
WARRIOR
®