

Flask Users, Sessions and Authentication

AUTHENTICATING WITH SESSIONS AND COOKIES



Mateo Prigl
SOFTWARE DEVELOPER



Demo



Implementing login with sessions



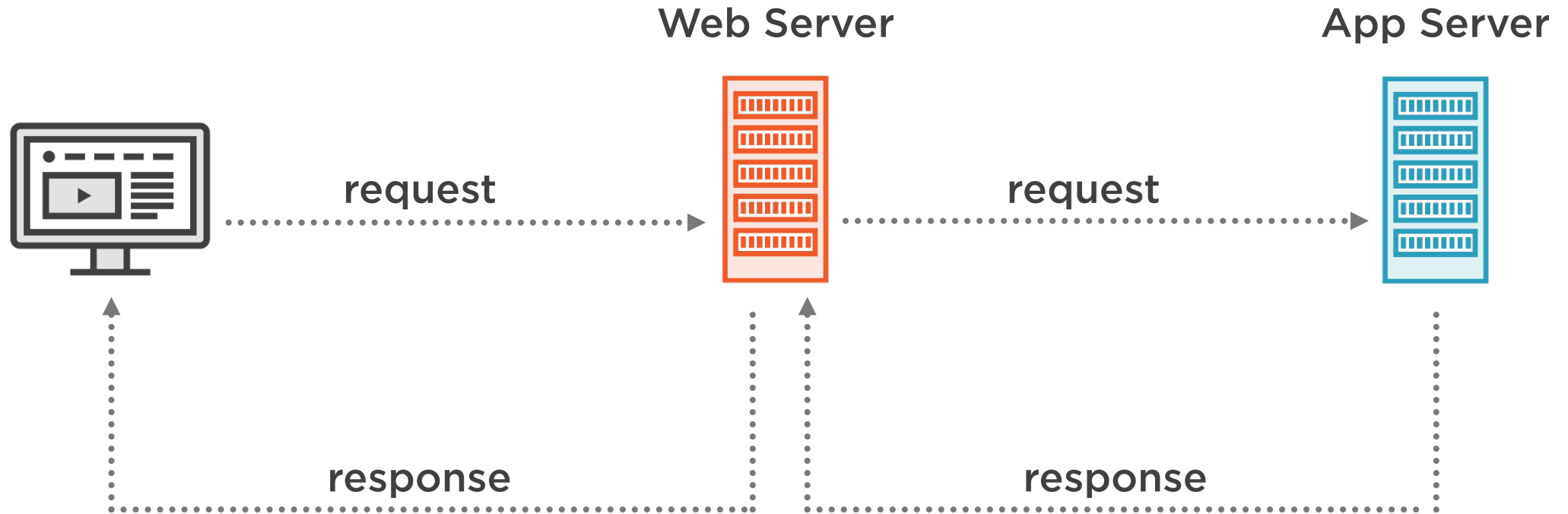
What we need
to implement

Current_user "global" variable

Available in all of the views and templates



Werkzeug



Werkzeug

`werkzeug.serving.run_simple()`



Werkzeug Server



request

Thread Pool



Werkzeug

`werkzeug.serving.run_simple()`

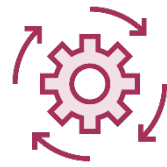


Werkzeug Server



request

Thread Pool



Werkzeug

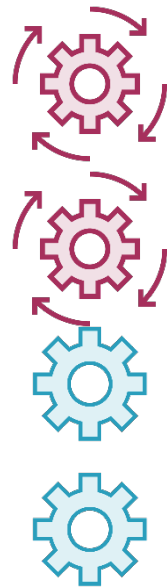
`werkzeug.serving.run_simple()`



Werkzeug Server



Thread Pool



Python

threads

greenlets



Werkzeug

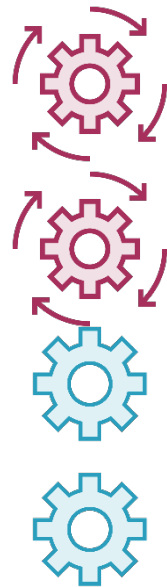
`werkzeug.serving.run_simple()`



Werkzeug Server



Thread Pool



Python

threads

greenlets

"thread local storage"



Flask Context "globals"

Objects

Purpose


<code>current_app</code>	Holds the active application instance
<code>g</code>	Provides a temporary storage during the request lifetime
<code>request</code>	Holds the contents of an HTTP request
<code>session</code>	Dictionary for "remembering" values between requests



Current user with the g object

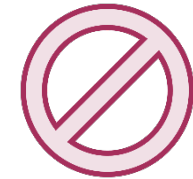
First execution of the function

get_current_user() function

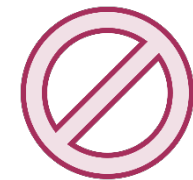
```
_current_user = g._current_user
if _current_user is None:
    if session.get("user_id"):
        user = User.query.get(session.get("user_id"))
        if user:
            _current_user = g._current_user = user

if _current_user is None:
    _current_user = User()
return _current_user
```

g (application context)




_current_user (function scope)



Current user with the g object

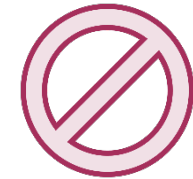
First execution of the function

get_current_user() function

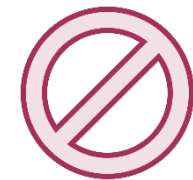
```
_current_user = g._current_user
if _current_user is None:
    if session.get("user_id"):
        user = User.query.get(session.get("user_id"))
        if user:
            _current_user = g._current_user = user

if _current_user is None:
    _current_user = User()
return _current_user
```

g (application context)



_current_user (function scope)



Current user with the g object

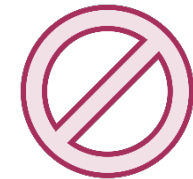
First execution of the function

`get_current_user()` function

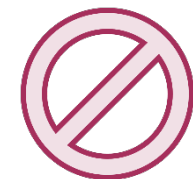
```
_current_user = g._current_user
if _current_user is None:
    if session.get("user_id"):
        👉 user = User.query.get(session.get("user_id"))
        if user:
            _current_user = g._current_user = user

if _current_user is None:
    _current_user = User()
return _current_user
```

g (application context)



_current_user (function scope)



Current user with the g object

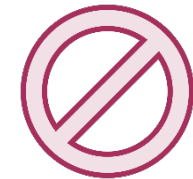
First execution of the function

`get_current_user()` function

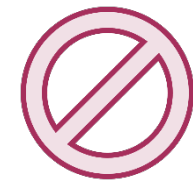
```
_current_user = g._current_user
if _current_user is None:
    if session.get("user_id"):
        user = User.query.get(session.get("user_id"))
        if user:
            🖱️ _current_user = g._current_user = user

if _current_user is None:
    _current_user = User()
return _current_user
```

g (application context)



_current_user (function scope)



Current user with the g object

First execution of the function

get_current_user() function

```
_current_user = g._current_user
if _current_user is None:
    if session.get("user_id"):
        user = User.query.get(session.get("user_id"))
        if user:
            🖱️ _current_user = g._current_user = user

if _current_user is None:
    _current_user = User()
return _current_user
```

g (application context)

g._current_user

_current_user (function scope)



Current user with the g object

First execution of the function

get_current_user() function

```
_current_user = g._current_user
if _current_user is None:
    if session.get("user_id"):
        user = User.query.get(session.get("user_id"))
        if user:
            🖱️ _current_user = g._current_user = user

if _current_user is None:
    _current_user = User()
return _current_user
```

g (application context)

g._current_user



_current_user (function scope)



Current user with the g object

First execution of the function

get_current_user() function

```
_current_user = g._current_user
if _current_user is None:
    if session.get("user_id"):
        user = User.query.get(session.get("user_id"))
        if user:
            _current_user = g._current_user = user
```

👉

```
if _current_user is None:
    _current_user = User()
return _current_user
```

g (application context)

g._current_user



_current_user (function scope)



Current user with the g object

First execution of the function

get_current_user() function

```
_current_user = g._current_user
if _current_user is None:
    if session.get("user_id"):
        user = User.query.get(session.get("user_id"))
        if user:
            _current_user = g._current_user = user

if _current_user is None:
    _current_user = User()
return _current_user
```



g (application context)

g._current_user





_current_user (function scope)





Current user with the g object

Second execution of the function

get_current_user() function

```
 _current_user = g._current_user
 if _current_user is None:
    if session.get("user_id"):
        user = User.query.get(session.get("user_id"))
        if user:
            _current_user = g._current_user = user
```

```
 if _current_user is None:
    _current_user = User()
 return _current_user
```

g (application context)

g._current_user



_current_user (function scope)



Current user with the g object

Second execution of the function

get_current_user() function

```
_current_user = g._current_user
if _current_user is None:
    if session.get("user_id"):
        user = User.query.get(session.get("user_id"))
        if user:
            _current_user = g._current_user = user

if _current_user is None:
    _current_user = User()
return _current_user
```



g (application context)

g._current_user



_current_user (function scope)



Demo



"Remembering" with cookies



Remember Me

Browser



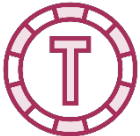
remember_token

d76WfovQihEIPbf0szvFVHL4XKQ



user_id

23



remember_token

d76WfovQihEIPbf0szvFVHL4XKQ



remember_hash

pbkdf2:sha256:150000\$ACZJLTuK\$
6a3e8ef330dfc3dcab637f71746c20
14d88c0493f8ac4daac359a1f947711
45c

User instance

id	23
username	...
email	...
description	...
location	...
password_hash	...
remember_hash	pbkdf2:sha256:150000\$ACZJLTuK\$6a3e8ef330dfc3dcab637f71746c2014d88c0493f8ac4daac359a1f94771145c

* The cookie data will be encrypted



Remember Me

Browser



remember_token

d76WfovQihEIPbf0szvFVHL4XKQ



user_id

23



remember_token

d76WfovQihEIPbf0szvFVHL4XKQ



user_id

23


* The cookie data will be encrypted




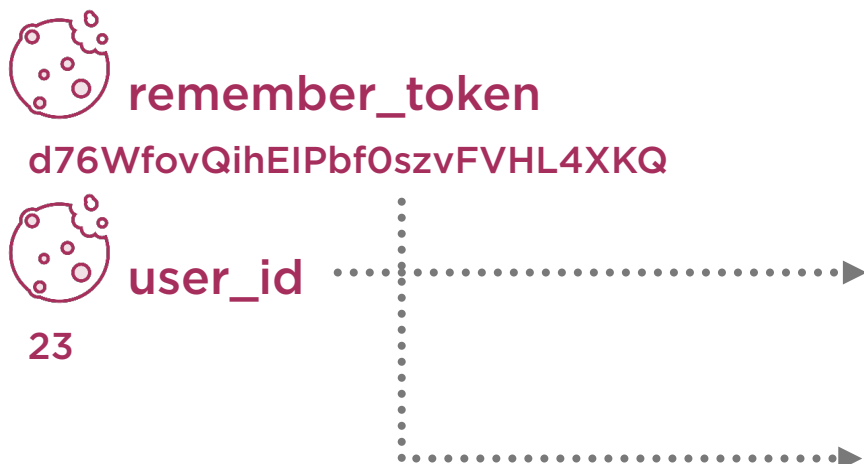
Remember Me

Browser



 **remember_token**
d76WfovQihEIPbf0szvFVHL4XKQ

 **user_id**
23



User instance

id	23
username	...
email	...
description	...
location	...
password_hash	...
remember_hash	pbkdf2:sha256:150000\$ACZJLTuK\$6a3e8ef330dfc3dcab637f71746c2014d88c0493f8ac4daac359a1f94771145c

* The cookie data will be encrypted



Remember Me

Browser



remember_token

d76WfovQihEIPbf0szvFVHL4XKQ



user_id

23

* The cookie data will be encrypted

User instance

id	23
username	...
email	...
description	...
location	...
password_hash	...
remember_hash	pbkdf2:sha256:150000\$ACZJLTuK\$6a3e8ef330dfc3dcab637f71746c2014d88c0493f8ac4daac359a1f94771145c



Remember Me

Browser 1



remember_token

d76WfovQihEIPbfOszvFVHL4XKQ

Browser 2



User instance

id	23
username	...
email	...
description	...
location	...
password_hash	...
remember_hash	pbkdf2:sha256:150000\$ACZJLTuK\$6a3e8ef330dfc3dcab637f71746c2014d88c0493f8ac4daac359a1f94771145c



Remember Me

Browser 1



remember_token

d76WfovQihEIPbfOszvFVHL4XKQ

Browser 2



remember_token

VWFtGuDJwiRSgcGcJNxPITE79t4

User instance

id	23
username	...
email	...
description	...
location	...
password_hash	...
remember_hash	pbkdf2:sha256:150000\$ACZJLTuK\$6a3e8ef330dfc3dcab637f71746c2014d88c0493f8ac4daac359a1f94771145c



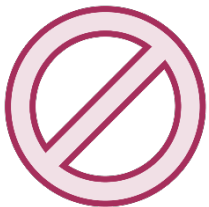
Remember Me

Browser 1



remember_token

d76WfovQihEIPbfOszvFVHL4XKQ



Browser 2



remember_token

VWFtGuDJwiRSgcGcJNxPITE79t4



User instance

id	23
username	...
email	...
description	...
location	...
password_hash	...
remember_hash	pbkdf2:sha256:150000\$zeoltcuw\$911367b0d9a4f0c3e5eeee0ec254a1ca5ad00e52ee47c2c3eb15887a5a28fe9b



Remember Me

Remember instance

id	1
user_id	23
remember_hash	pbkdf2:sha256:1...

Browser 1



 remember_token

d76WfovQihEIPbfOszvFVHL4XKQ

Remember instance

id	1
user_id	23
remember_hash	pbkdf2:sha256:1...

Browser 2



 remember_token

VWFtGuDJwiRSgcGcJNxPITE79t4

User instance

id	23
username	...
email	...
description	...
location	...
password_hash	...



Remember Me

Remember instance

id	1
user_id	23
remember_hash	pbkdf2:sha256:1...

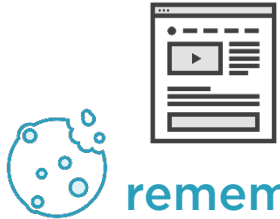
Remember instance

id	1
user_id	23
remember_hash	pbkdf2:sha256:1...

User instance

id	23
username	...
email	...
description	...
location	...
password_hash	...

Browser 1

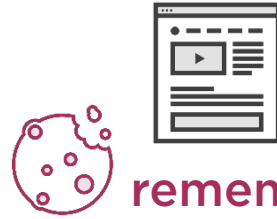


remember_token

d76WfovQihEIPbfOszvFVHL4XKQ



Browser 2



remember_token

VWFtGuDJwiRSgcGcJNxPITE79t4

