

SESSIONS AND AUTH DATA FLOW

Not web security!

AAA

- **Authentication**

- “this person is who they say they are”

- **Authorization**

- “this person is allowed to do X, Y, Z”

- **Accounting**

- “who the heck is using all our bandwidth?”

AAA

- **Authentication**

- “this person is who they say they are”

- **Authorization**

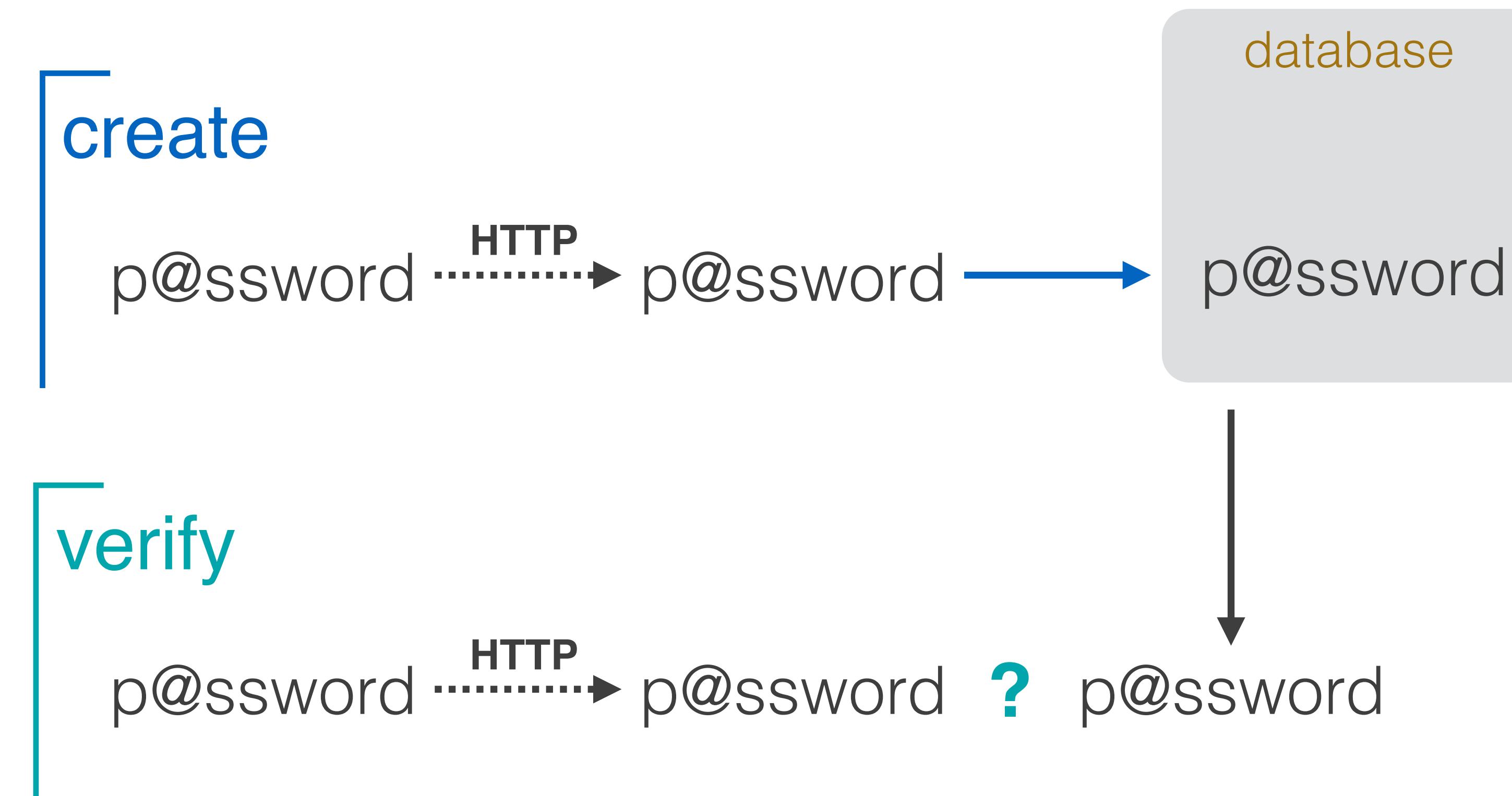
- “this person is allowed to do X, Y, Z”

- **Accounting**

- “who the heck is using all our bandwidth?”



LOGIN/SIGNUP



STAYING LOGGED IN



THE PROBLEM

What if we want to store some information about each client/server relationship (session)?



IDEAS?



IDEAS?

- **script variables**



IDEAS?

- **script variables**
- **database documents**



SCRIPT VARIABLES?



SCRIPT VARIABLES?

Data will not persist across browser pages



DATABASE DOCUMENTS?



DATABASE DOCUMENTS?

*Yes, but login credentials would have to be sent
with EVERY request*





cookie!



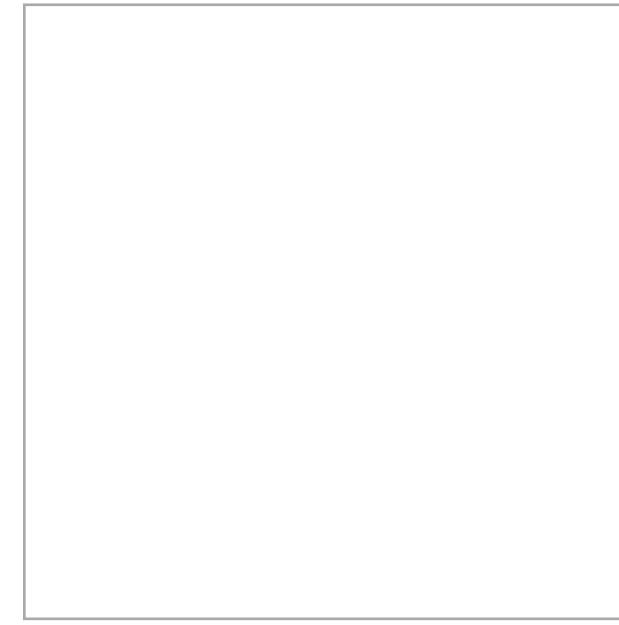


= small text file

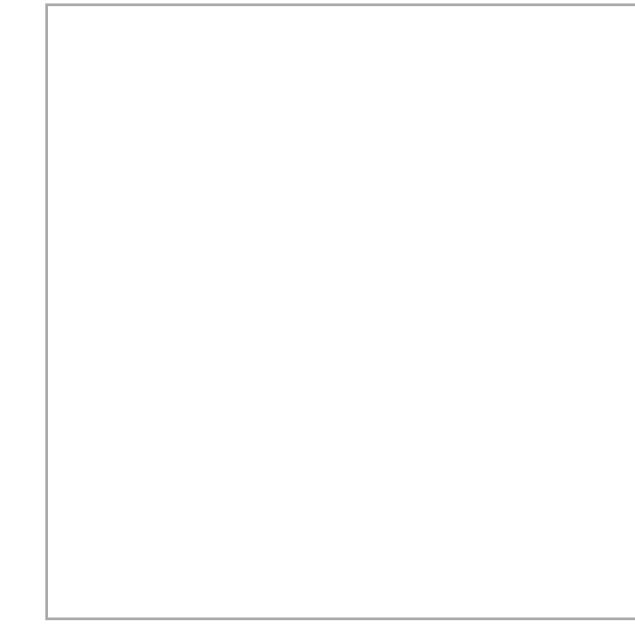


HTTP

client



“the internet”



server





HTTP

client

request

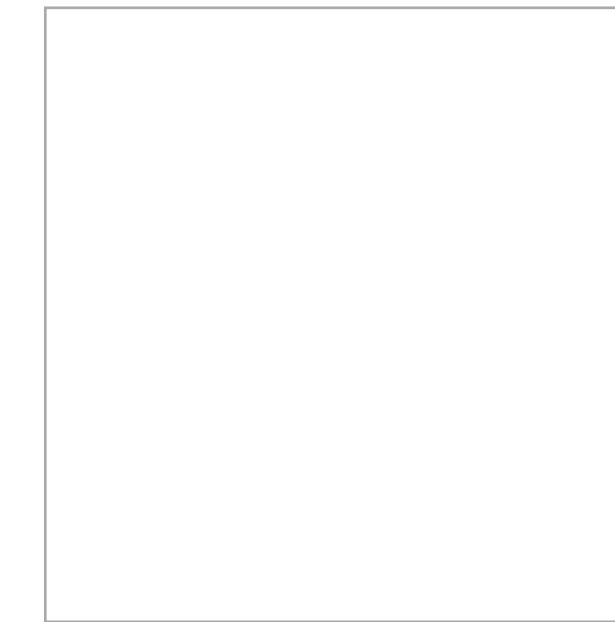
“the internet”

server

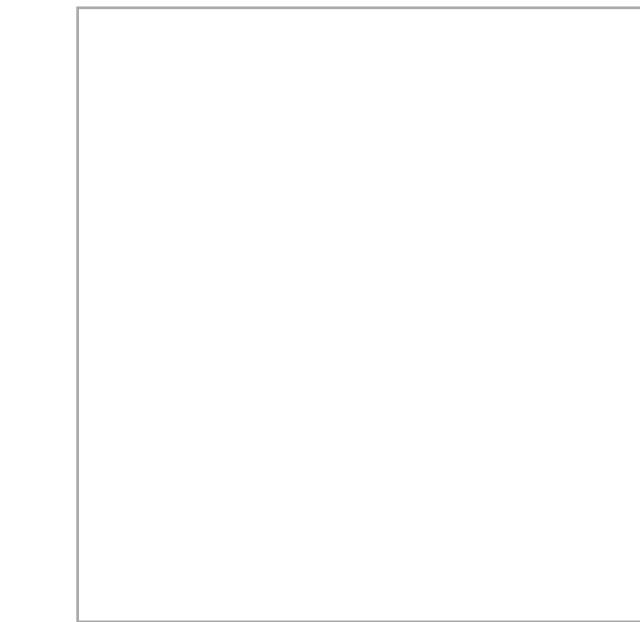


HTTP

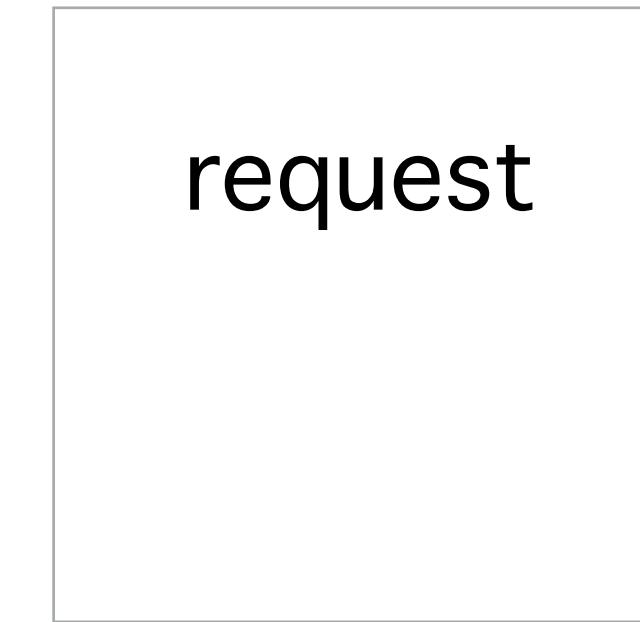
client



“the internet”



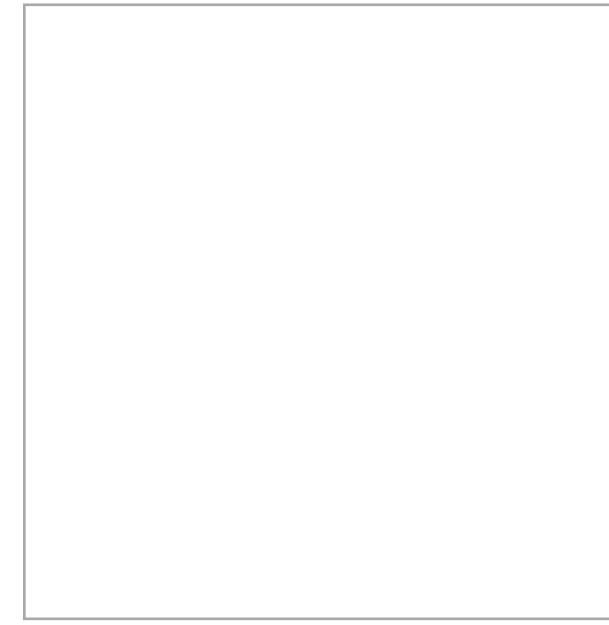
server



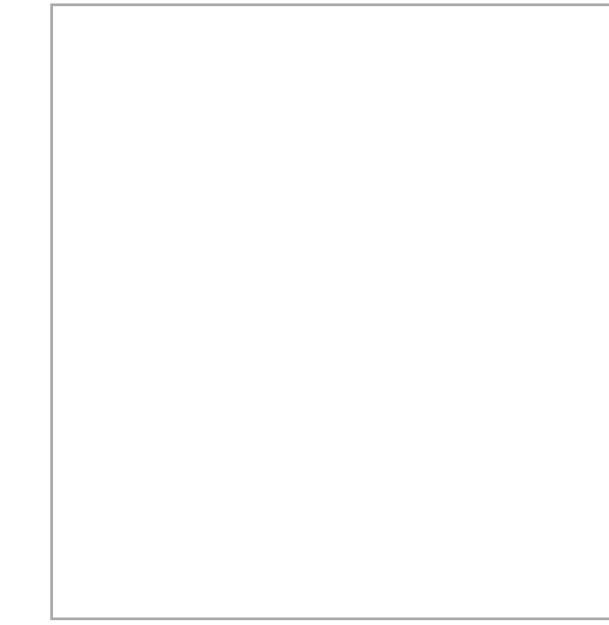


HTTP

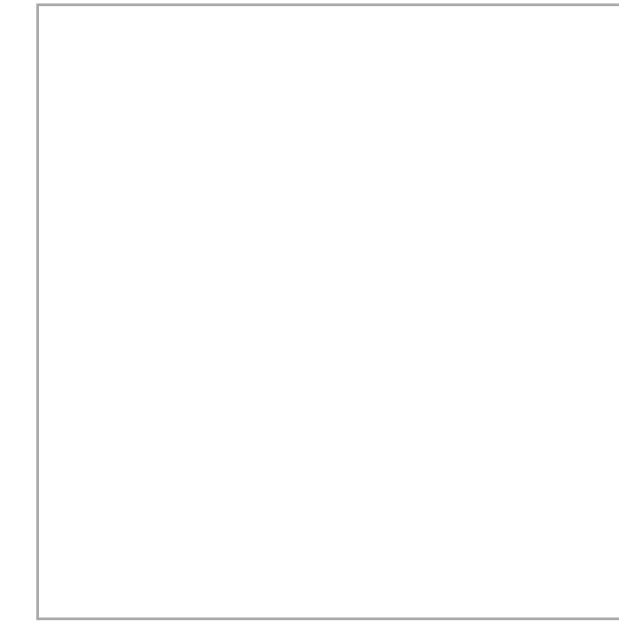
client



“the internet”



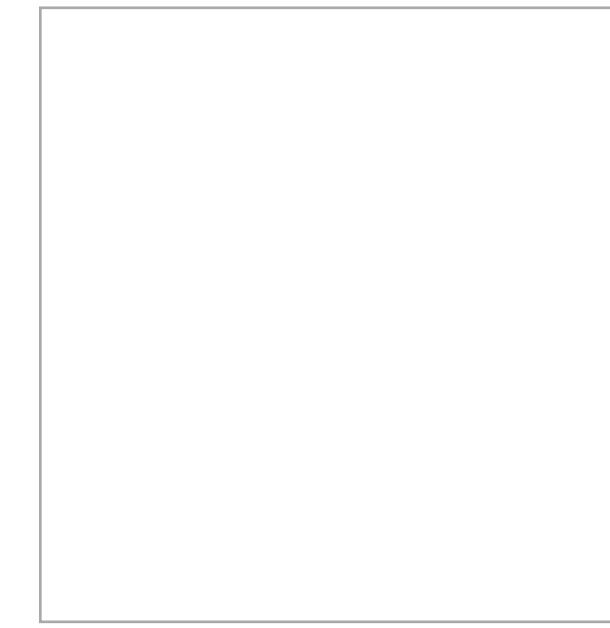
server



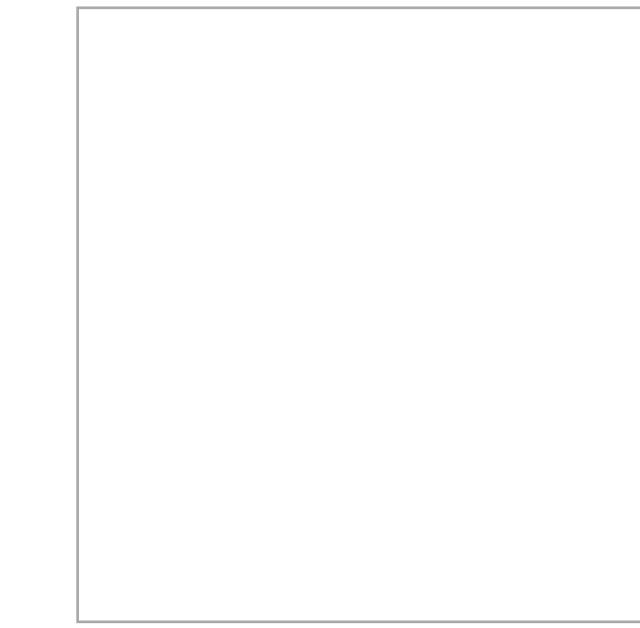


HTTP

client



“the internet”



server





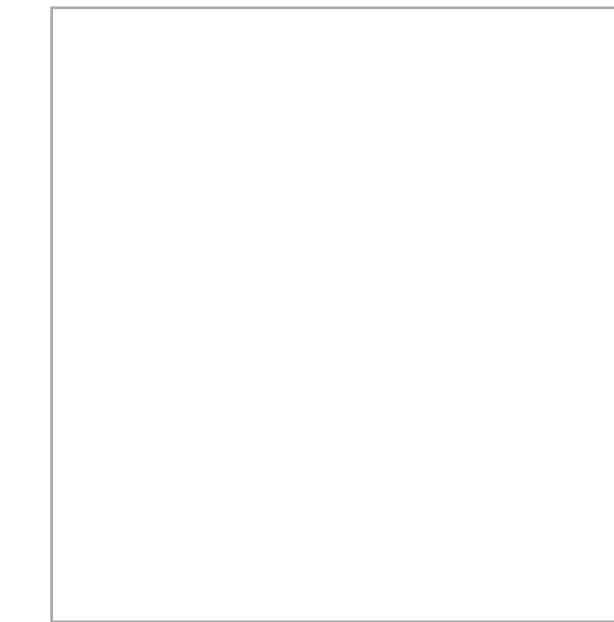
HTTP

client



response

“the internet”



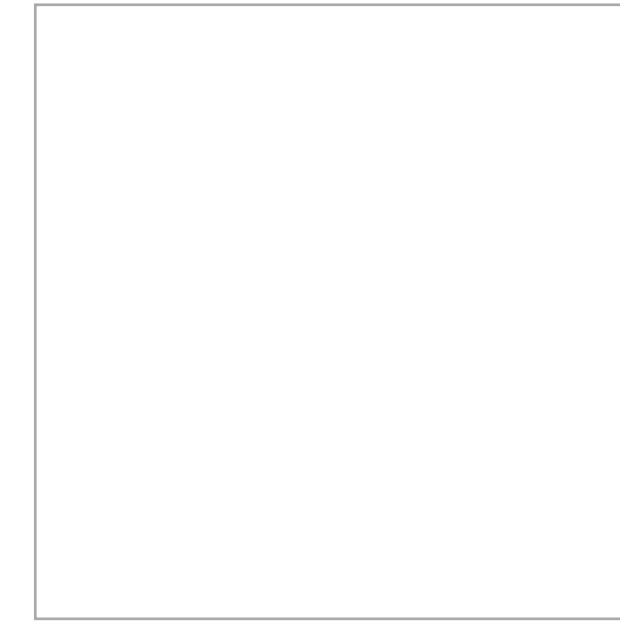
server



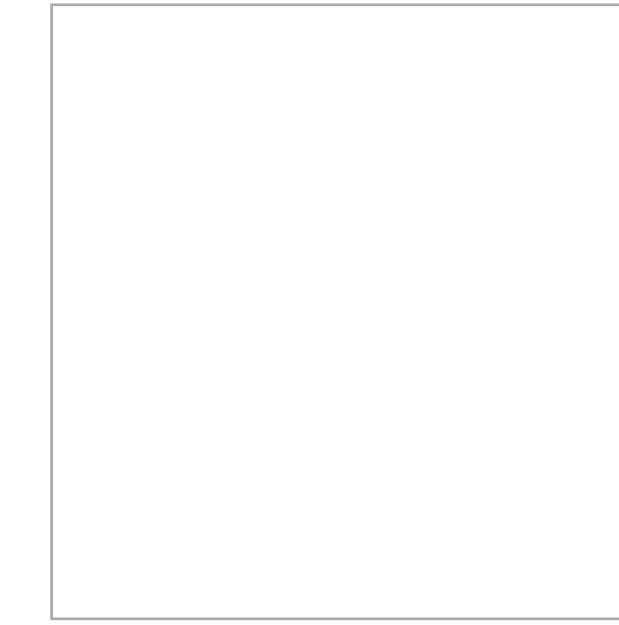


WITH COOKIES

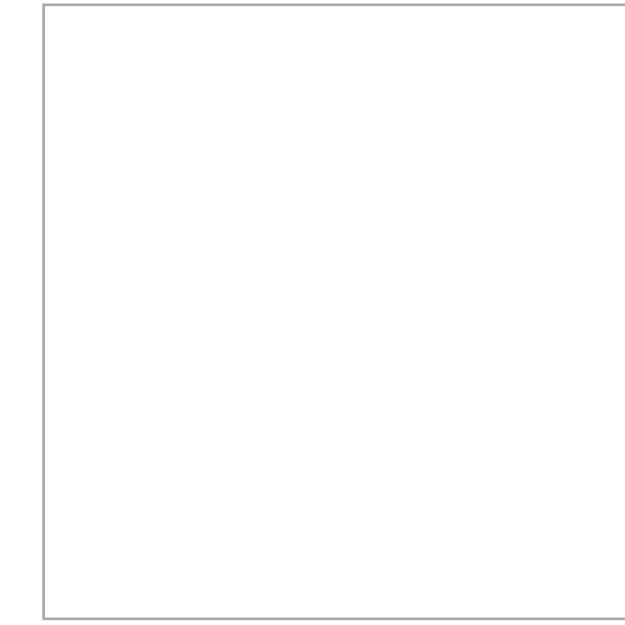
client



“the internet”



server





WITH COOKIES

client

request

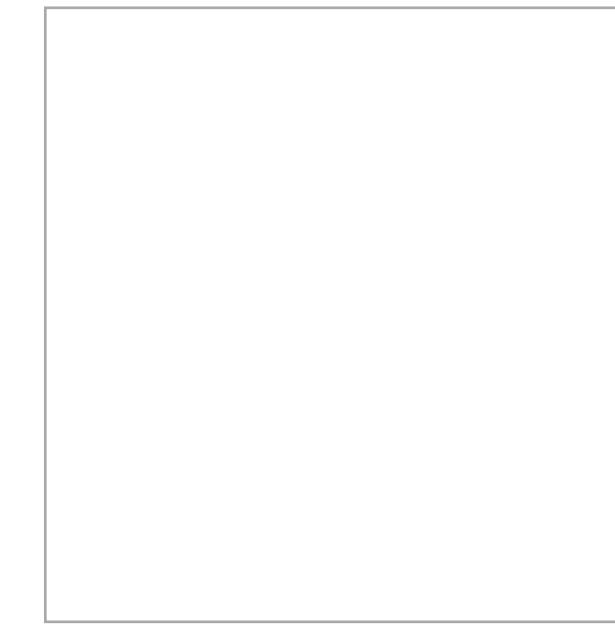
“the internet”

server

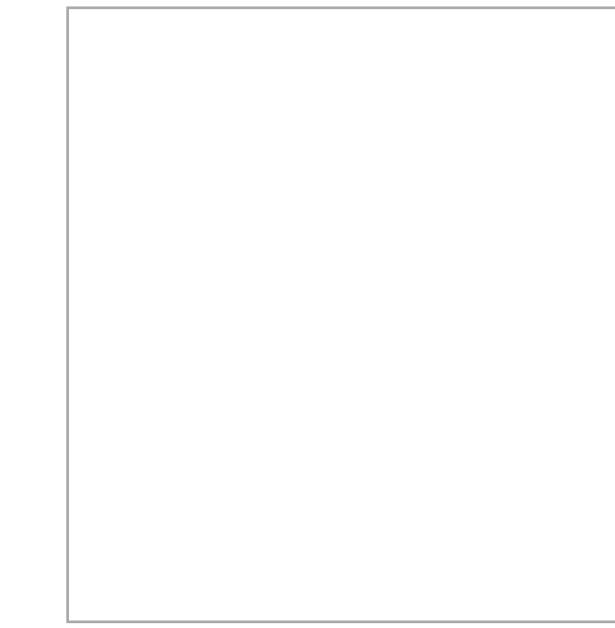


WITH COOKIES

client



“the internet”



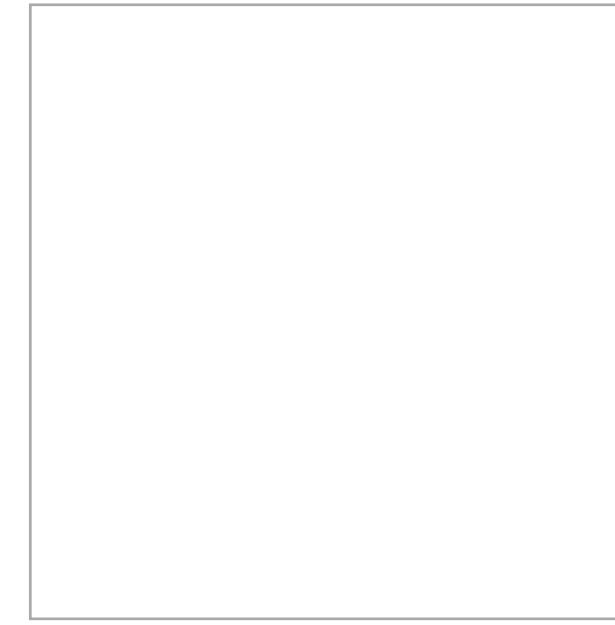
server



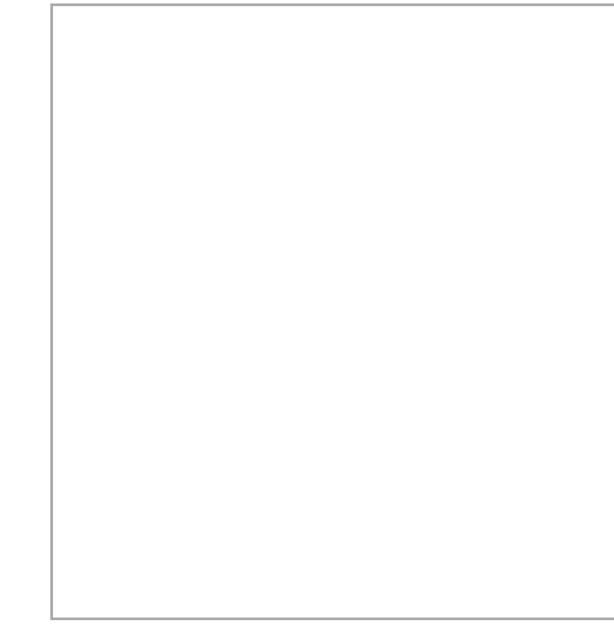


WITH COOKIES

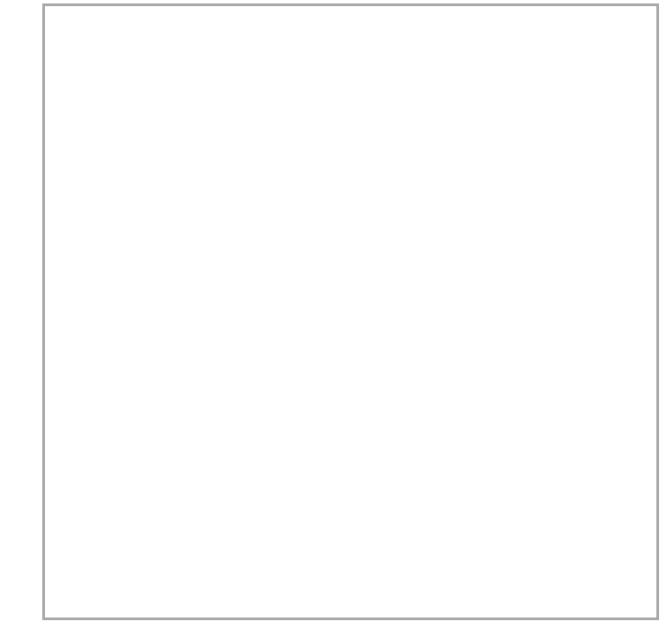
client



“the internet”

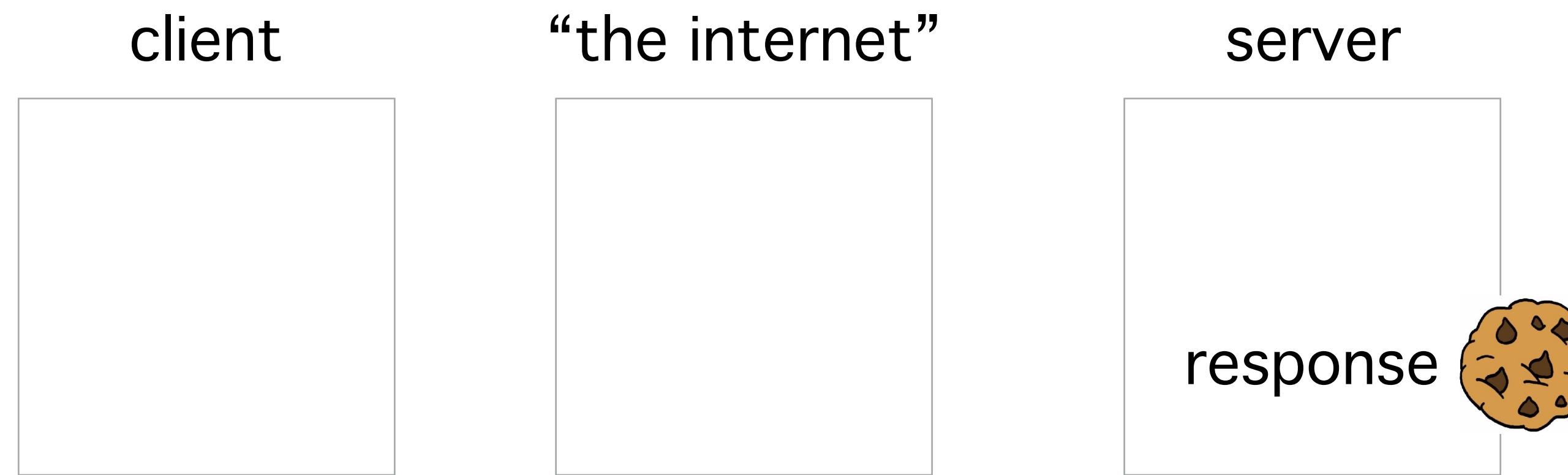


server



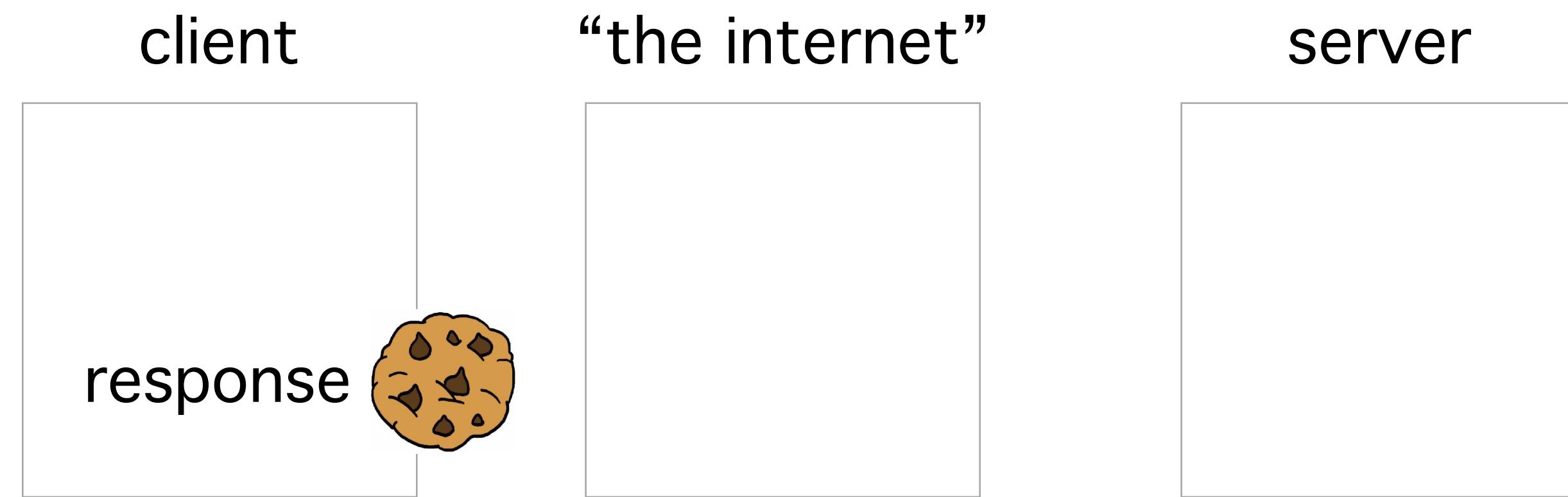


WITH COOKIES





WITH COOKIES



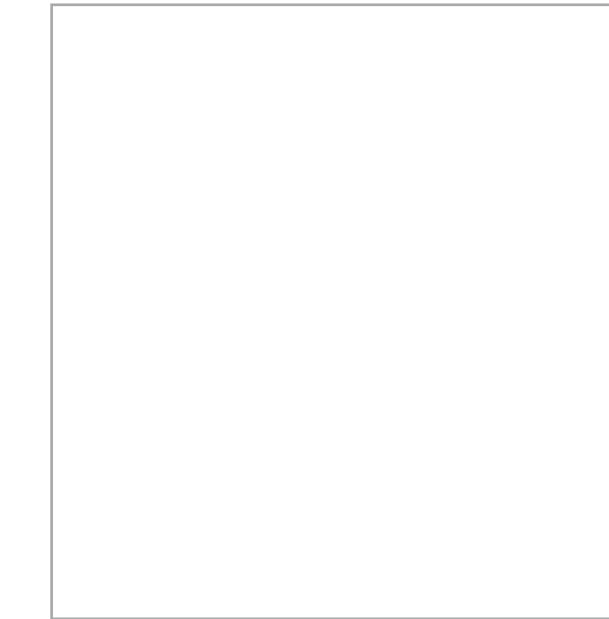


WITH COOKIES

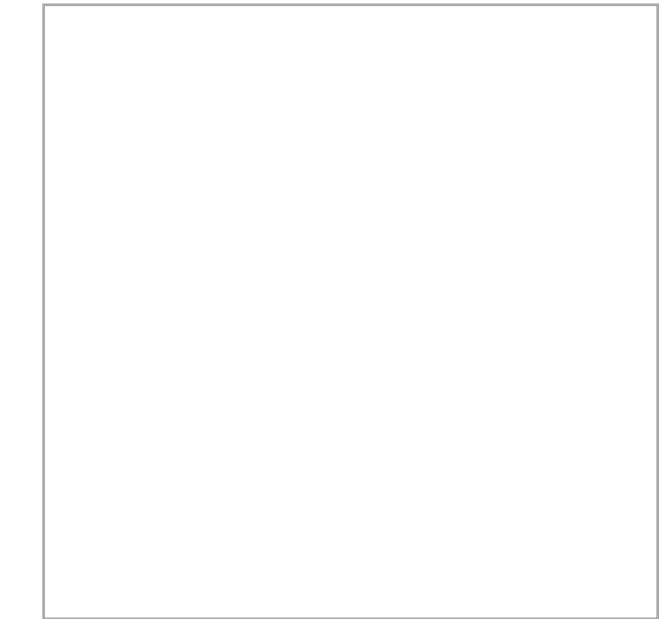
client



“the internet”

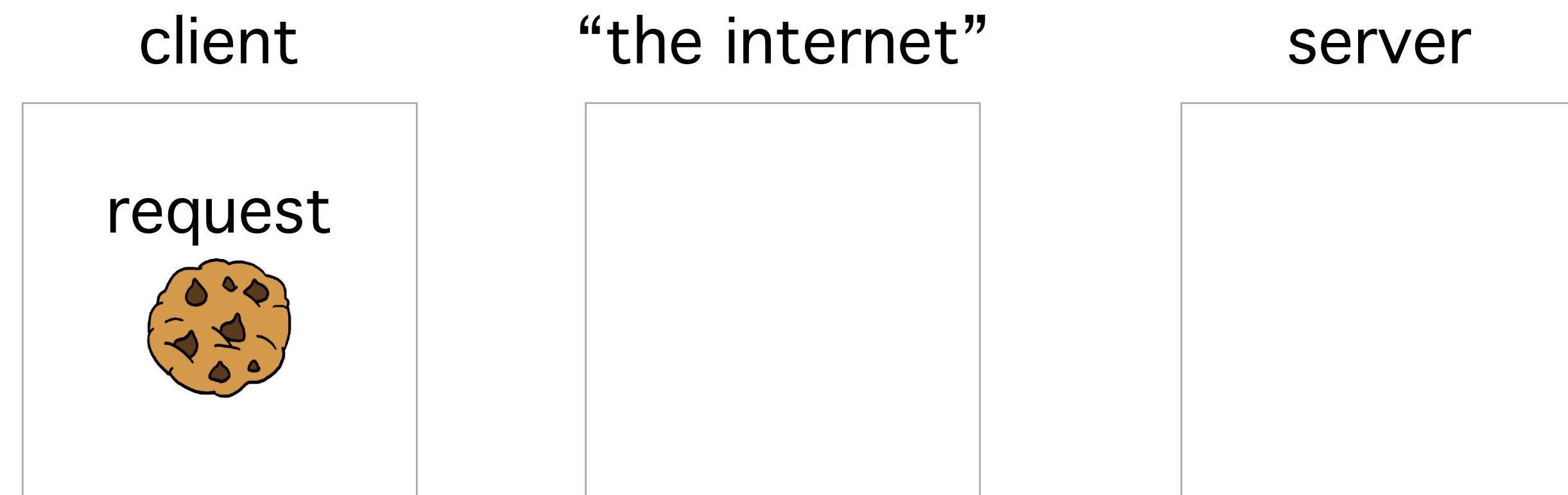


server



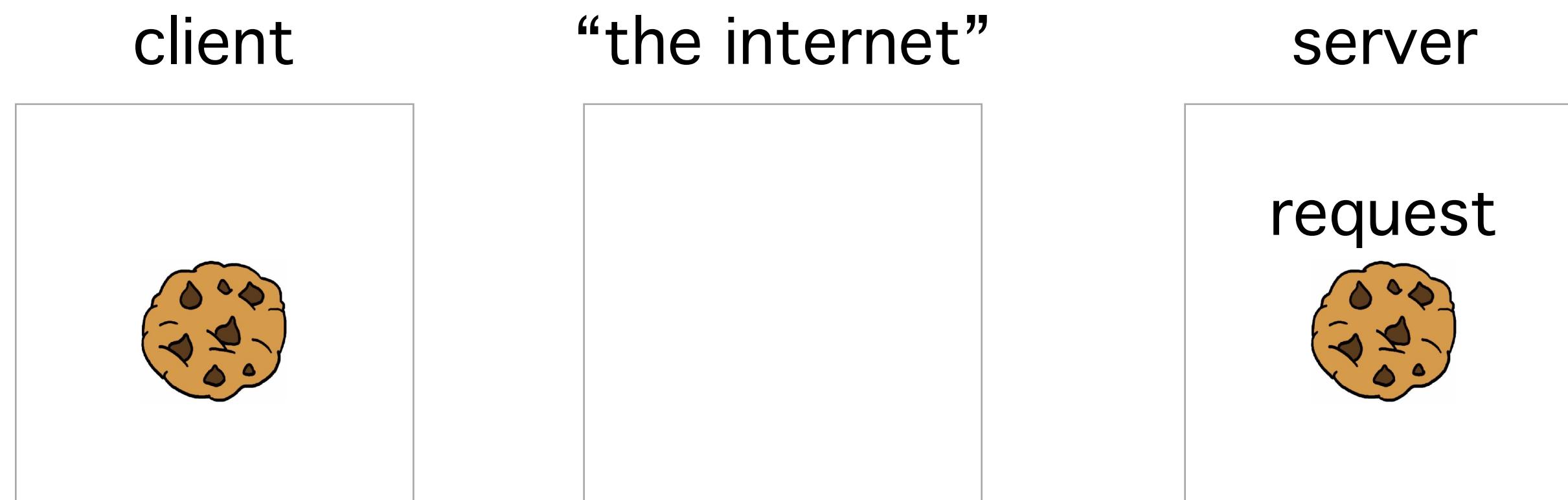


WITH COOKIES



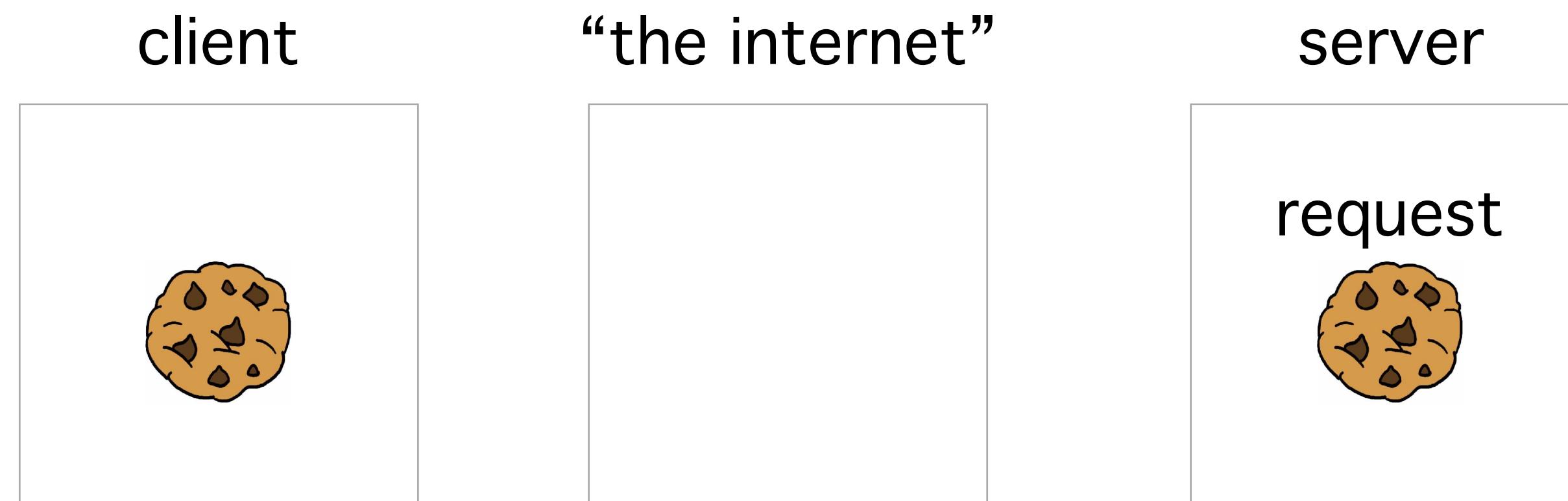


WITH COOKIES





WITH COOKIES

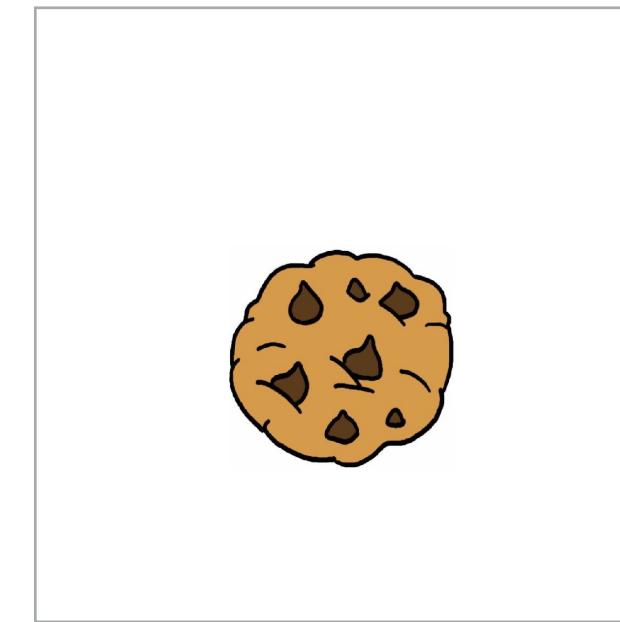


**Do something
with cookie**

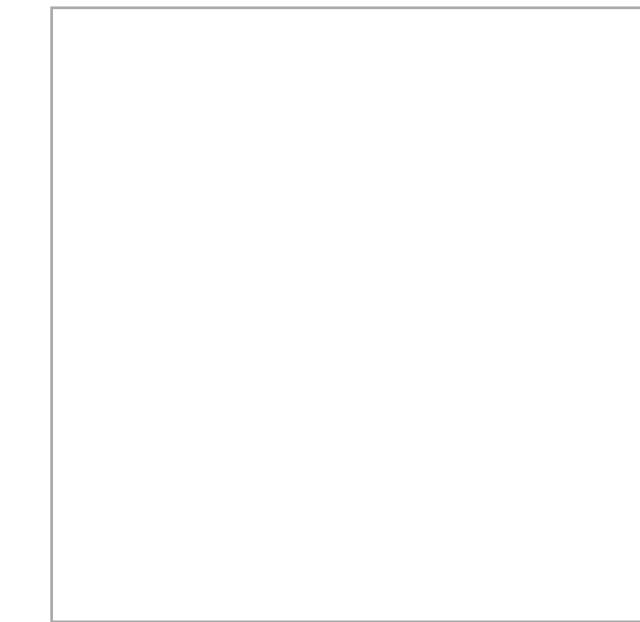


WITH COOKIES

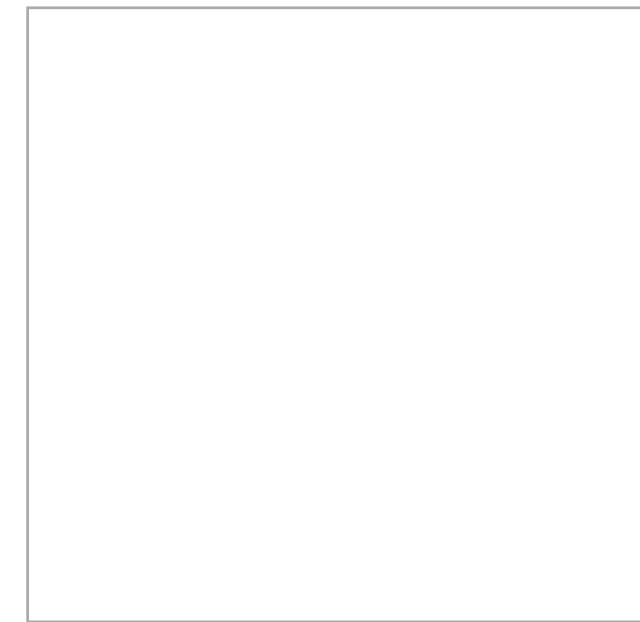
client



“the internet”



server



**Do something
with cookie**

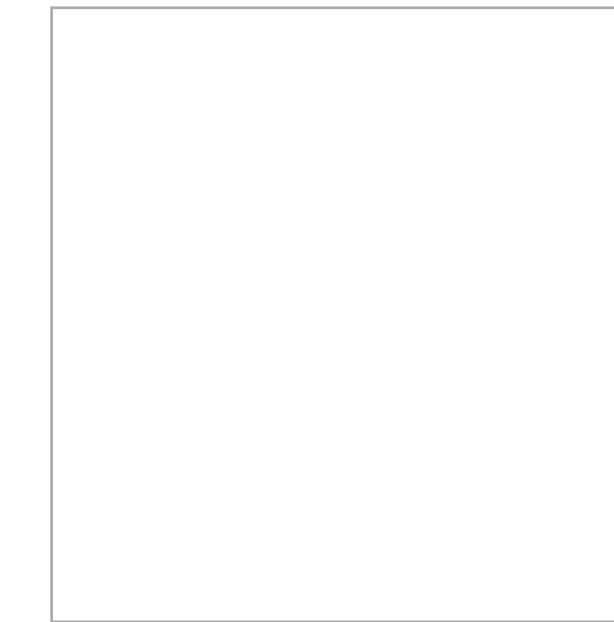


WITH COOKIES

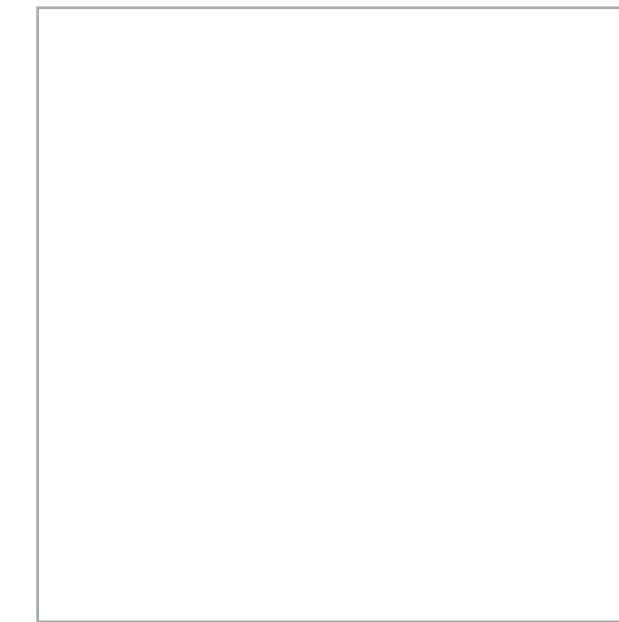
client



“the internet”

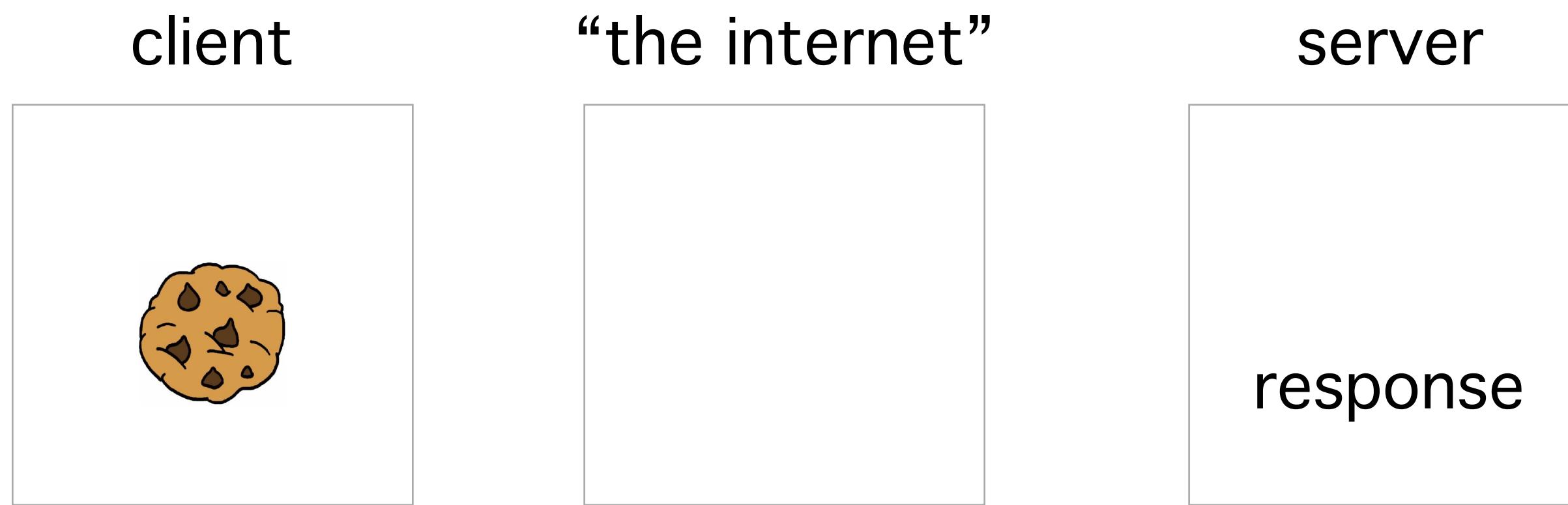


server





WITH COOKIES



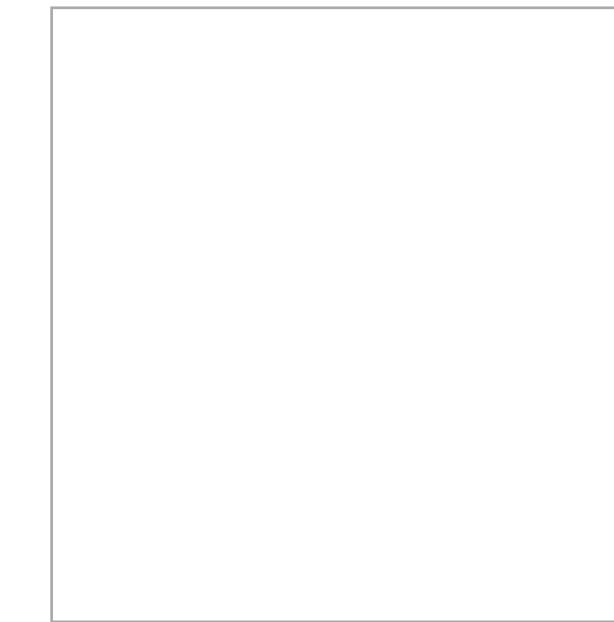


WITH COOKIES

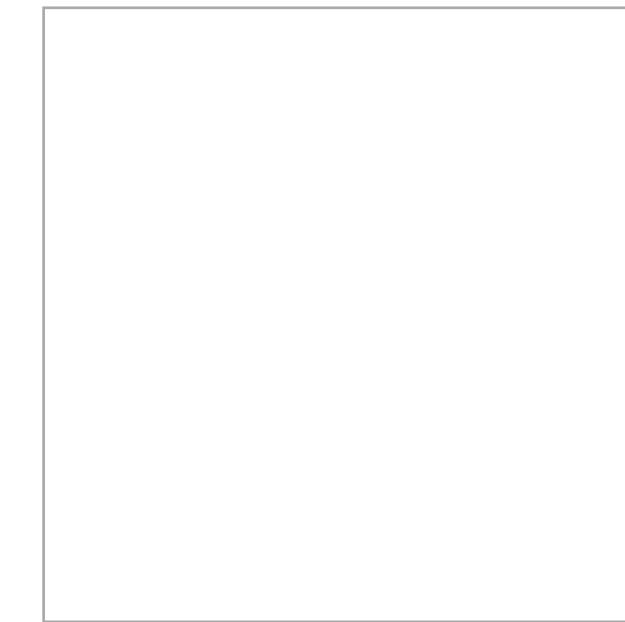
client



“the internet”



server





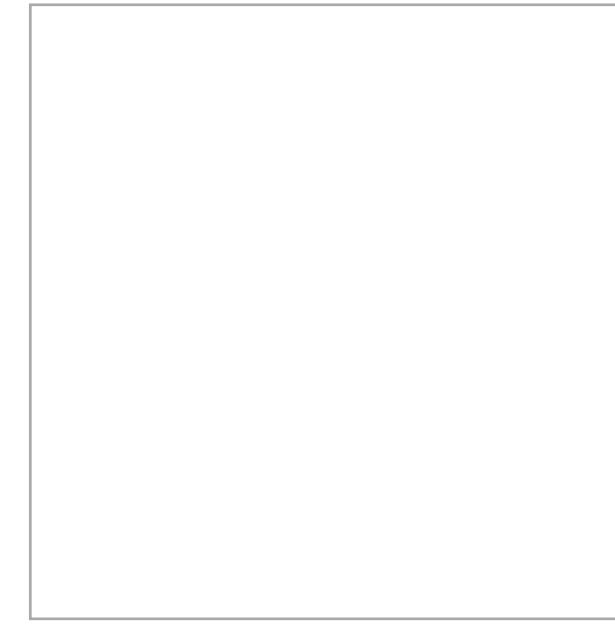
COOKIES & SESSIONS

No need to authenticate for every request

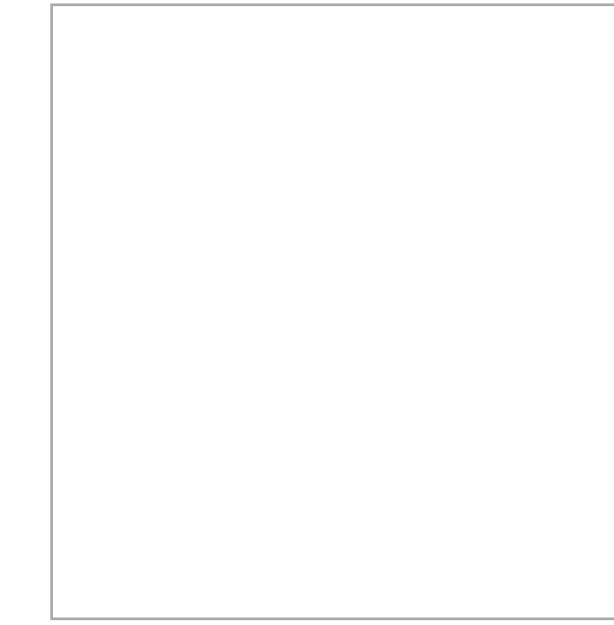


SESSIONS

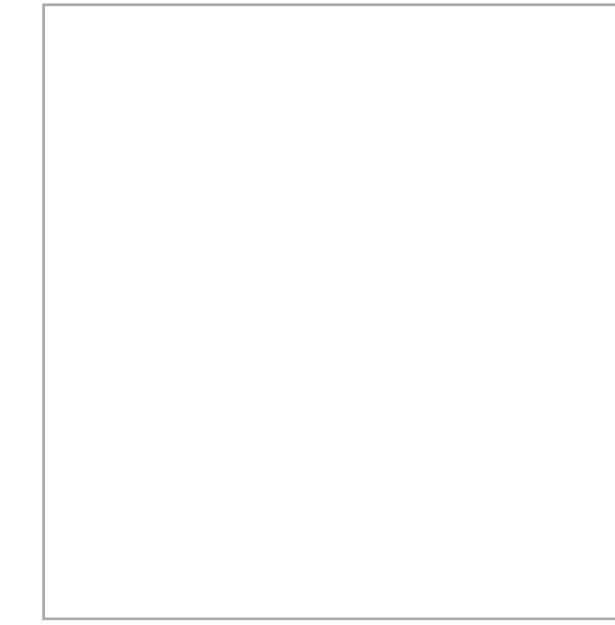
client



“the internet”



server





SESSIONS

client

request

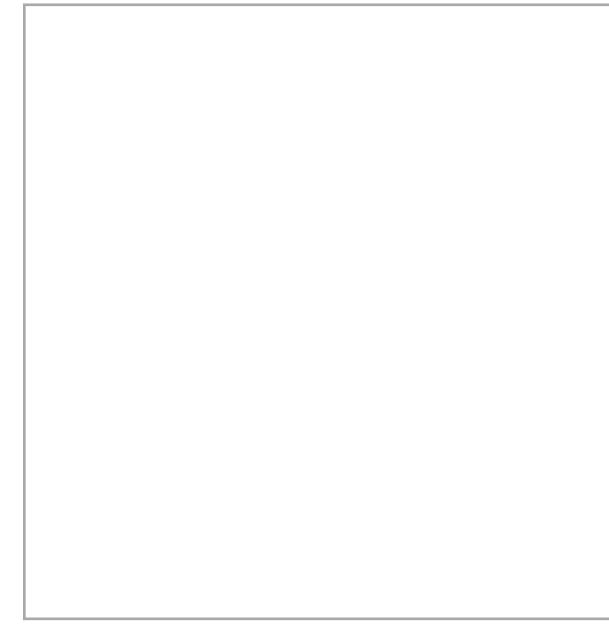
“the internet”

server

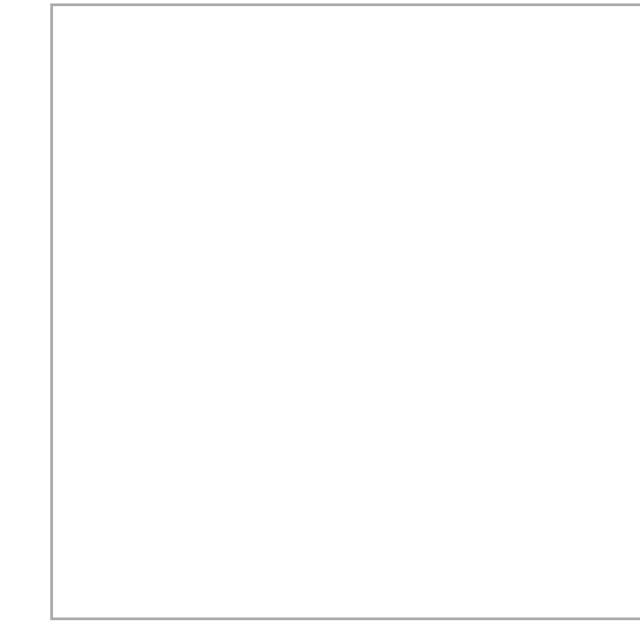


SESSIONS

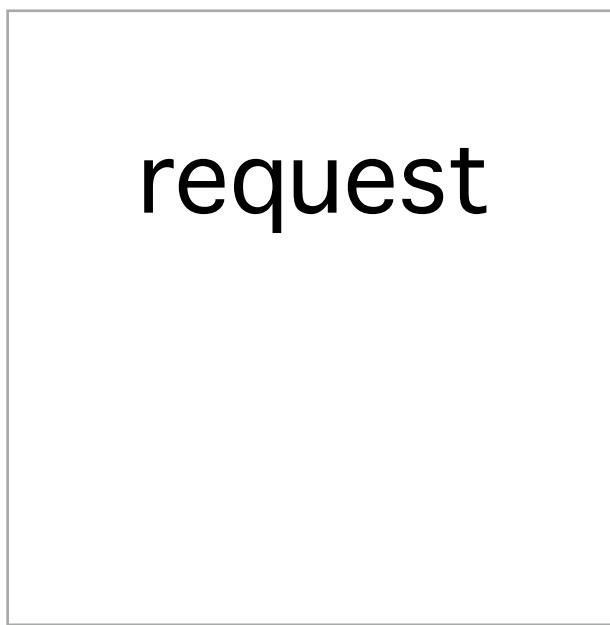
client



“the internet”



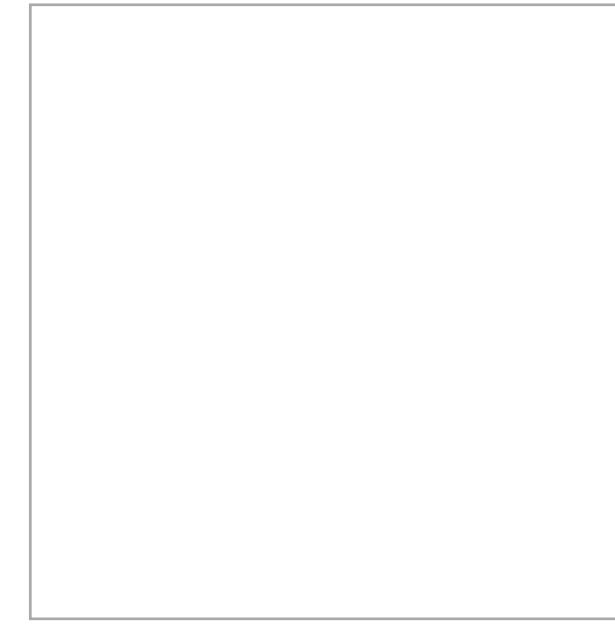
server



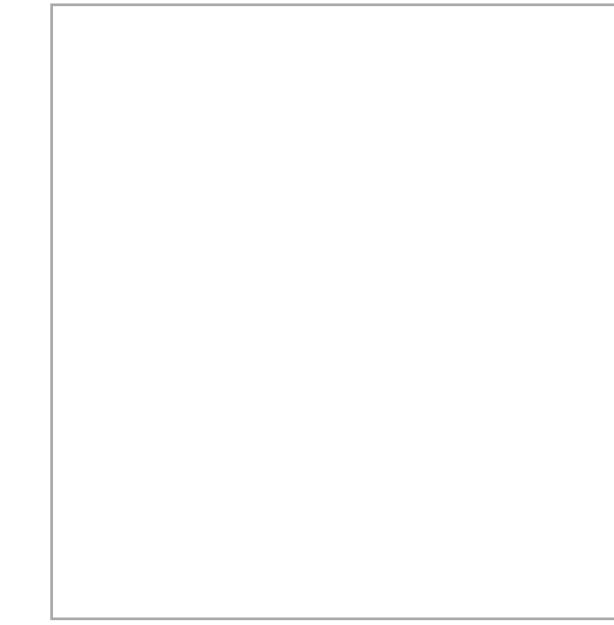


SESSIONS

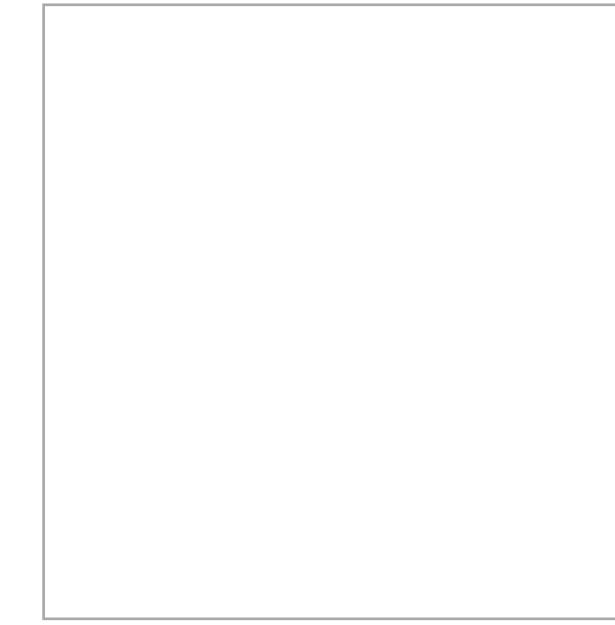
client



“the internet”



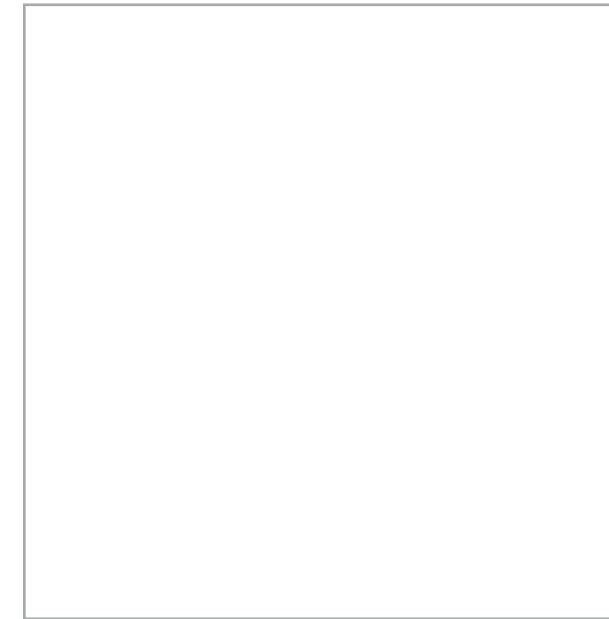
server



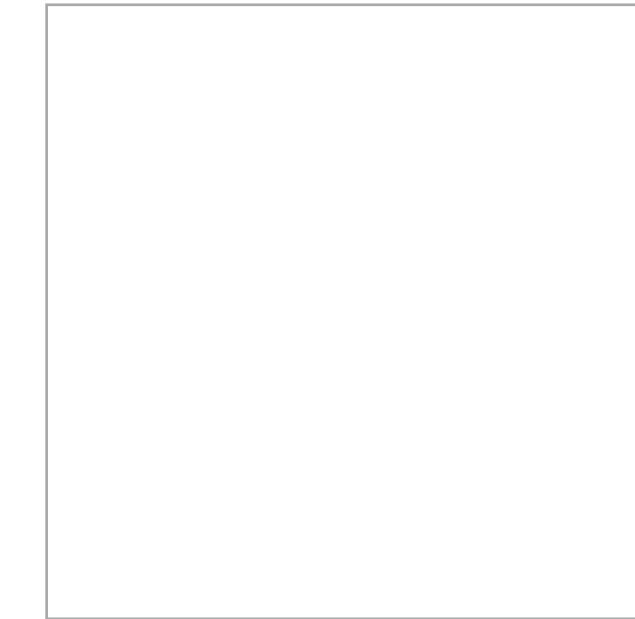


SESSIONS

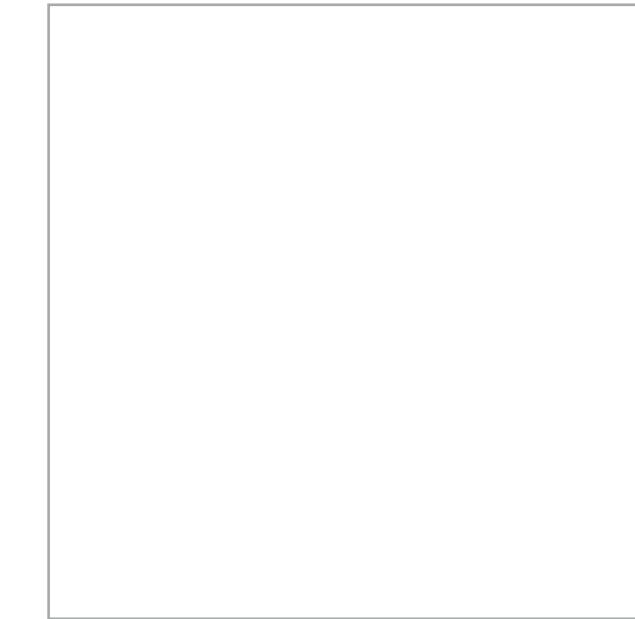
client



“the internet”



server

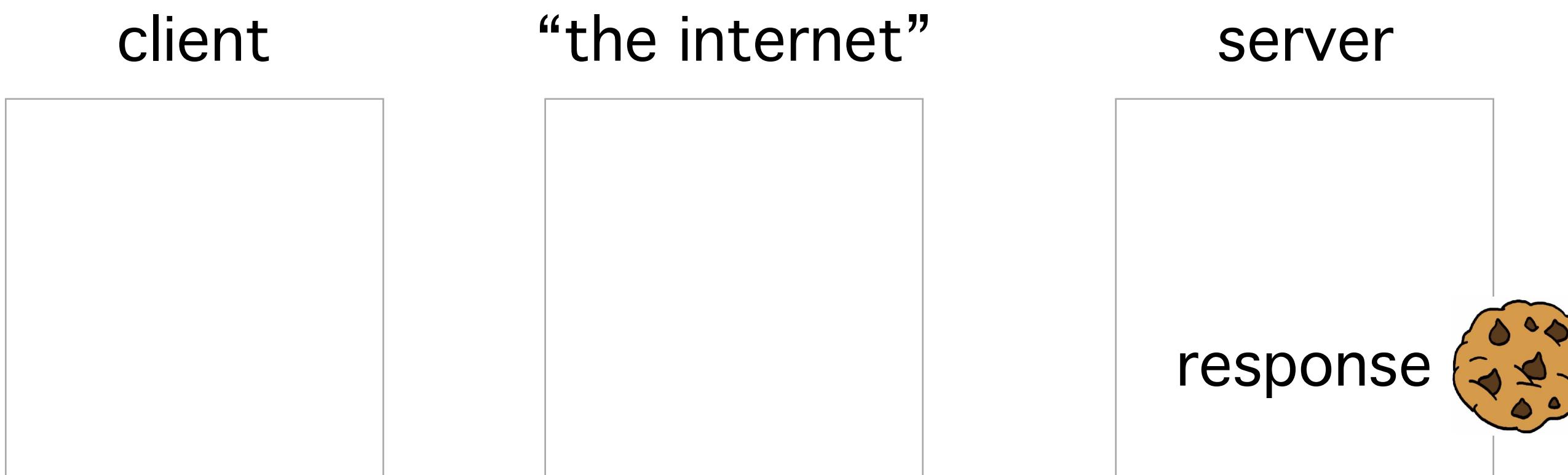


**Make server
session**

sessions[id] = {}



SESSIONS



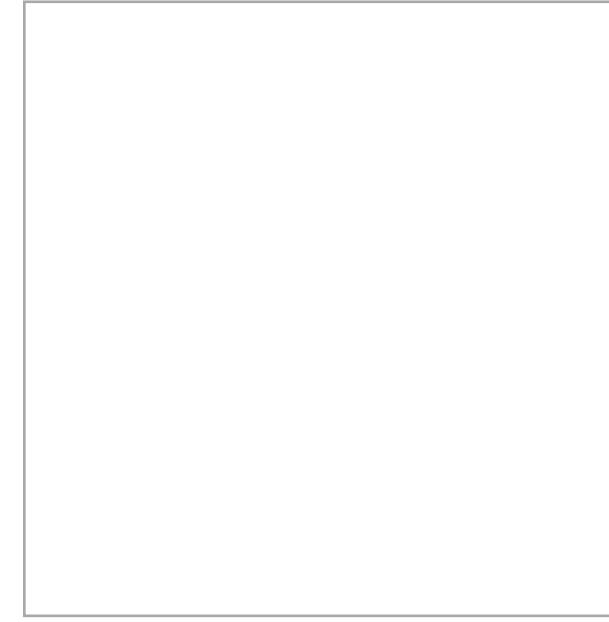
Make server session

sessions[id] = {}

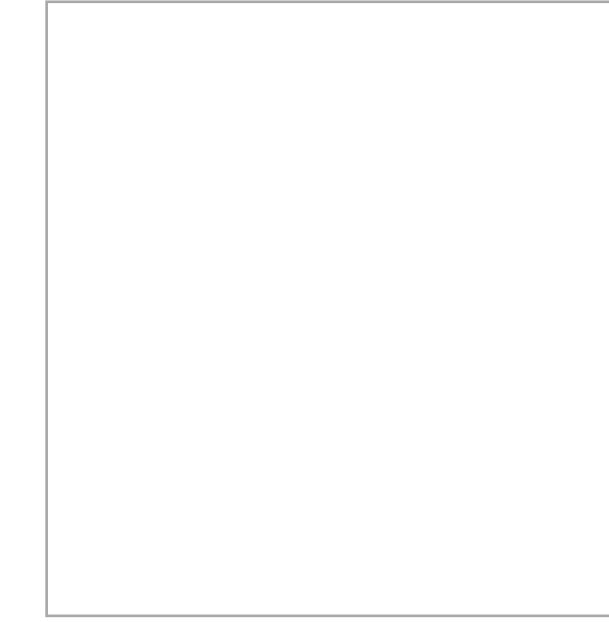


SESSIONS

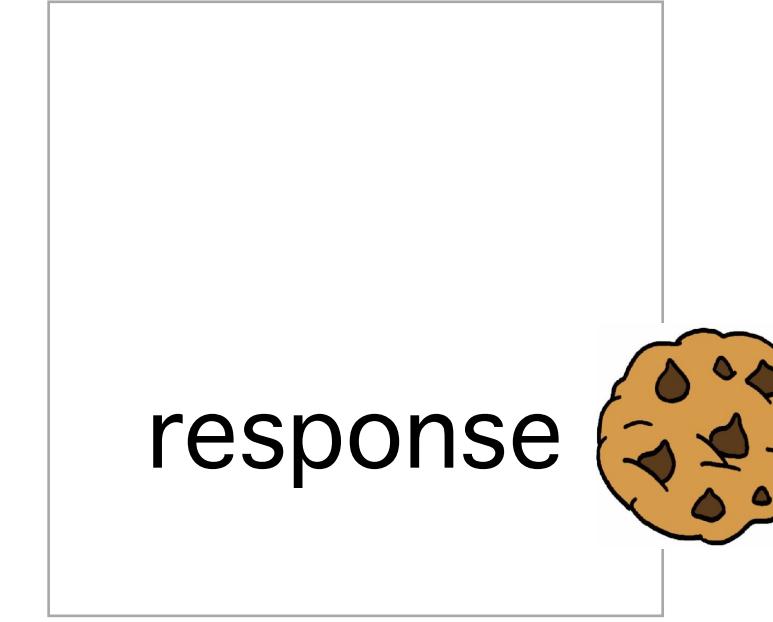
client



“the internet”

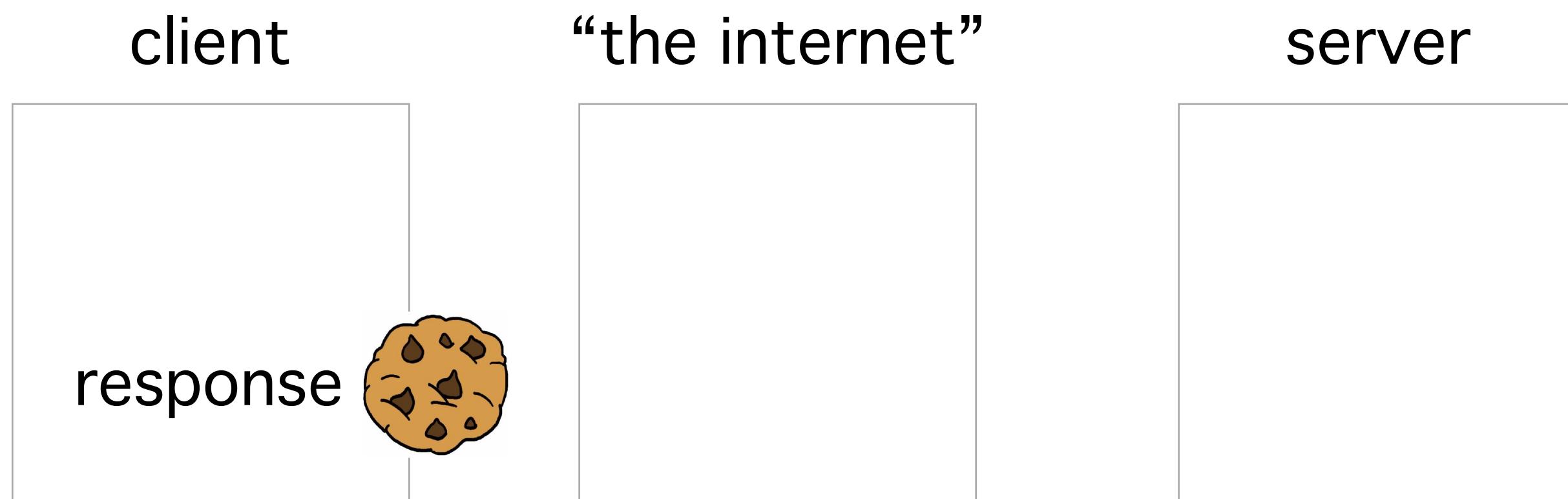


server





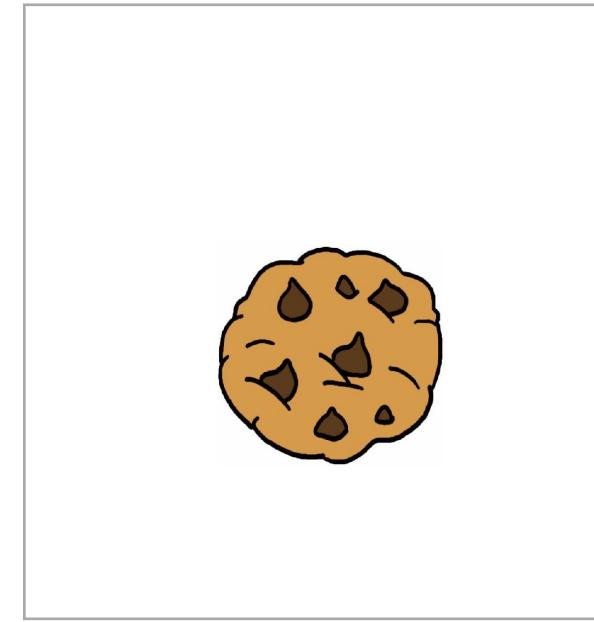
SESSIONS



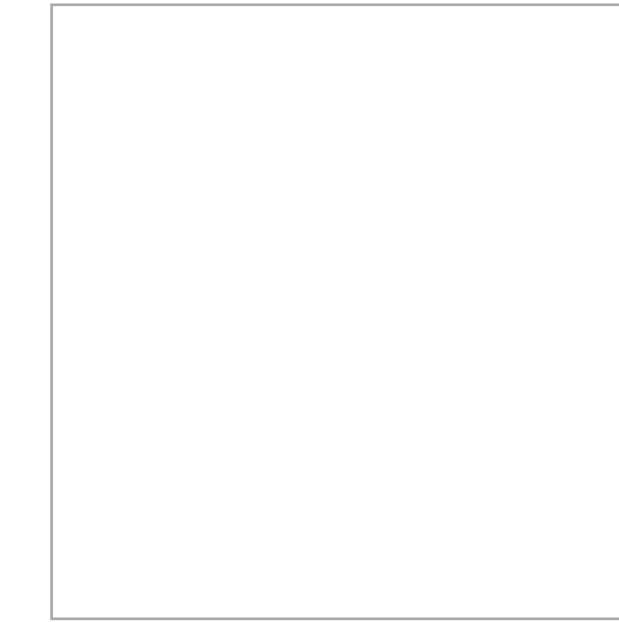


SESSIONS

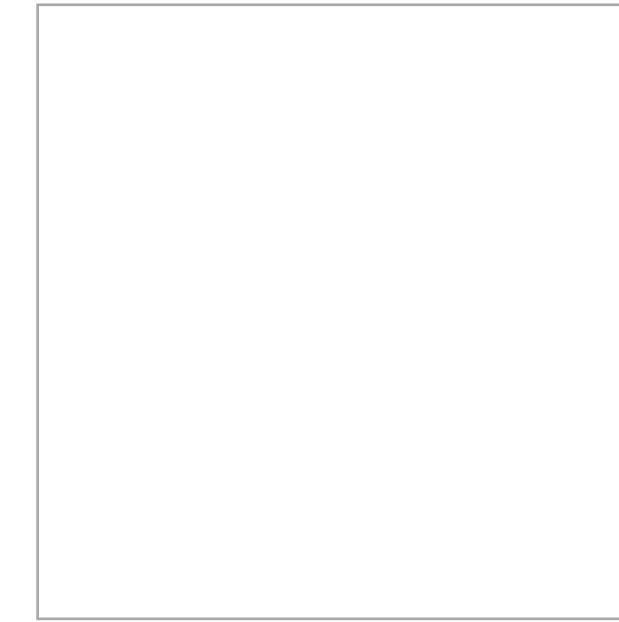
client



“the internet”



server





SESSIONS

client

request



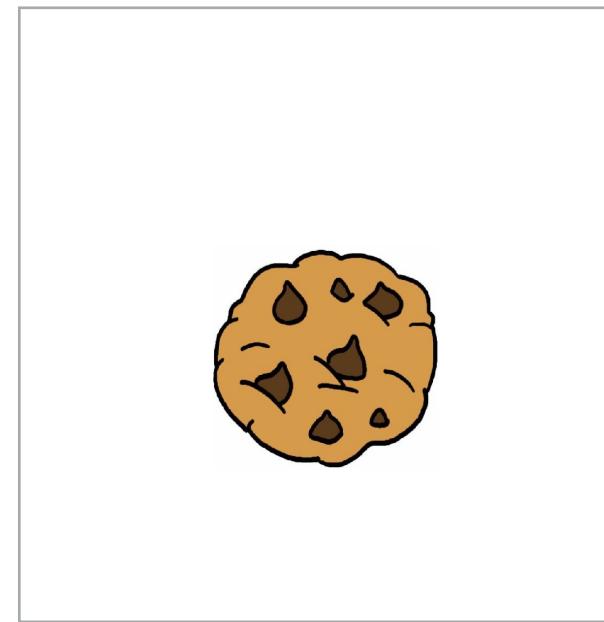
“the internet”

server

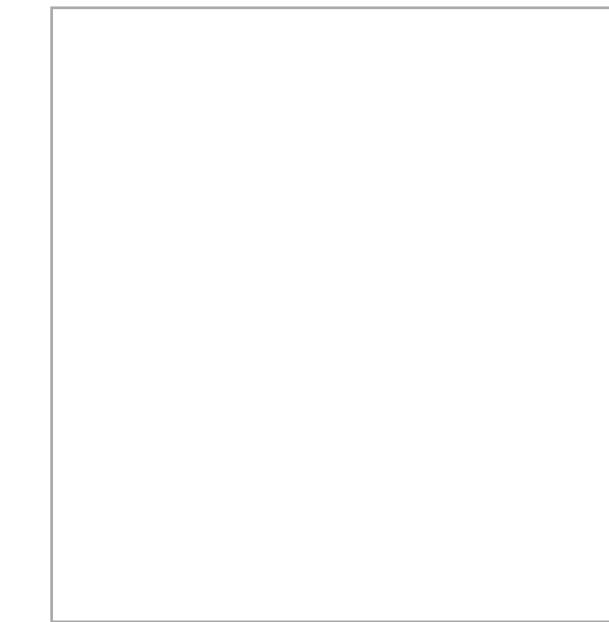


SESSIONS

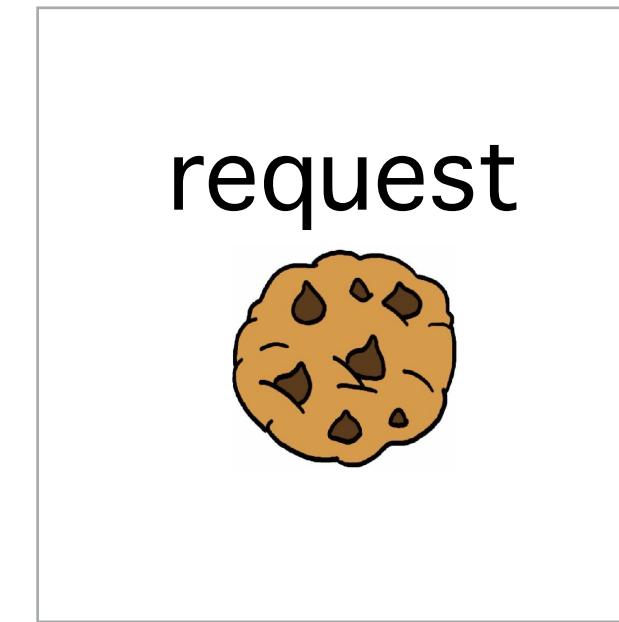
client



“the internet”



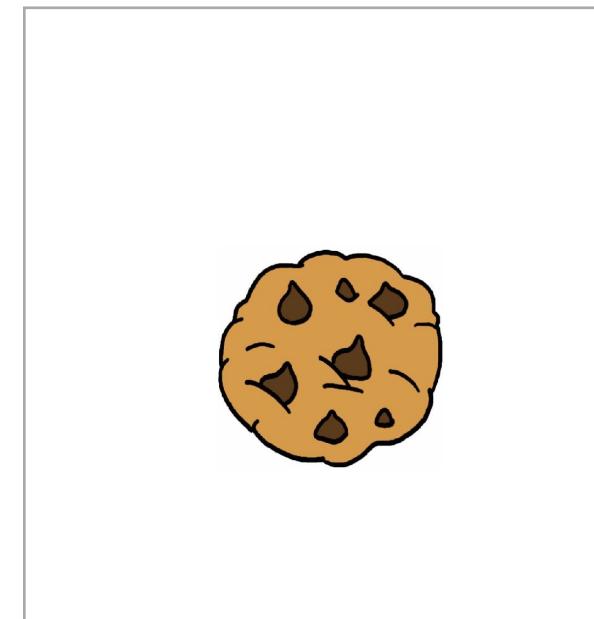
server



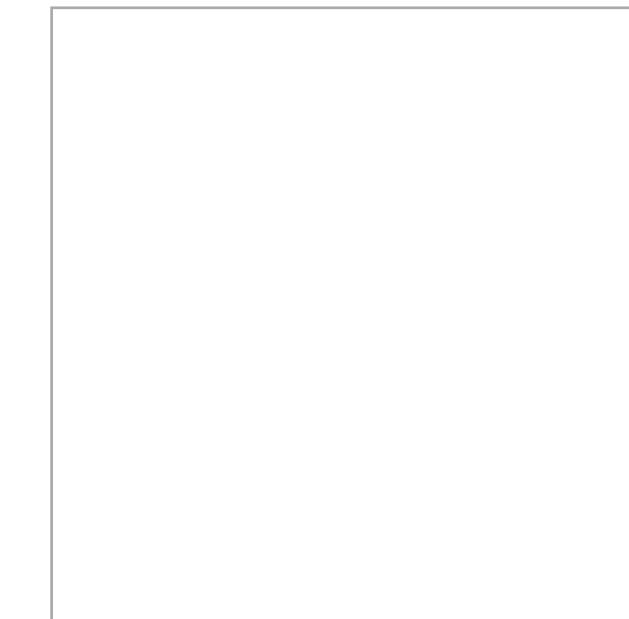


SESSIONS

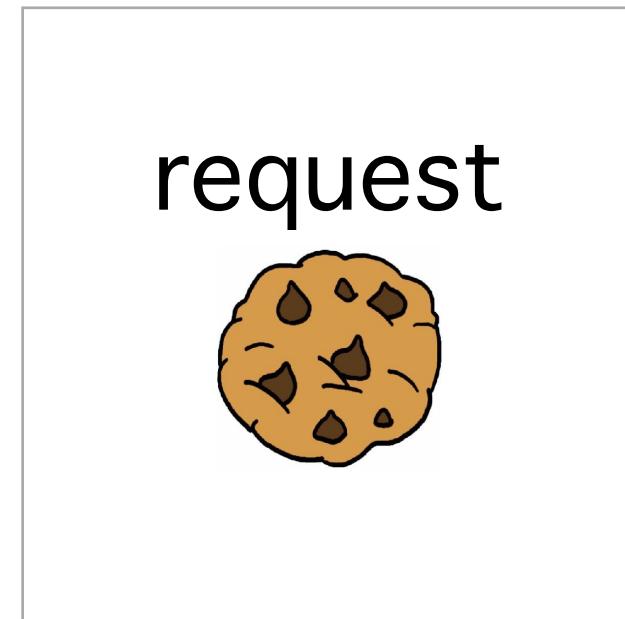
client



“the internet”



server



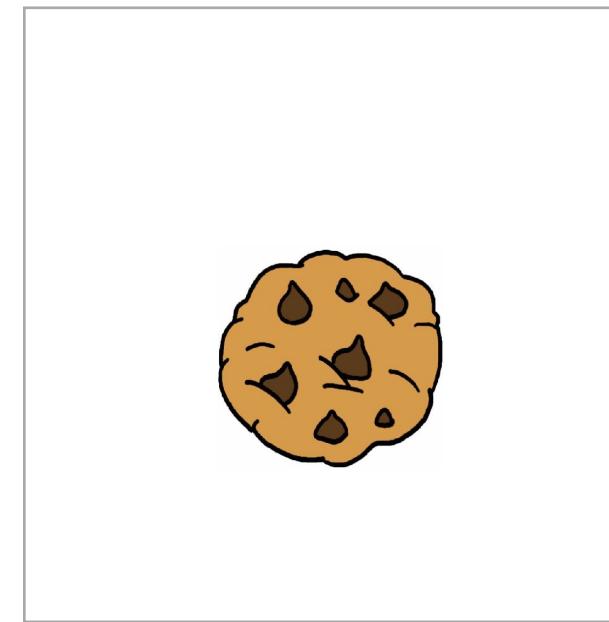
**Look up
session**

***req.session =
sessions[id]***

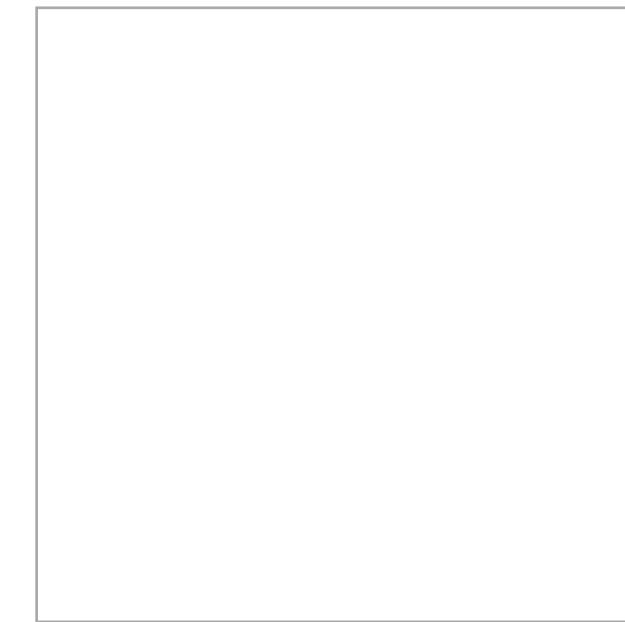


SESSIONS

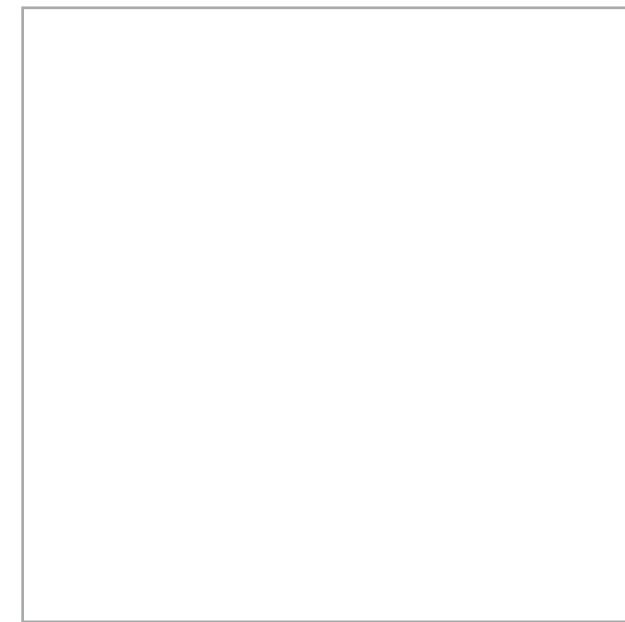
client



“the internet”



server



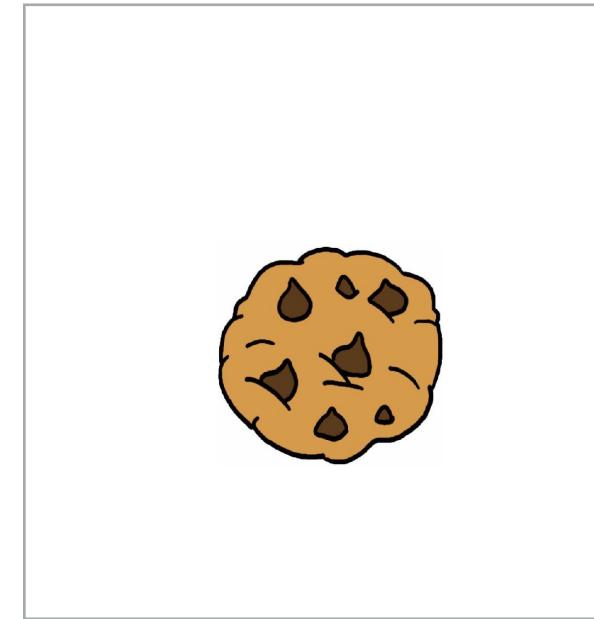
**Look up
session**

***req.session =
sessions[id]***

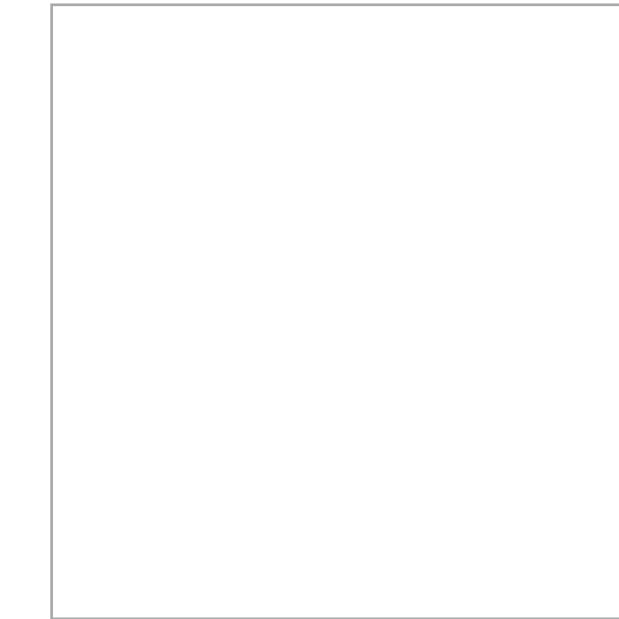


SESSIONS

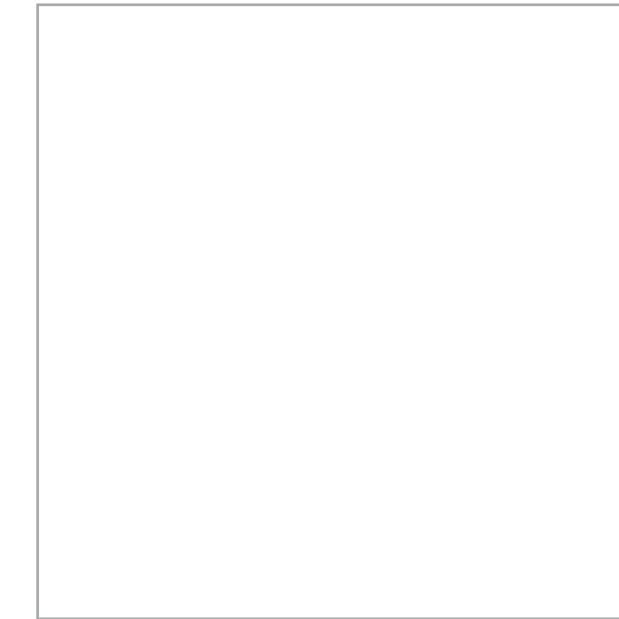
client



“the internet”



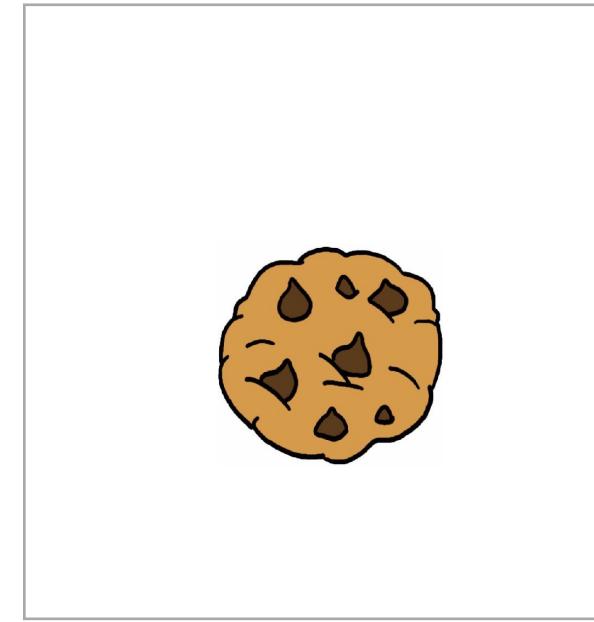
server



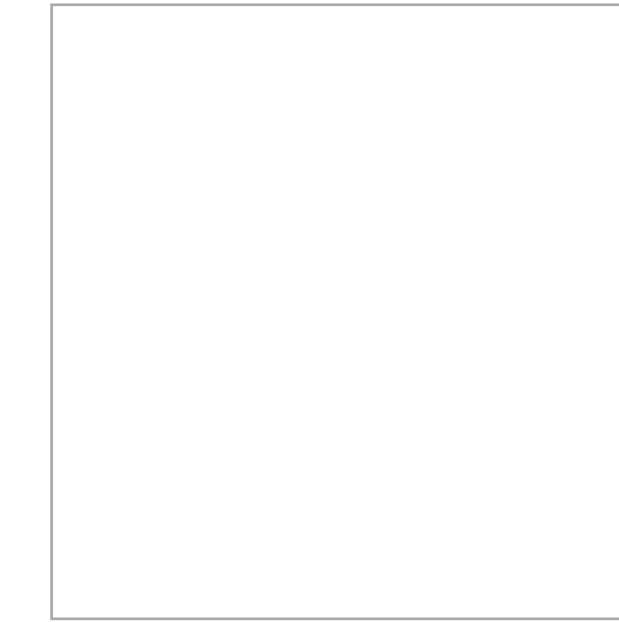


SESSIONS

client



“the internet”



server



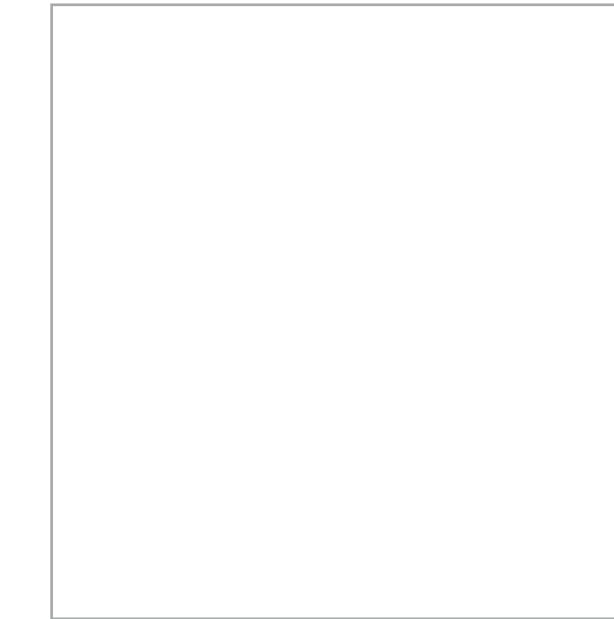


SESSIONS

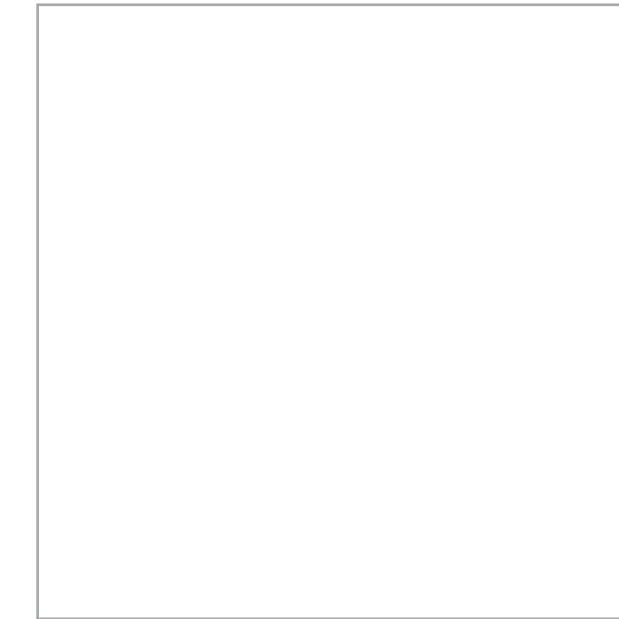
client



“the internet”



server





COOKIES & SESSIONS

- **Server gives client a cookie with ID only**
- **Client keeps cookie and sends with all requests**
- **Server loads request-specific session (stored in RAM)**





SESSIONS

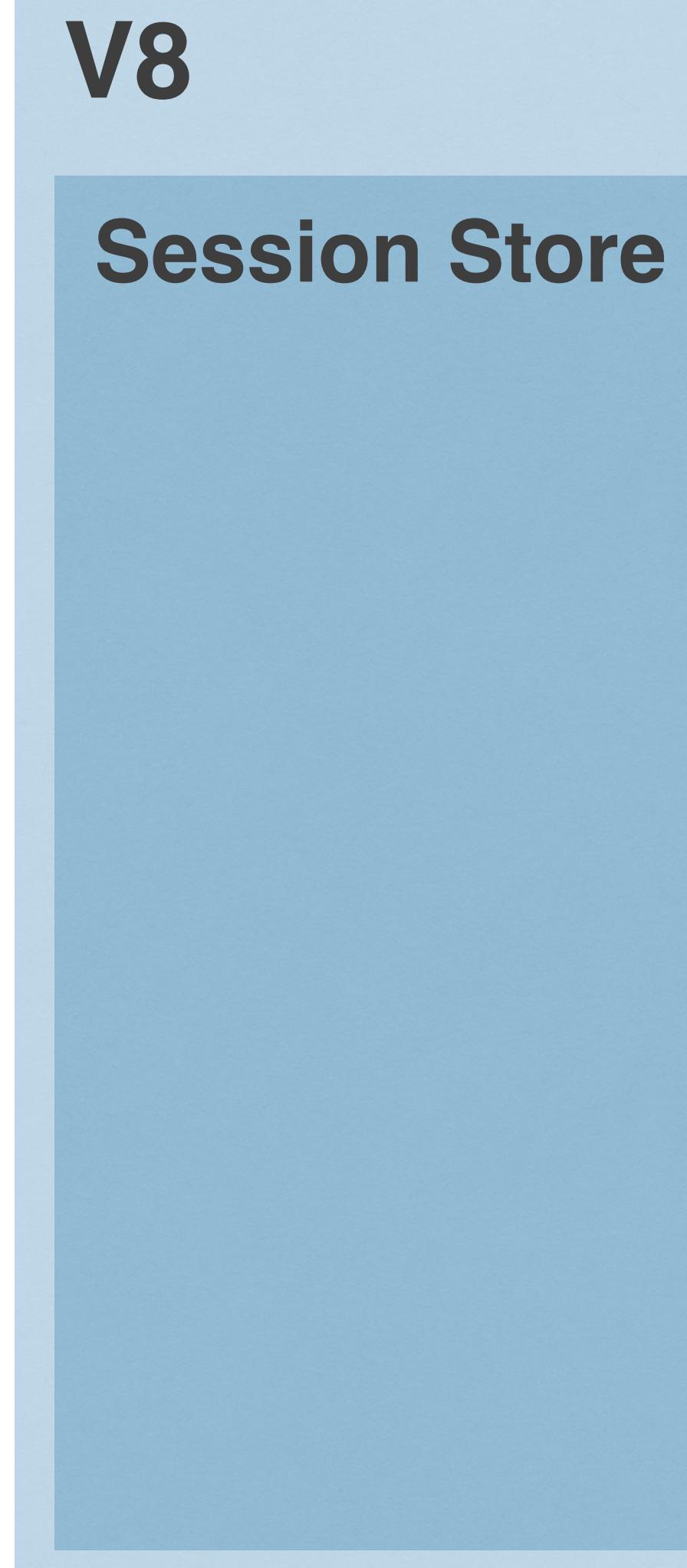


SESSIONS
IN

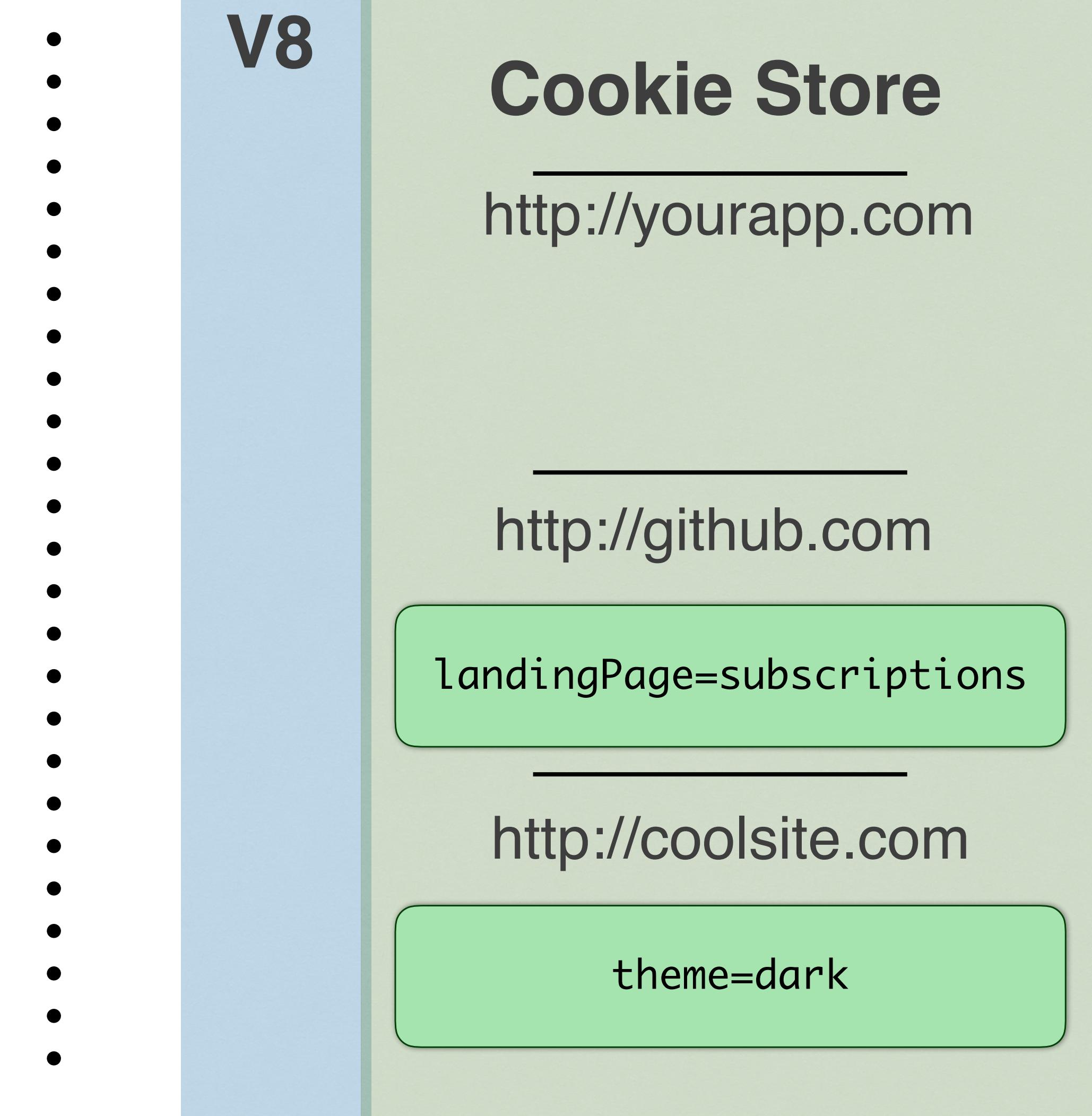


**SESSIONS
IN
DETAIL.**

Server (Backend)

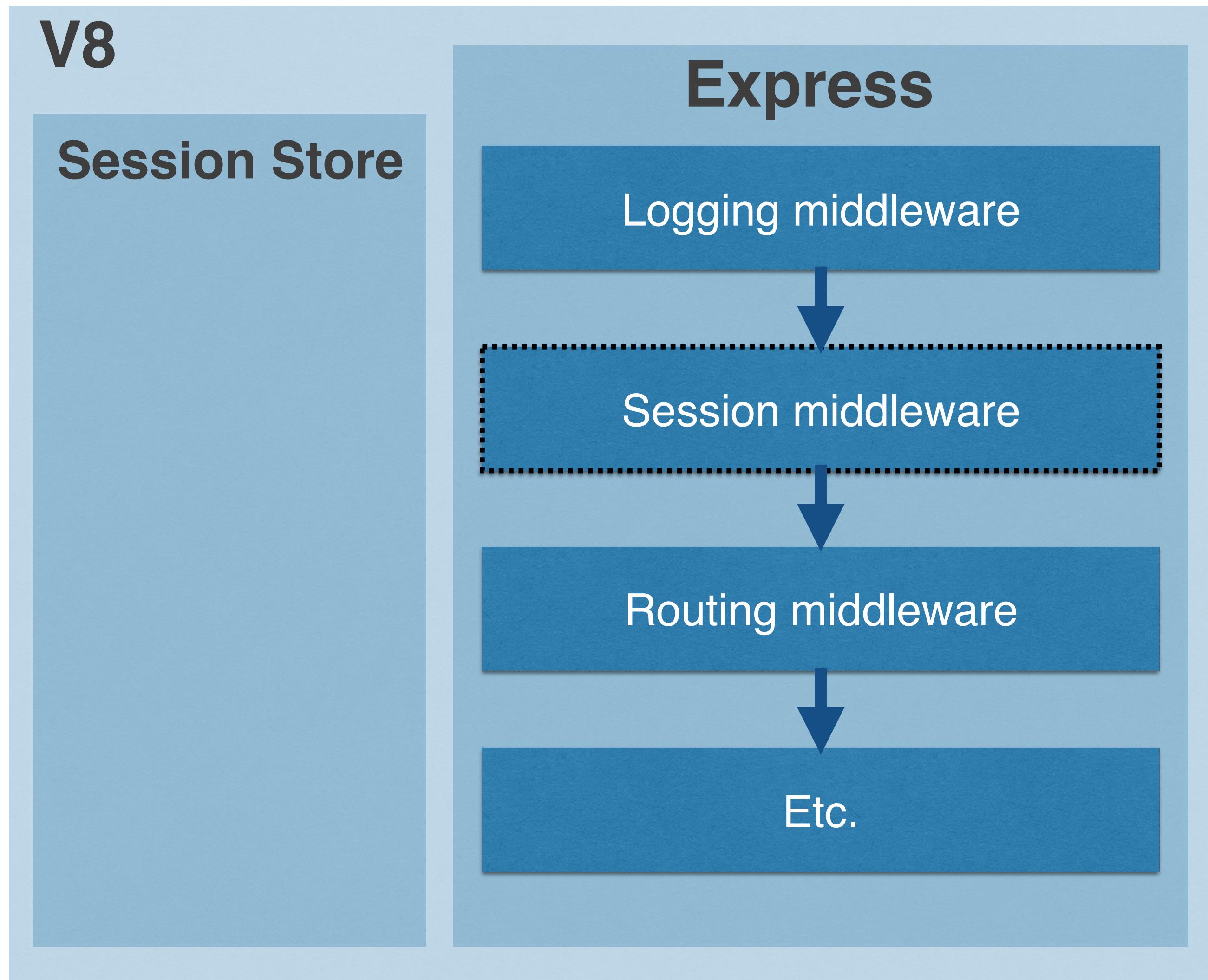


Internet (HTTP)



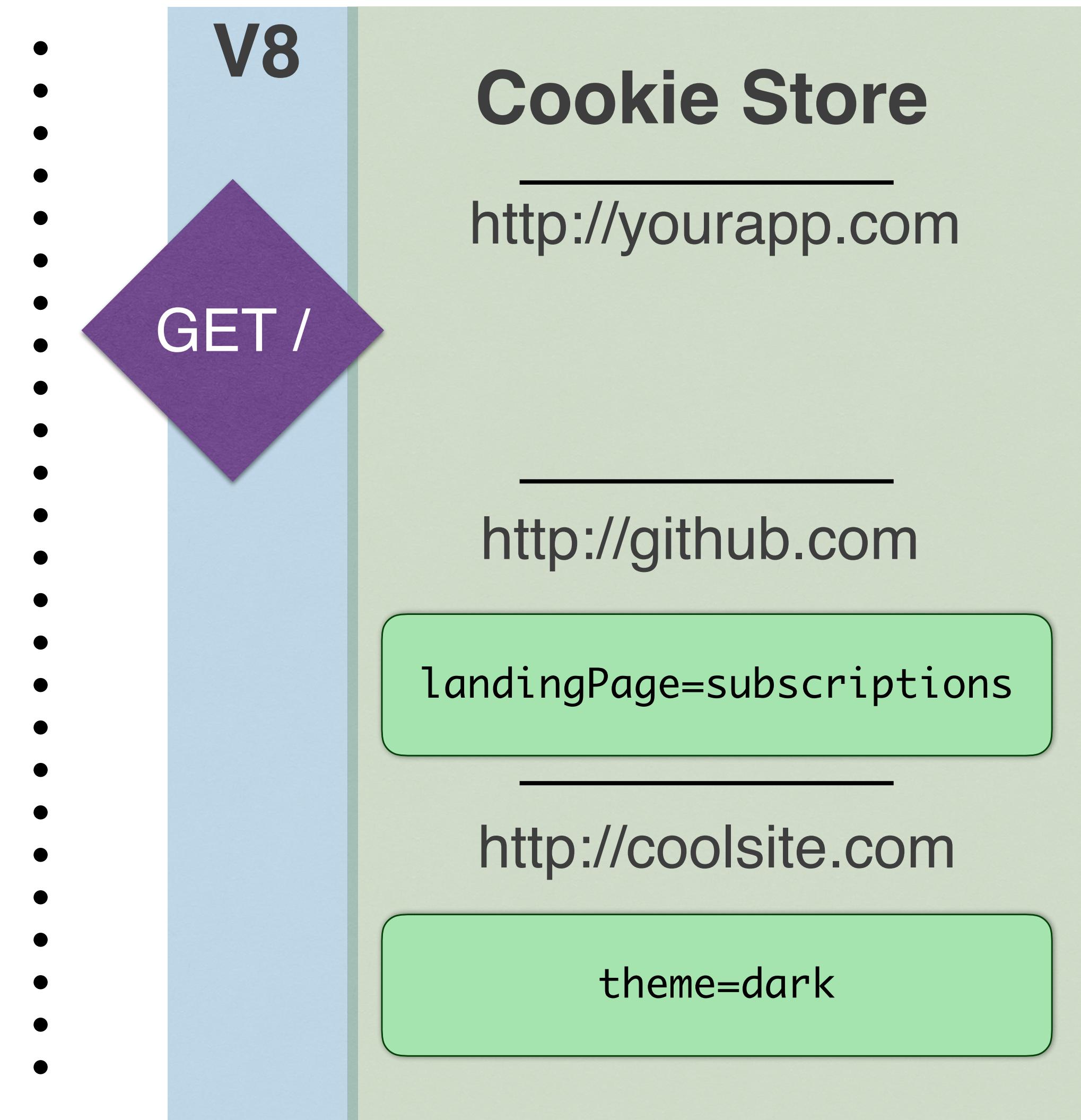
http://yourapp.com

Server (Backend)

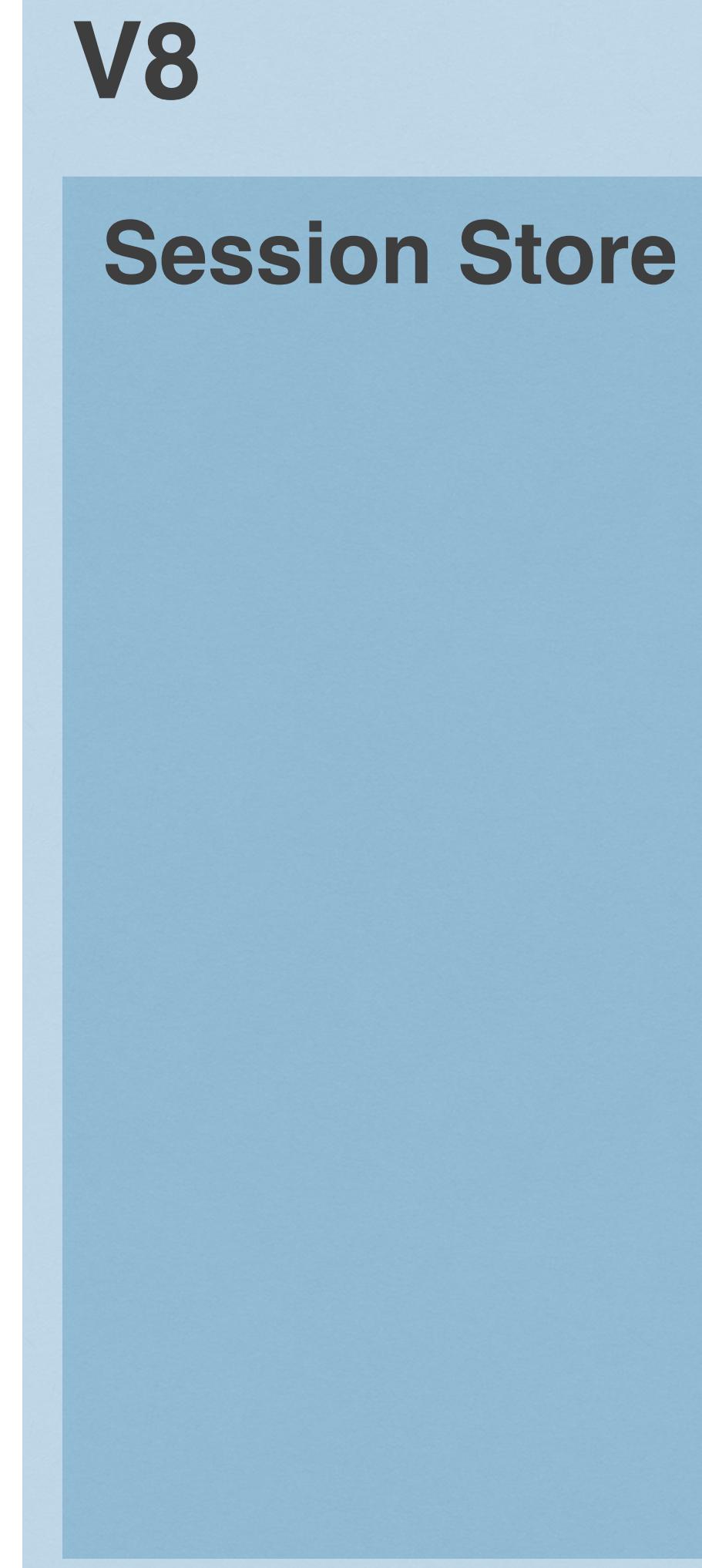


<http://yourapp.com>

Internet (HTTP)

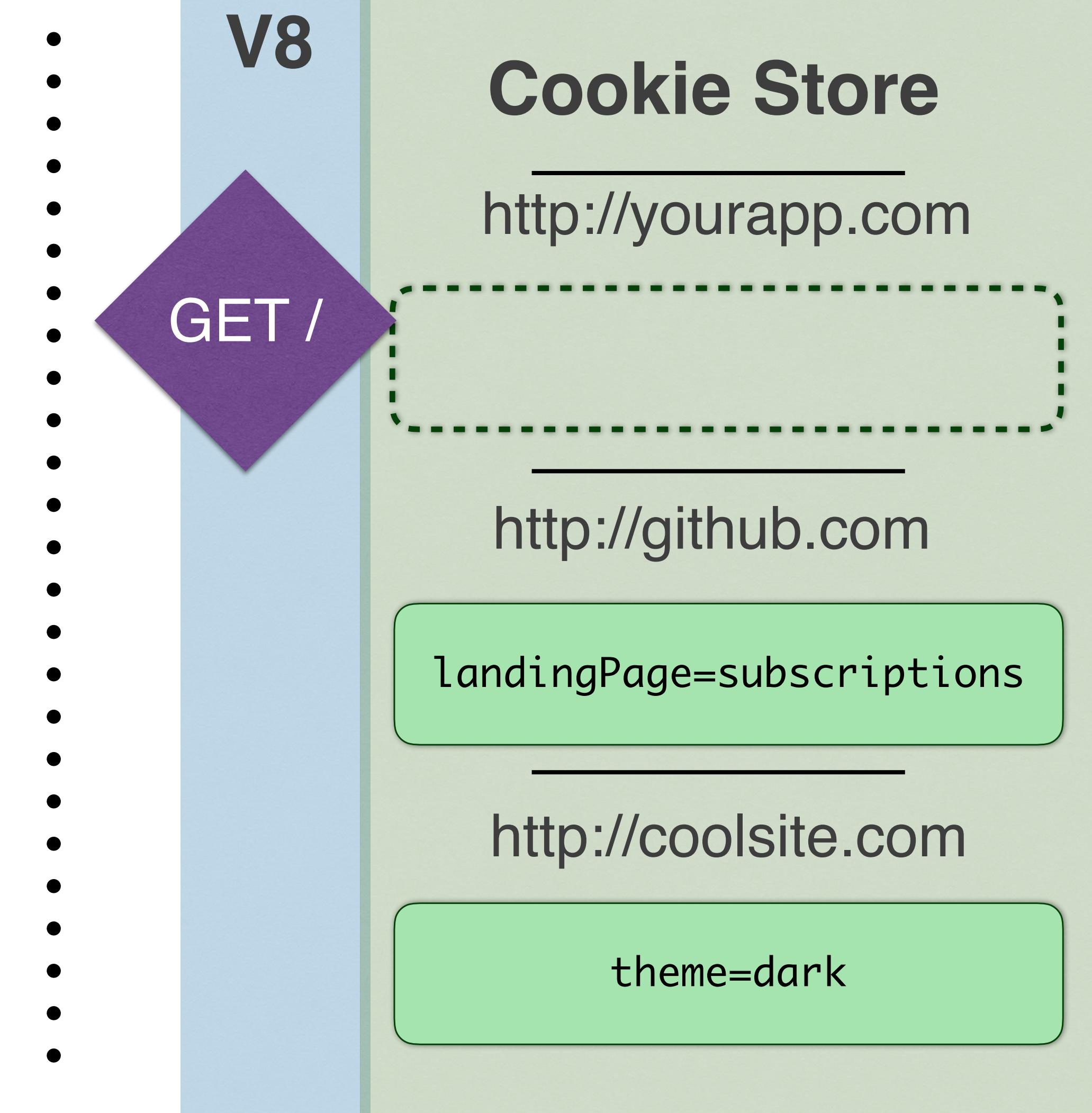


Server (Backend)



<http://yourapp.com>

Internet (HTTP)



HTTP REQUEST

(headers)

GET / HTTP/1.1
Host: yourapp.com
Connection: keep-alive
Accept: text/html
User-Agent: Chrome/
48.0.2564.116
...etc...

(body)

HTTP REQUEST

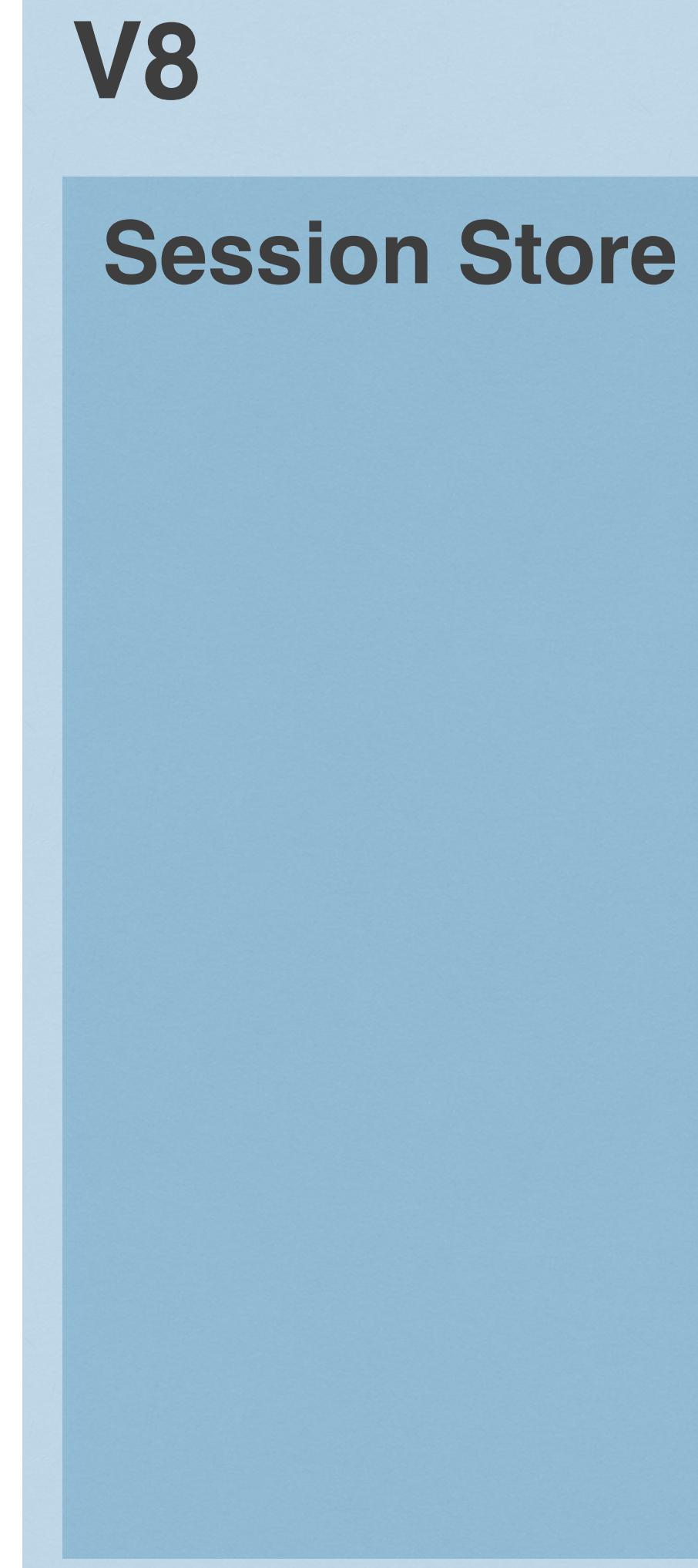
(headers)

(body)

GET / HTTP/1.1
Host: yourapp.com
Connection: keep-alive
Accept: text/html
User-Agent: Chrome/
48.0.2564.116
...etc...

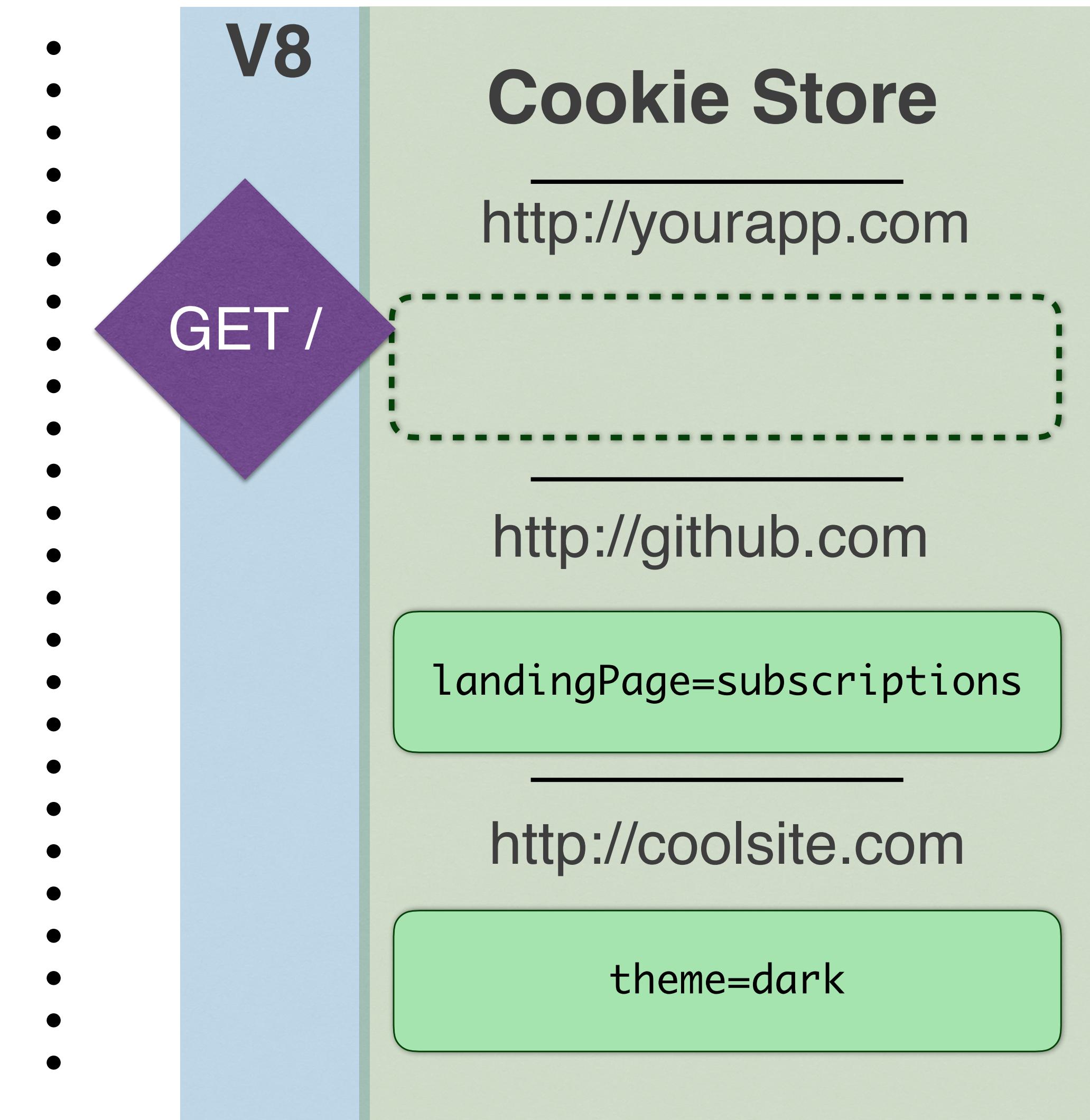
...no cookie info (yet)!

Server (Backend)

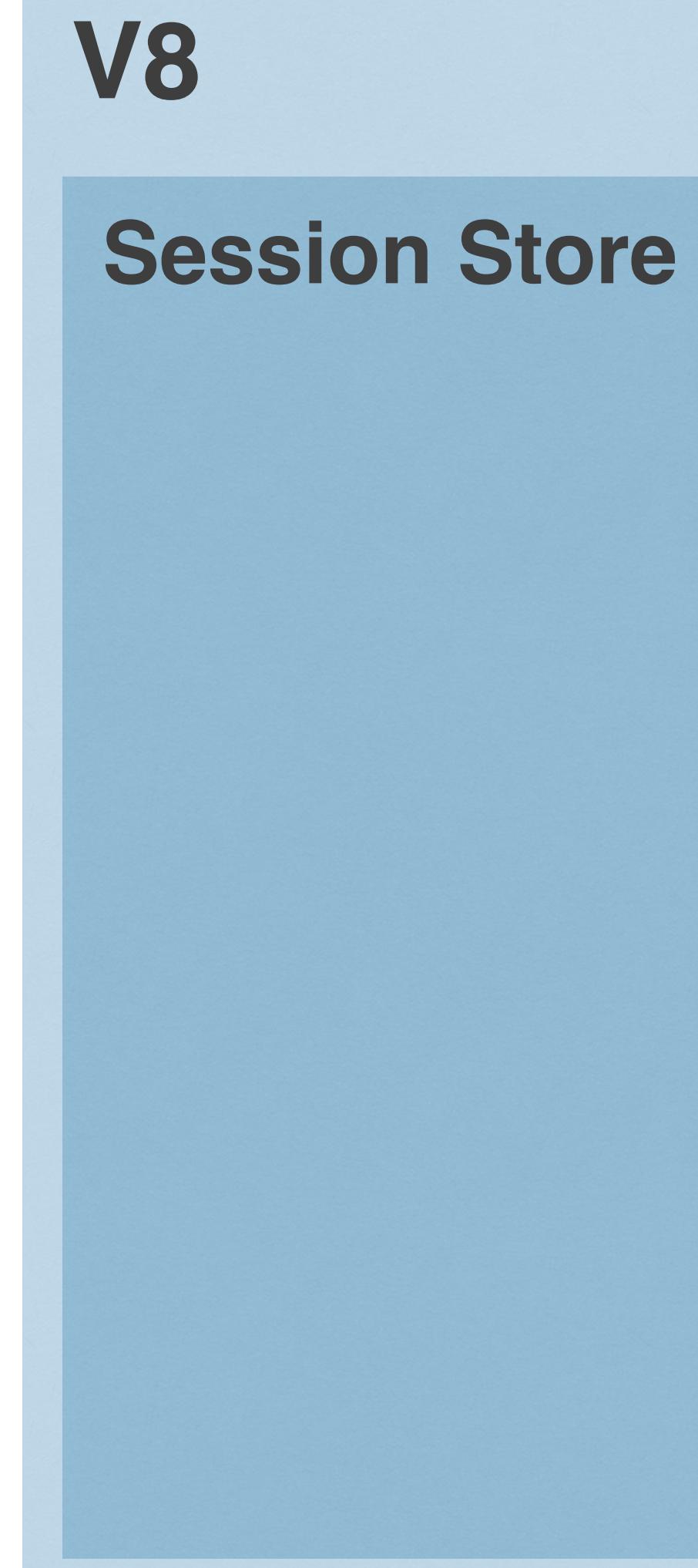


<http://yourapp.com>

Internet (HTTP)

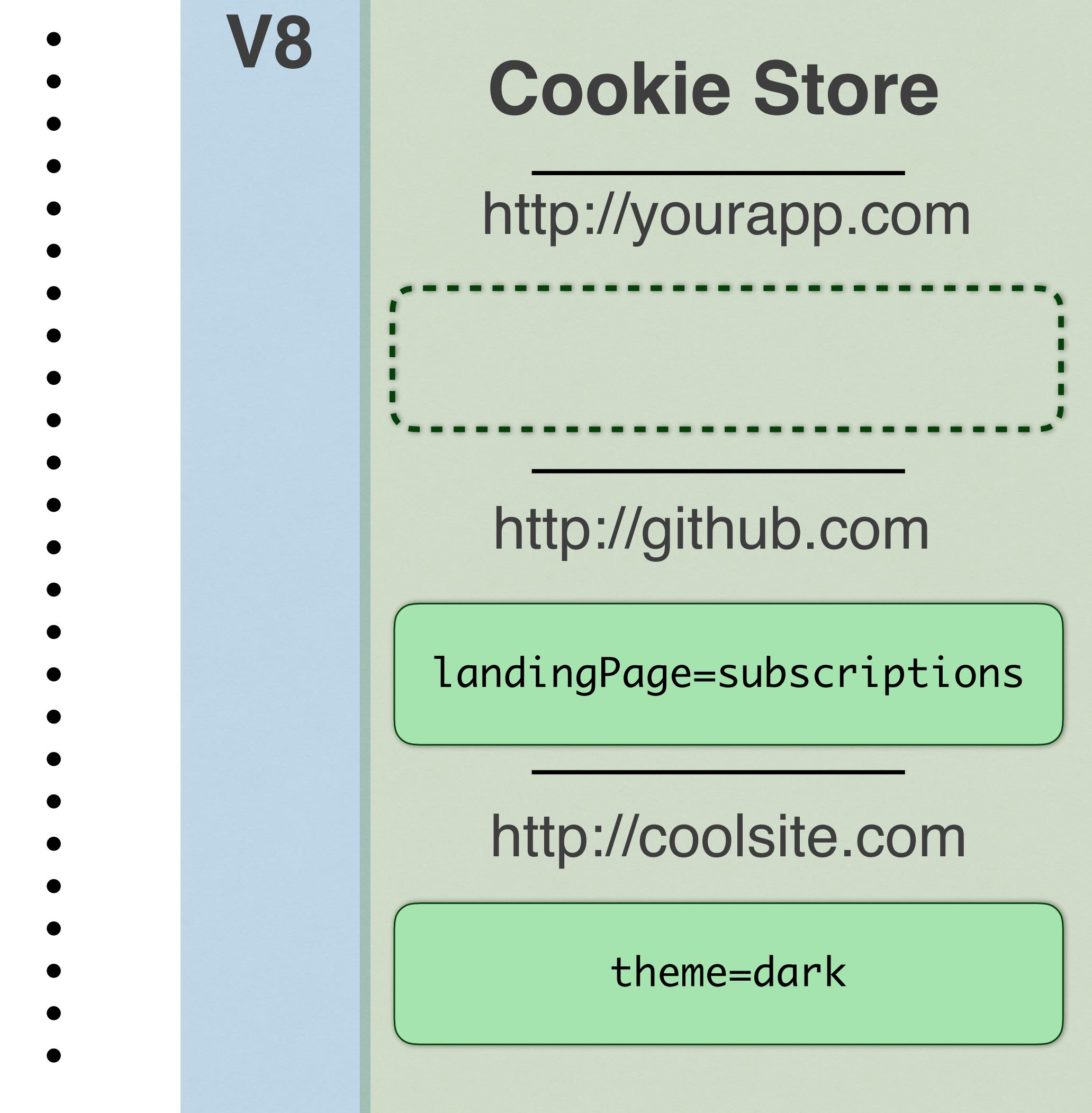


Server (Backend)

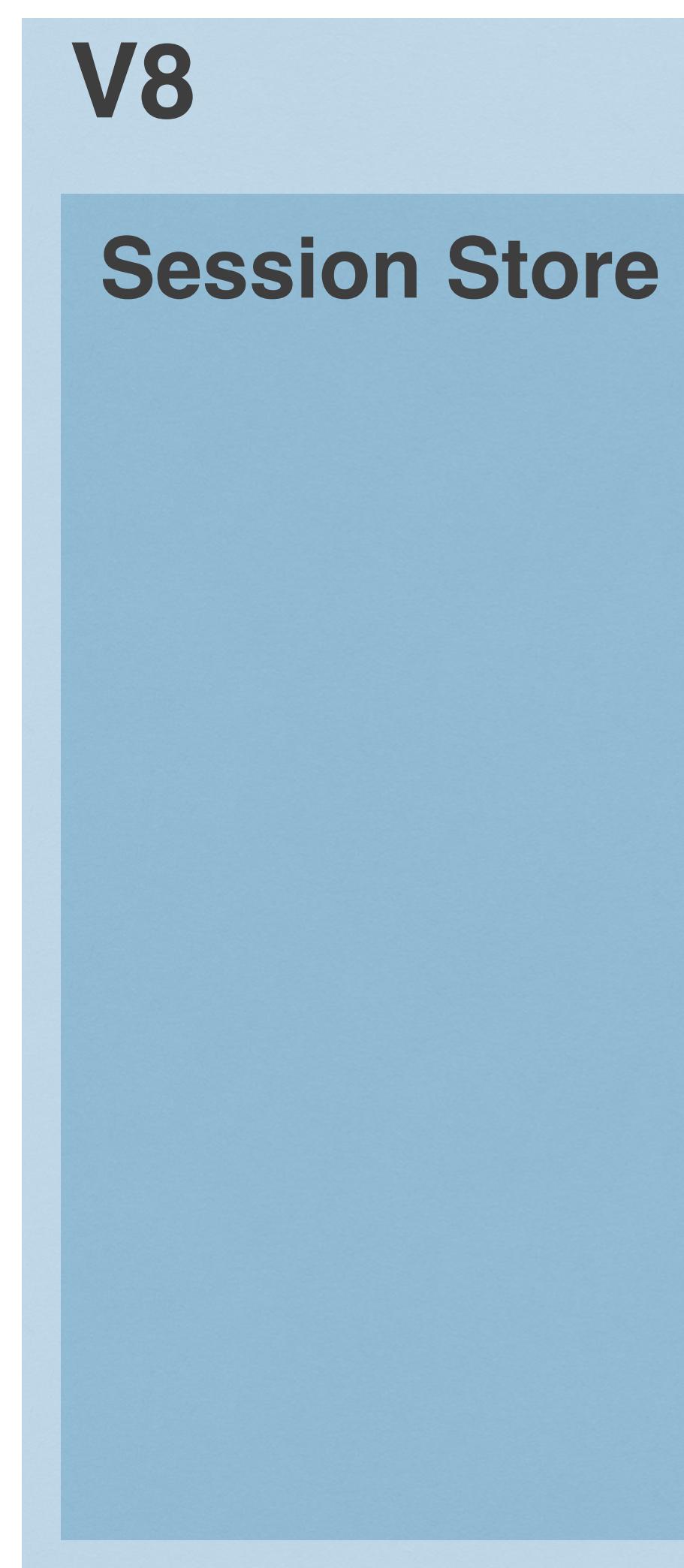


<http://yourapp.com>

Internet (HTTP)

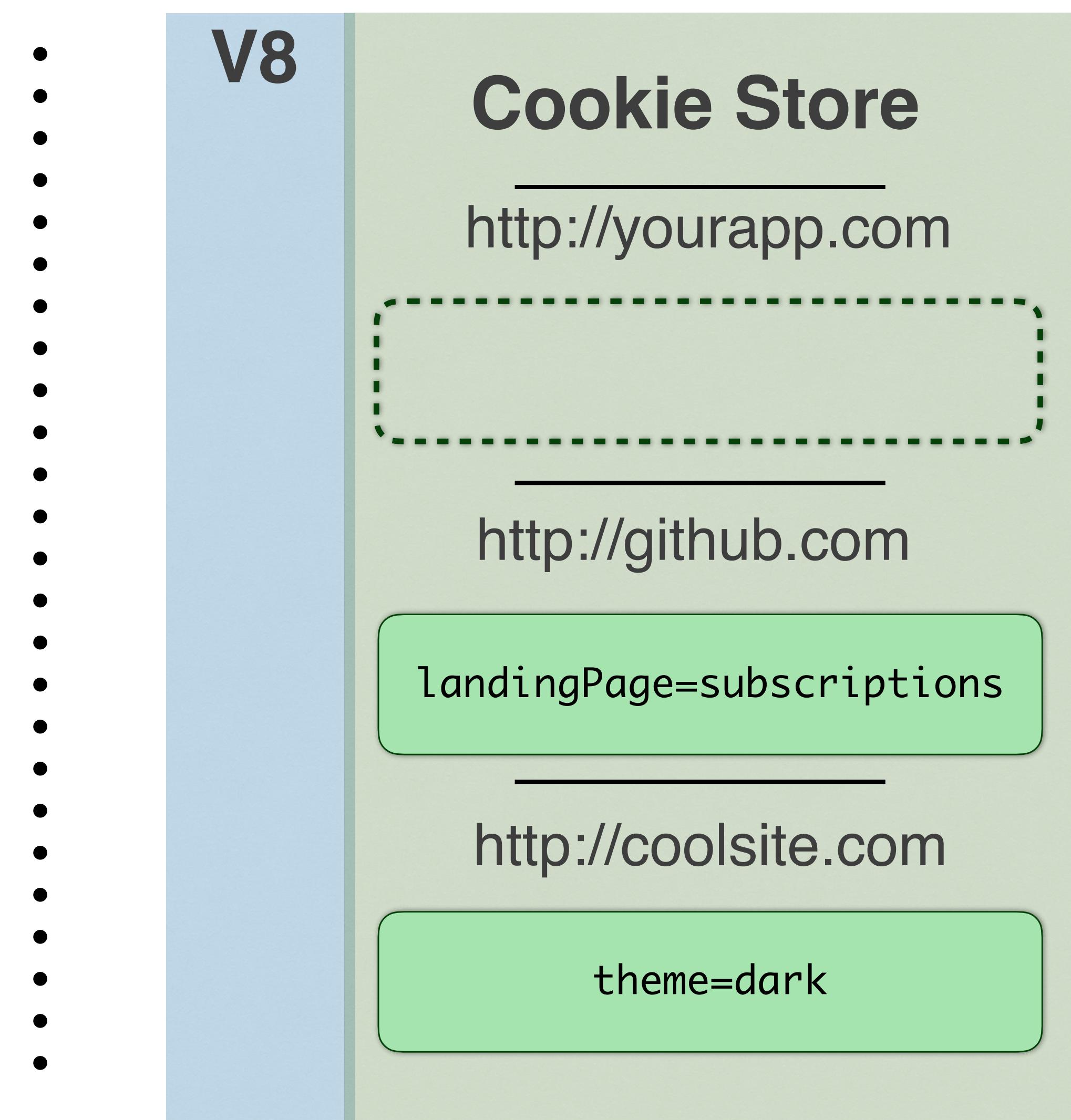


Server (Backend)

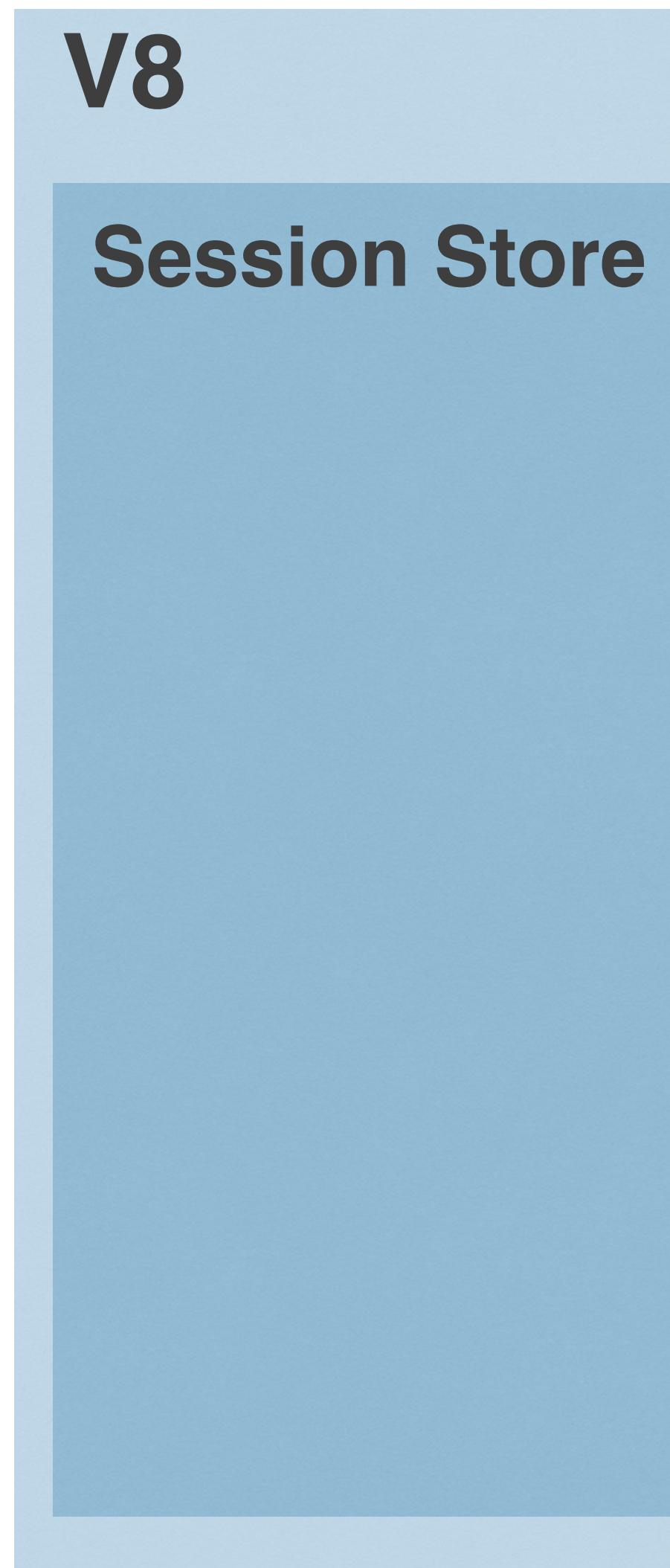


<http://yourapp.com>

Internet (HTTP)

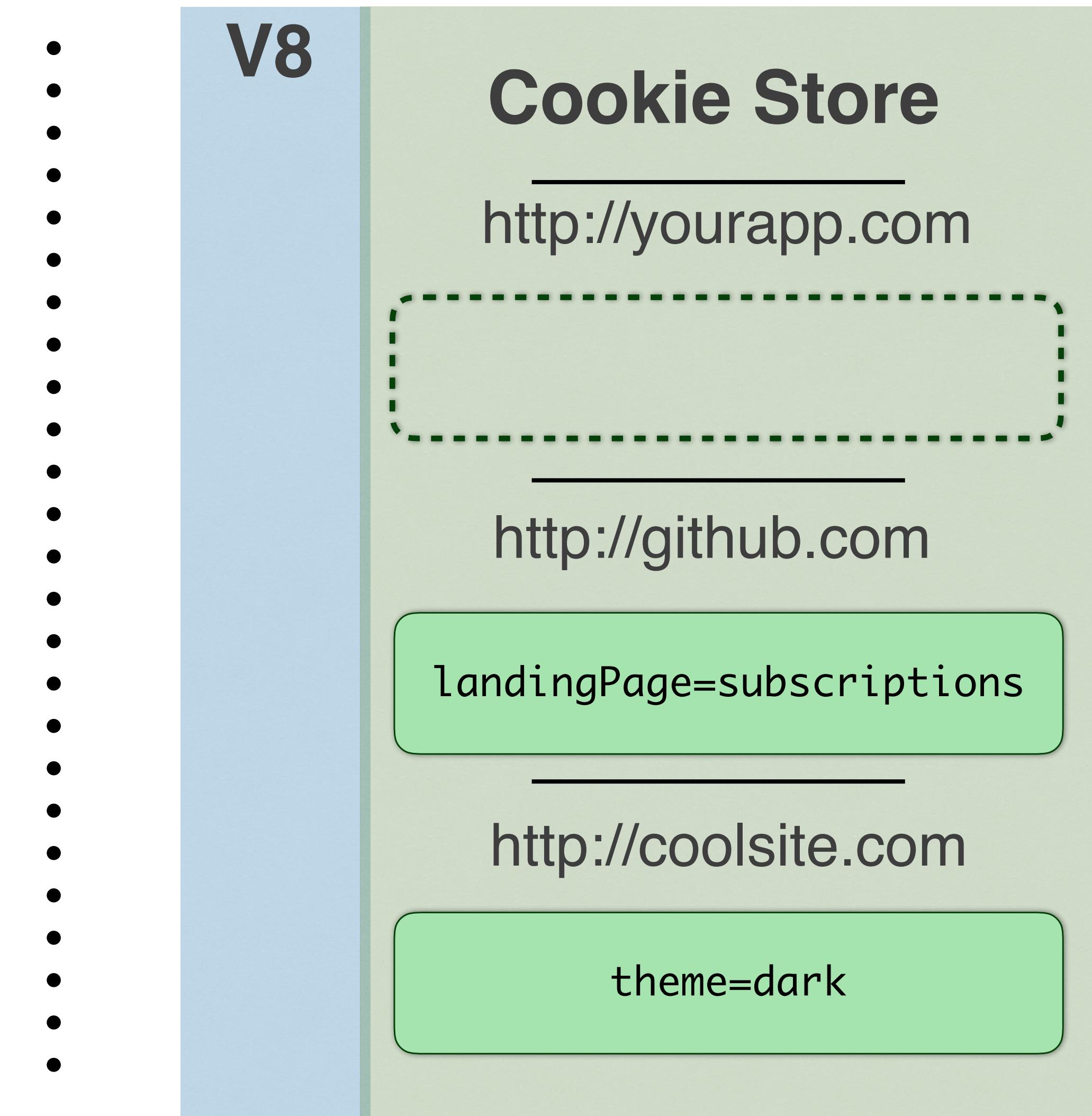


Server (Backend)



<http://yourapp.com>

Internet (HTTP)



HTTP REQUEST

(headers)

GET / HTTP/1.1
Host: yourapp.com
Connection: keep-alive
Accept: text/html
User-Agent: Chrome/
48.0.2564.116
...etc...

(body)

HTTP REQUEST

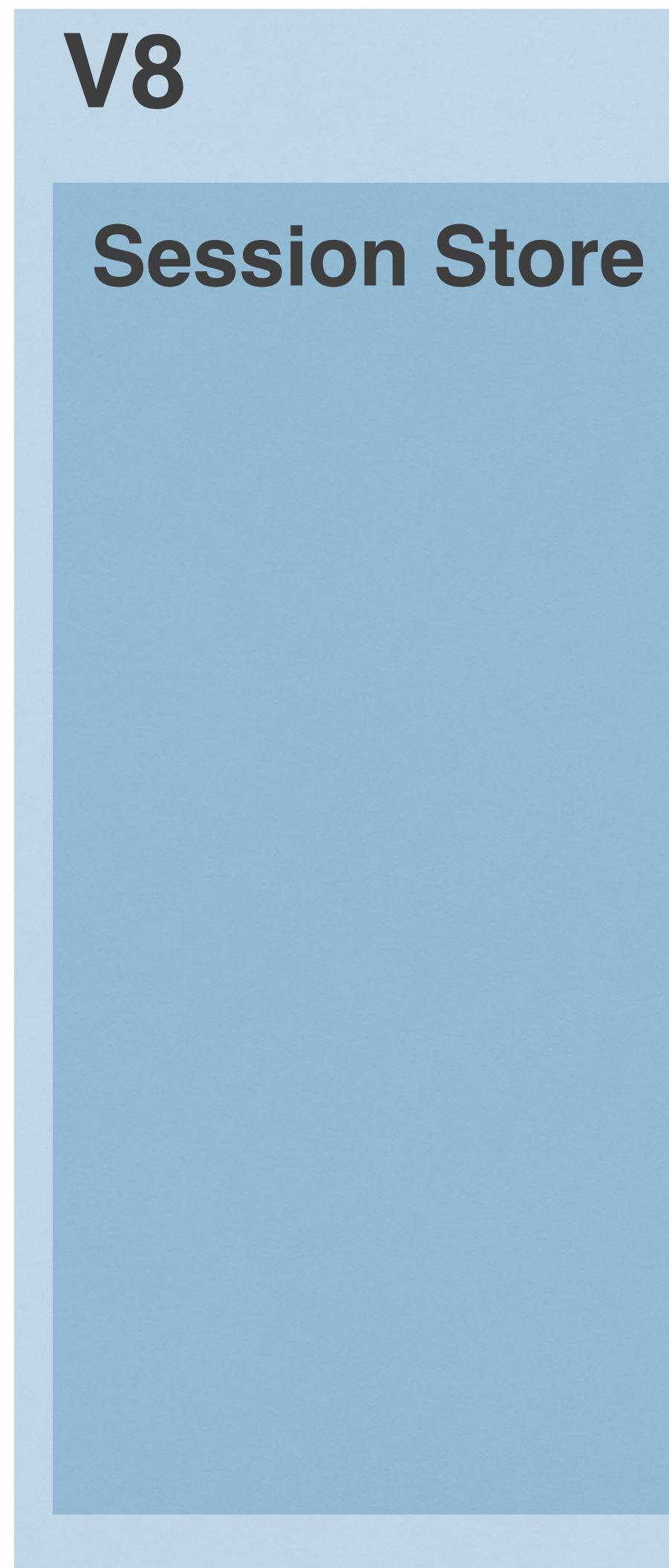
(headers)

(body)

GET / HTTP/1.1
Host: yourapp.com
Connection: keep-alive
Accept: text/html
User-Agent: Chrome/
48.0.2564.116
...etc...

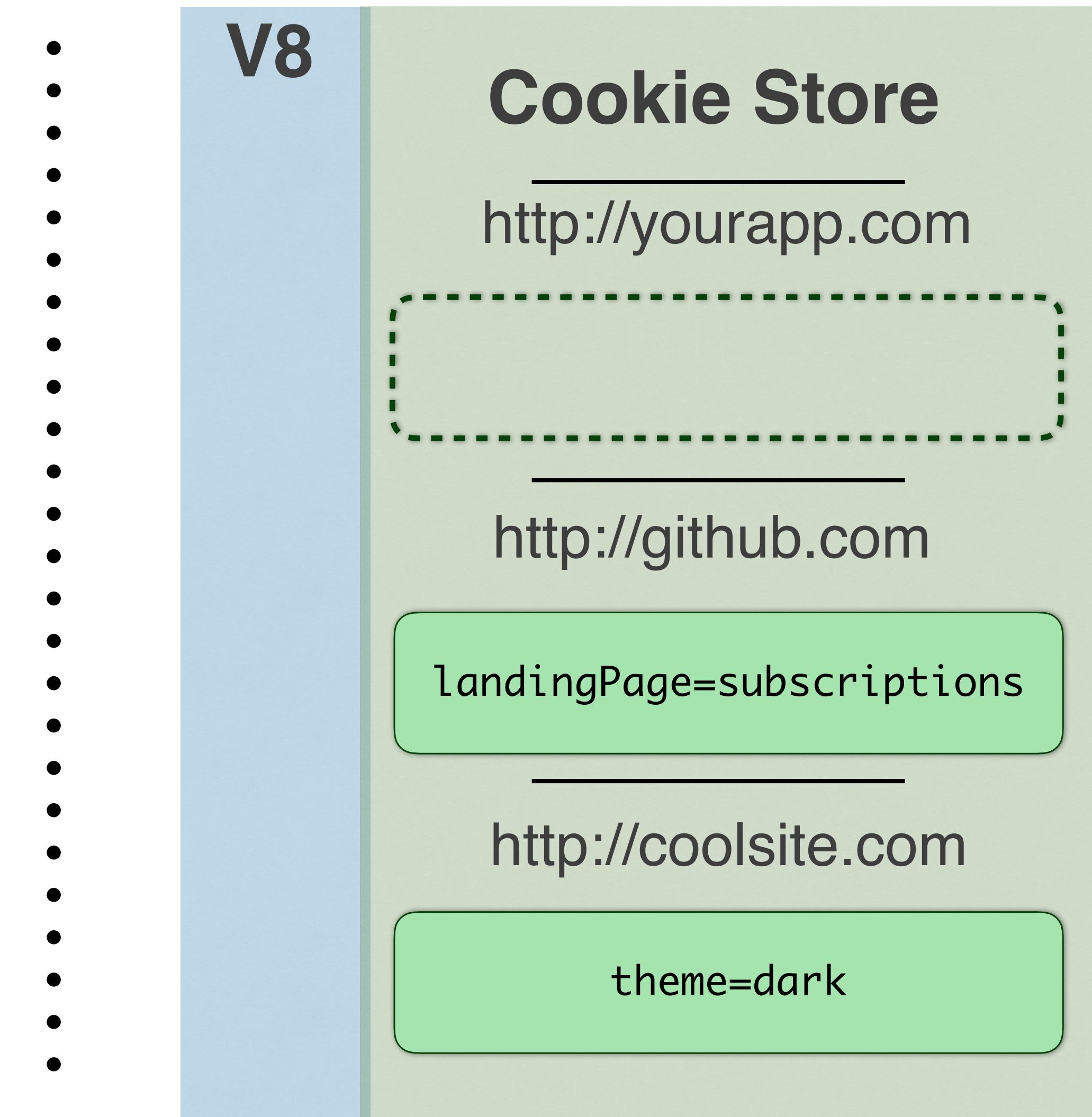
still no cookie info...
session middleware:
"let's make a session!"

Server (Backend)

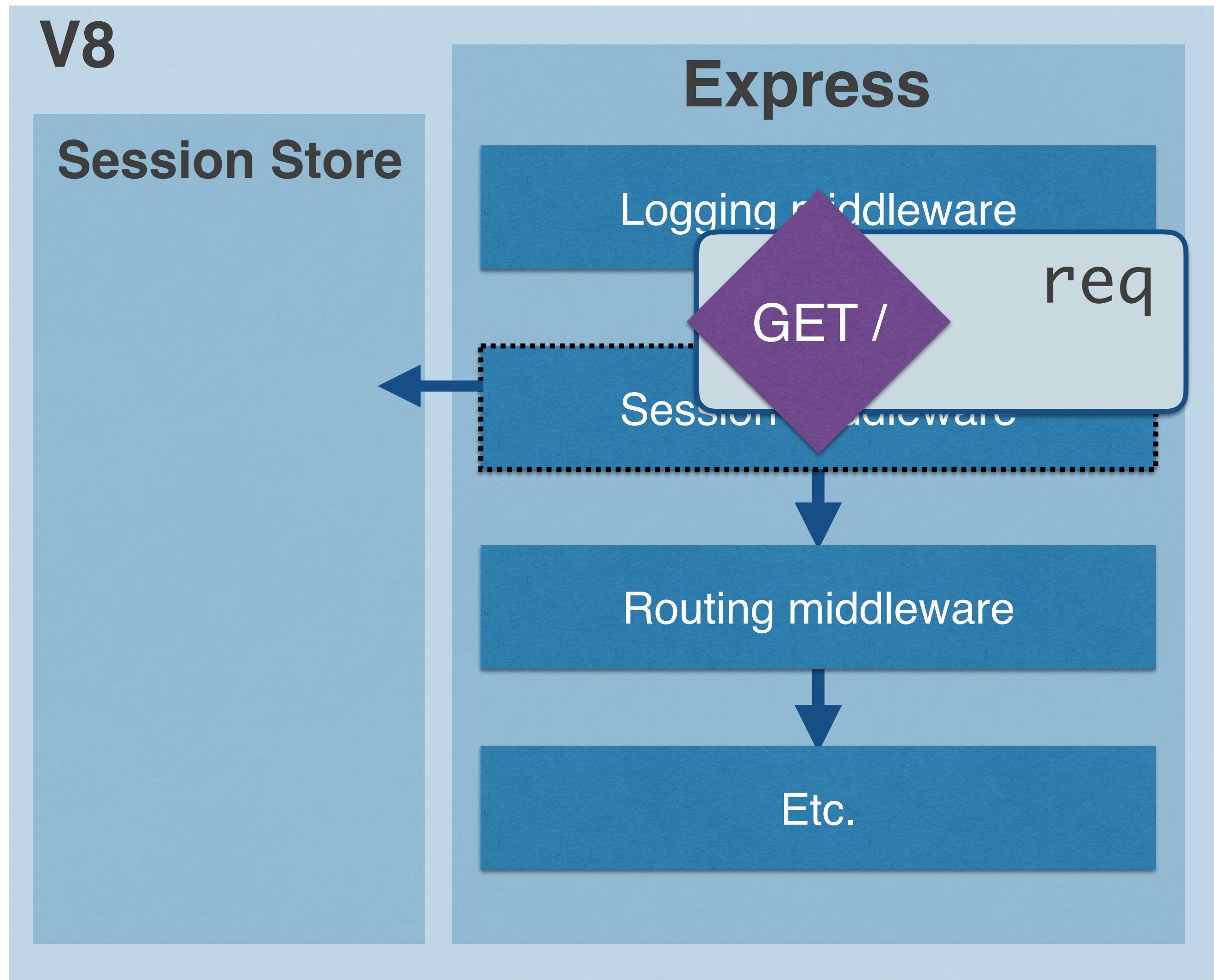


<http://yourapp.com>

Internet (HTTP)



Server (Backend)



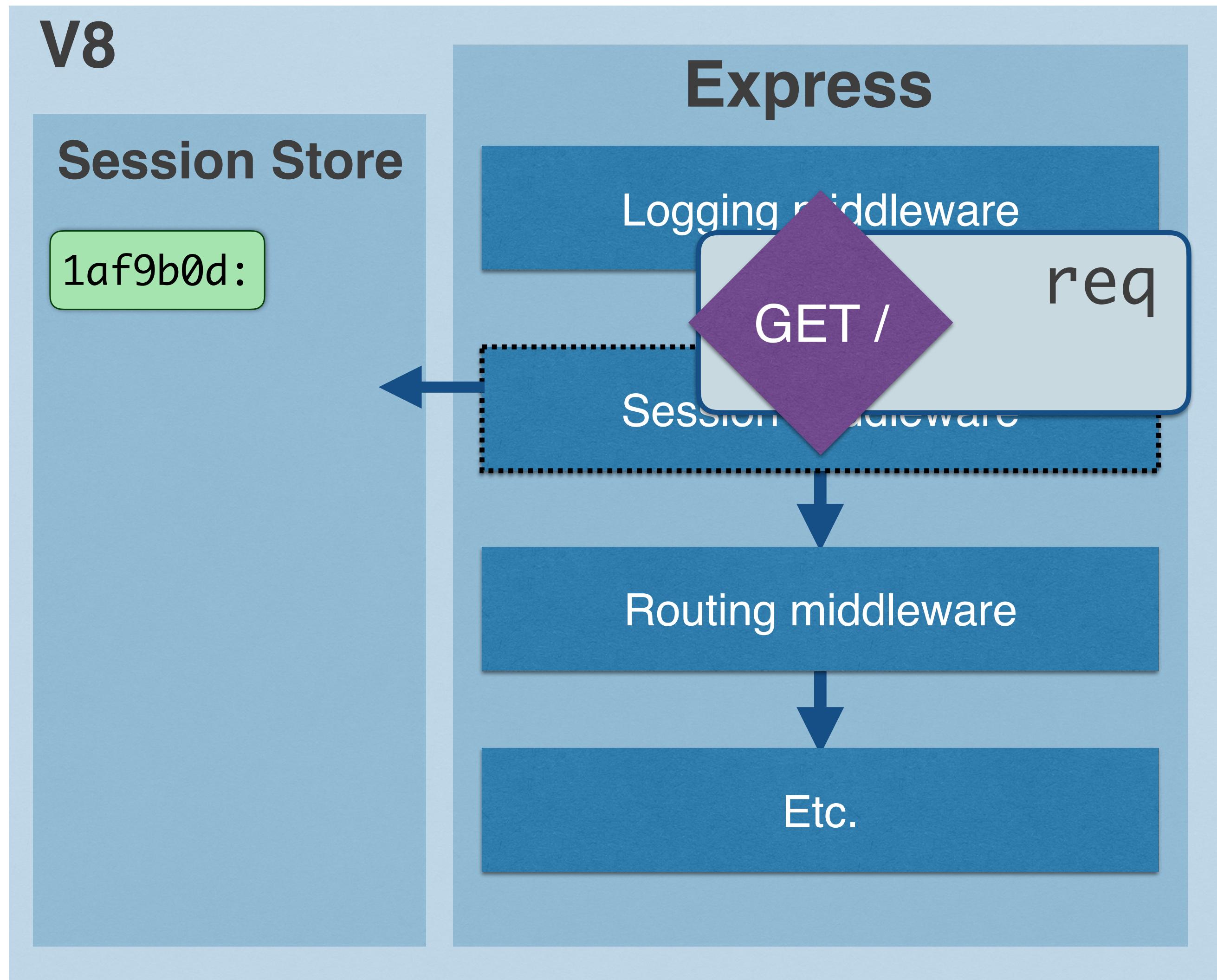
<http://yourapp.com>

Internet (HTTP)



Client (Browser)

Server (Backend)

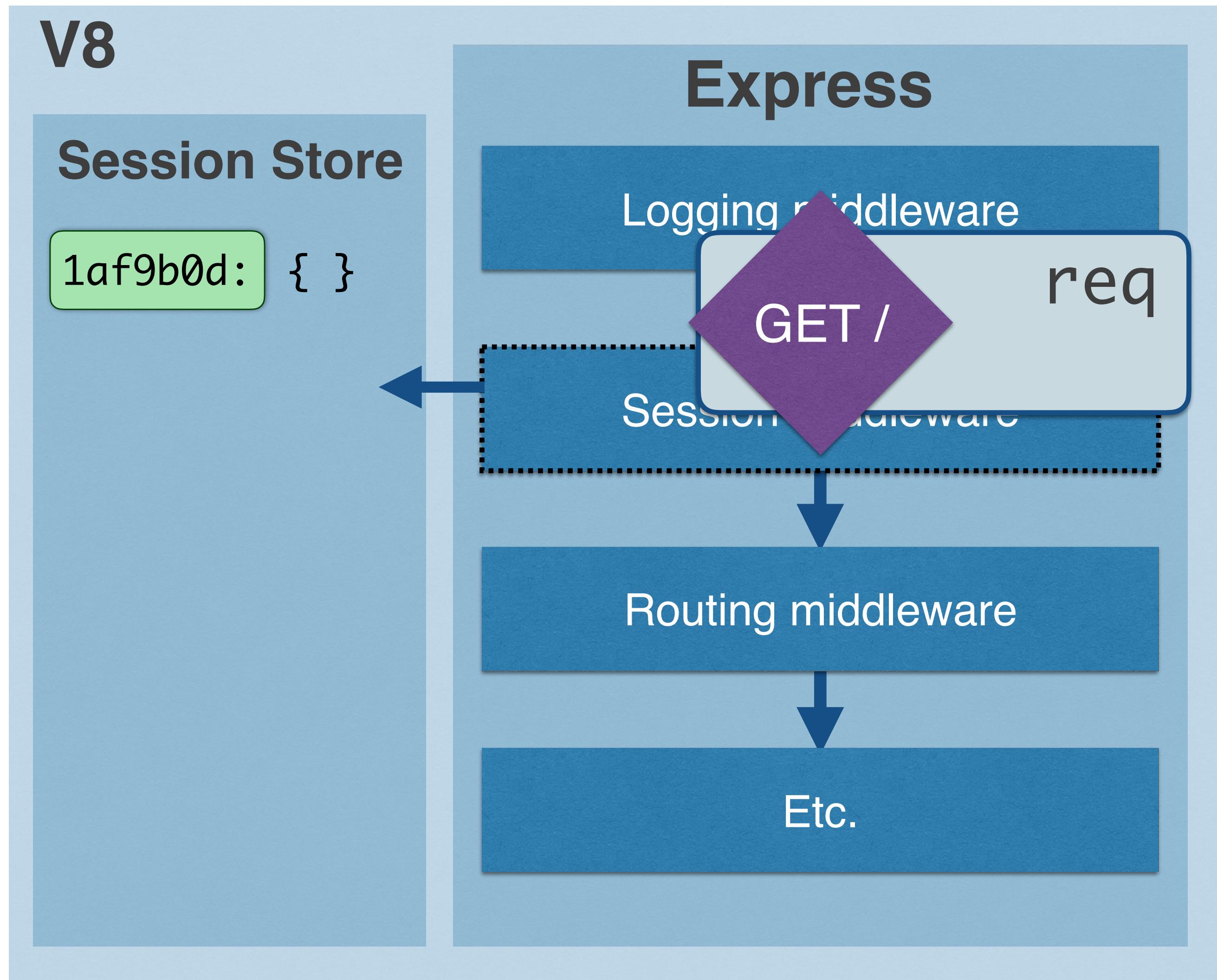


<http://yourapp.com>

Internet (HTTP)



Server (Backend)



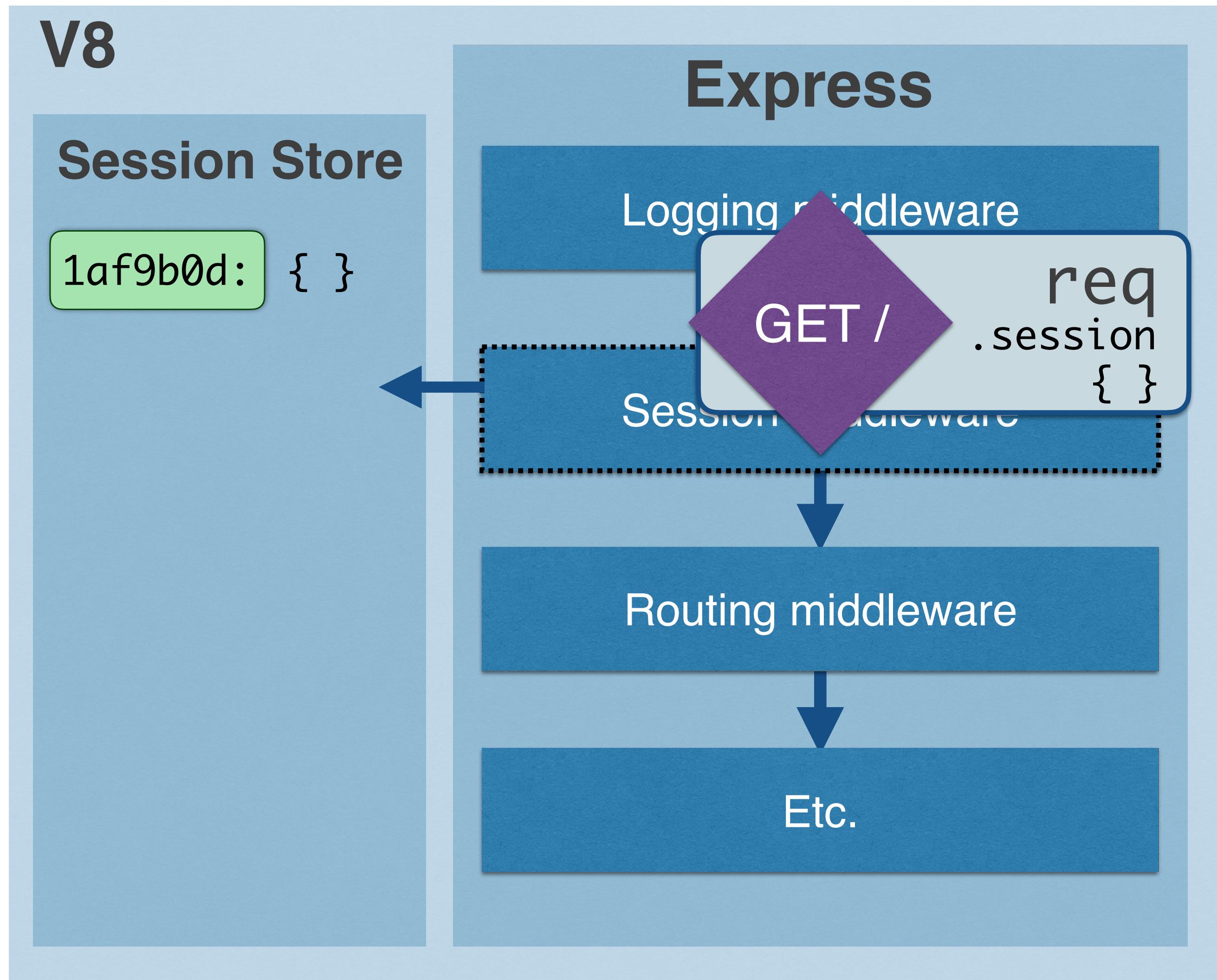
<http://yourapp.com>

Internet (HTTP)



Client (Browser)

Server (Backend)



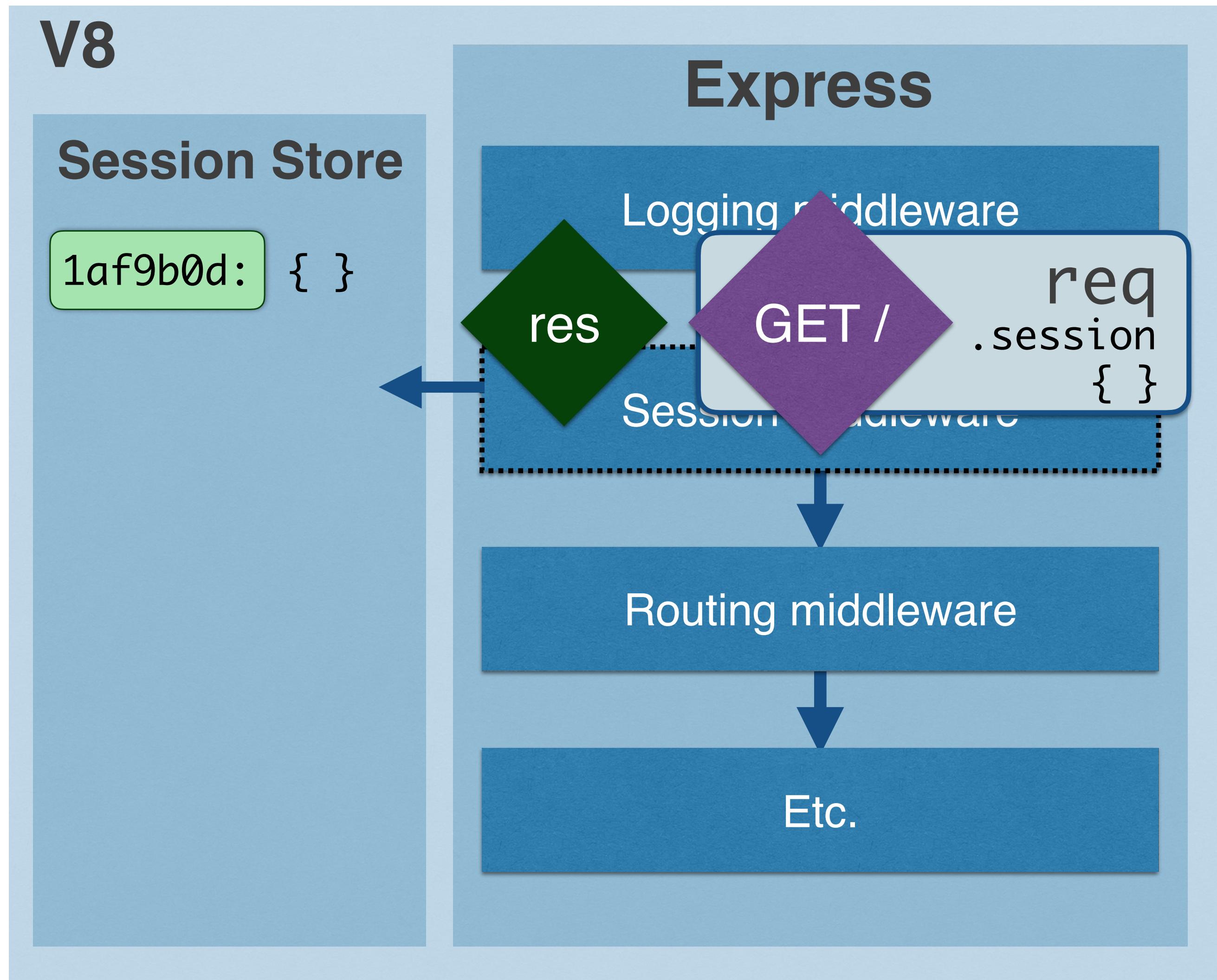
<http://yourapp.com>

Internet (HTTP)



AUTH

Server (Backend)



<http://yourapp.com>

Internet (HTTP)



HTTP RESPONSE

HTTP/1.x 200 OK
Transfer-Encoding: chunked
Date: Mon, 22 Feb 2016 18:30:00 GMT
Content-Type: text/html
Content-Encoding: gzip

(headers)

(body, after
routing is
done)

```
<!DOCTYPE html>
<html>
  <head>
    <title>Your Sweet App</title>
    <script src="/js/main.js"></script>
  </head> ...etc.
```

HTTP RESPONSE

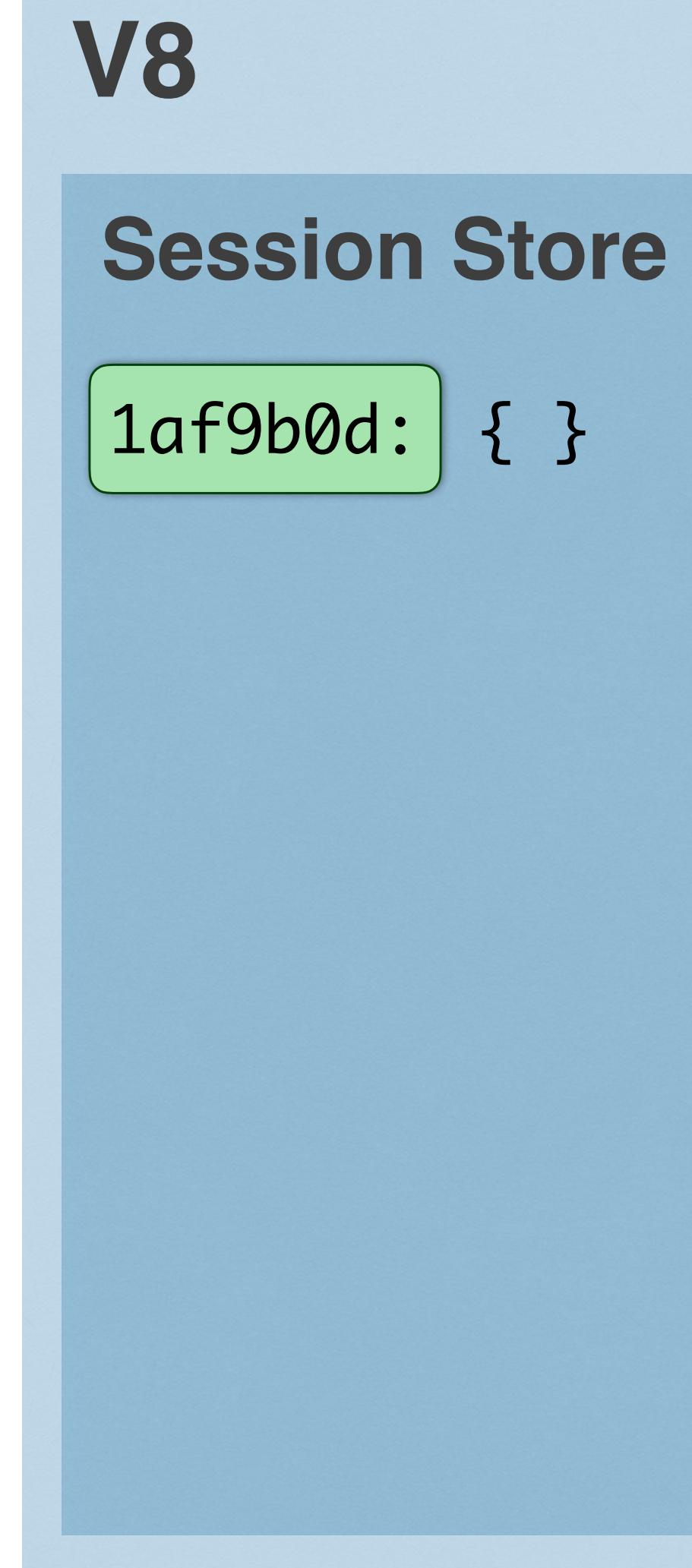
(headers)

HTTP/1.x 200 OK
Transfer-Encoding: chunked
Date: Mon, 22 Feb 2016 18:30:00 GMT
Content-Type: text/html
Content-Encoding: gzip
set-cookie: myUid=1af9b0d

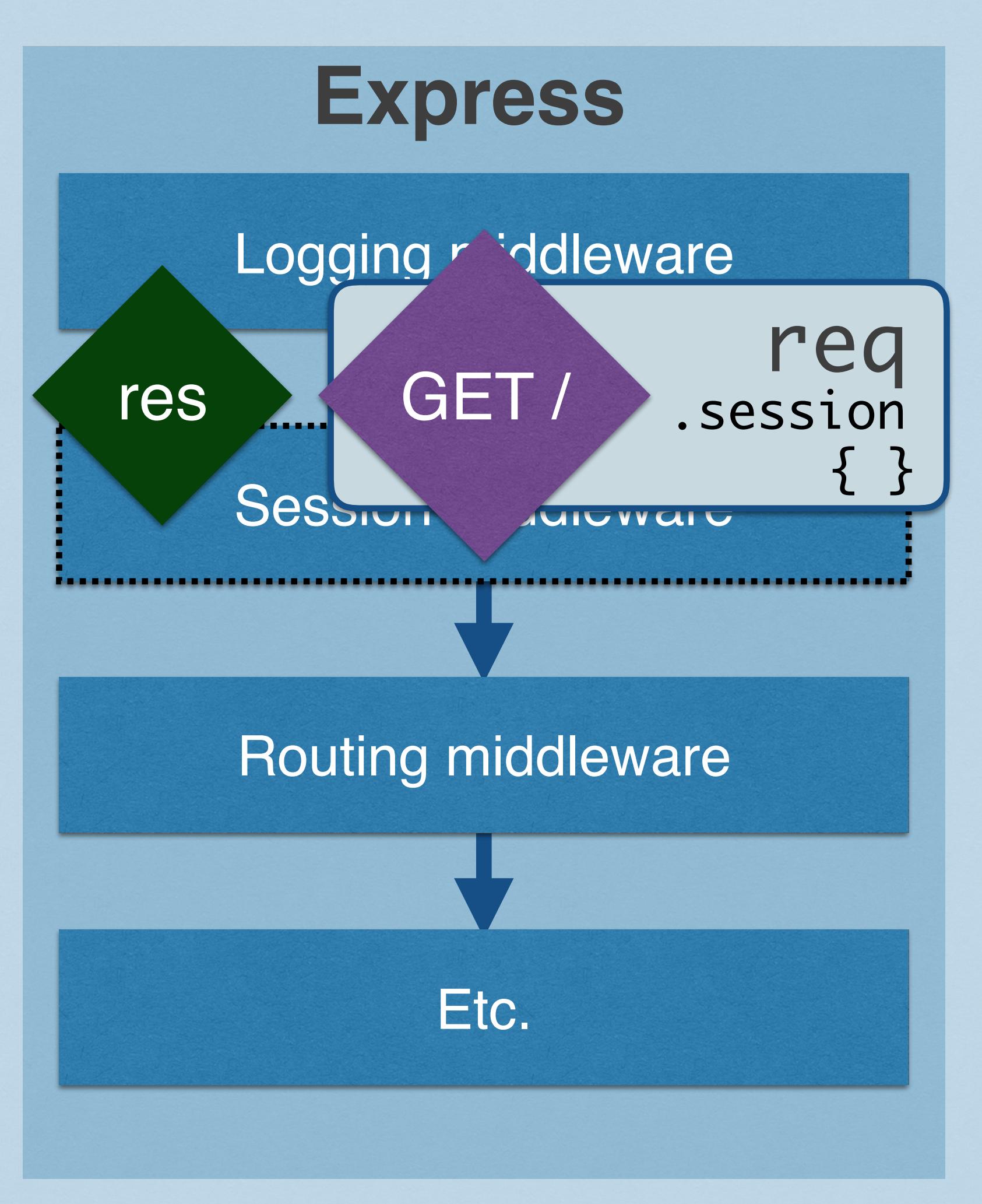
**(body, after
routing is
done)**

```
<!DOCTYPE html>
<html>
  <head>
    <title>Your Sweet App</title>
    <script src="/js/main.js"></script>
  </head> ...etc.
```

Server (Backend)



Internet (HTTP)

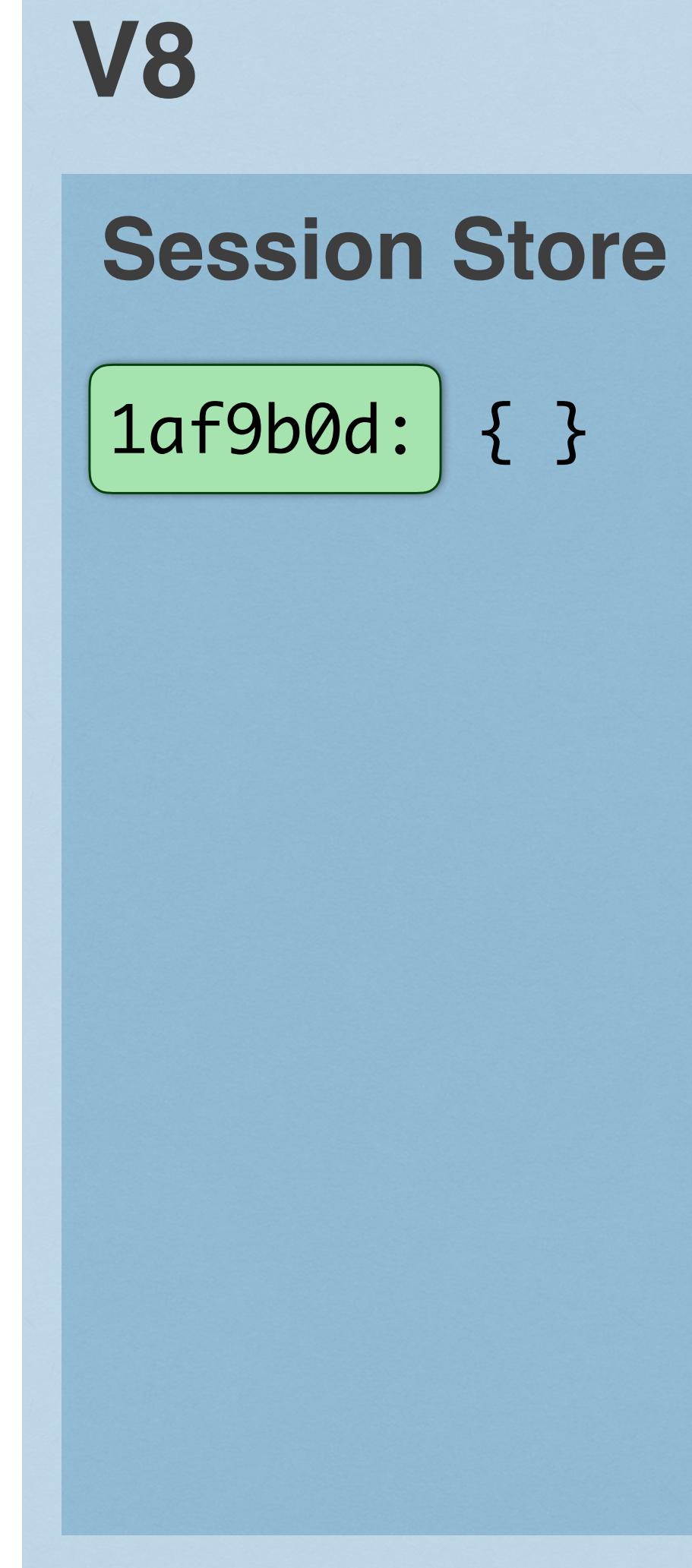


<http://yourapp.com>

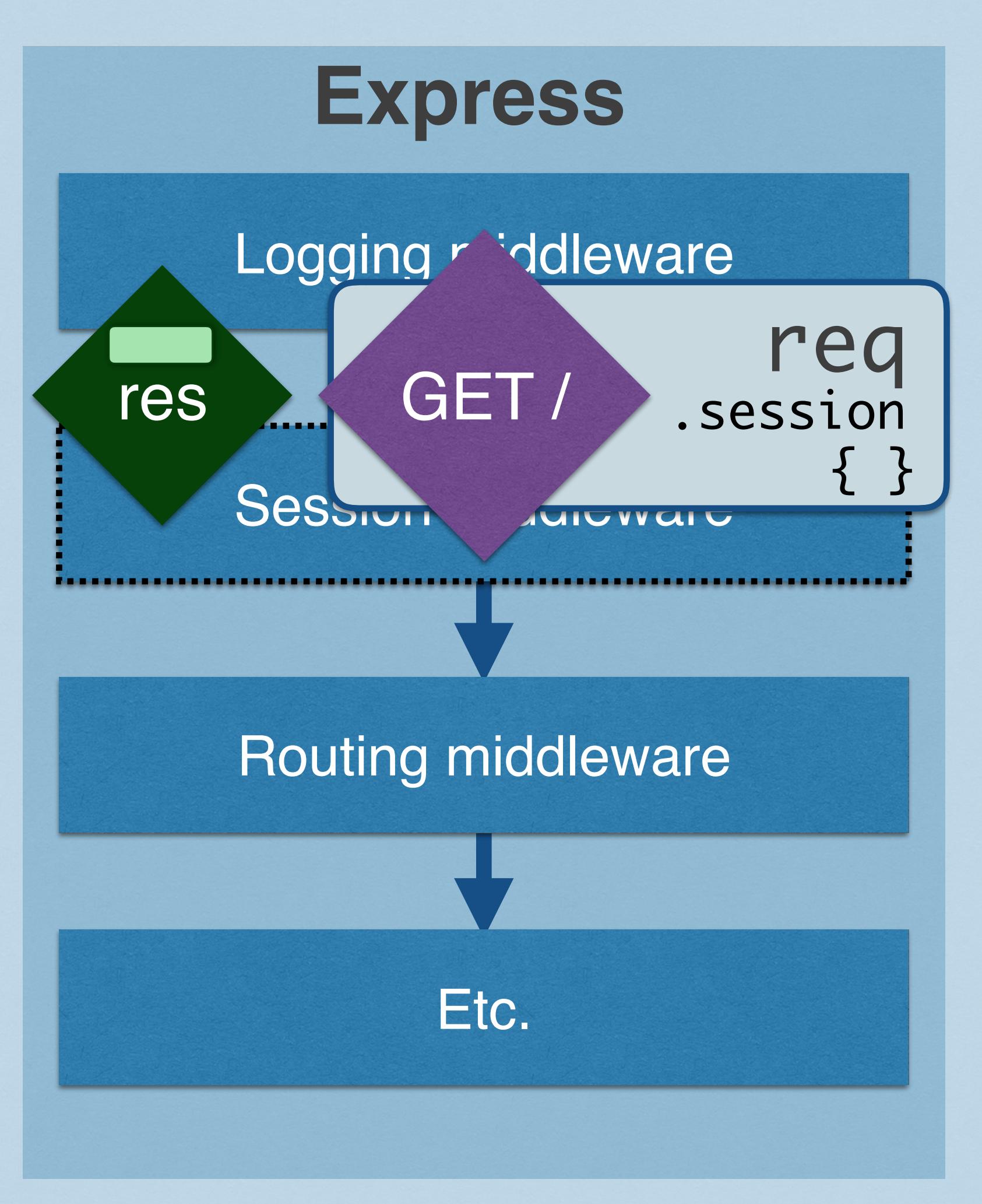
Client (Browser)



Server (Backend)

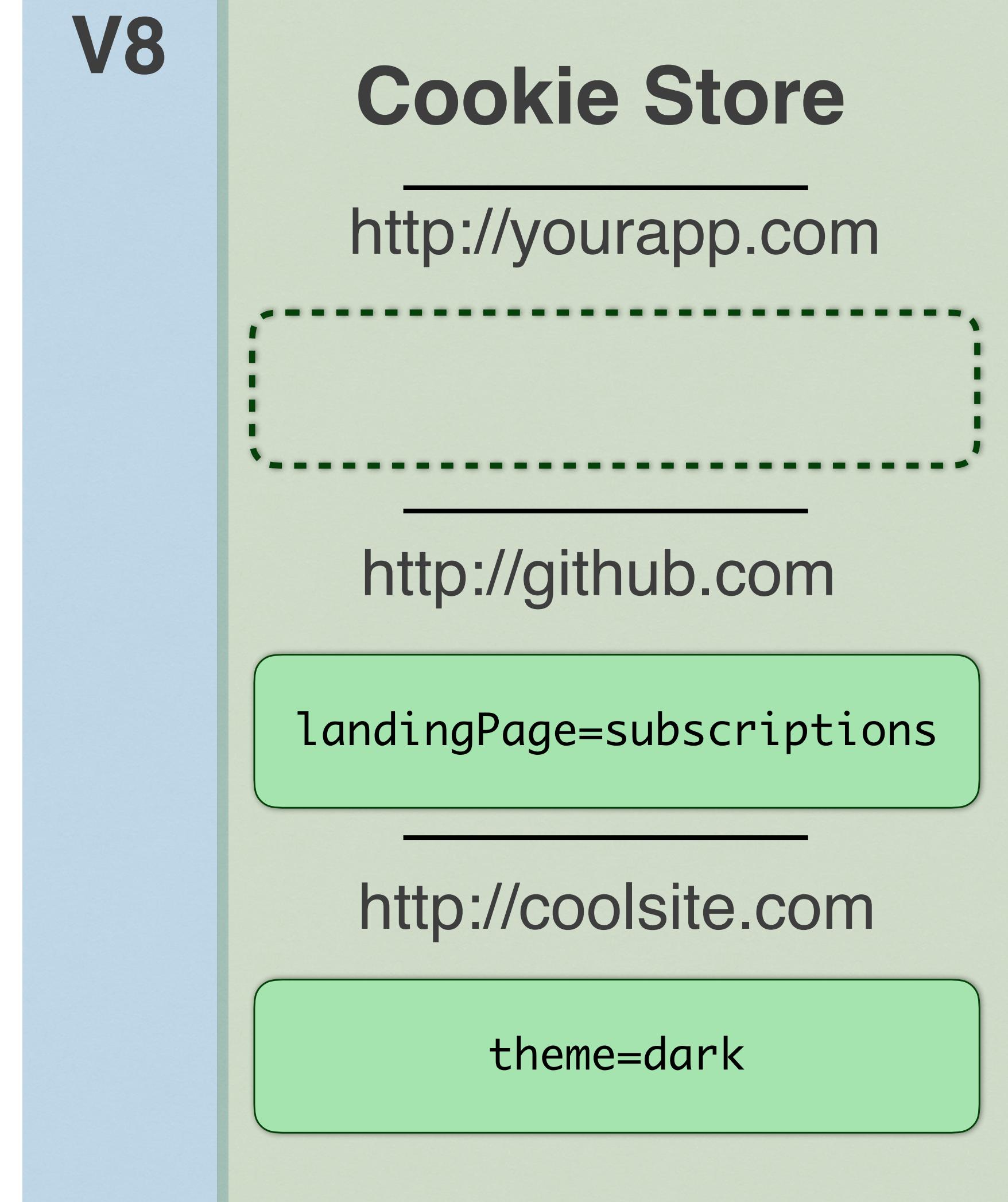


Internet (HTTP)

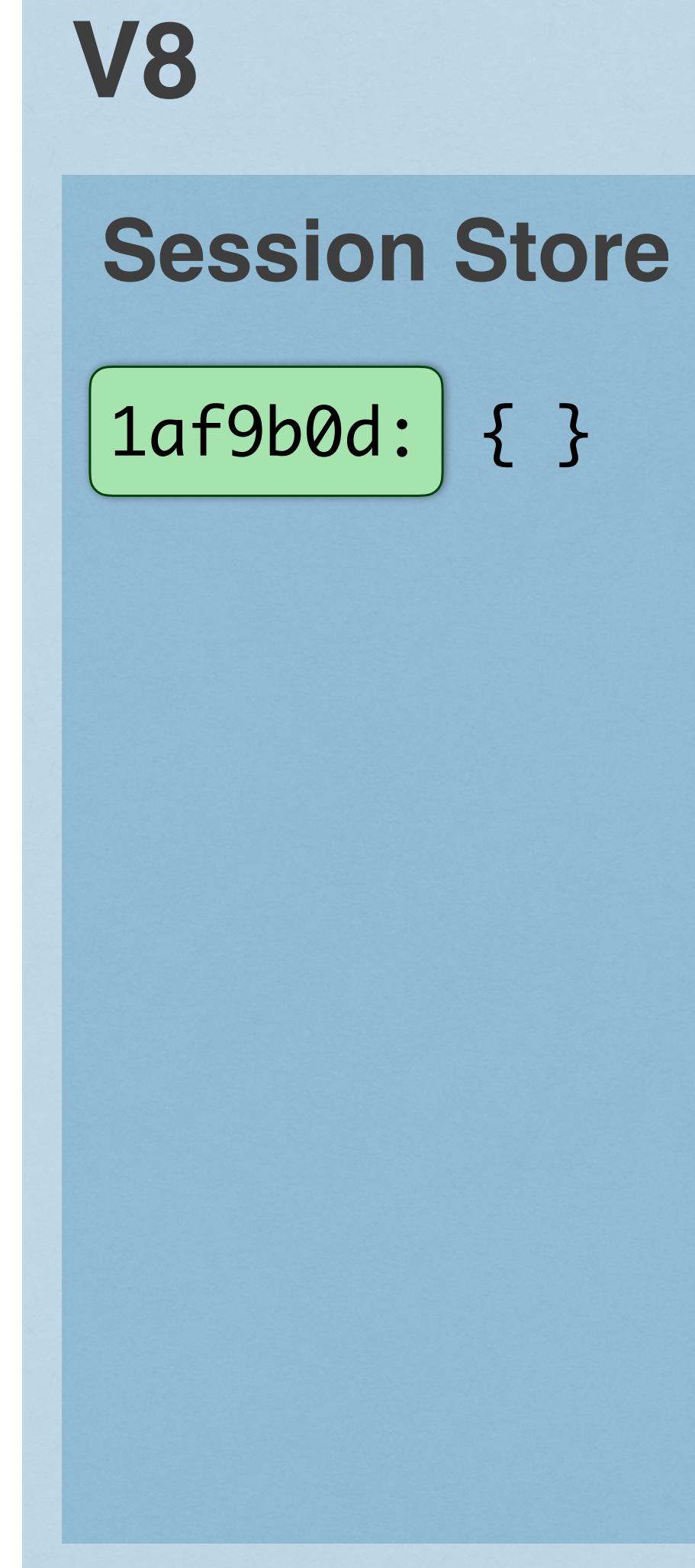


<http://yourapp.com>

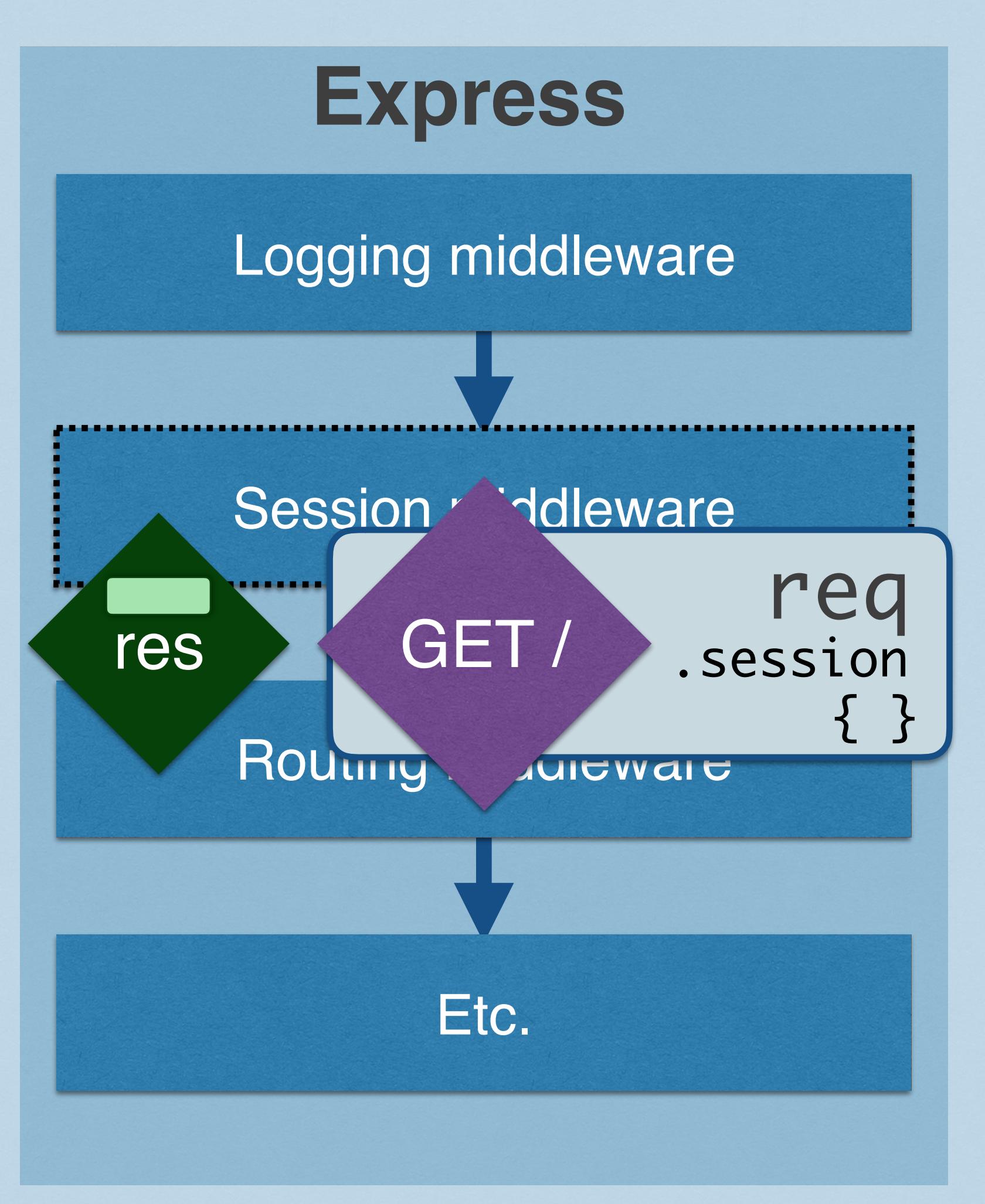
Client (Browser)



Server (Backend)



Internet (HTTP)

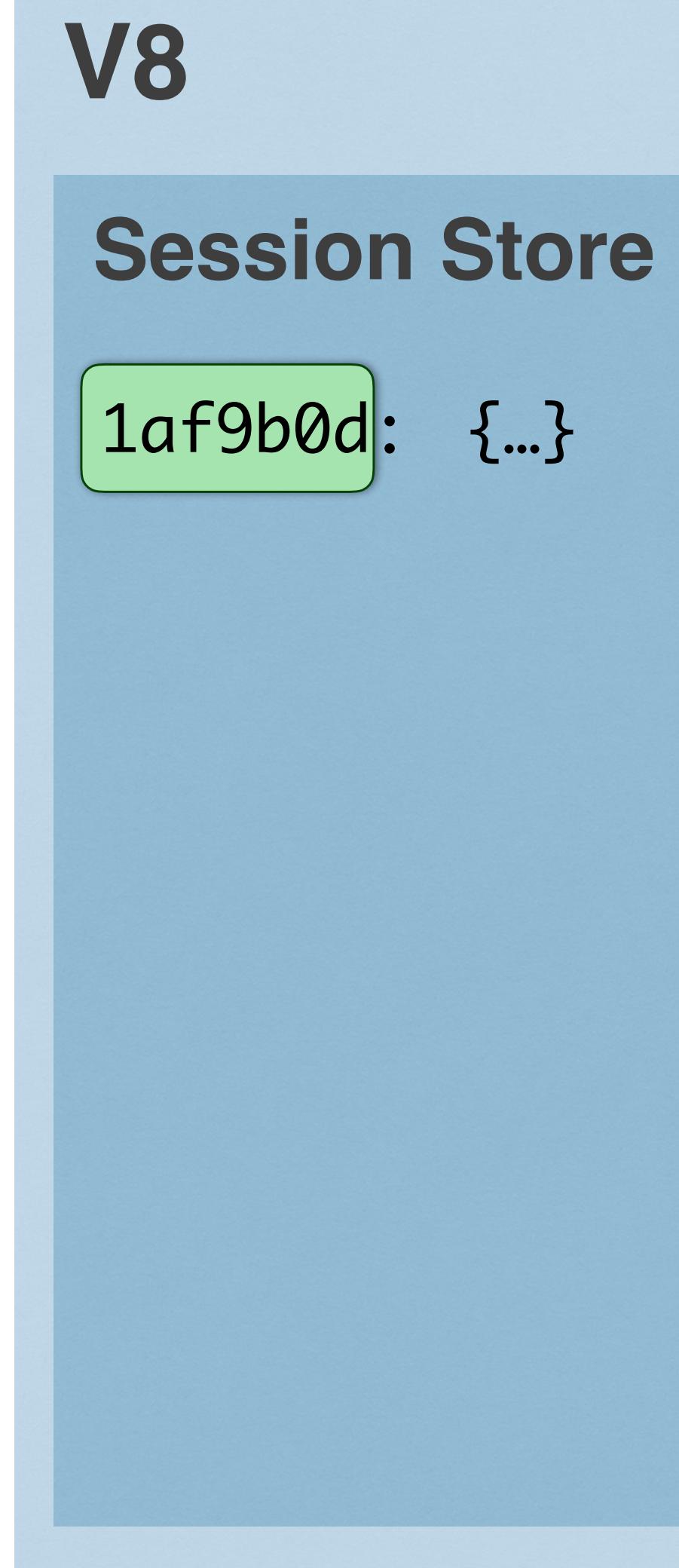


<http://yourapp.com>

Client (Browser)

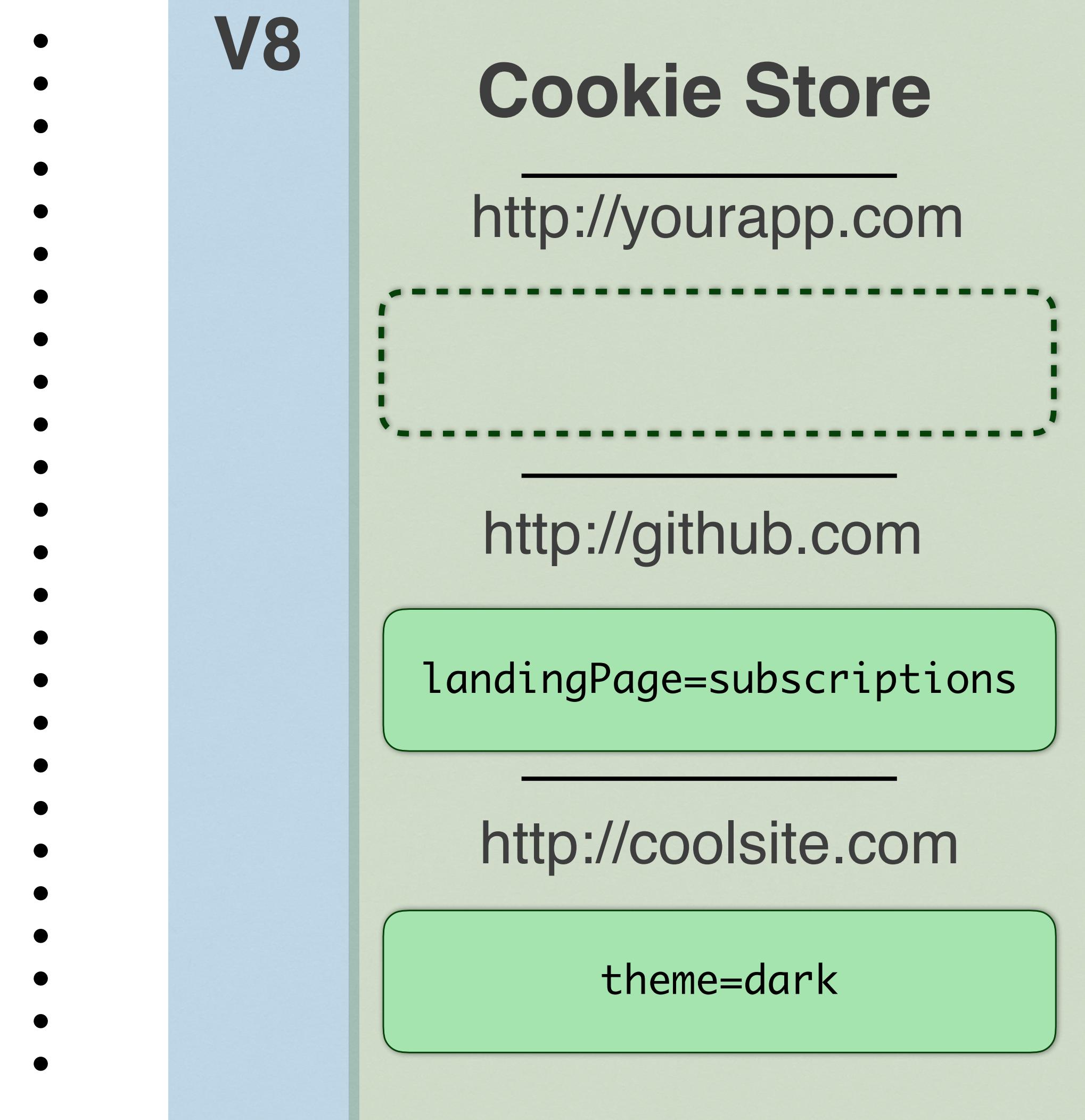


Server (Backend)

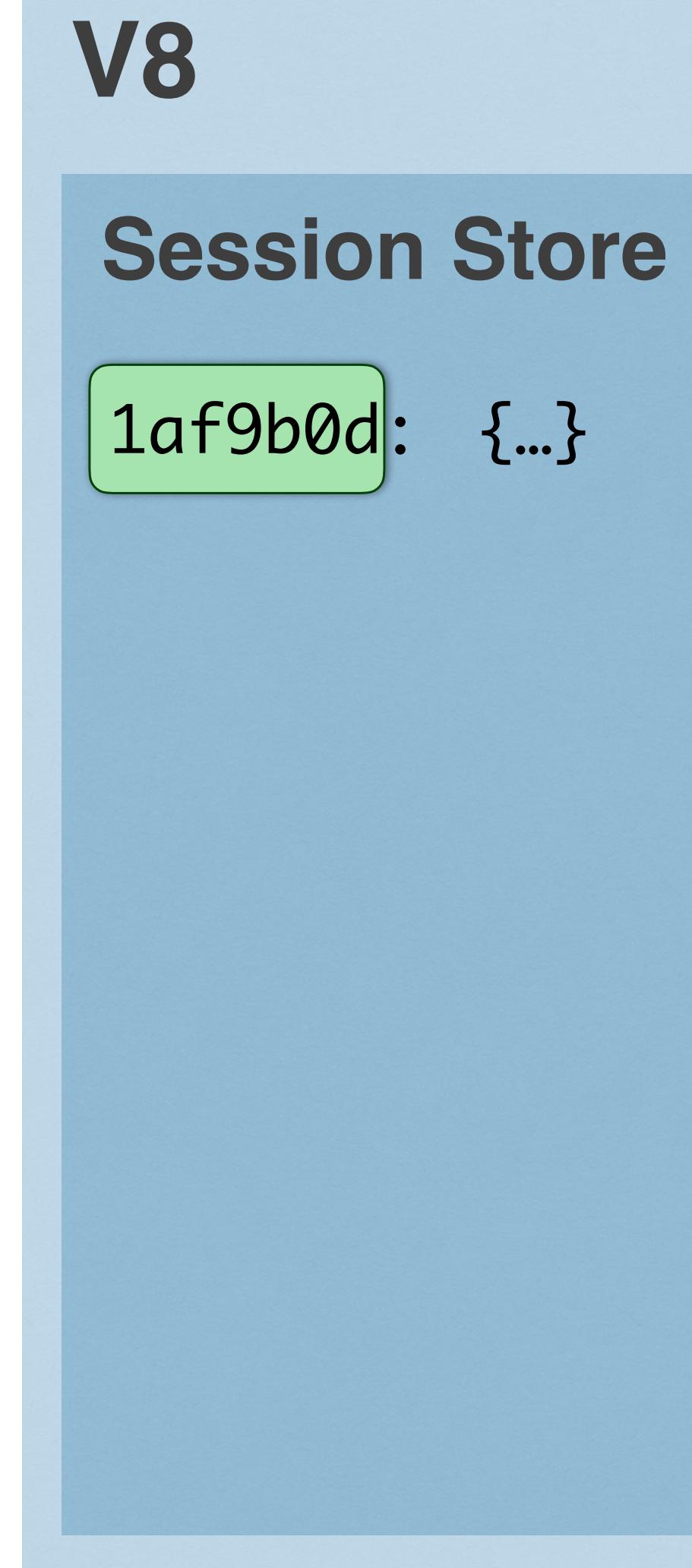


<http://yourapp.com>

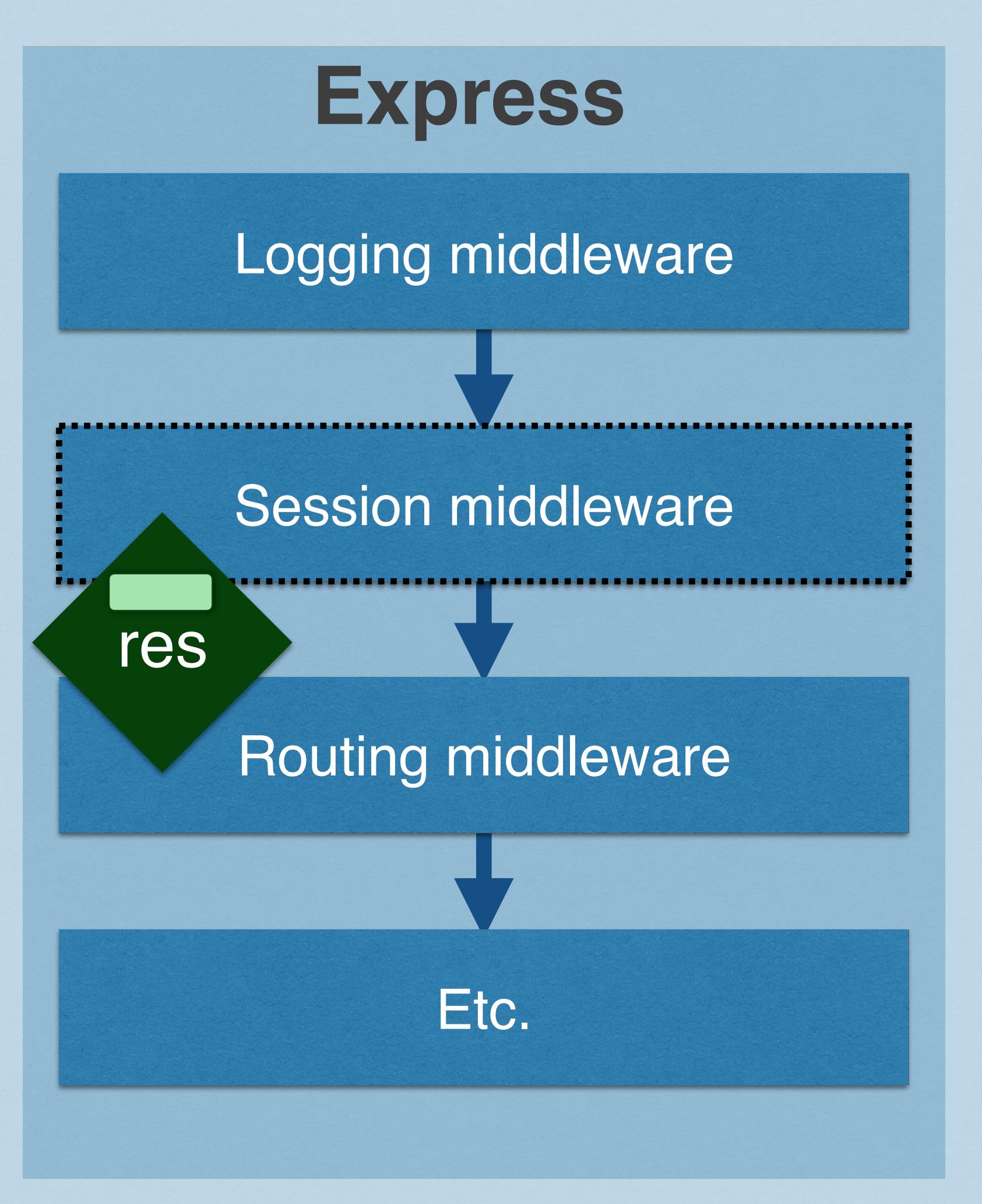
Internet (HTTP)



Server (Backend)

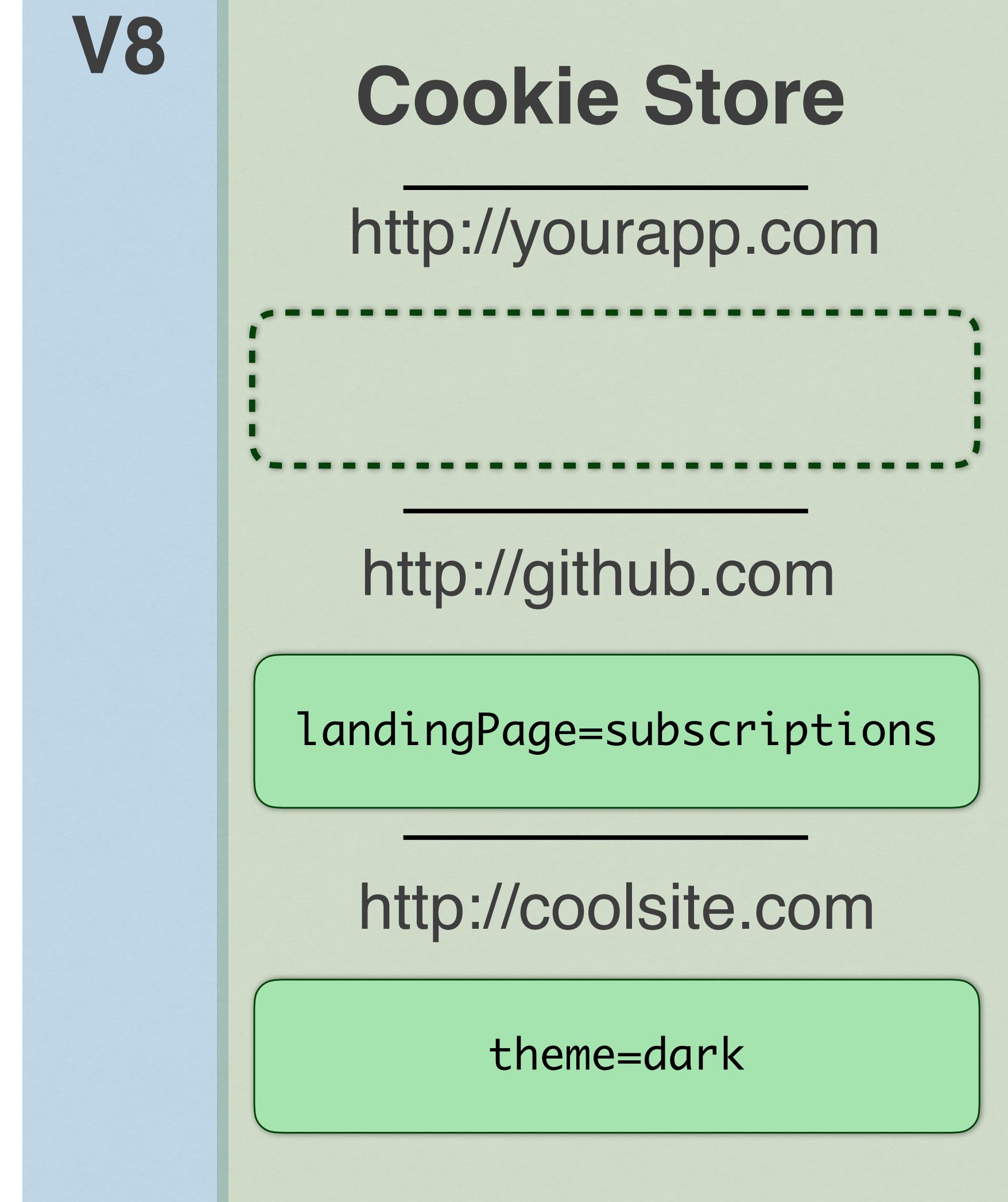


Internet (HTTP)

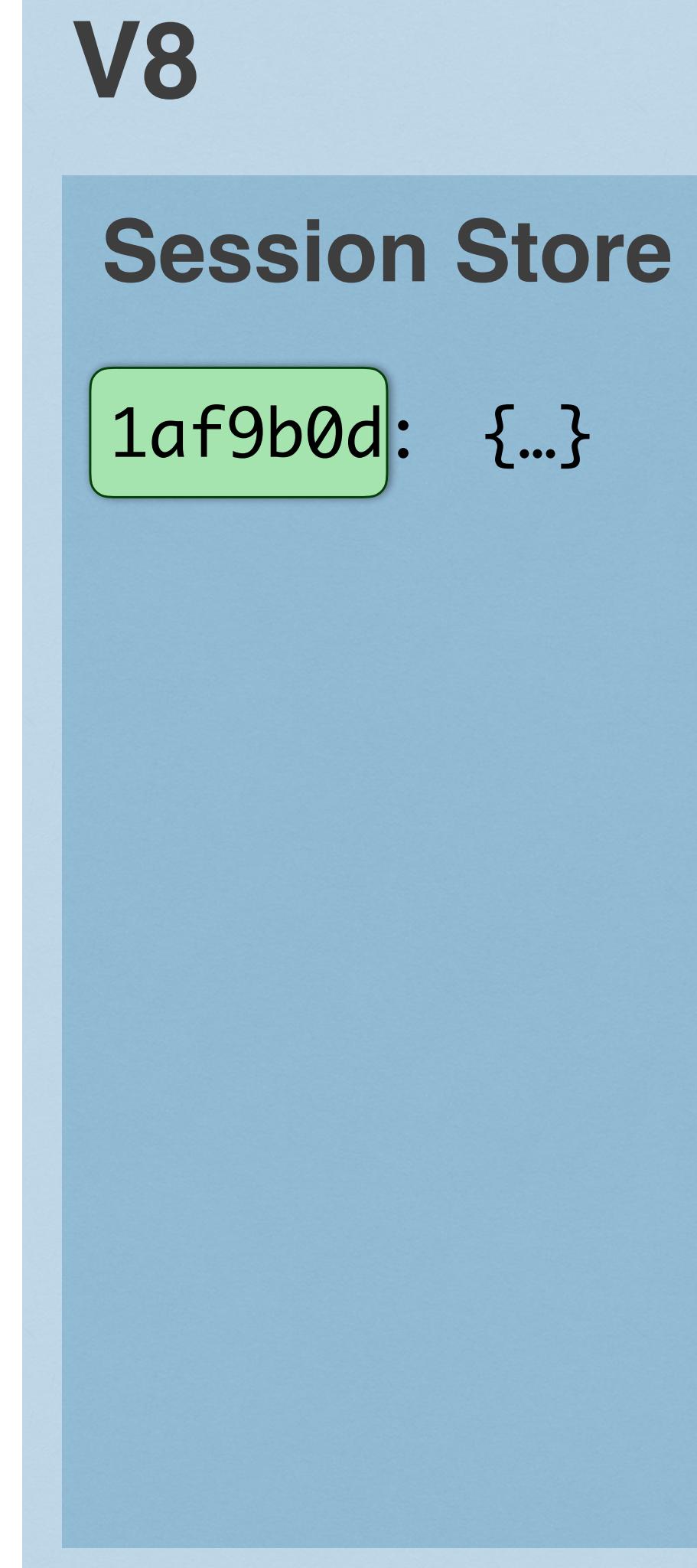


<http://yourapp.com>

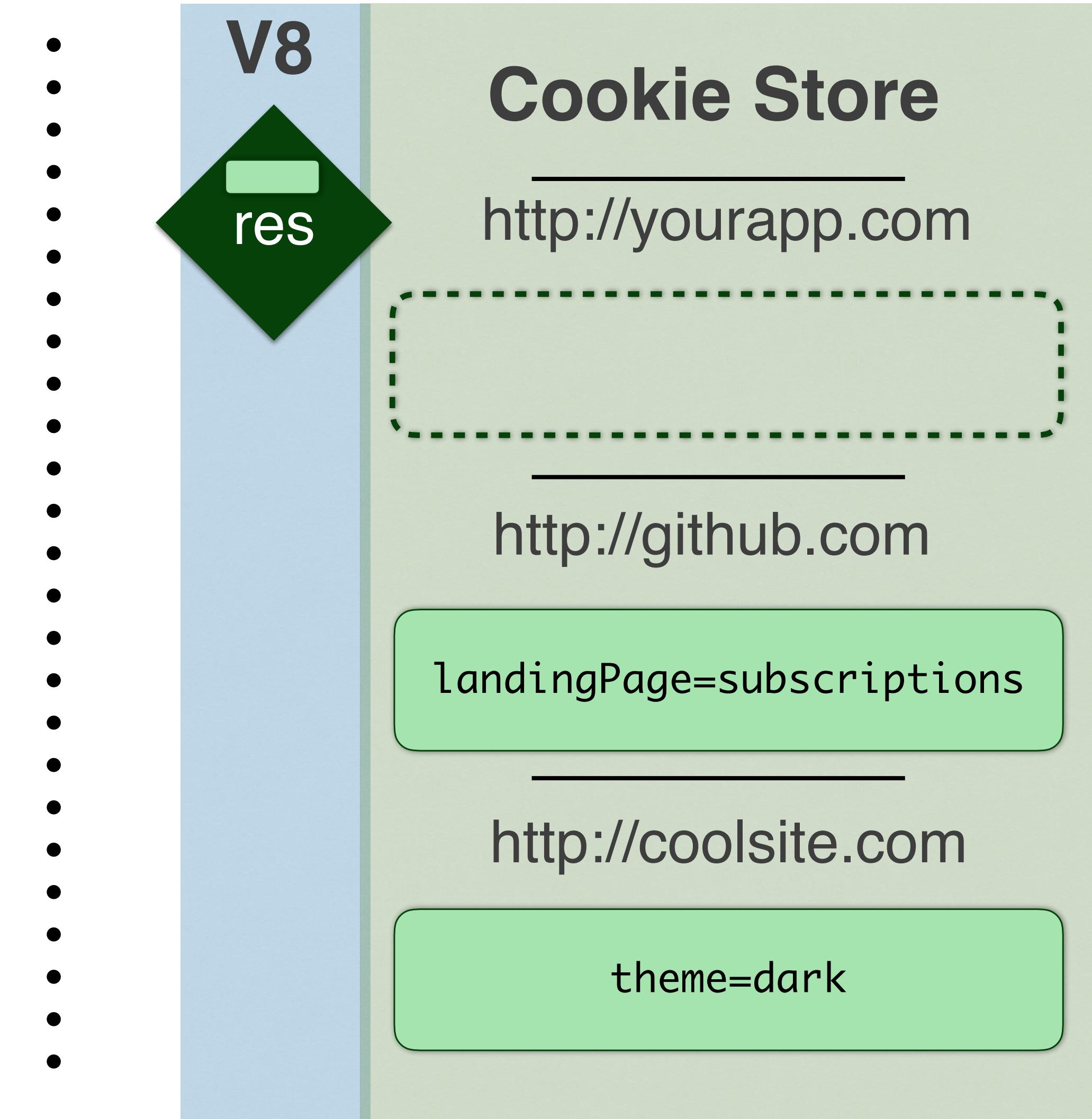
Client (Browser)



Server (Backend)



Internet (HTTP)



`http://yourapp.com`

HTTP RESPONSE

(headers)

HTTP/1.x 200 OK
Transfer-Encoding: chunked
Date: Mon, 22 Feb 2016 18:30:00 GMT
Content-Type: text/html
Content-Encoding: gzip
set-cookie: myUid=1af9b0d

**(body, after
routing is
done)**

```
<!DOCTYPE html>
<html>
  <head>
    <title>Your Sweet App</title>
    <script src="/js/main.js"></script>
  </head> ...etc.
```

HTTP RESPONSE

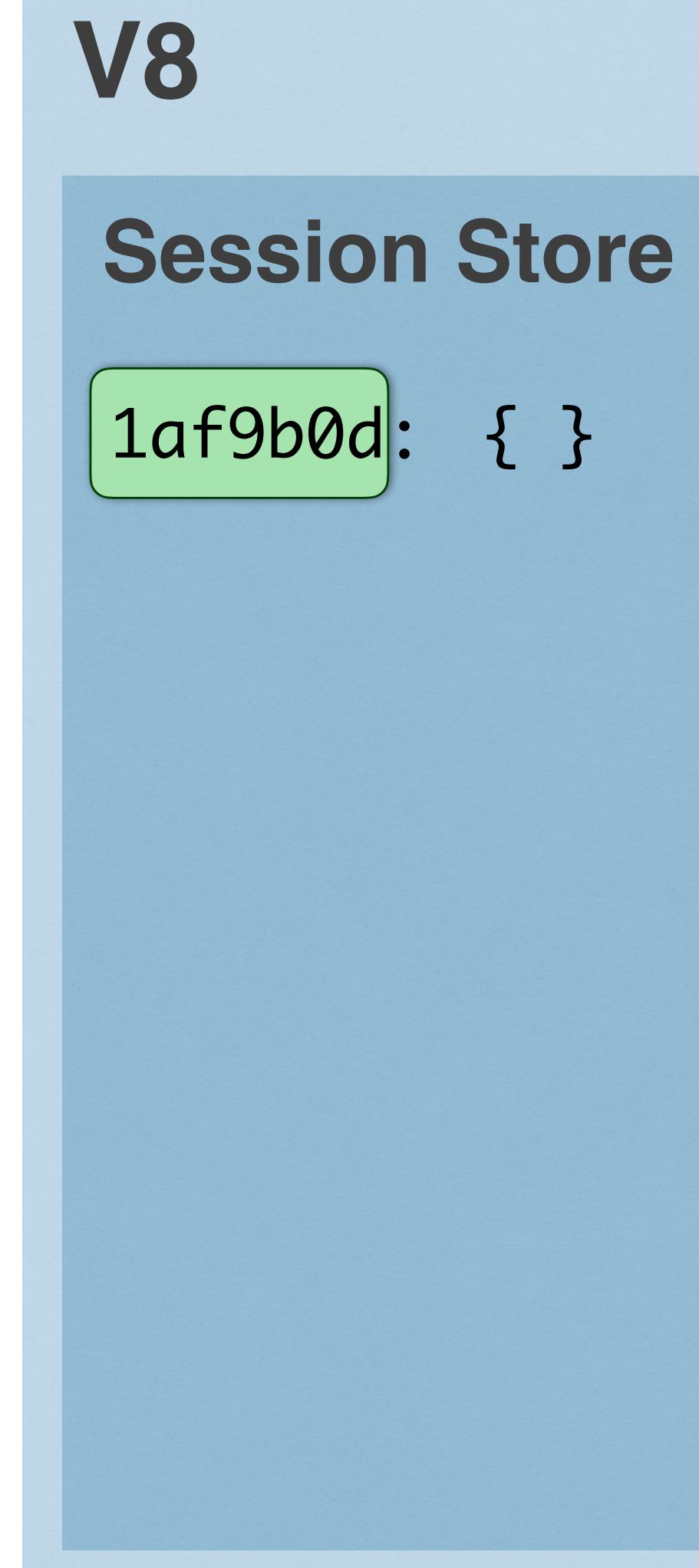
(headers)

HTTP/1.x 200 OK
Transfer-Encoding: chunked
Date: Mon, 22 Feb 2016 18:30:00 GMT
Content-Type: text/html
Content-Encoding: gzip
set-cookie: myUid=1af9b0d

(body, after
routing is
done)

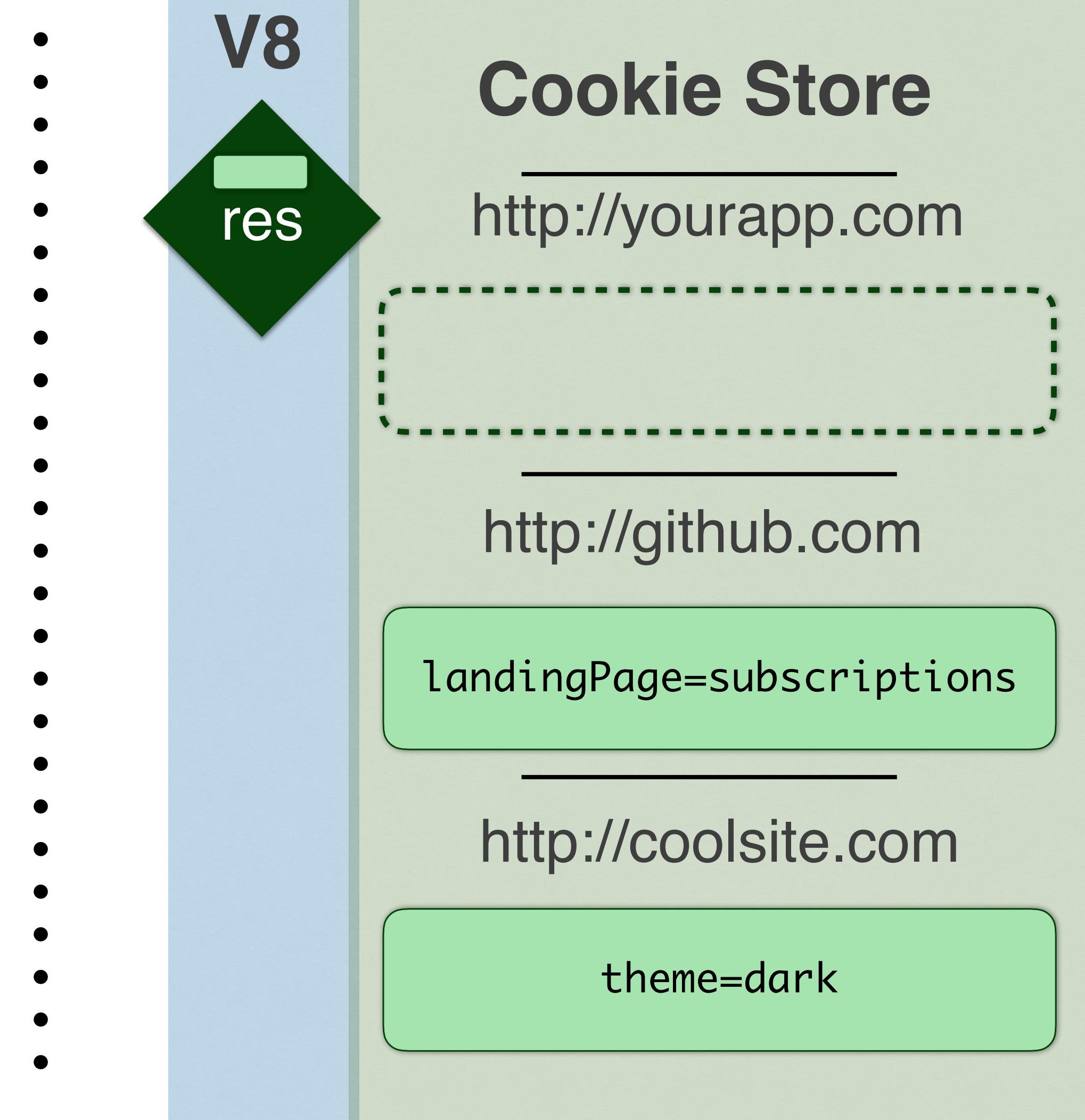
```
<!DOCTYPE html>
<html>
  <head>
    <title>Your Sweet App</title>
    <script src="/js/main.js"></script>
  </head> ...etc.
```

Server (Backend)

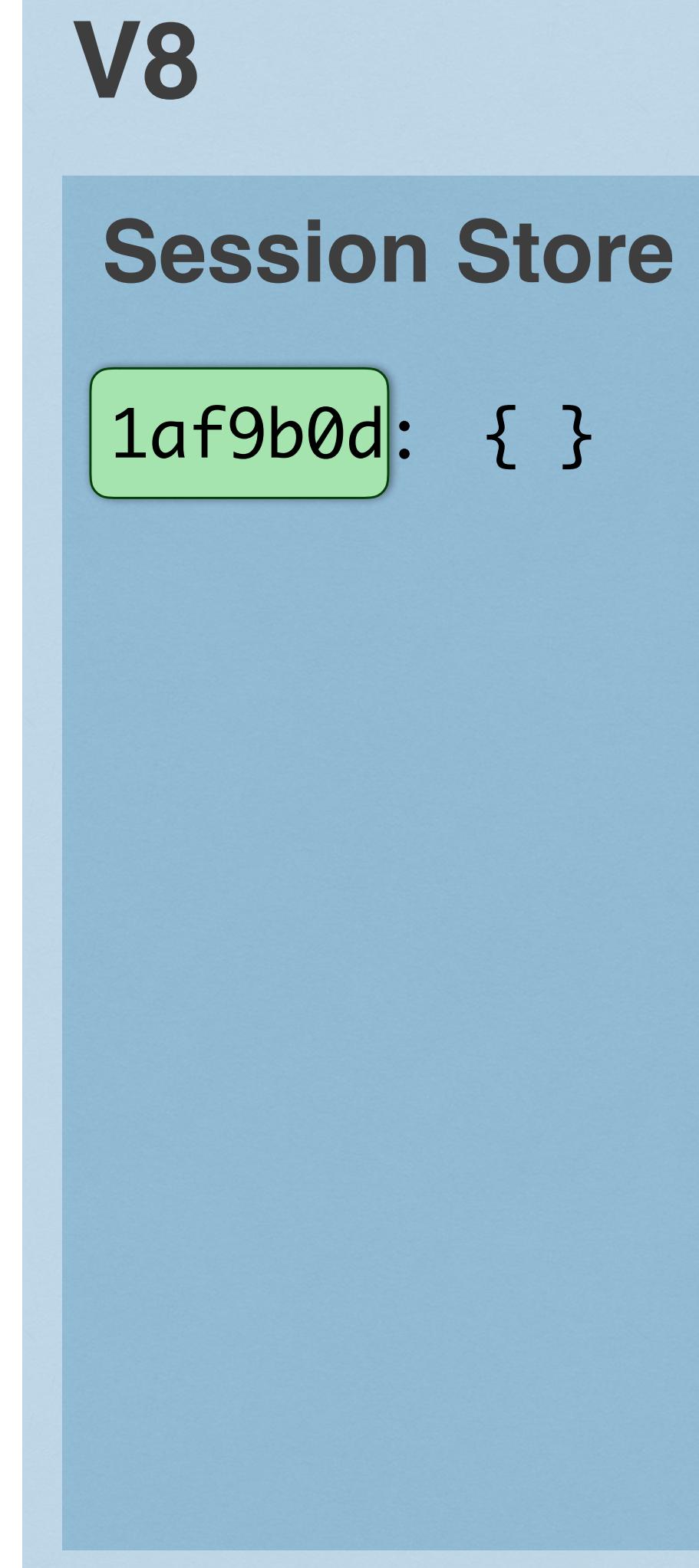


<http://yourapp.com>

Internet (HTTP)

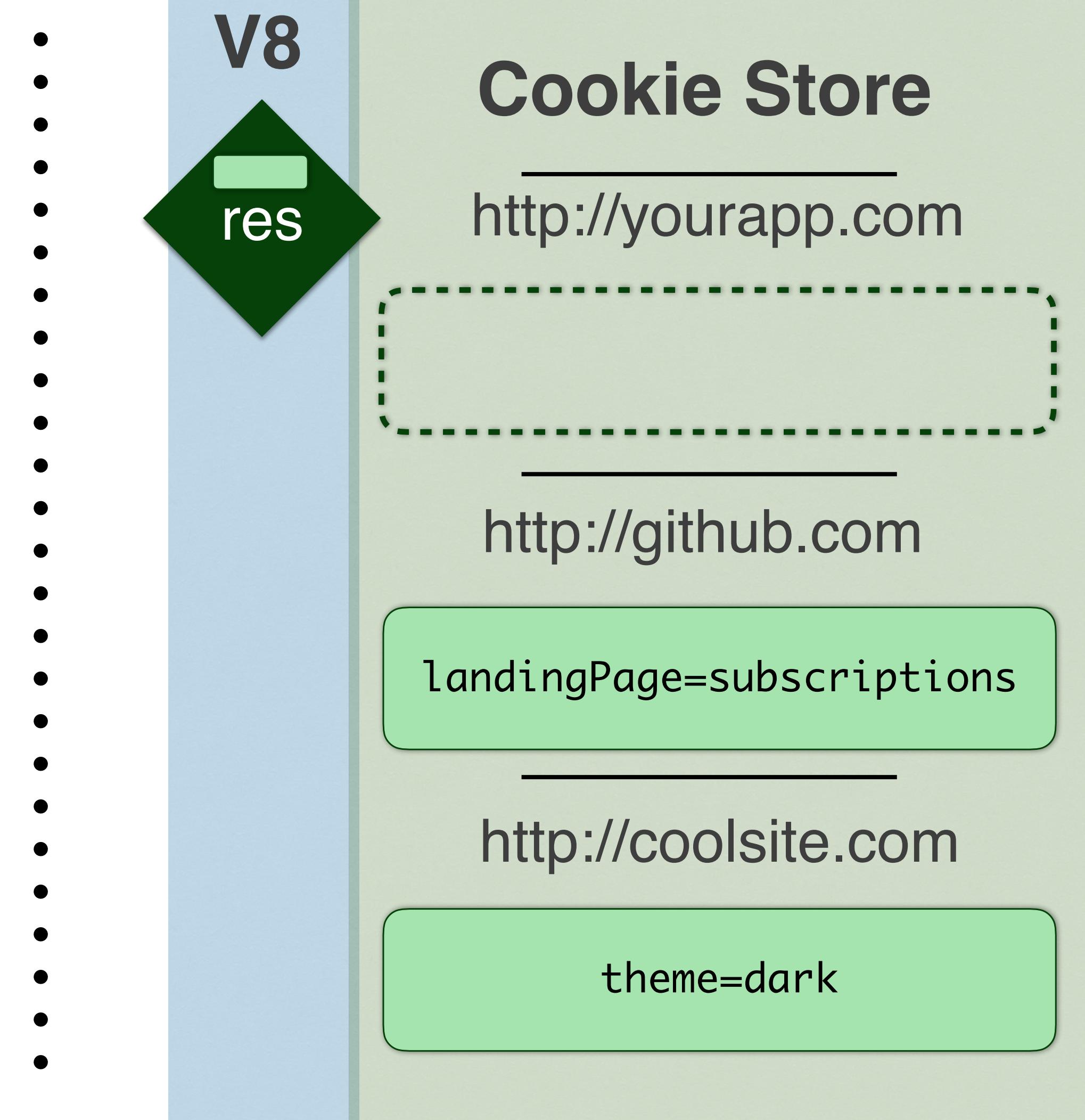


Server (Backend)



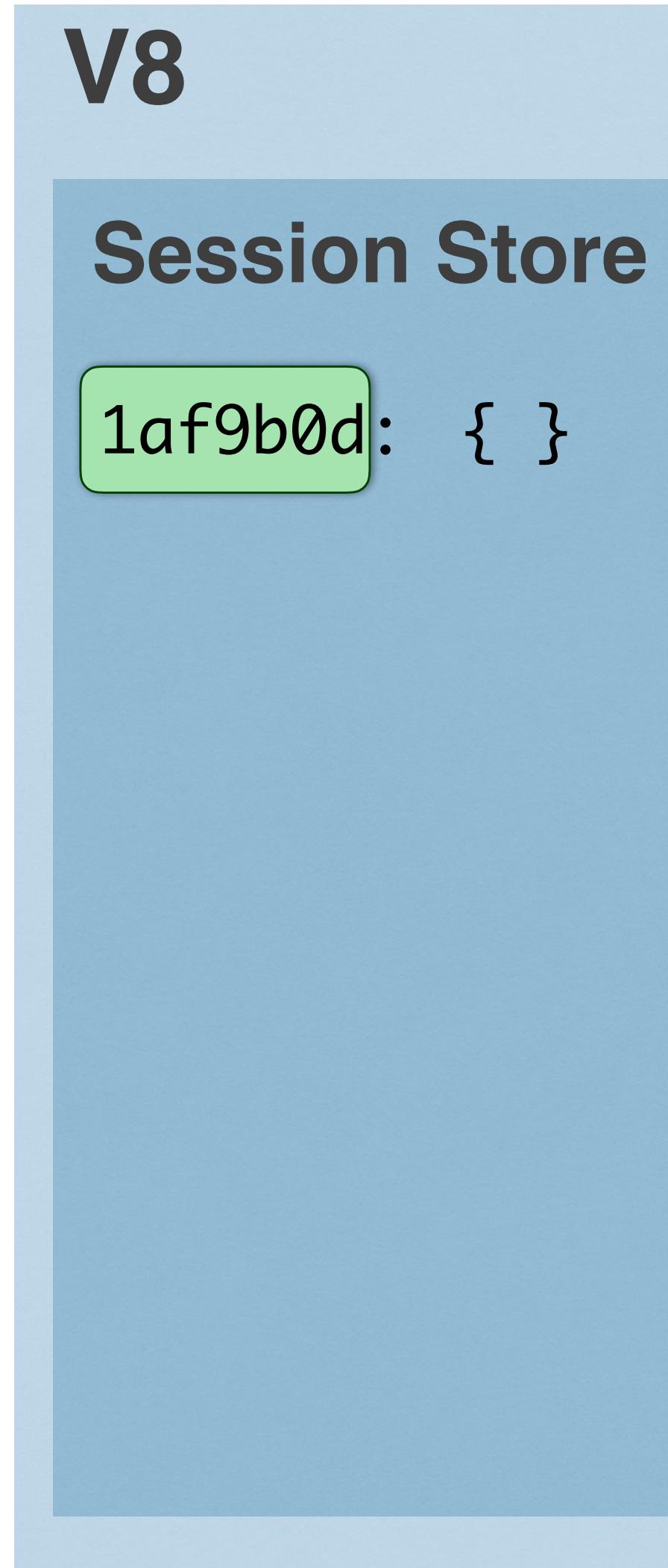
<http://yourapp.com>

Internet (HTTP)

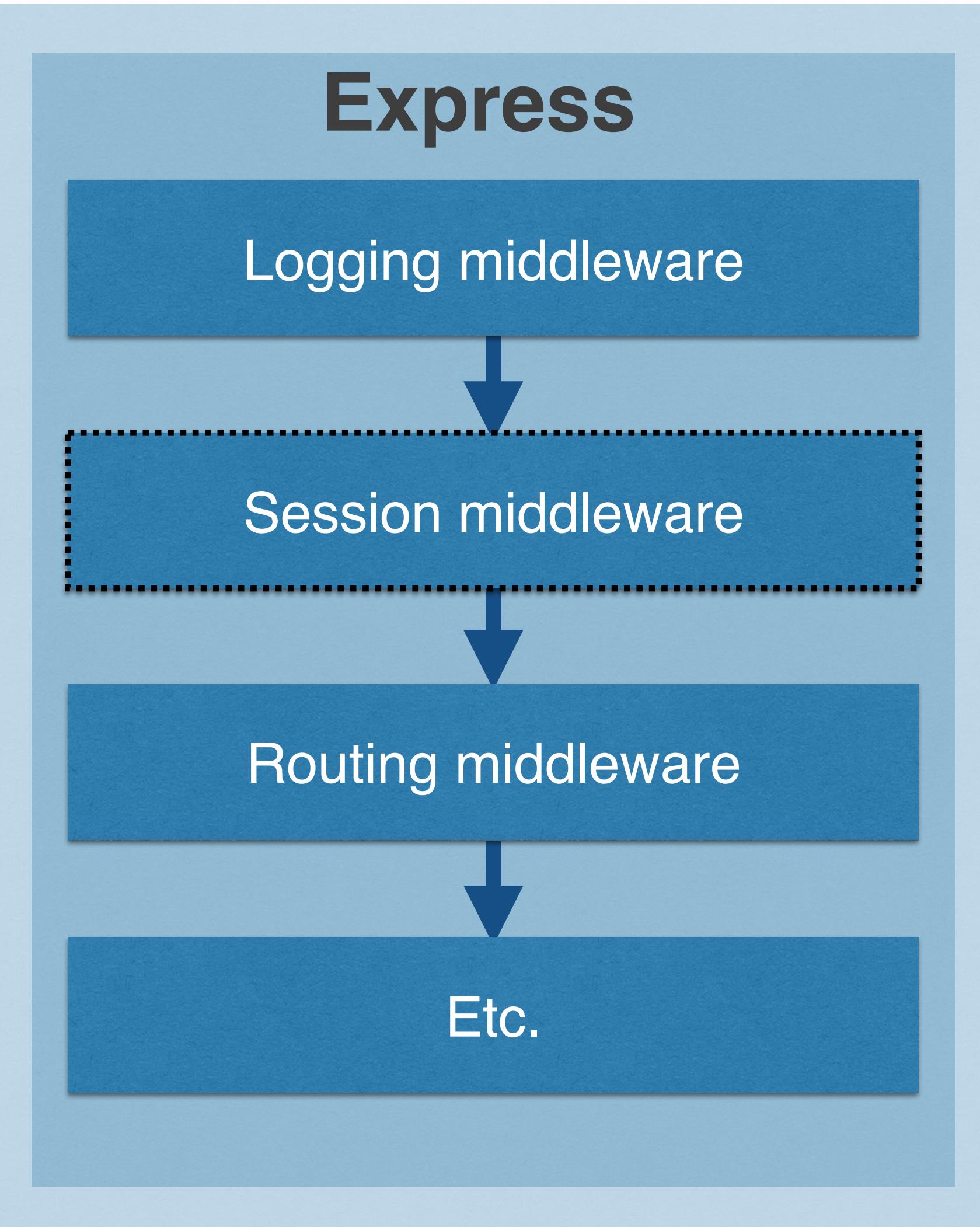


Client (Browser)

Server (Backend)

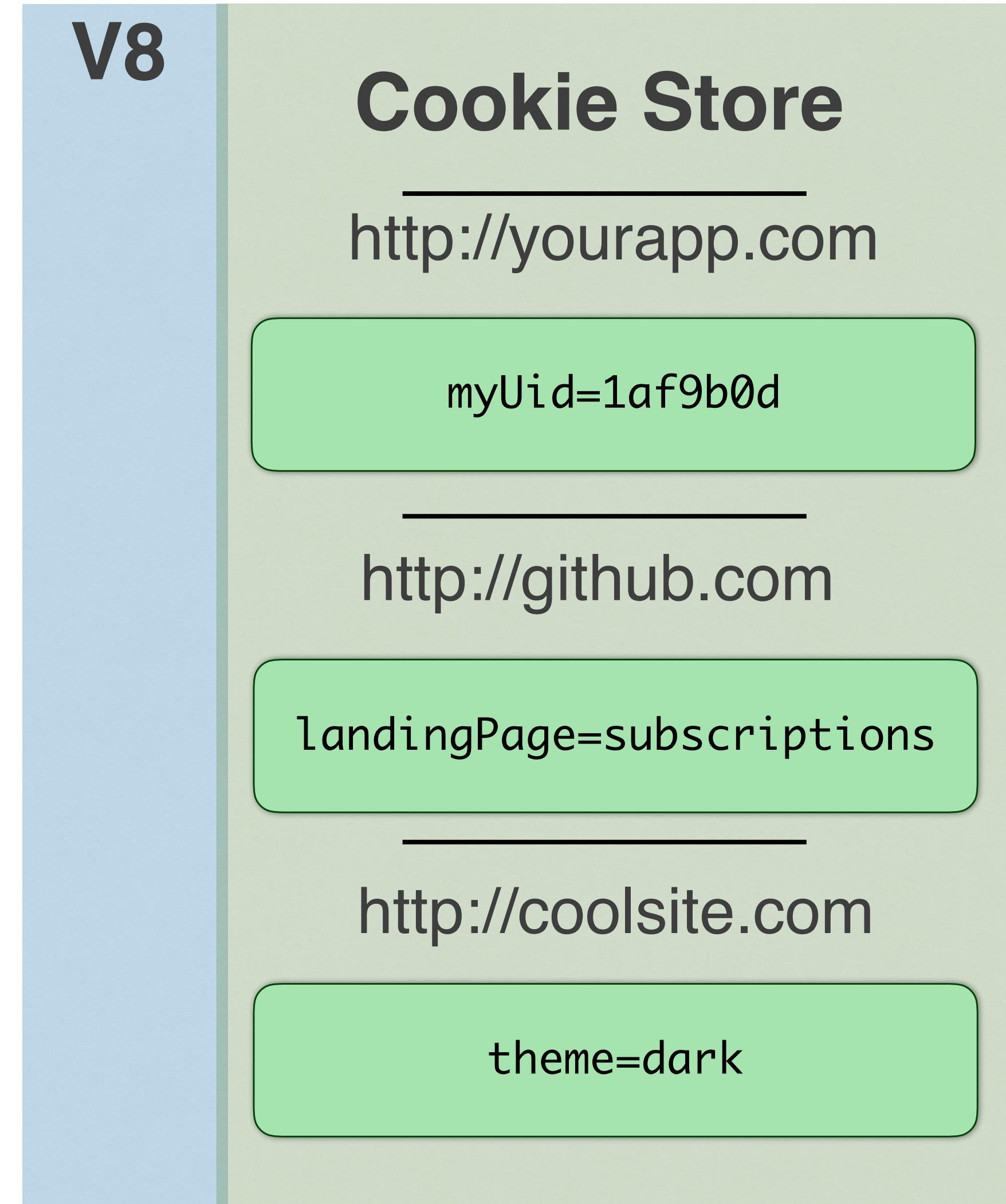


Internet (HTTP)

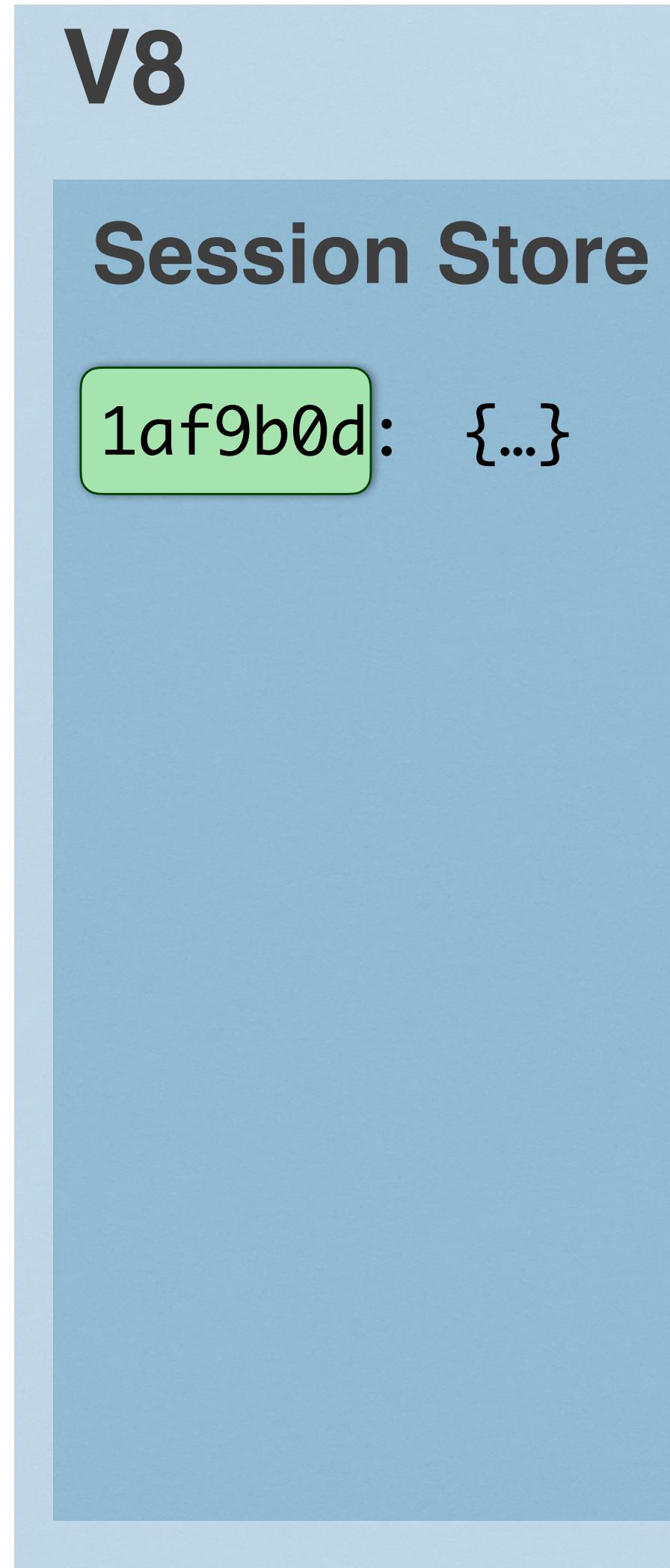


<http://yourapp.com>

Client (Browser)



Server (Backend)

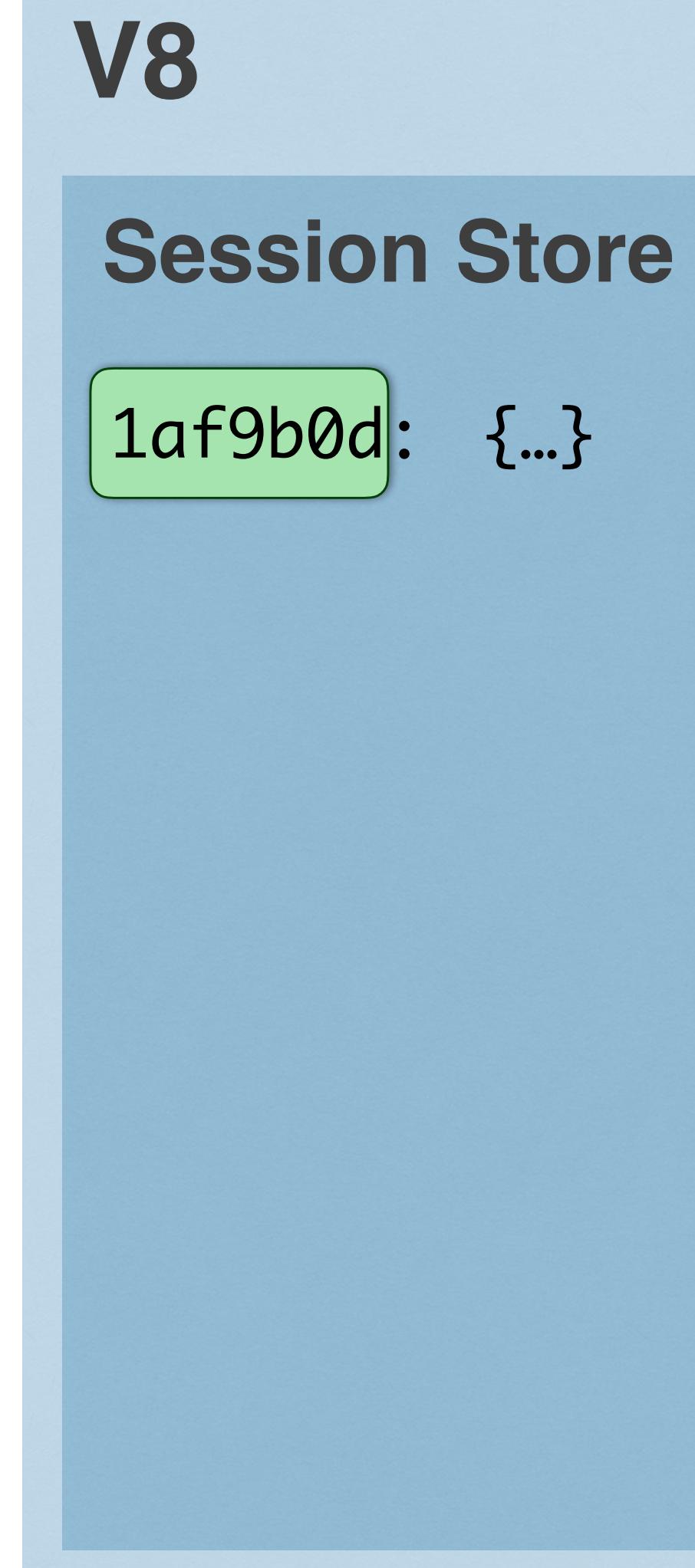


<http://yourapp.com>

Internet (HTTP)

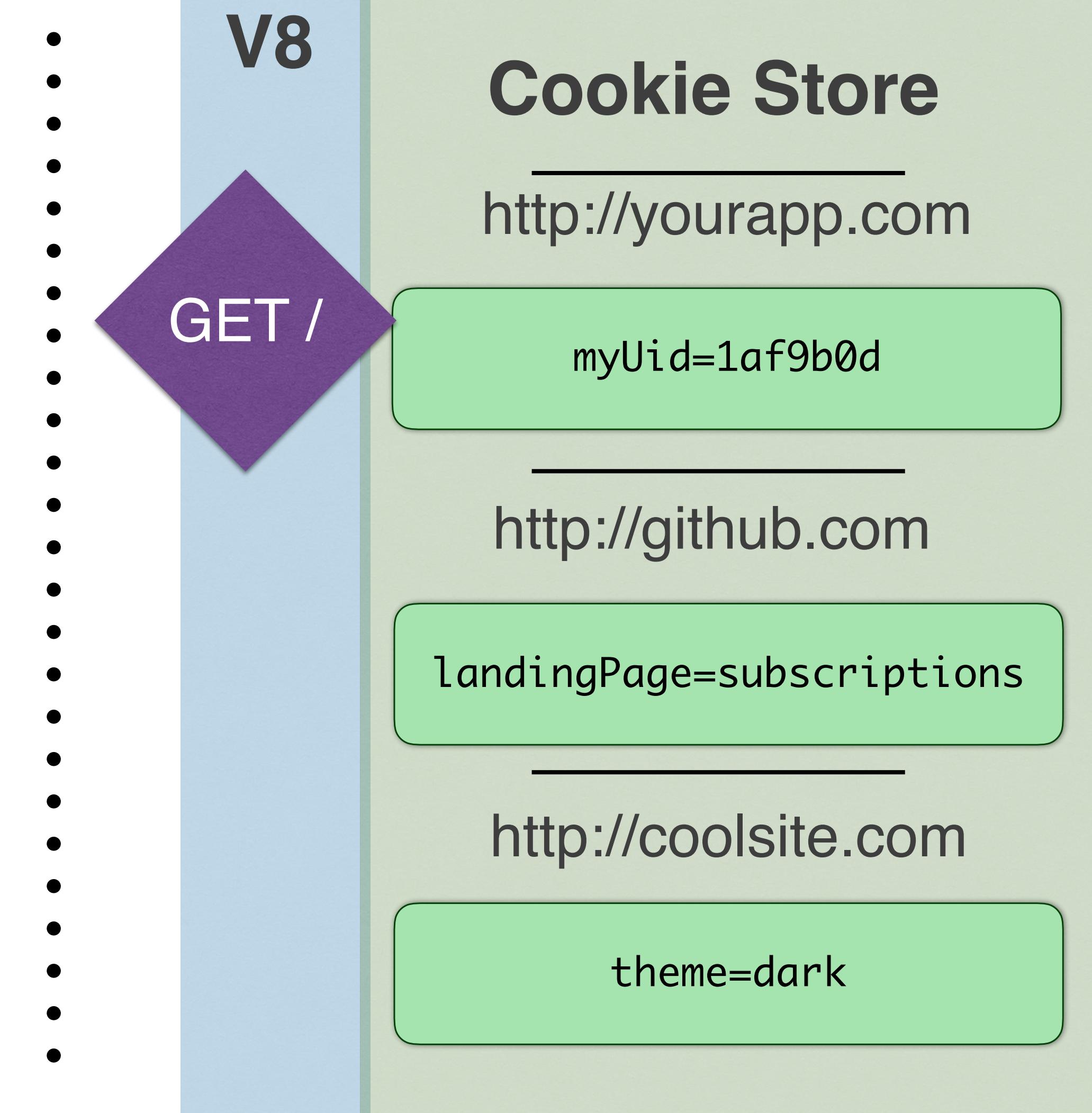


Server (Backend)



<http://yourapp.com>

Internet (HTTP)



HTTP REQUEST

(headers)

GET / HTTP/1.1
Host: yourapp.com
Connection: keep-alive
Accept: text/html
User-Agent: Chrome/
48.0.2564.116

(body)

HTTP REQUEST

(headers)

(body)

GET / HTTP/1.1
Host: yourapp.com
Connection: keep-alive
Accept: text/html
User-Agent: Chrome/
48.0.2564.116
Cookie: myUid=1af9b0d

HTTP REQUEST

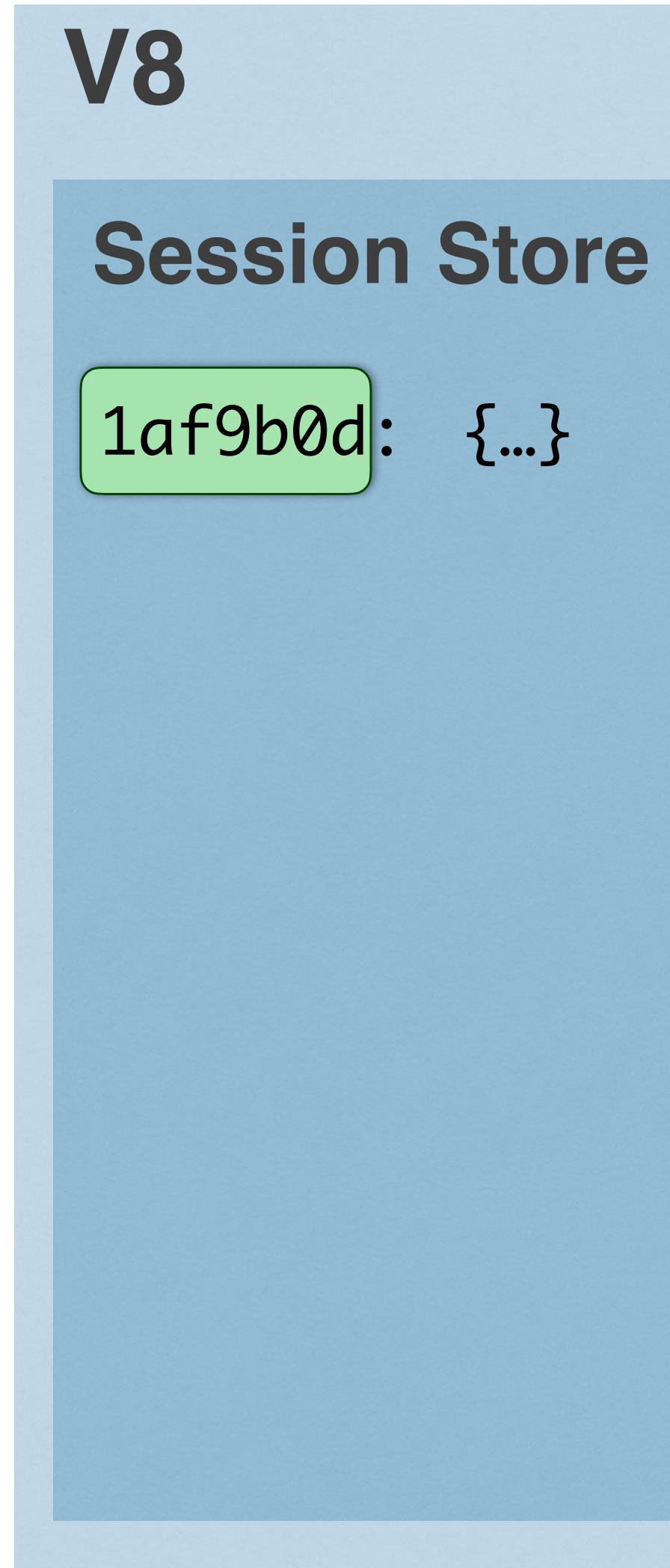
(headers)

(body)

GET / HTTP/1.1
Host: yourapp.com
Connection: keep-alive
Accept: text/html
User-Agent: Chrome/
48.0.2564.116
Cookie: myUid=1af9b0d

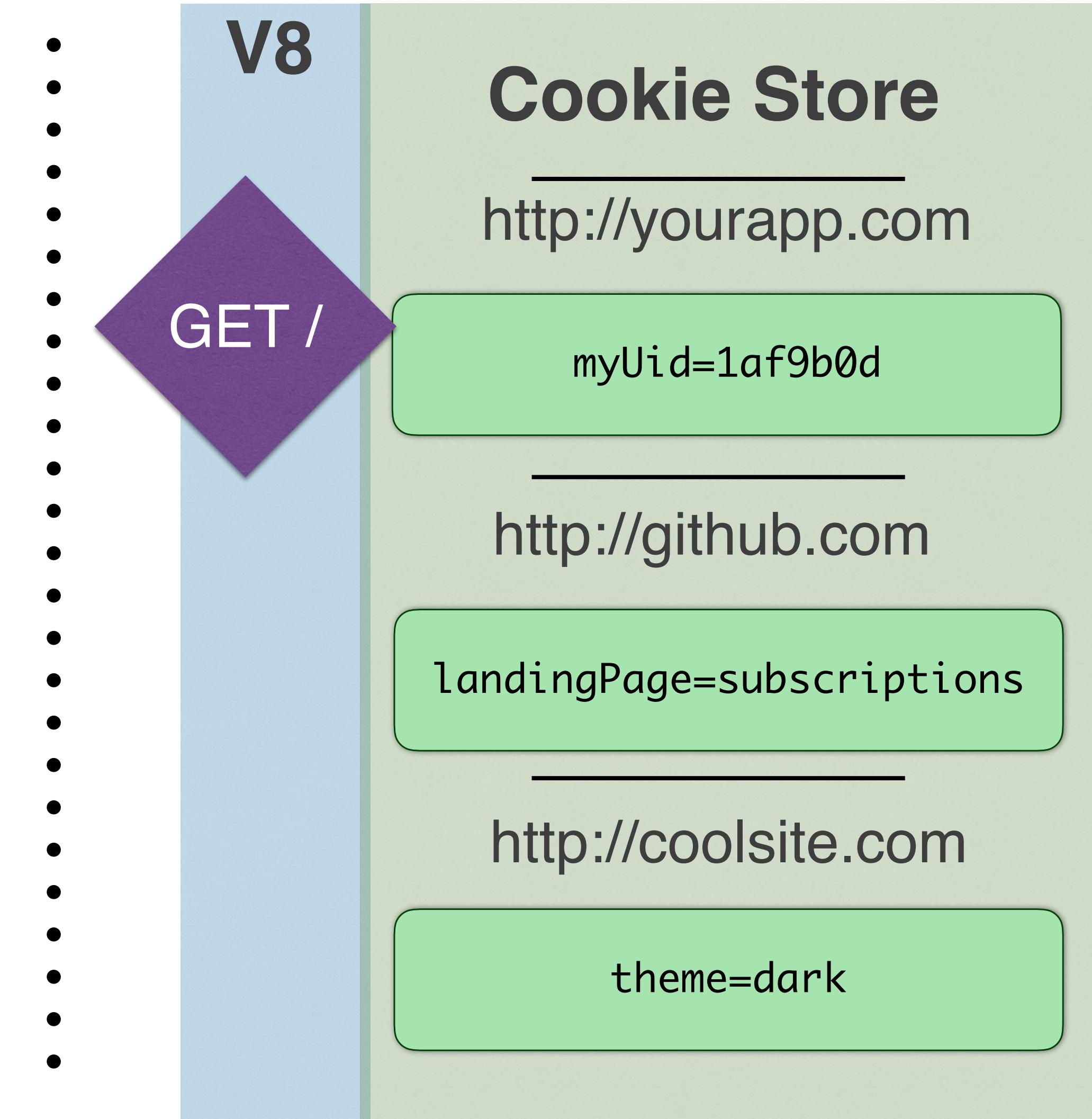
...attached cookie!

Server (Backend)

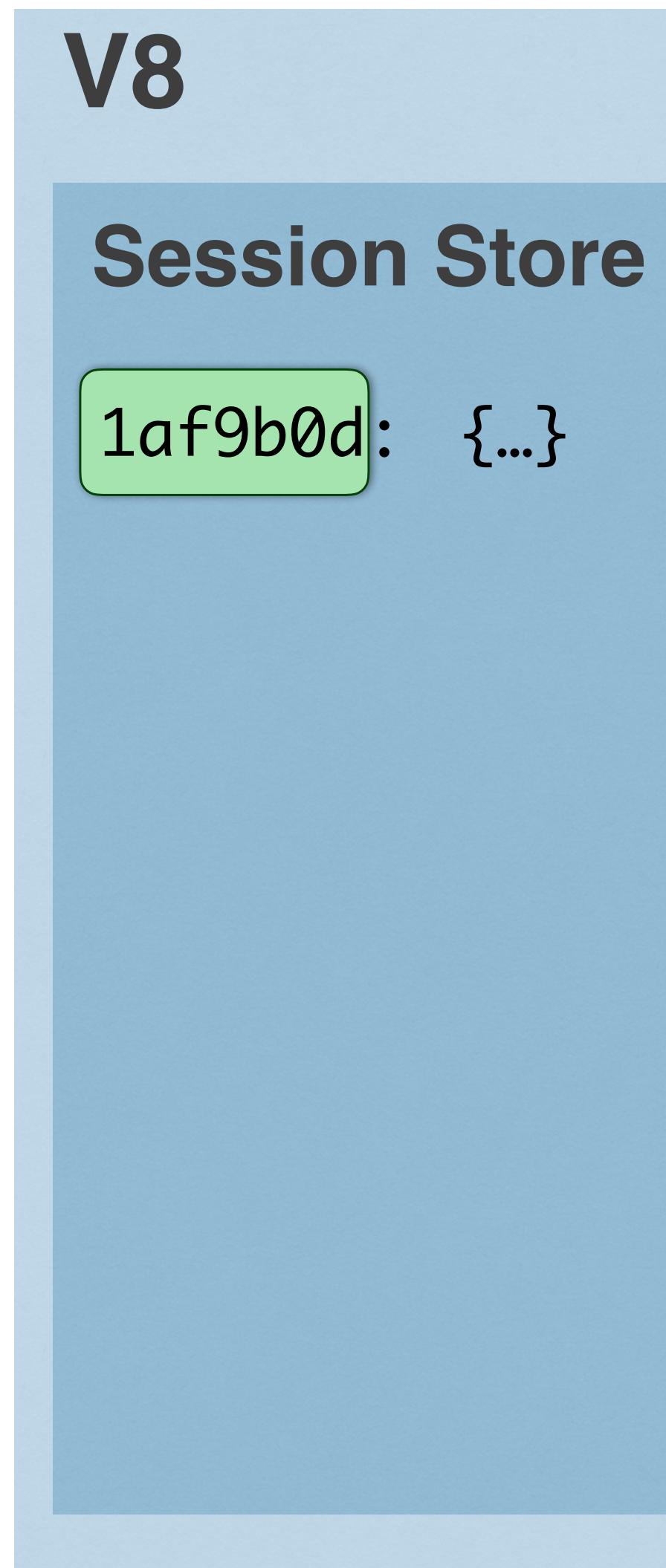


<http://yourapp.com>

Internet (HTTP)



Server (Backend)



<http://yourapp.com>

Internet (HTTP)

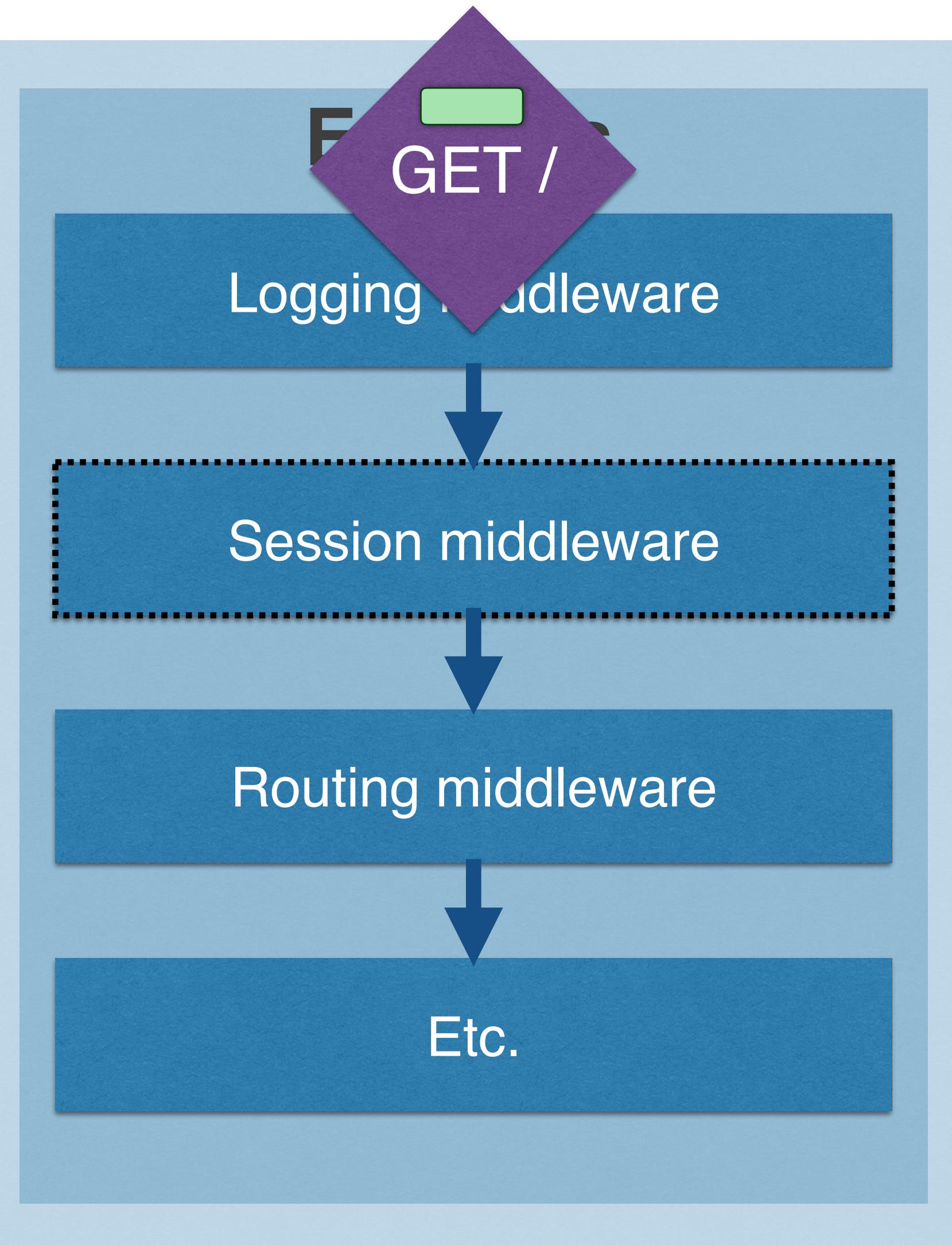


Server (Backend)

V8

Session Store

1af9b0d: {...}



<http://yourapp.com>

Internet (HTTP)

V8

Cookie Store

<http://yourapp.com>

myUid=1af9b0d

<http://github.com>

landingPage=subscriptions

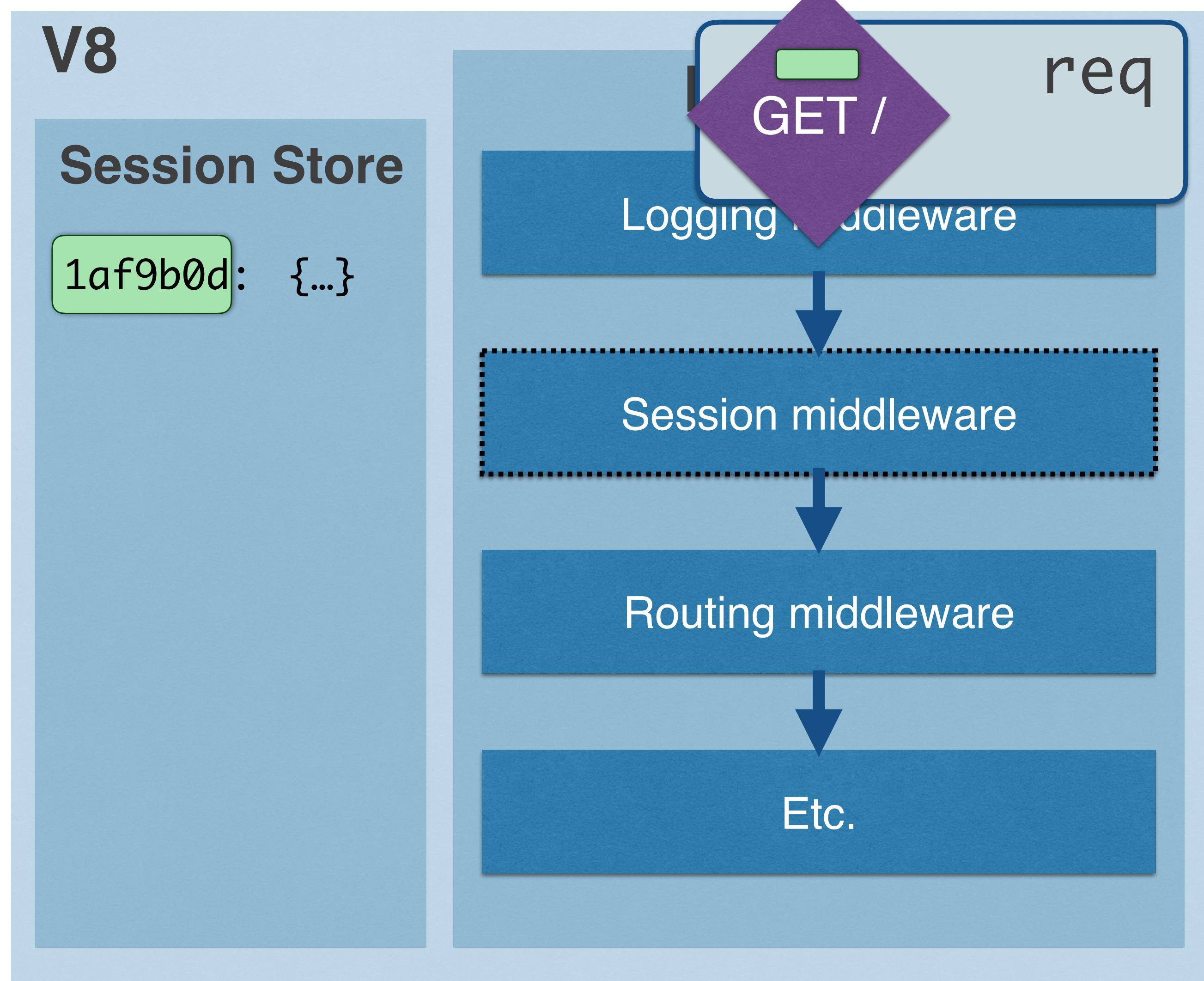
<http://coolsite.com>

theme=dark

Server (Backend)

Internet (HTTP)

Client (Browser)



<http://yourapp.com>

V8

Cookie Store

http://yourapp.com

myUid=1af9b0d

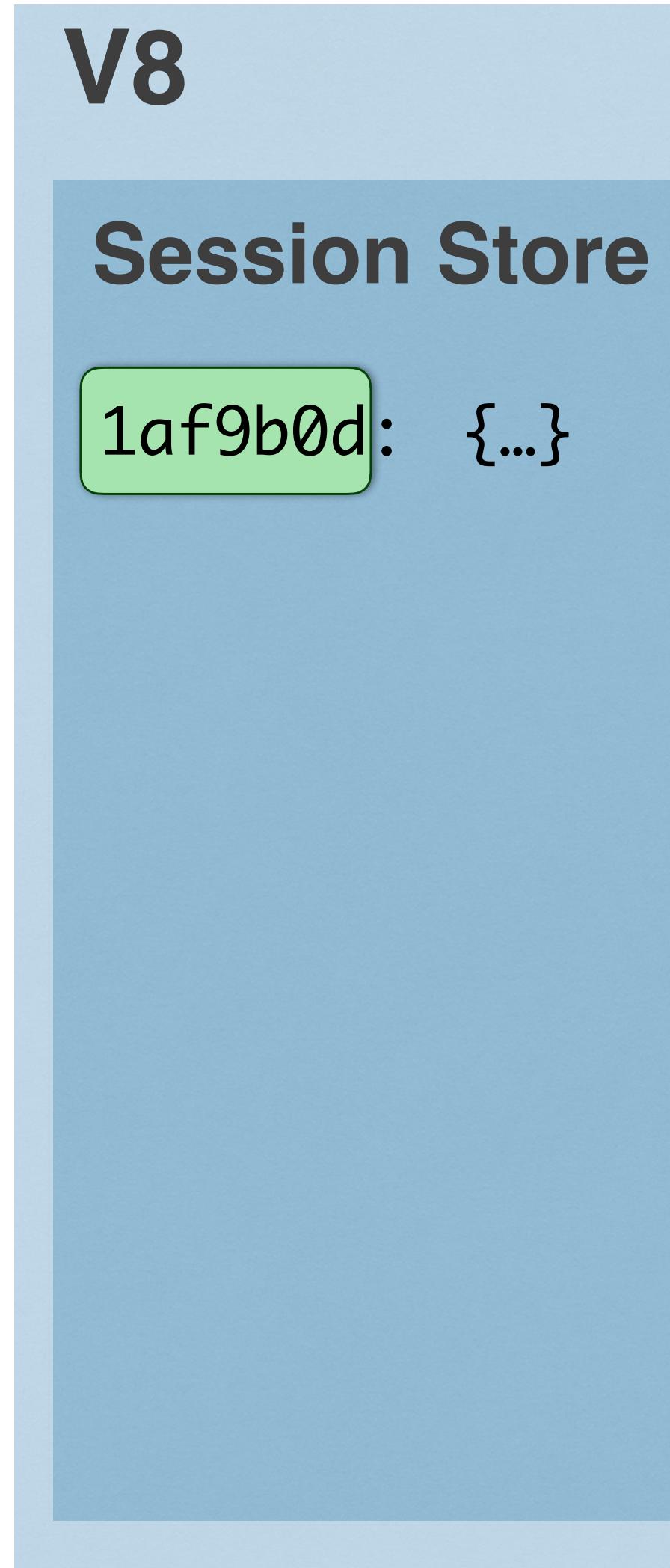
<http://github.com>

landingPage=subscriptions

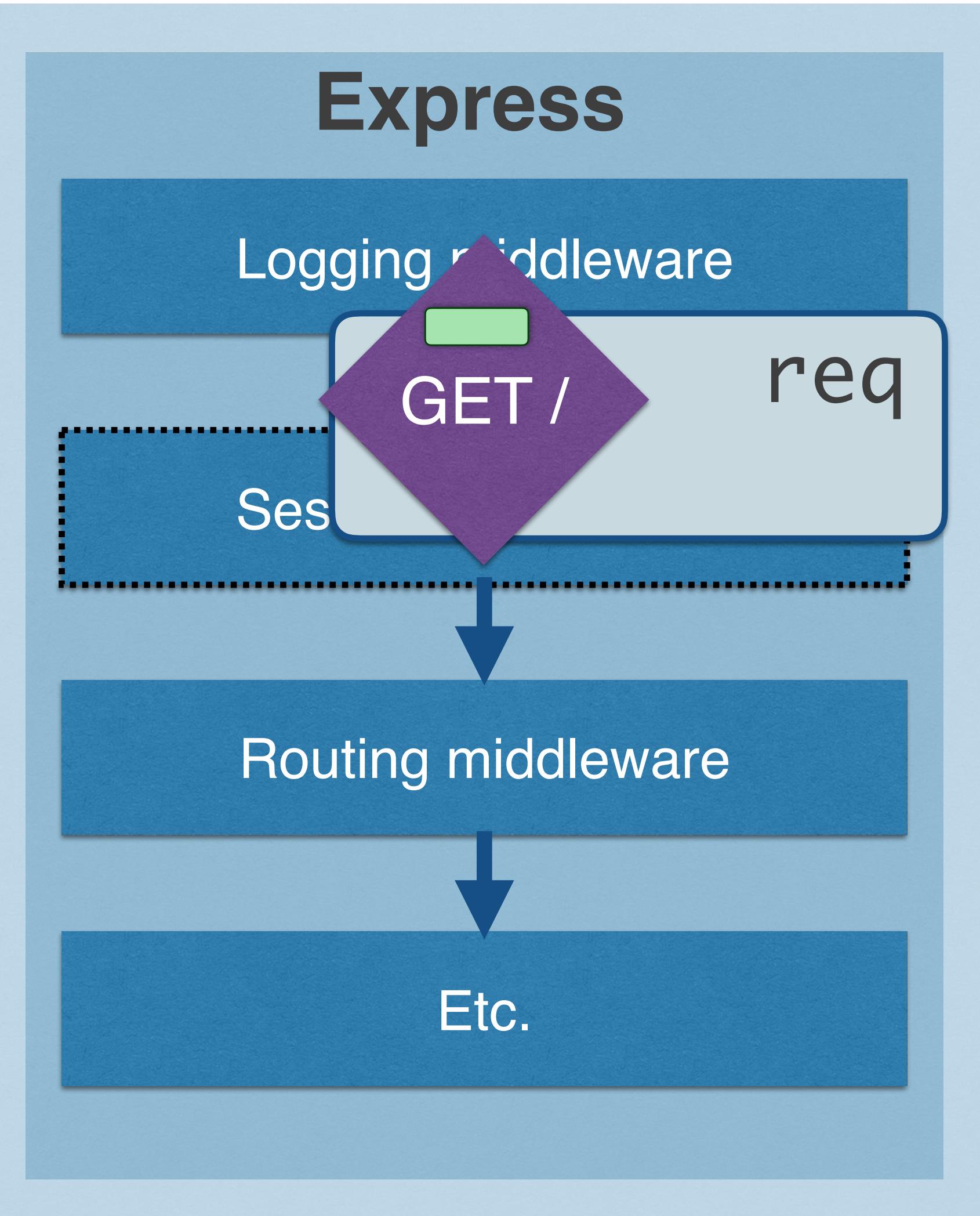
<http://coolsite.com>

theme=dark

Server (Backend)

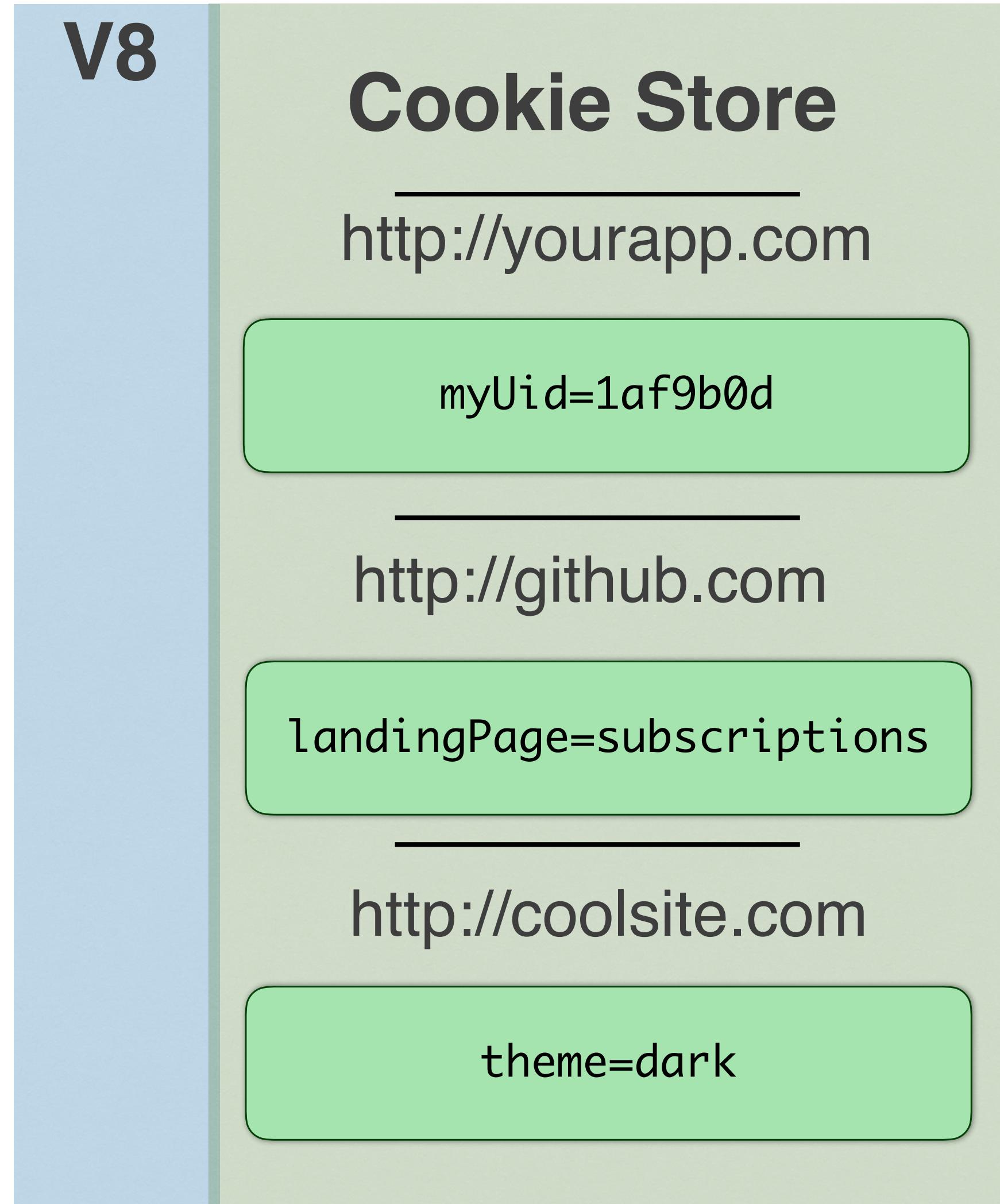


Internet (HTTP)



<http://yourapp.com>

Client (Browser)



HTTP REQUEST

(headers)

(body)

GET / HTTP/1.1
Host: yourapp.com
Connection: keep-alive
Accept: text/html
User-Agent: Chrome/
48.0.2564.116
Cookie: myUid=1af9b0d

HTTP REQUEST

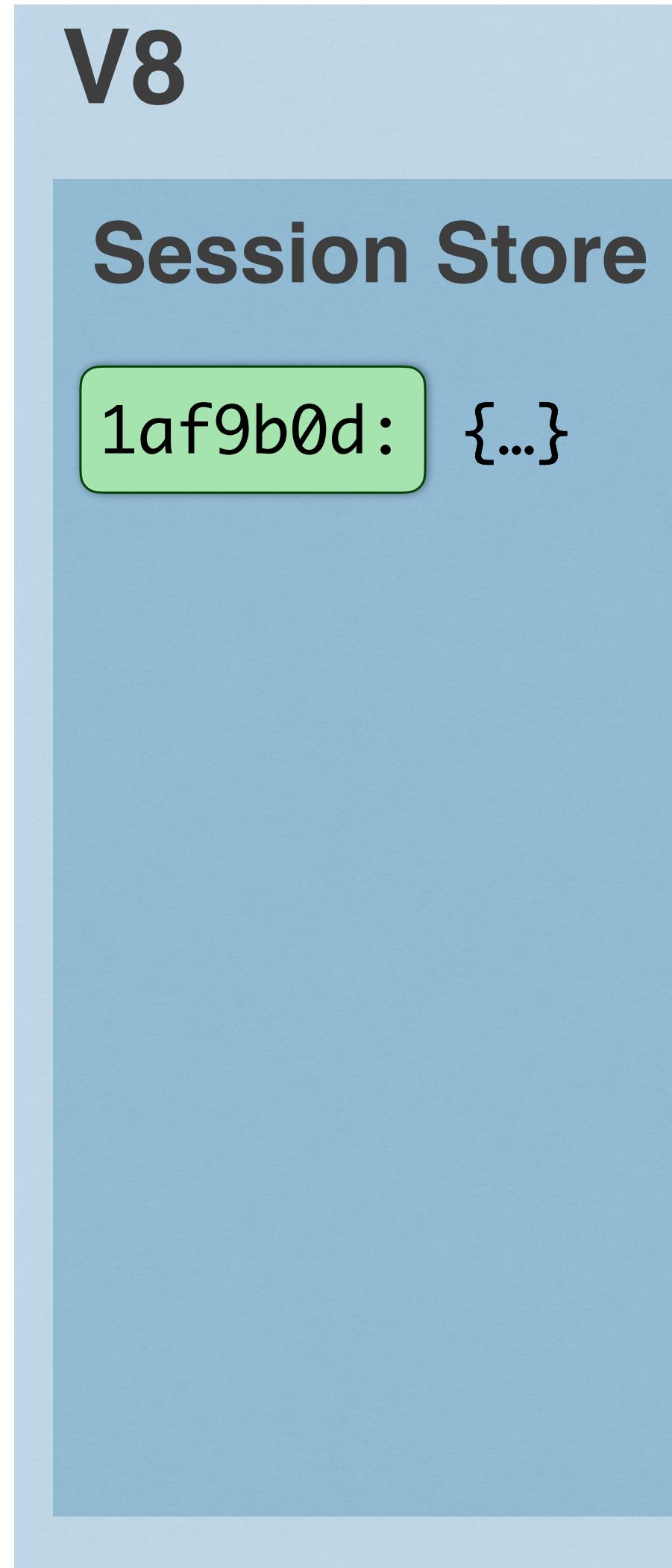
(headers)

(body)

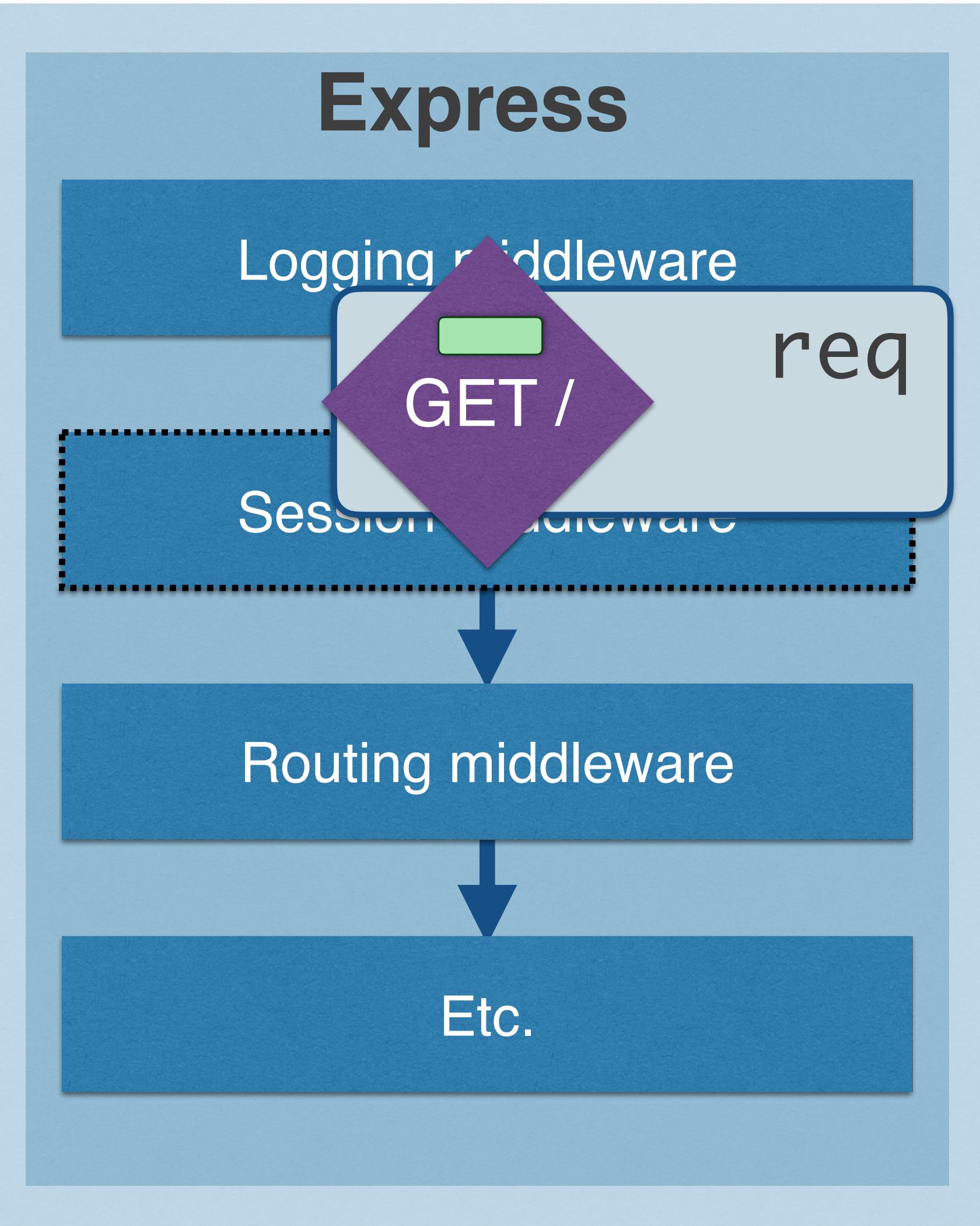
GET / HTTP/1.1
Host: yourapp.com
Connection: keep-alive
Accept: text/html
User-Agent: Chrome/
48.0.2564.116
Cookie: myUid=1af9b0d

attached cookie, so
session middleware:
let's look up the session!

Server (Backend)

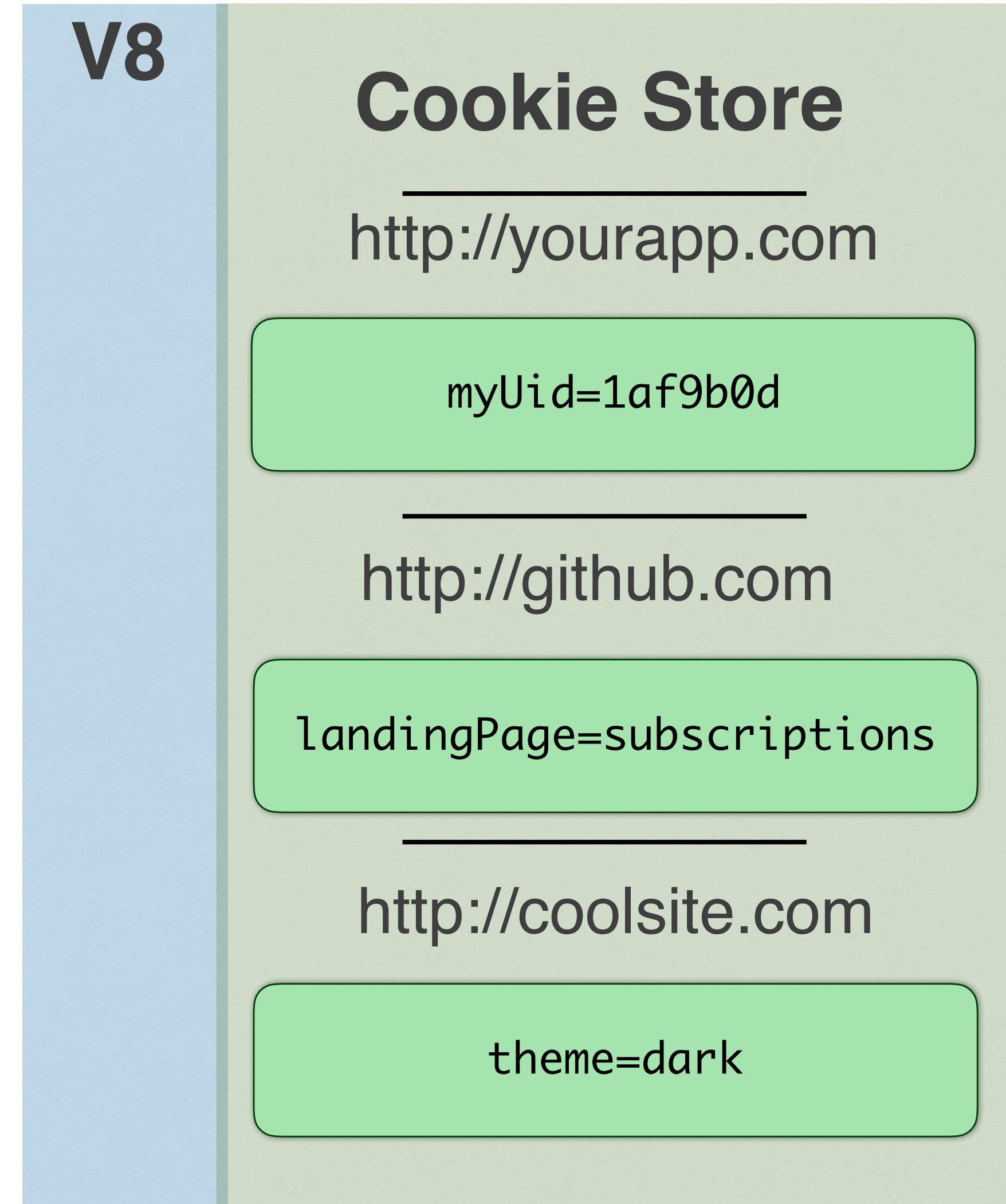


Internet (HTTP)

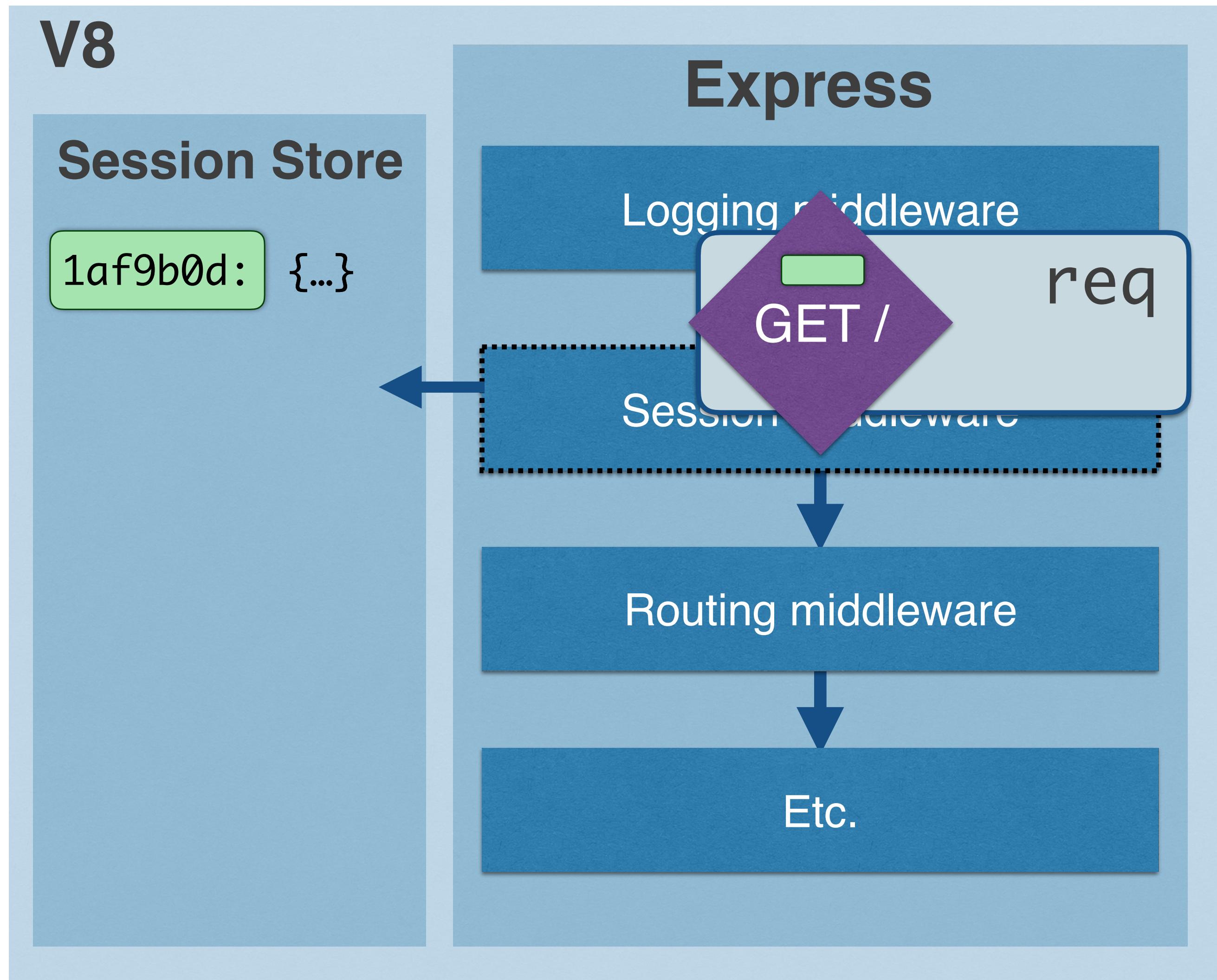


<http://yourapp.com>

Client (Browser)

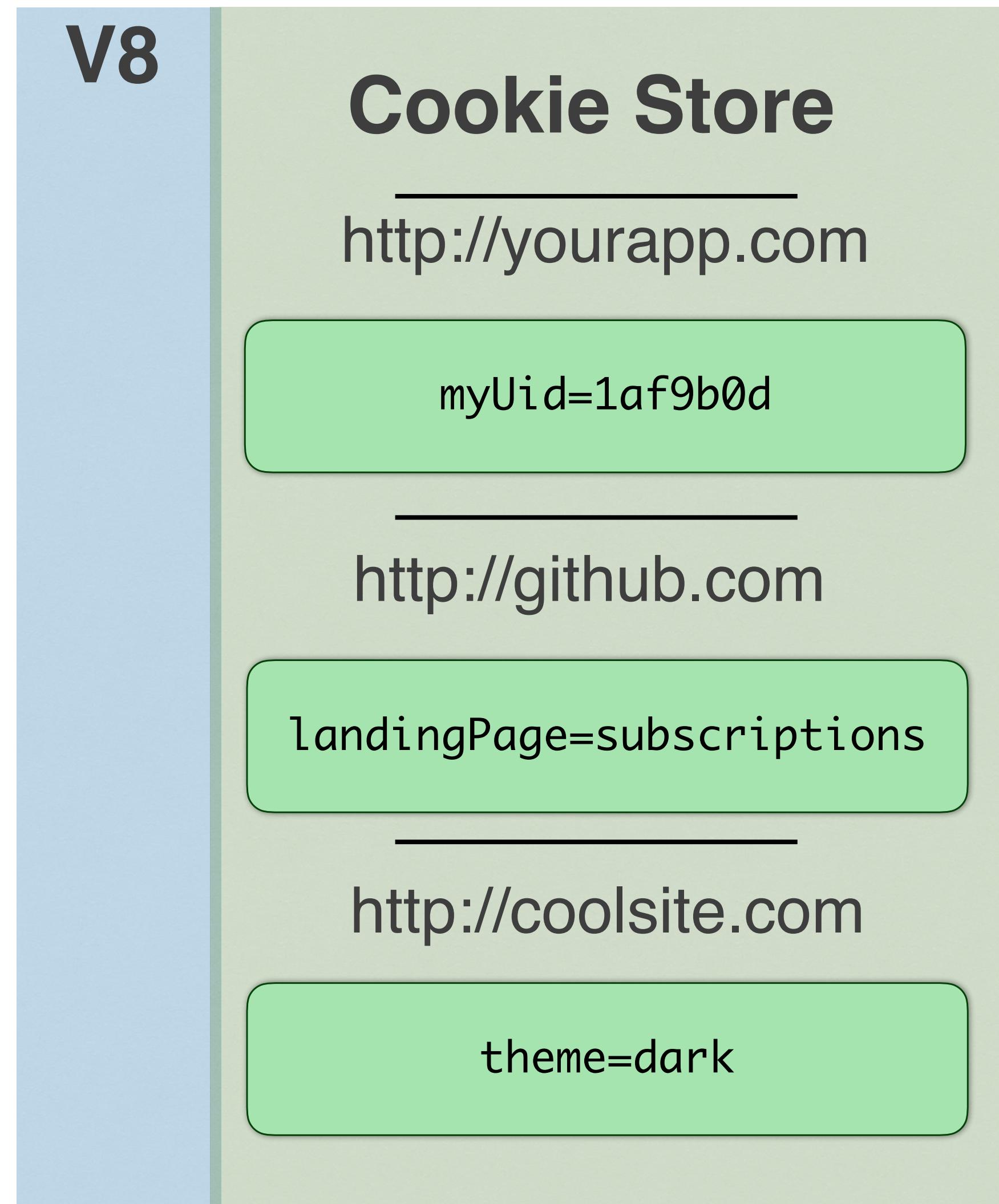


Server (Backend)



<http://yourapp.com>

Internet (HTTP)

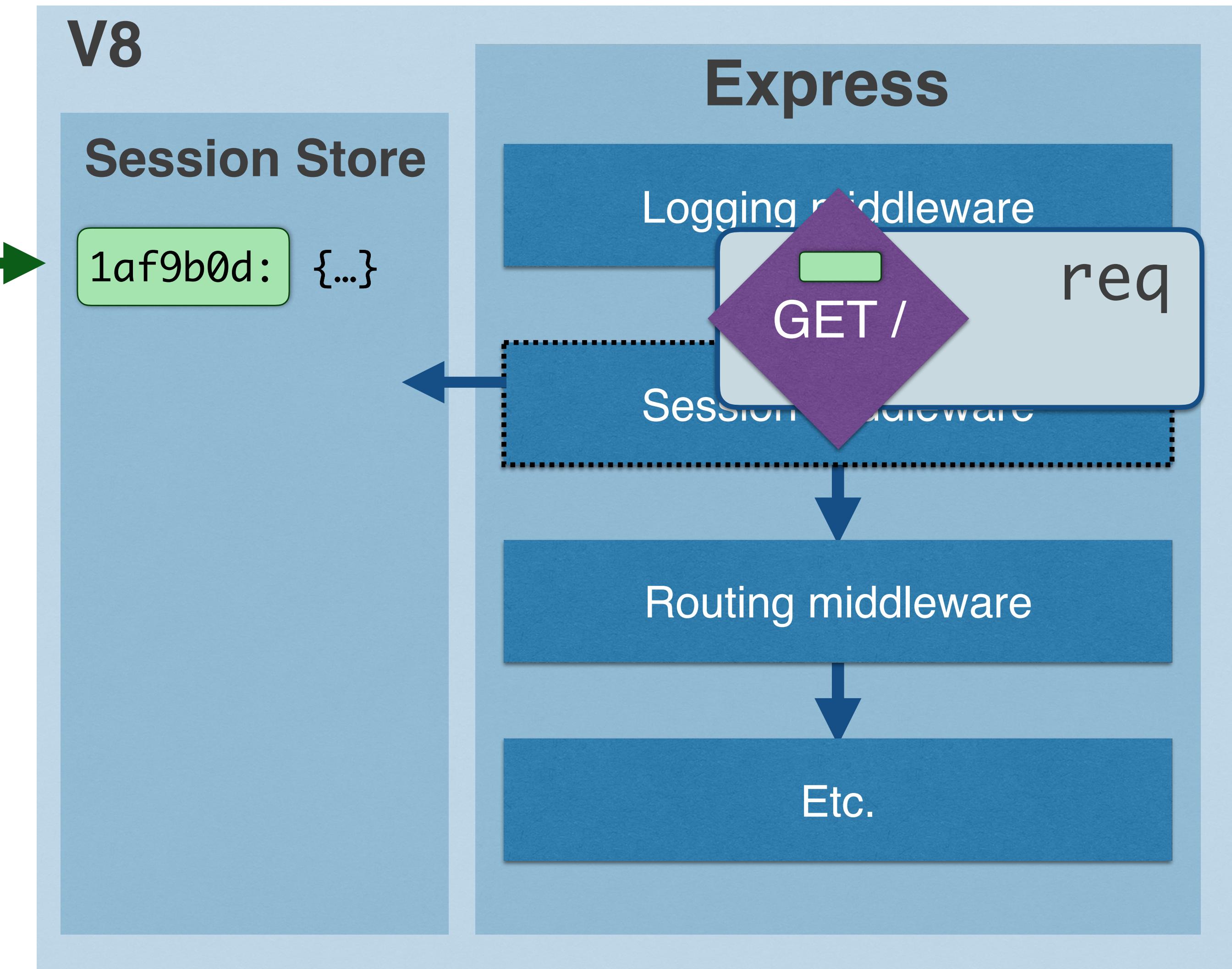


AUTH

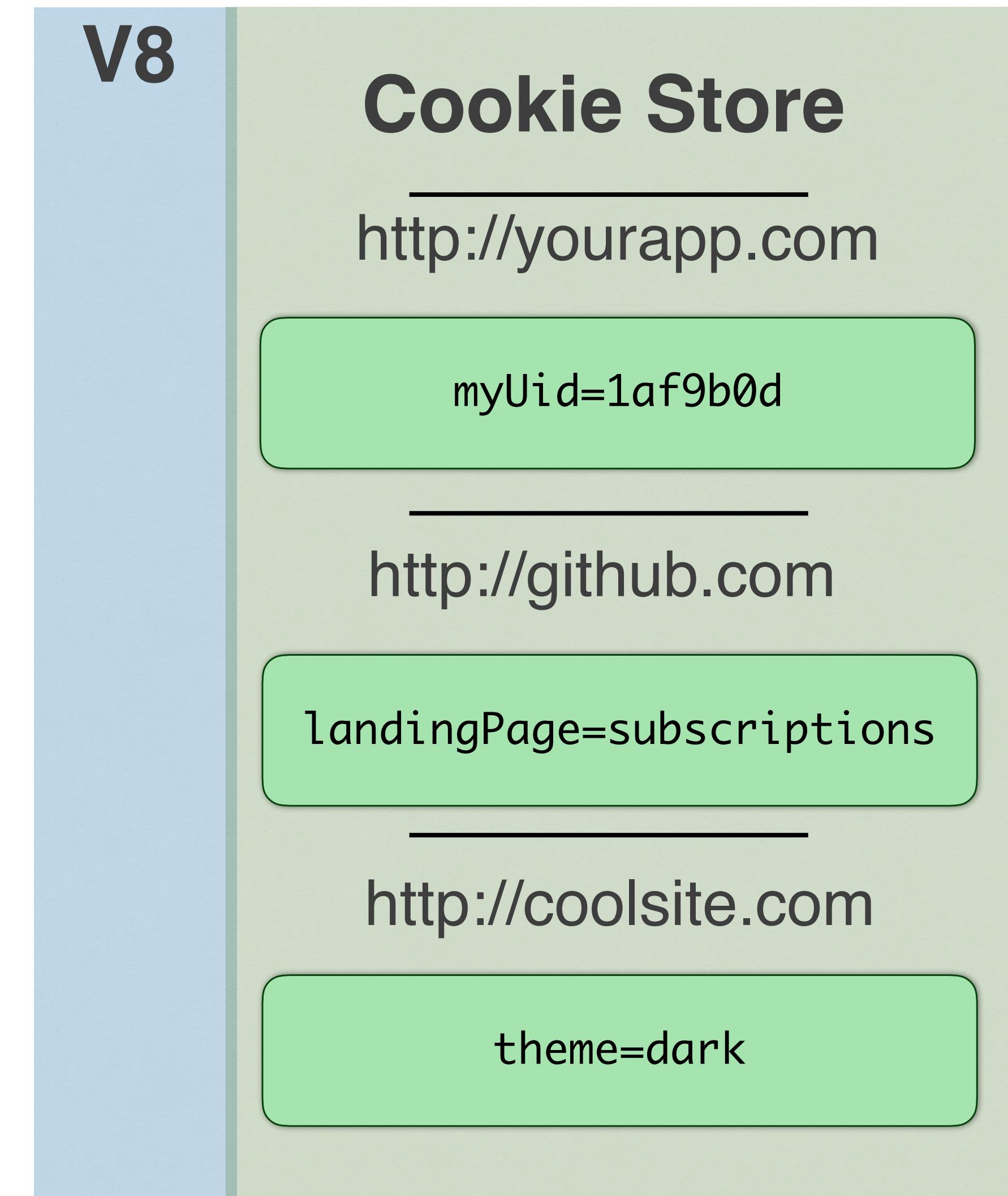
Server (Backend)

Internet (HTTP)

Client (Browser)



<http://yourapp.com>

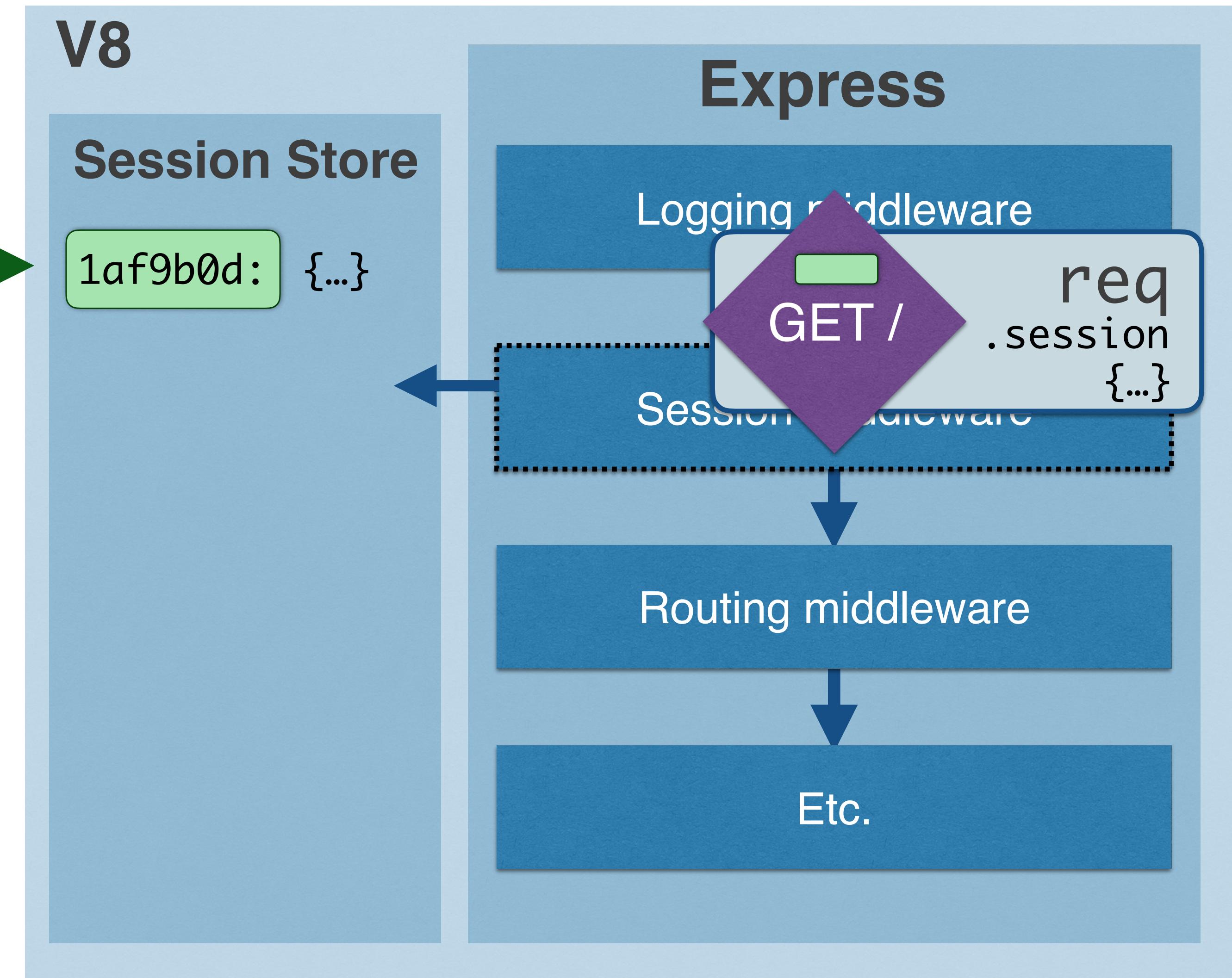


AUTH

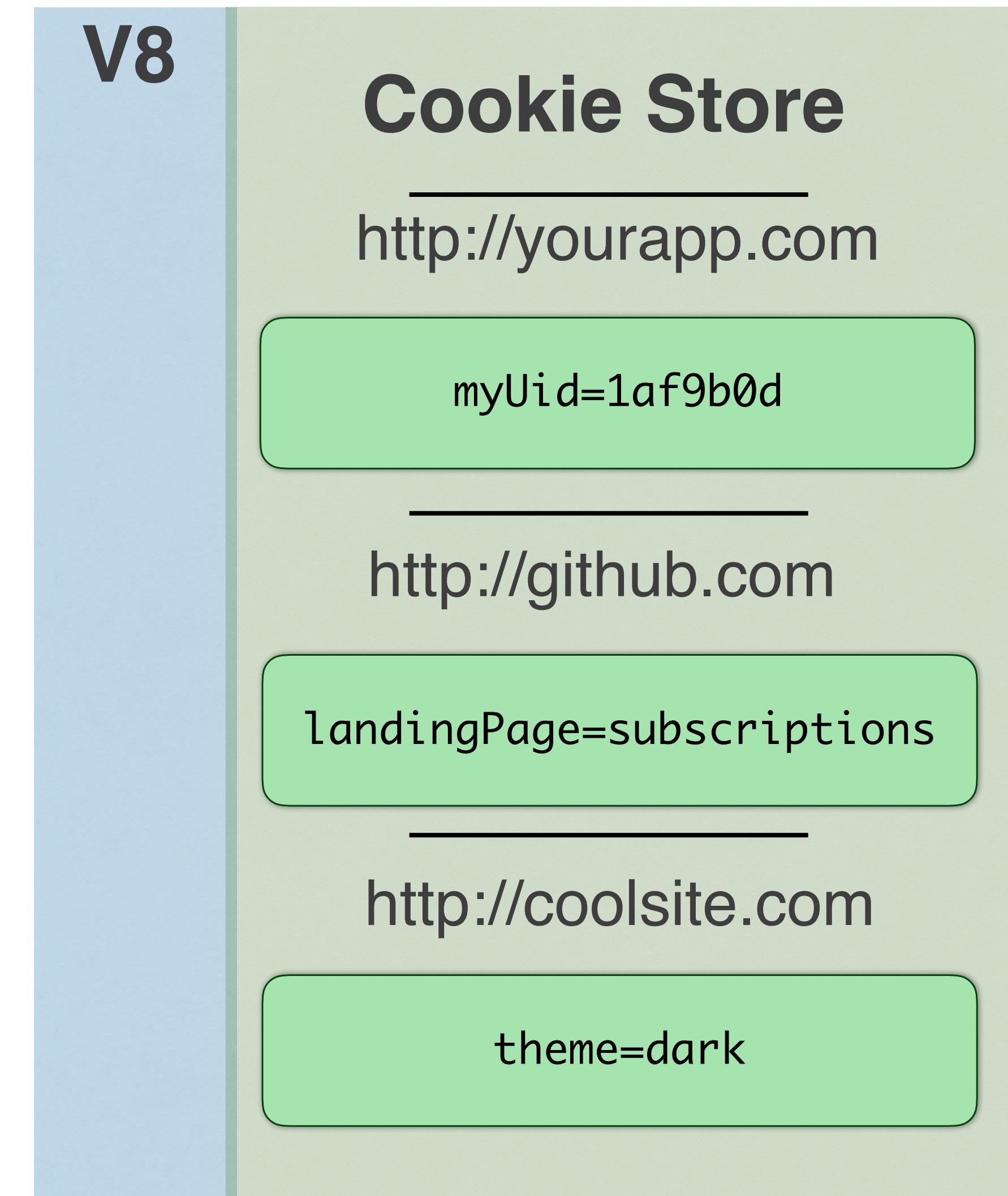
Server (Backend)

Internet (HTTP)

Client (Browser)



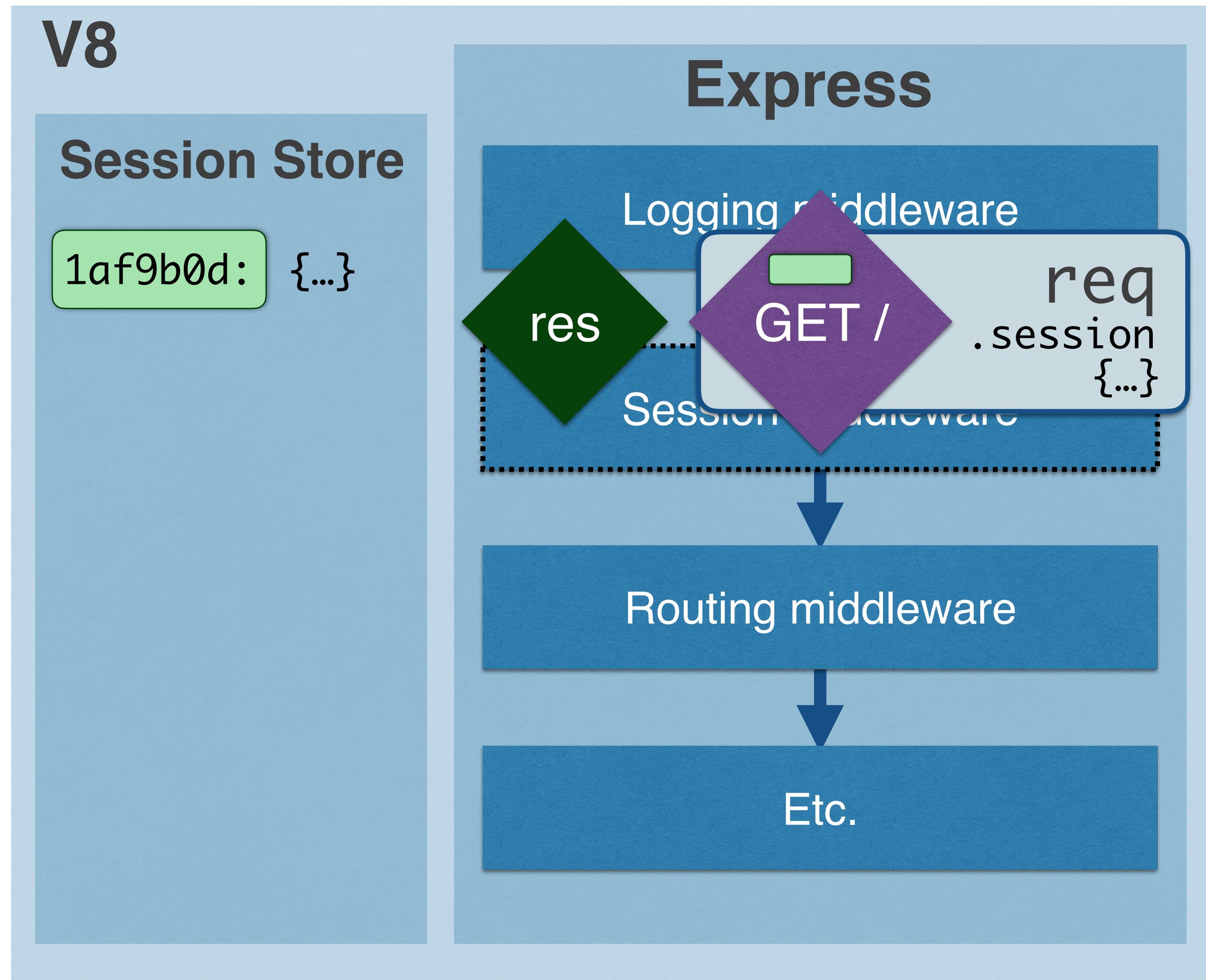
<http://yourapp.com>



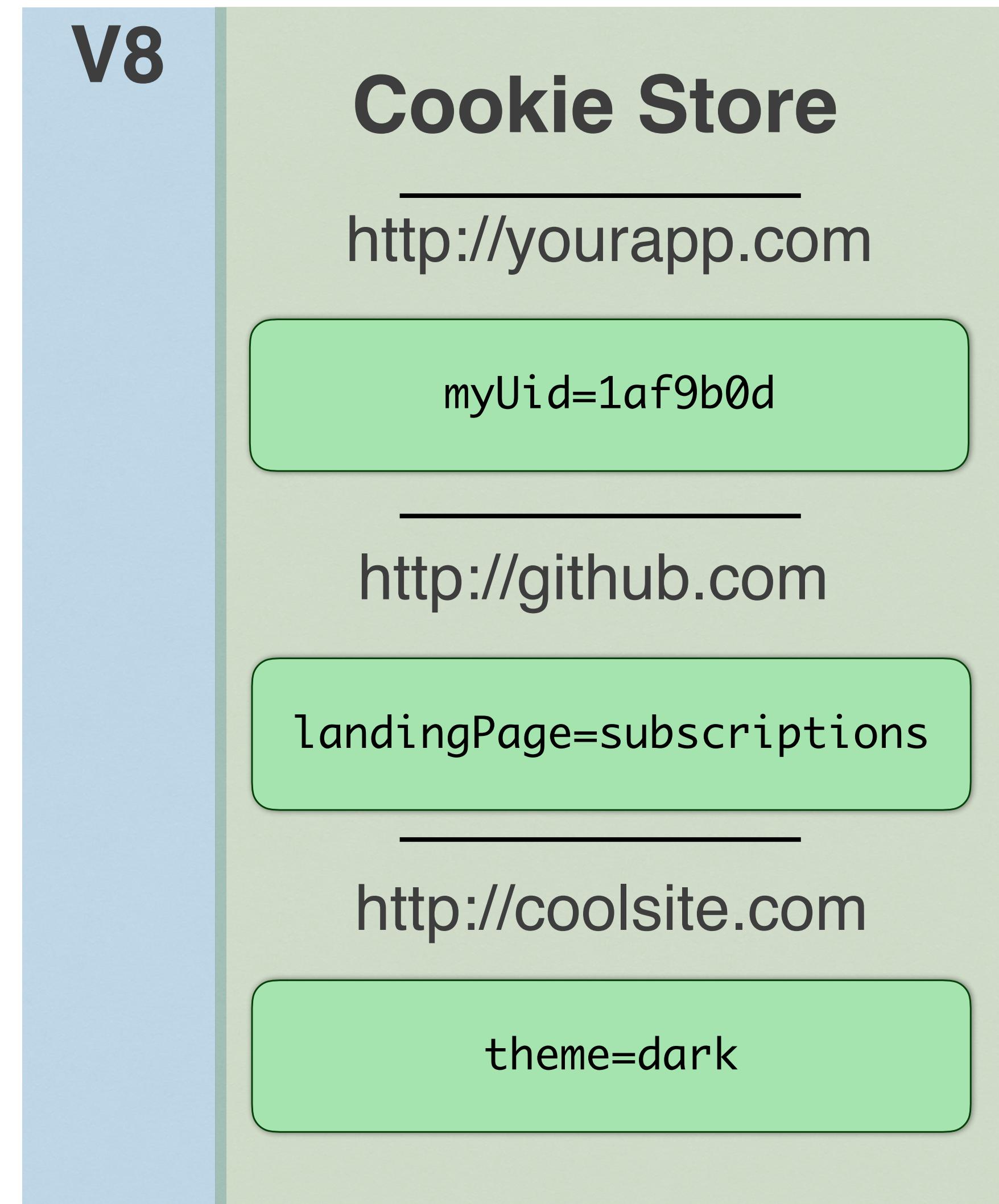
Server (Backend)

Internet (HTTP)

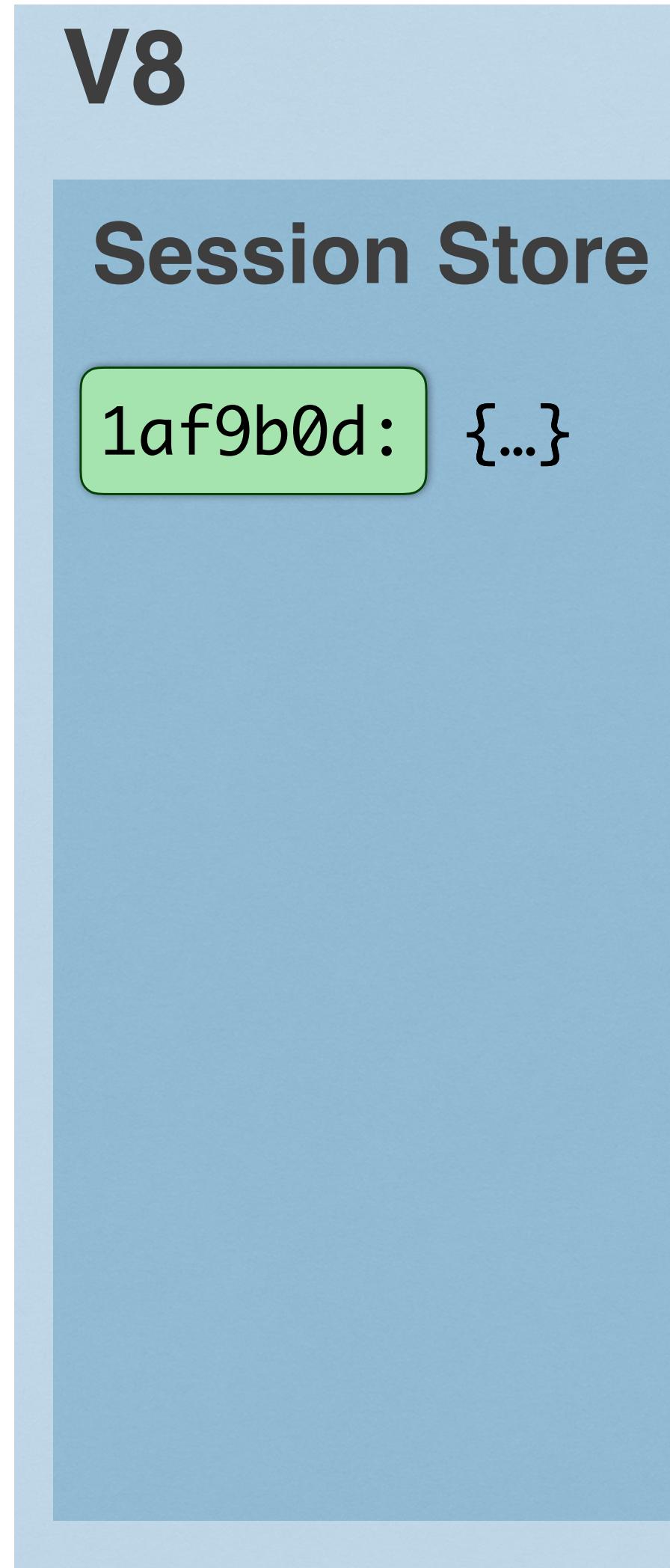
Client (Browser)



http://yourapp.com



Server (Backend)



<http://yourapp.com>

Internet (HTTP)

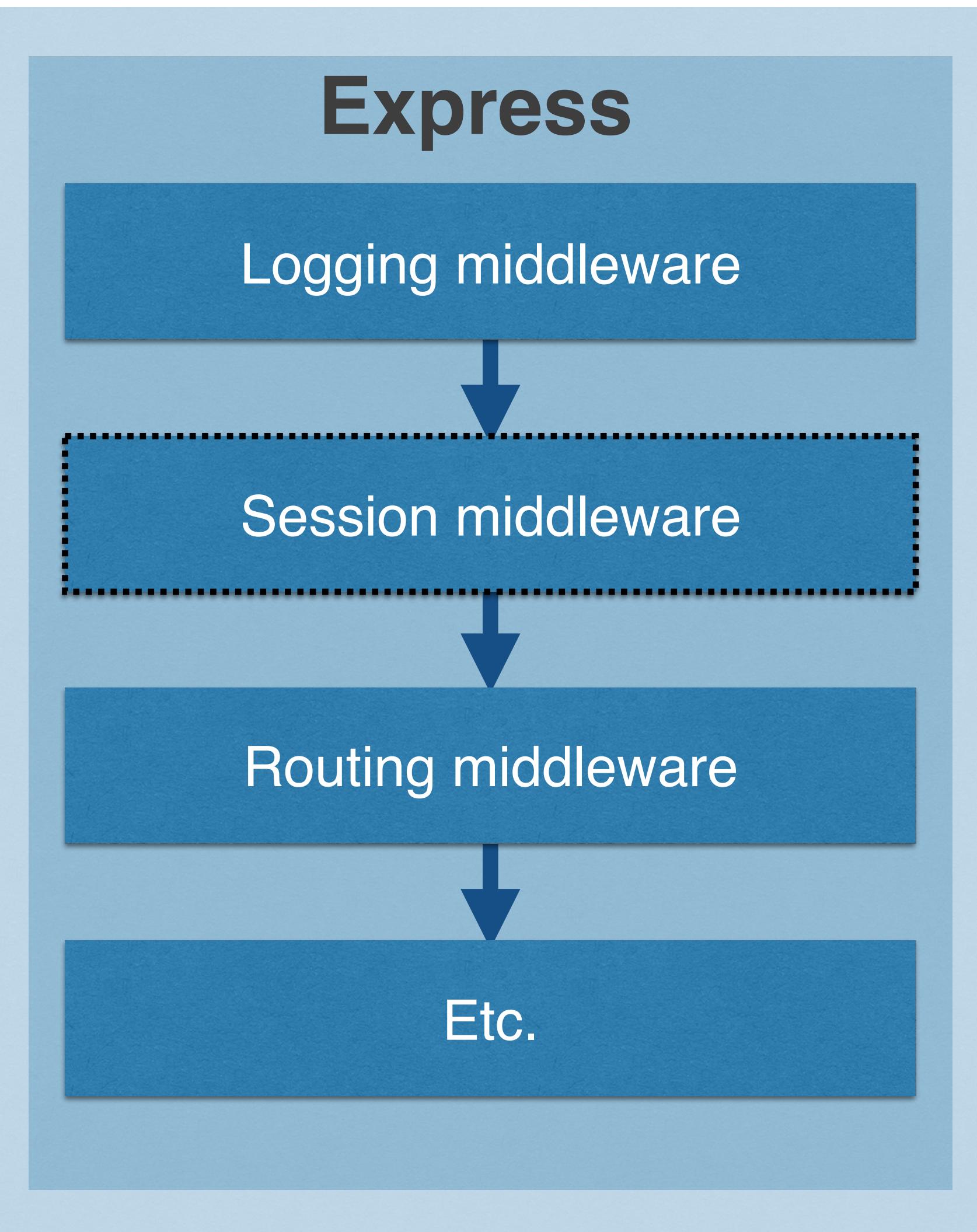


Multiple Sessions

Server (Backend)



Internet (HTTP)



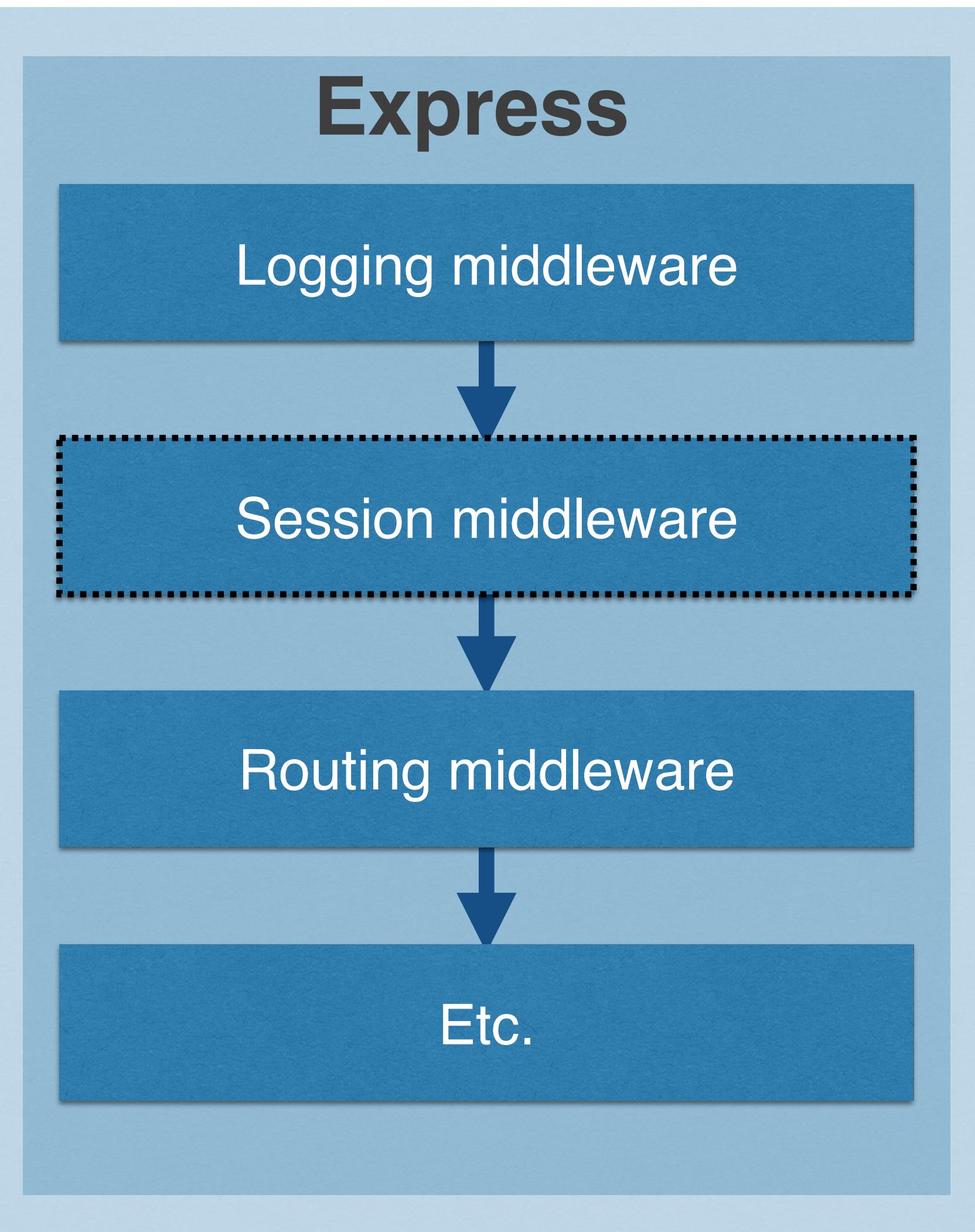
Client 1 (Browser)



Server (Backend)



Internet (HTTP)



Client 1 (Browser)

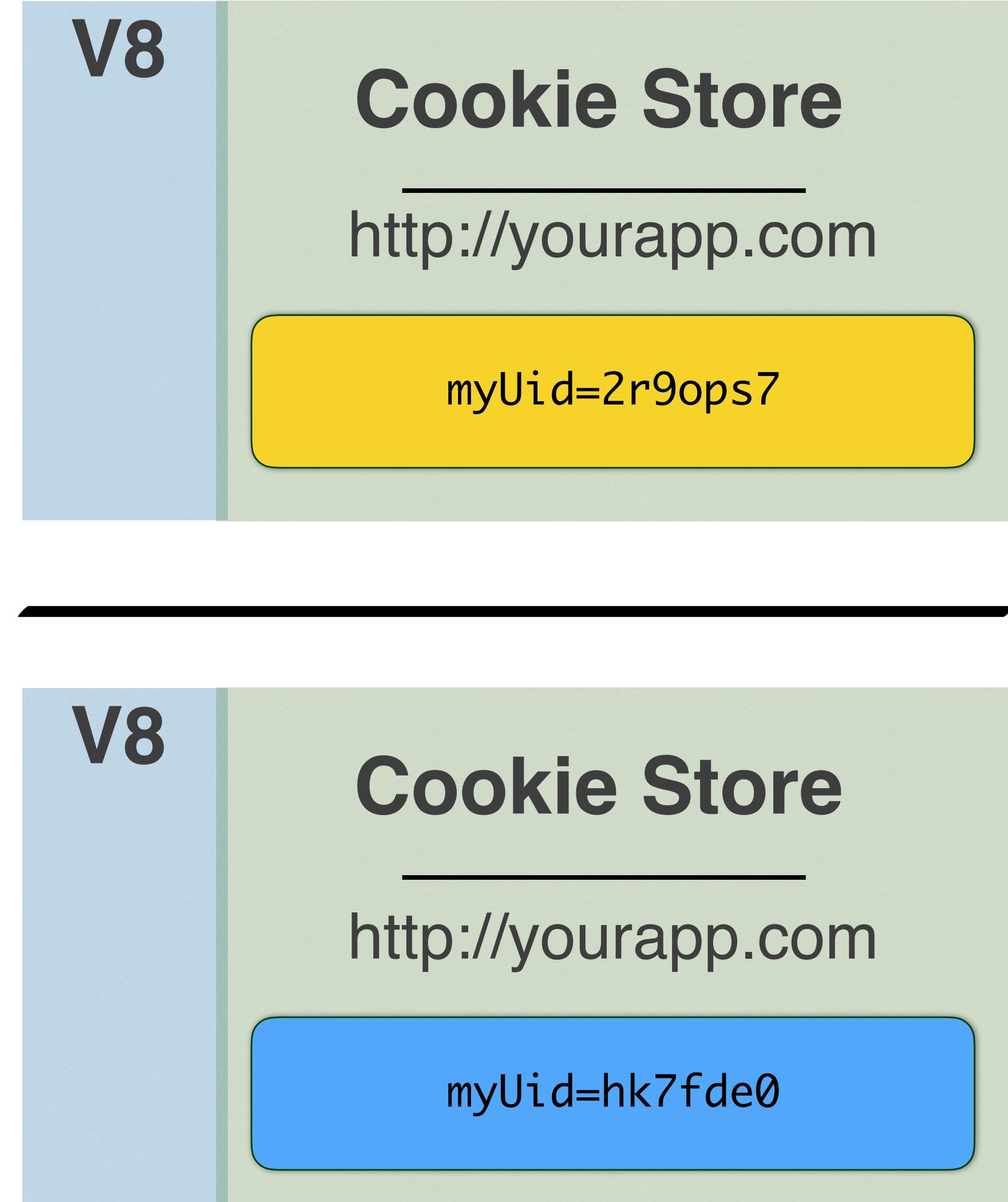


Server (Backend)



<http://yourapp.com>

Internet (HTTP)



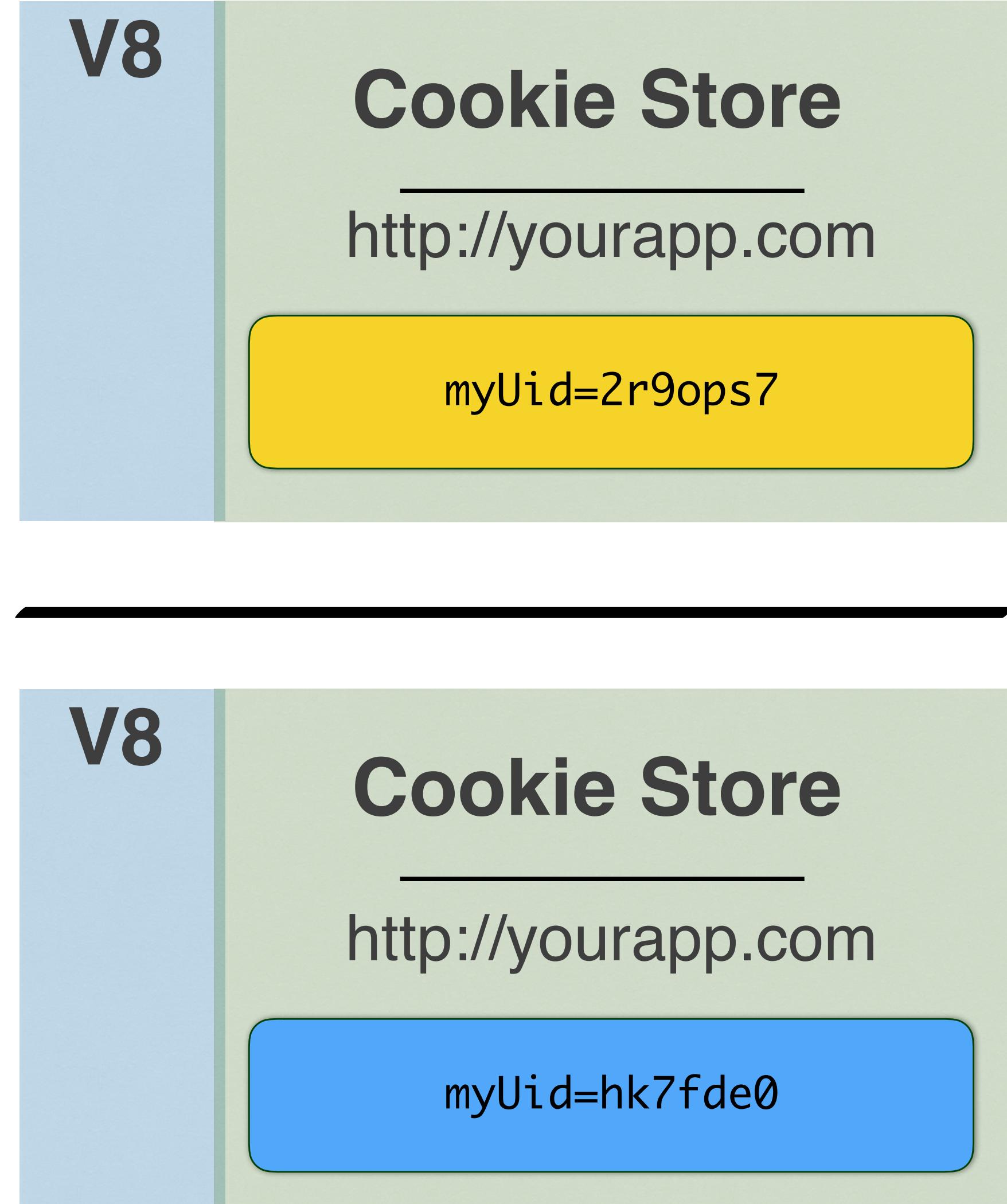
Client 2 (Browser)

Server (Backend)



<http://yourapp.com>

Internet (HTTP)

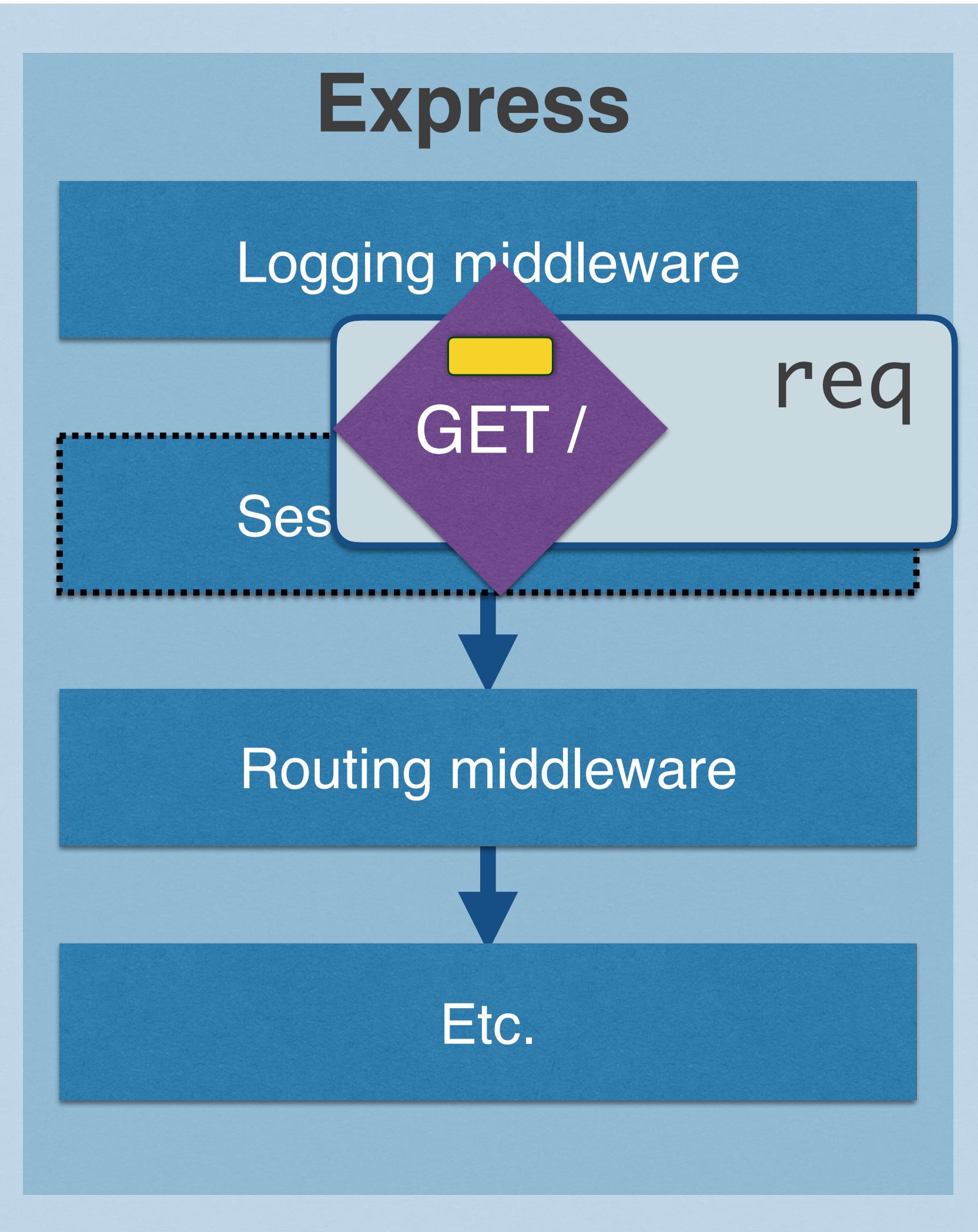


Client 2 (Browser)

Server (Backend)



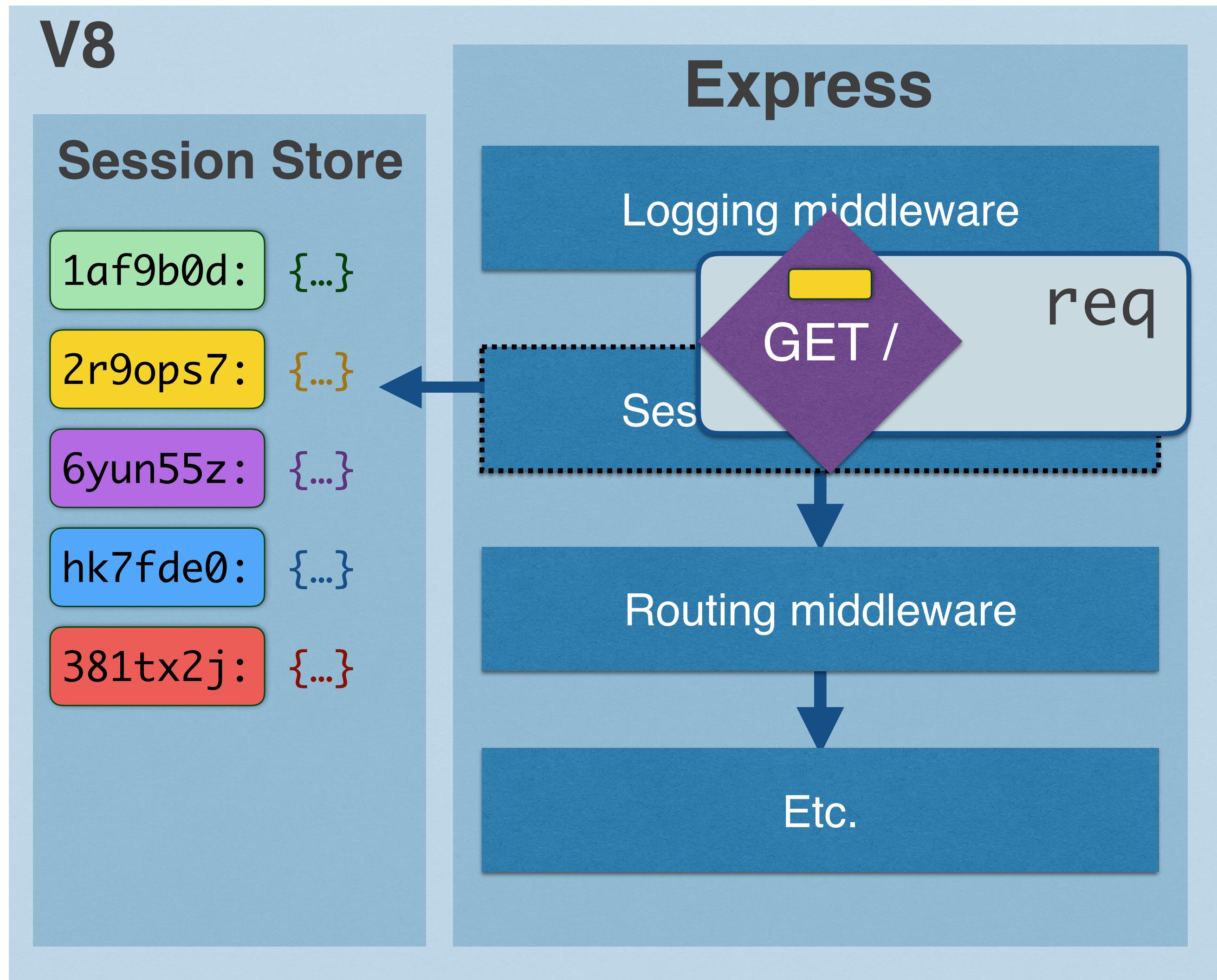
Internet (HTTP)



Client 1 (Browser)

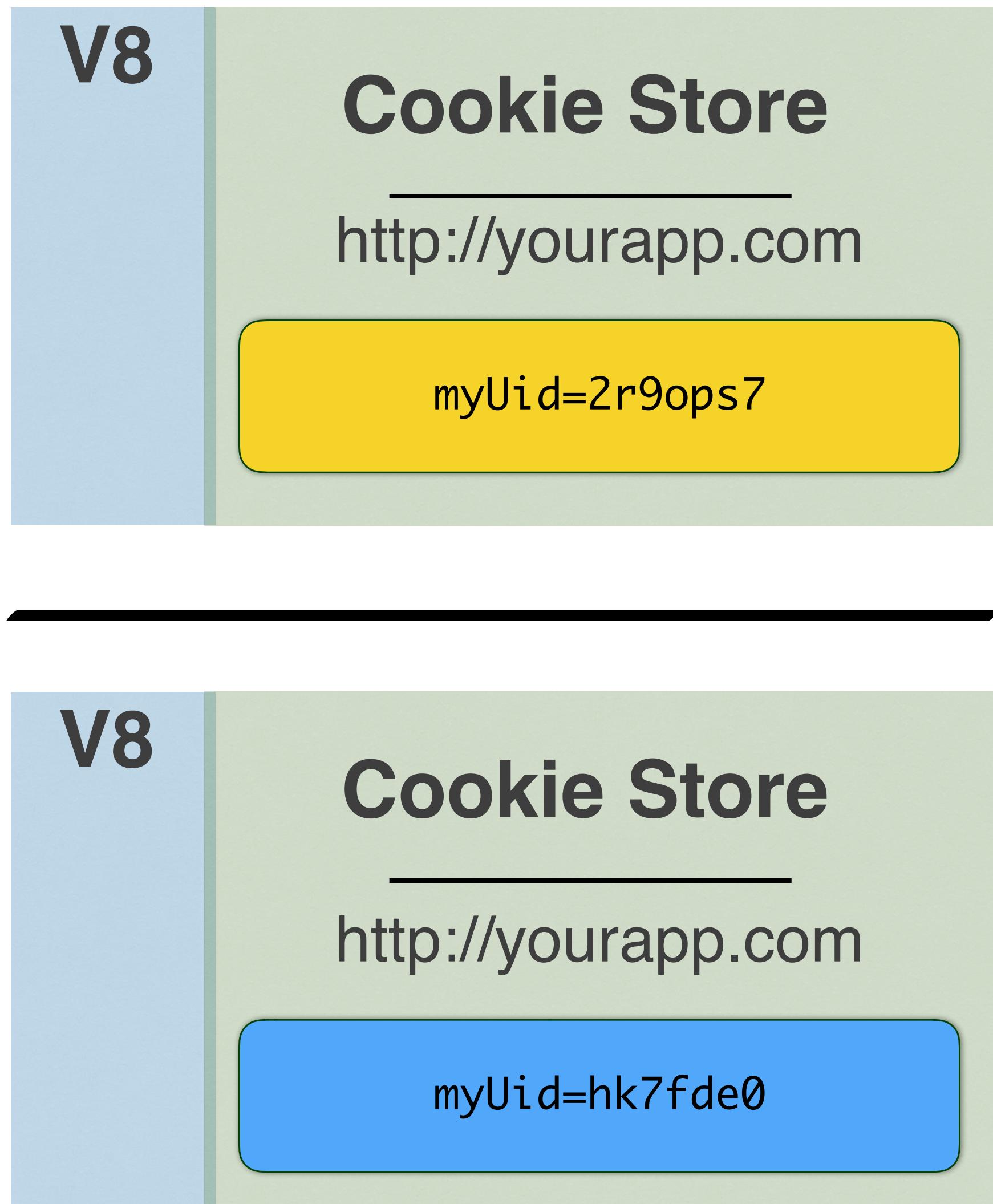


Server (Backend)



<http://yourapp.com>

Internet (HTTP)



Client 1 (Browser)

Cookie Store

<http://yourapp.com>

myUid=2r9ops7

V8

Cookie Store

<http://yourapp.com>

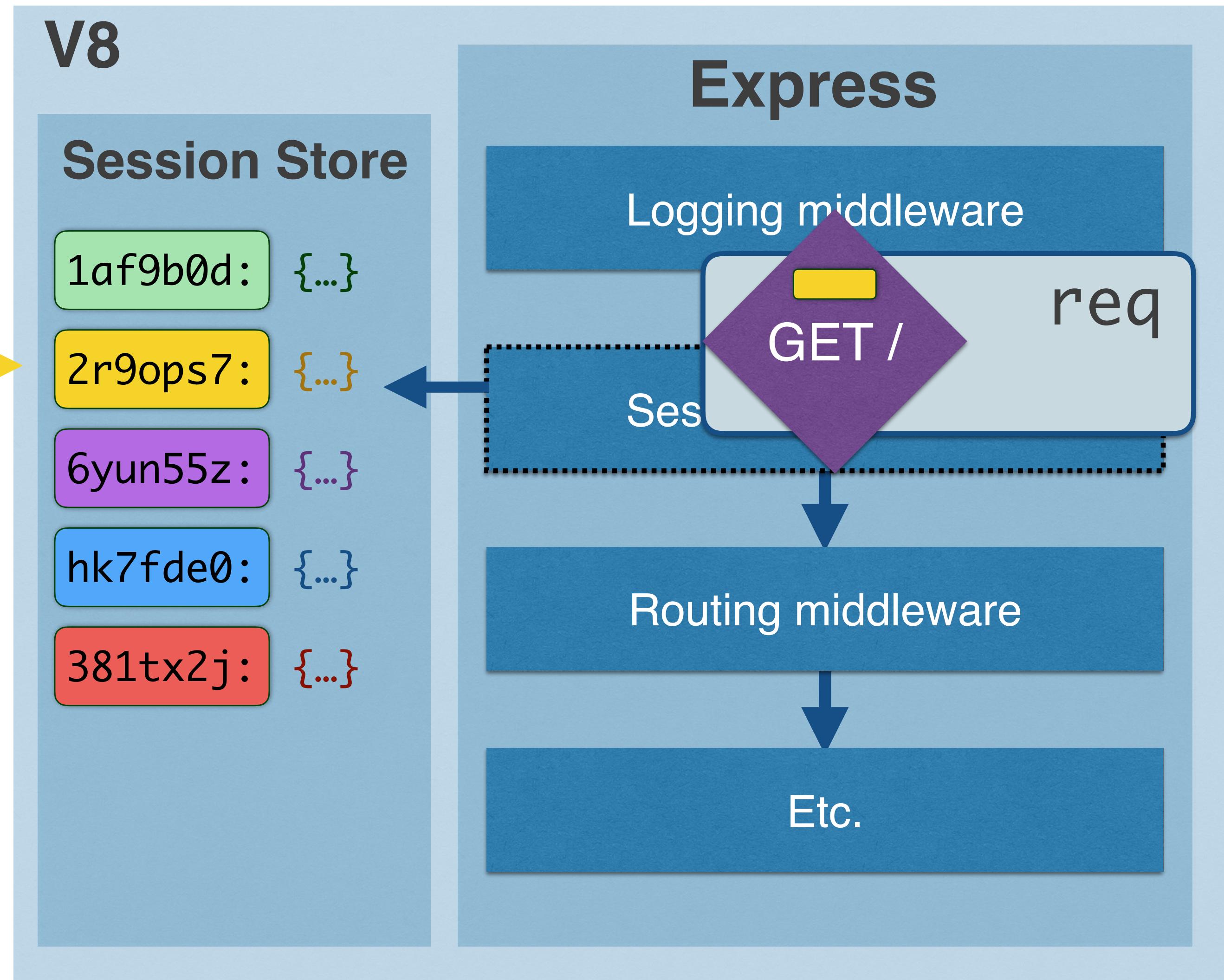
myUid=hk7fde0

Client 2 (Browser)

Server (Backend)

Internet (HTTP)

Client 1 (Browser)



<http://yourapp.com>

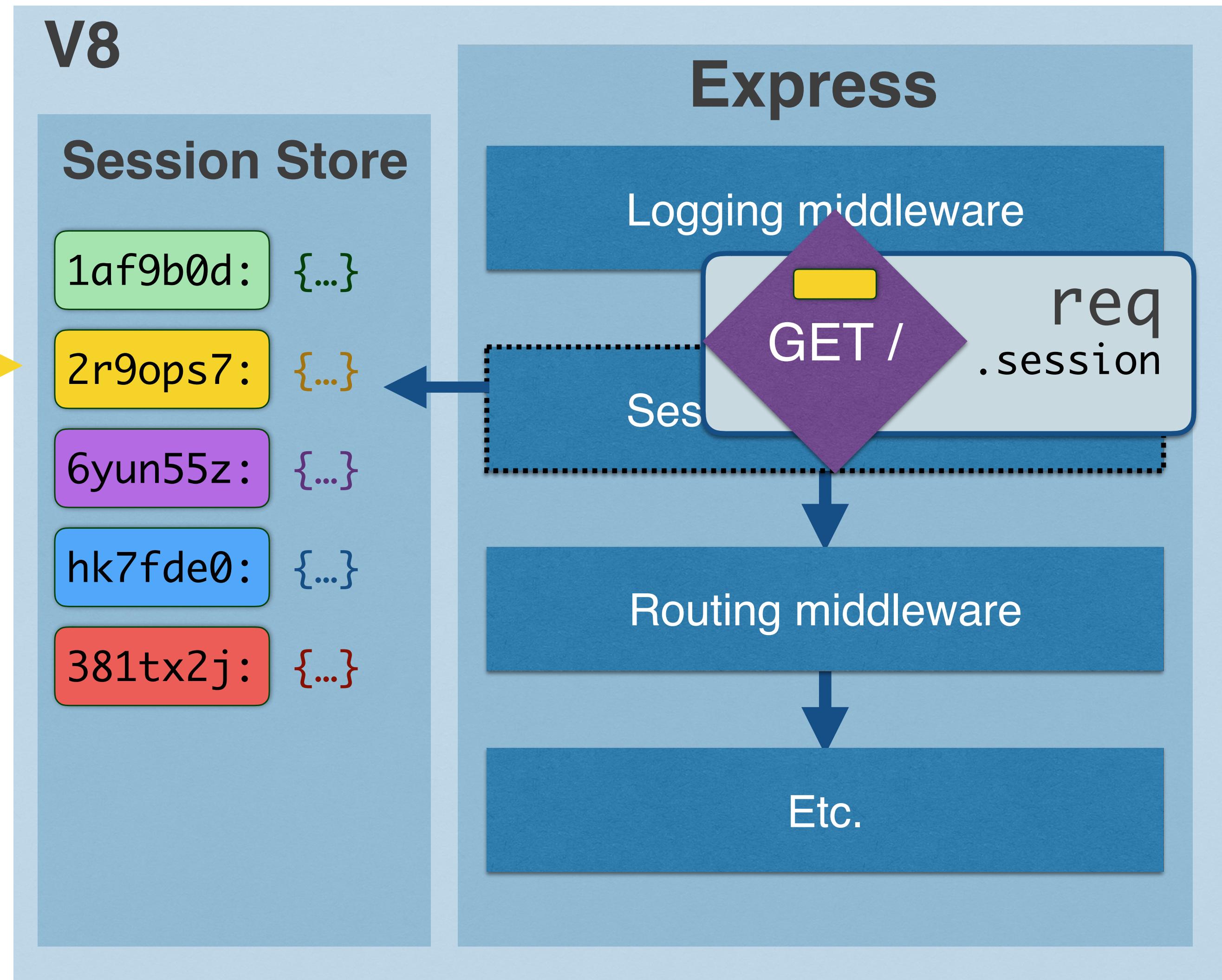


Client 2 (Browser)

Server (Backend)

Internet (HTTP)

Client 1 (Browser)



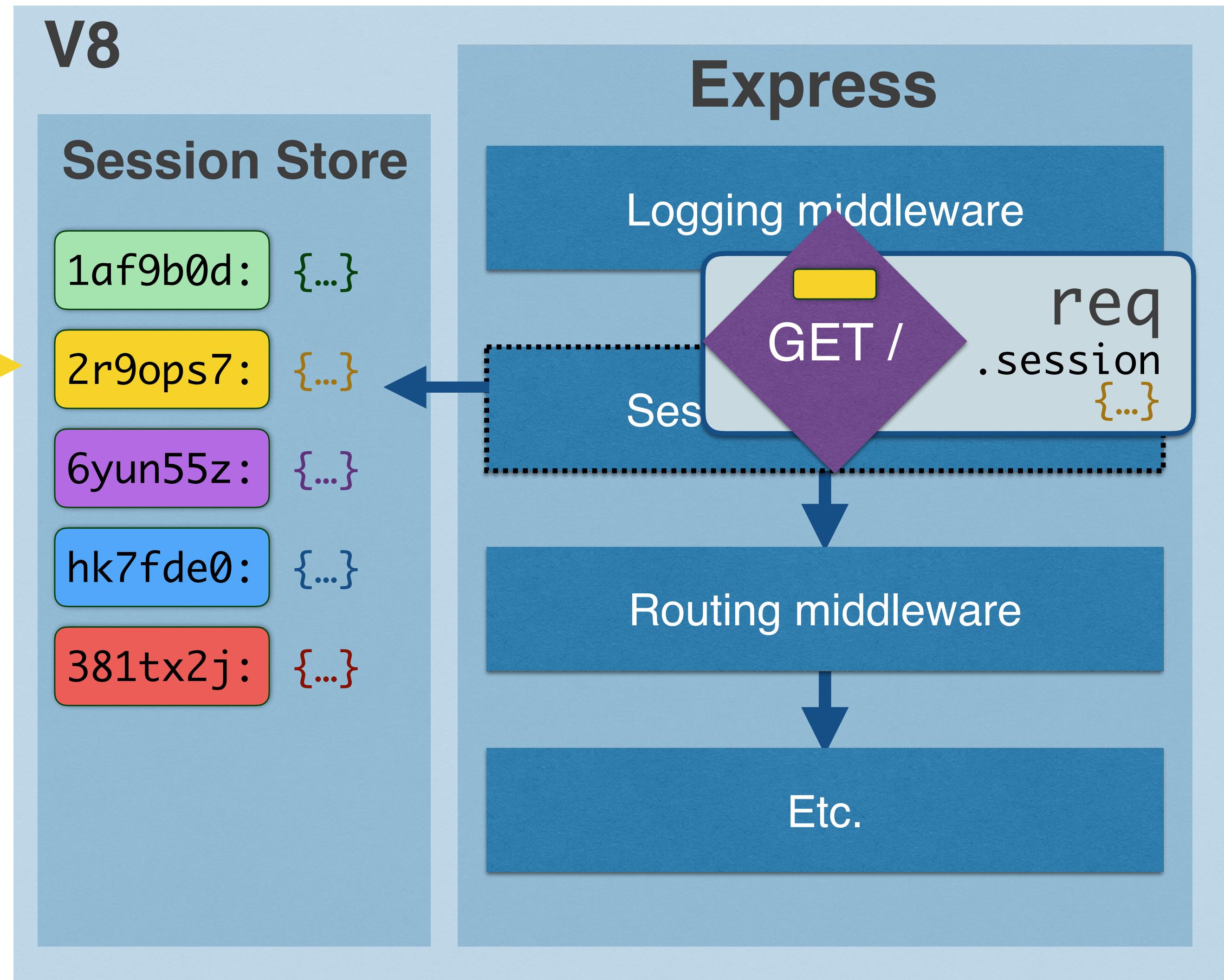
http://yourapp.com



Server (Backend)

Internet (HTTP)

Client 1 (Browser)



<http://yourapp.com>

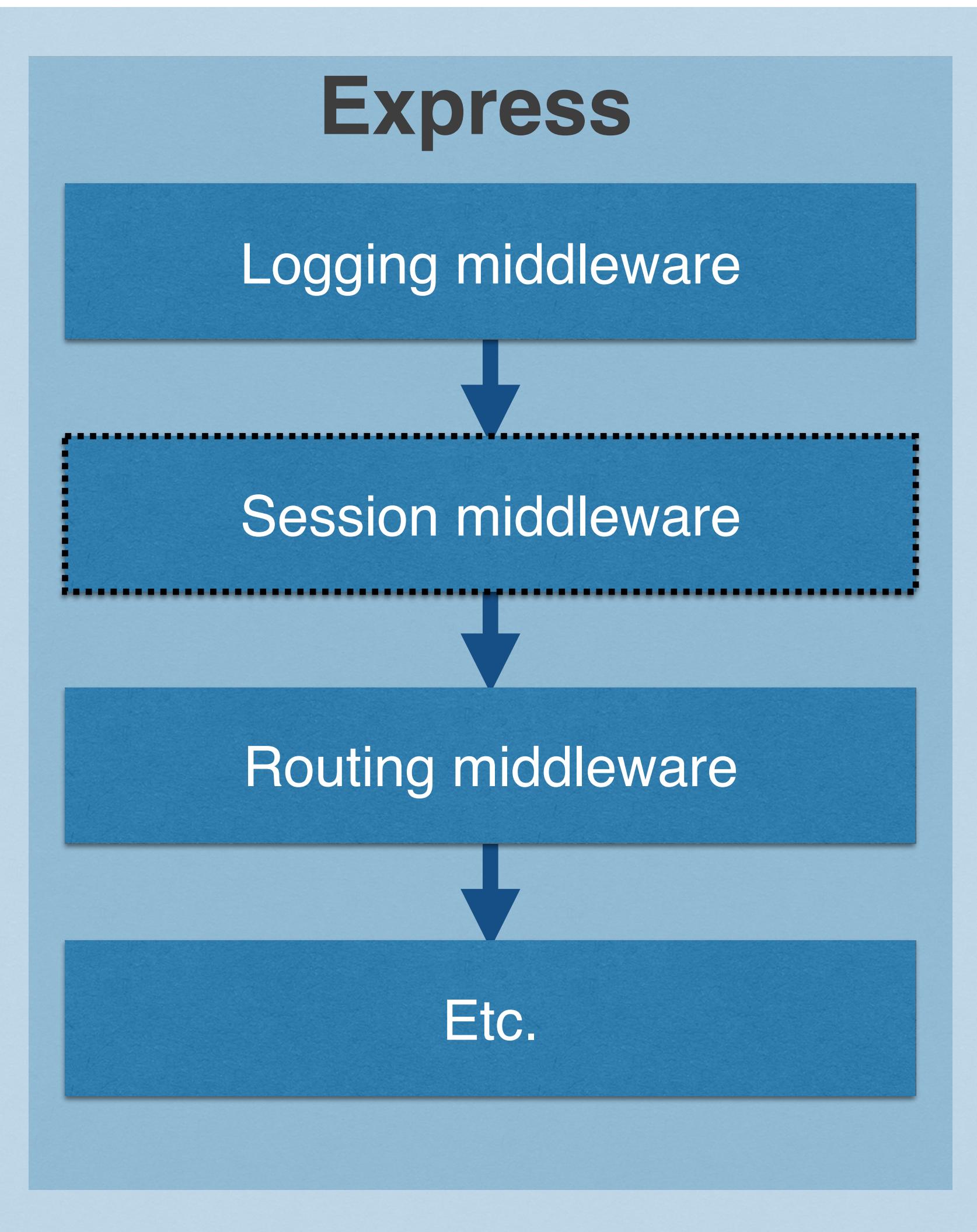


Client 2 (Browser)

Server (Backend)



Internet (HTTP)



Client 1 (Browser)



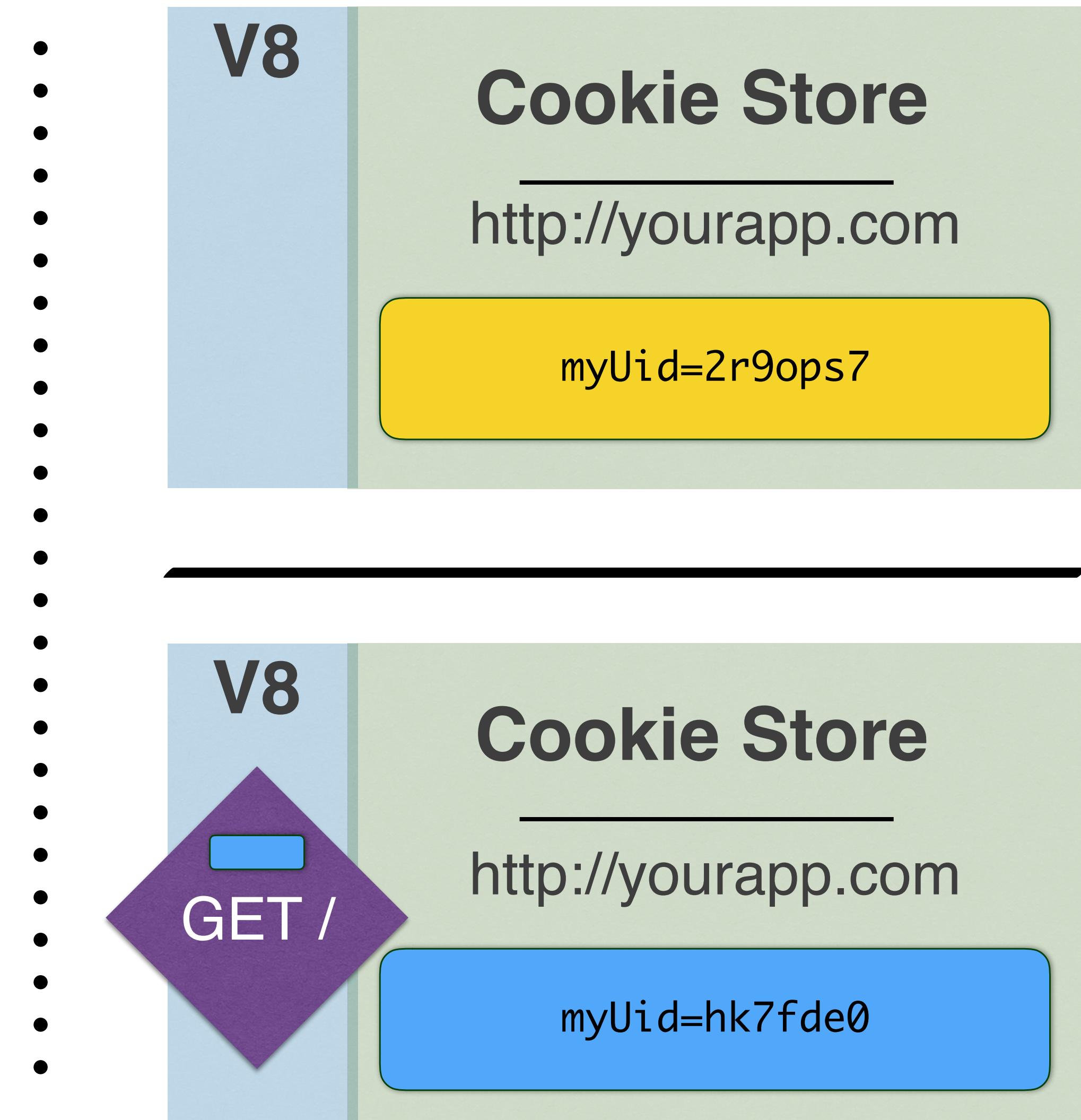
Client 2 (Browser)

Server (Backend)



<http://yourapp.com>

Internet (HTTP)



Server (Backend)



<http://yourapp.com>

Internet (HTTP)



Client 2 (Browser)

Server (Backend)



<http://yourapp.com>

Internet (HTTP)



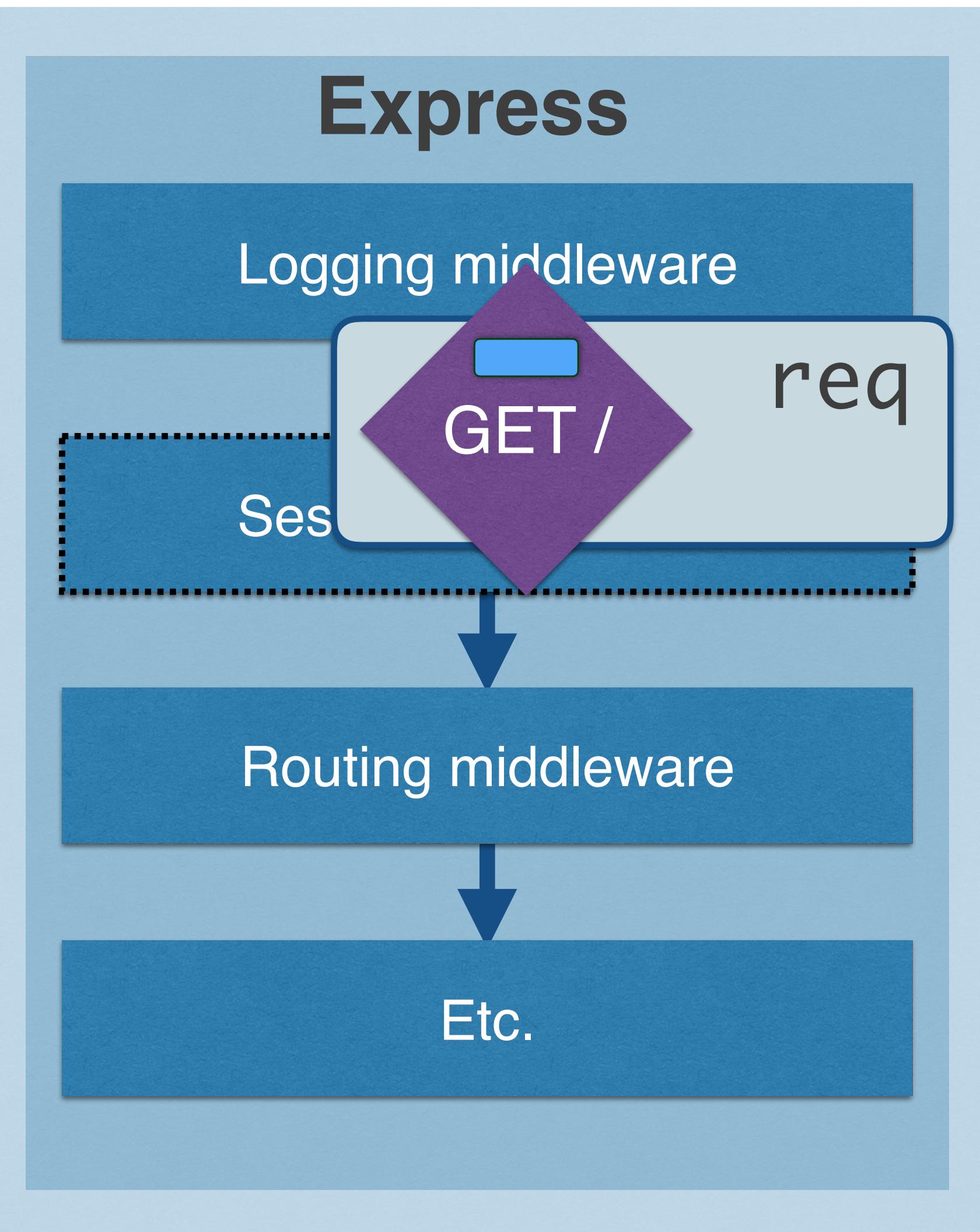
Client 2 (Browser)

Server (Backend)



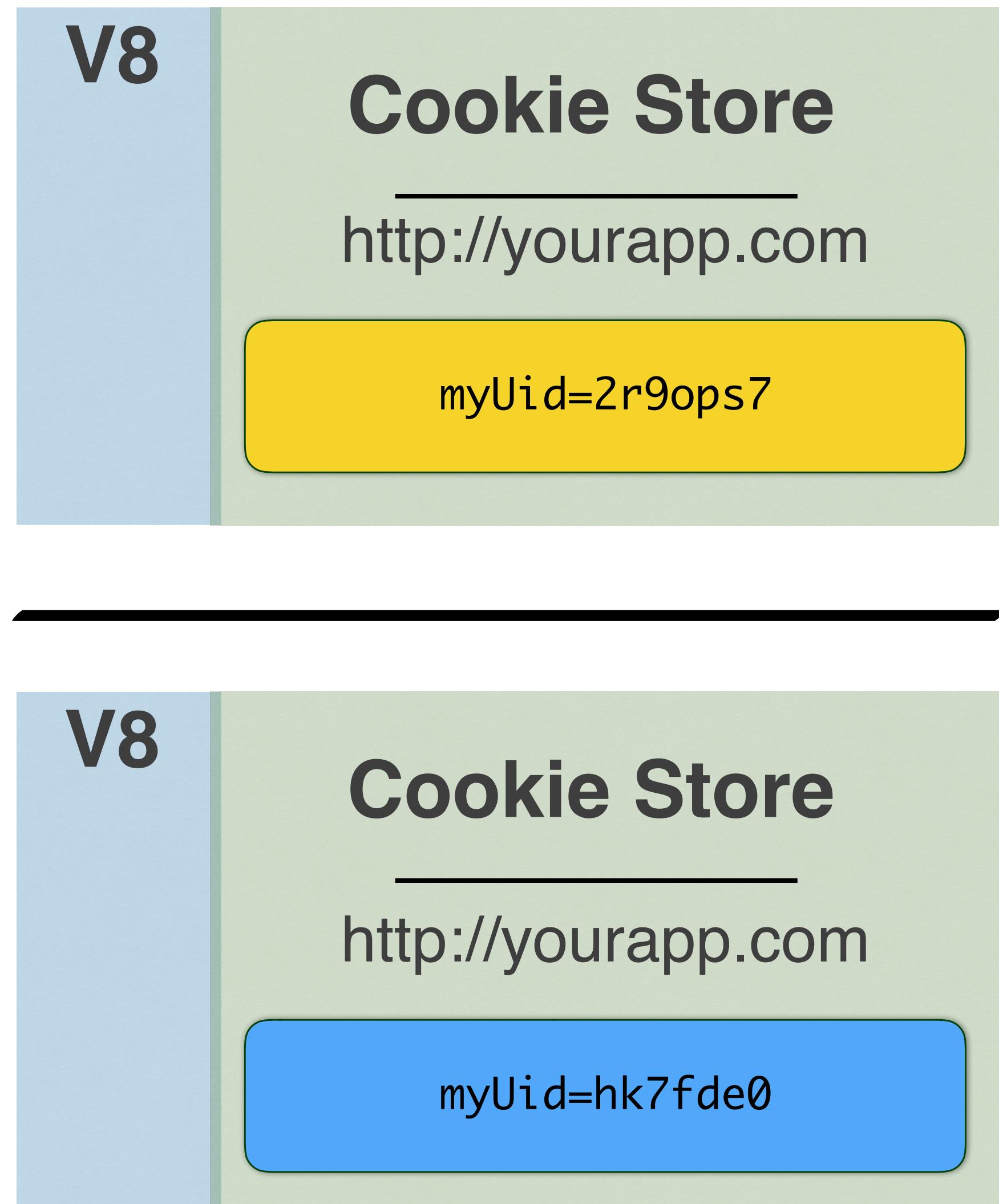
<http://yourapp.com>

Internet (HTTP)



39

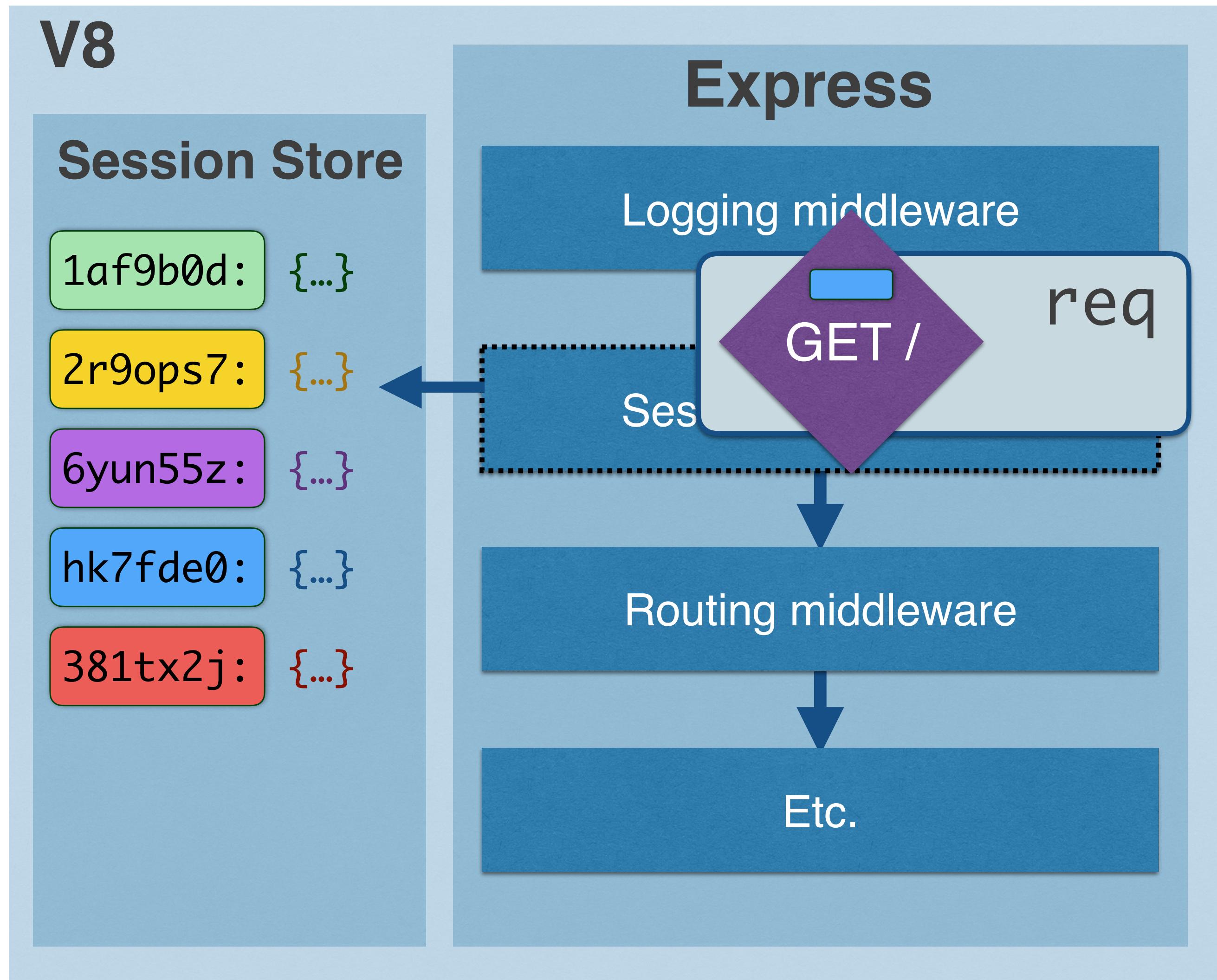
Client 1 (Browser)



Client 2 (Browser)

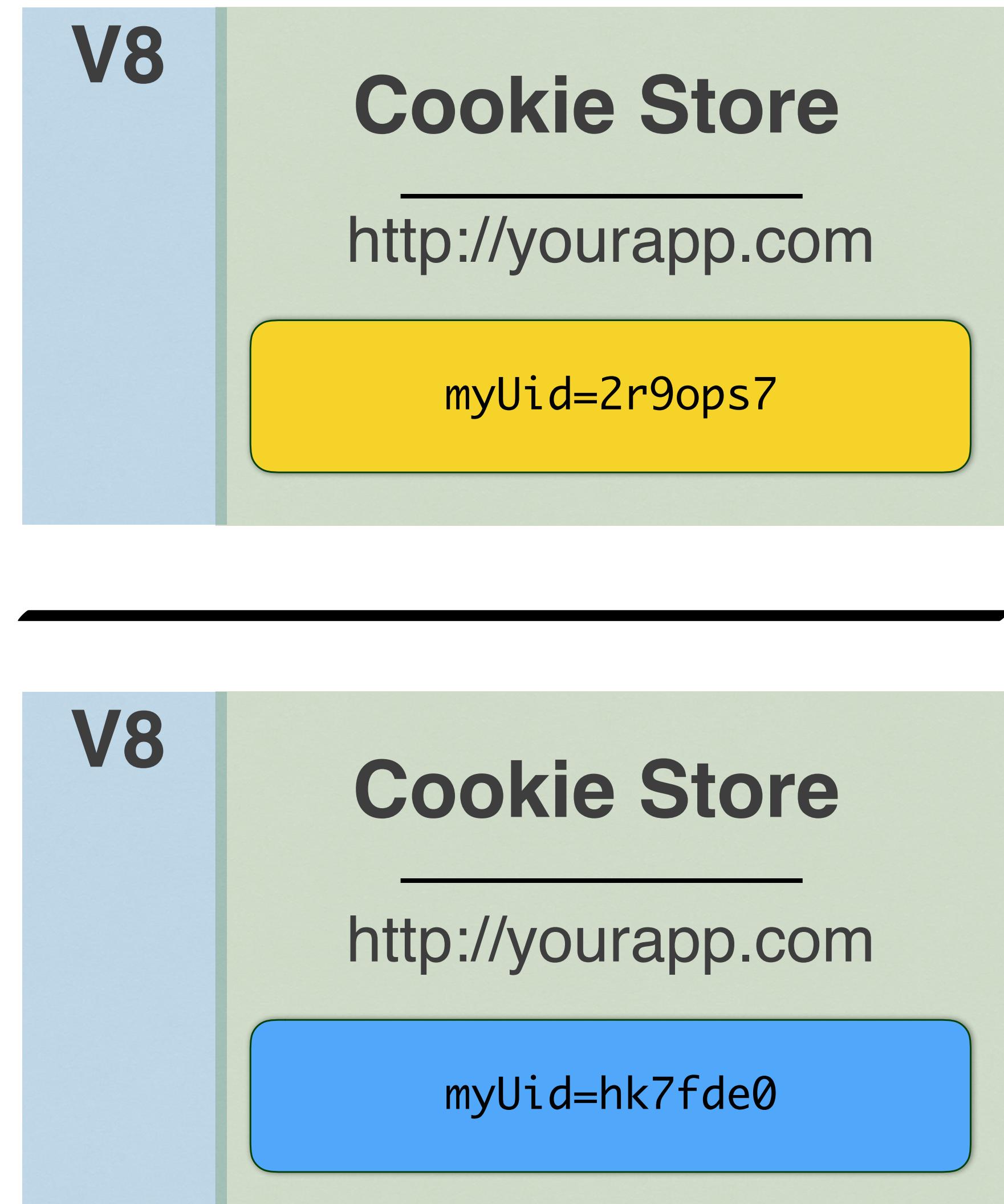
AUTH

Server (Backend)



<http://yourapp.com>

Internet (HTTP)

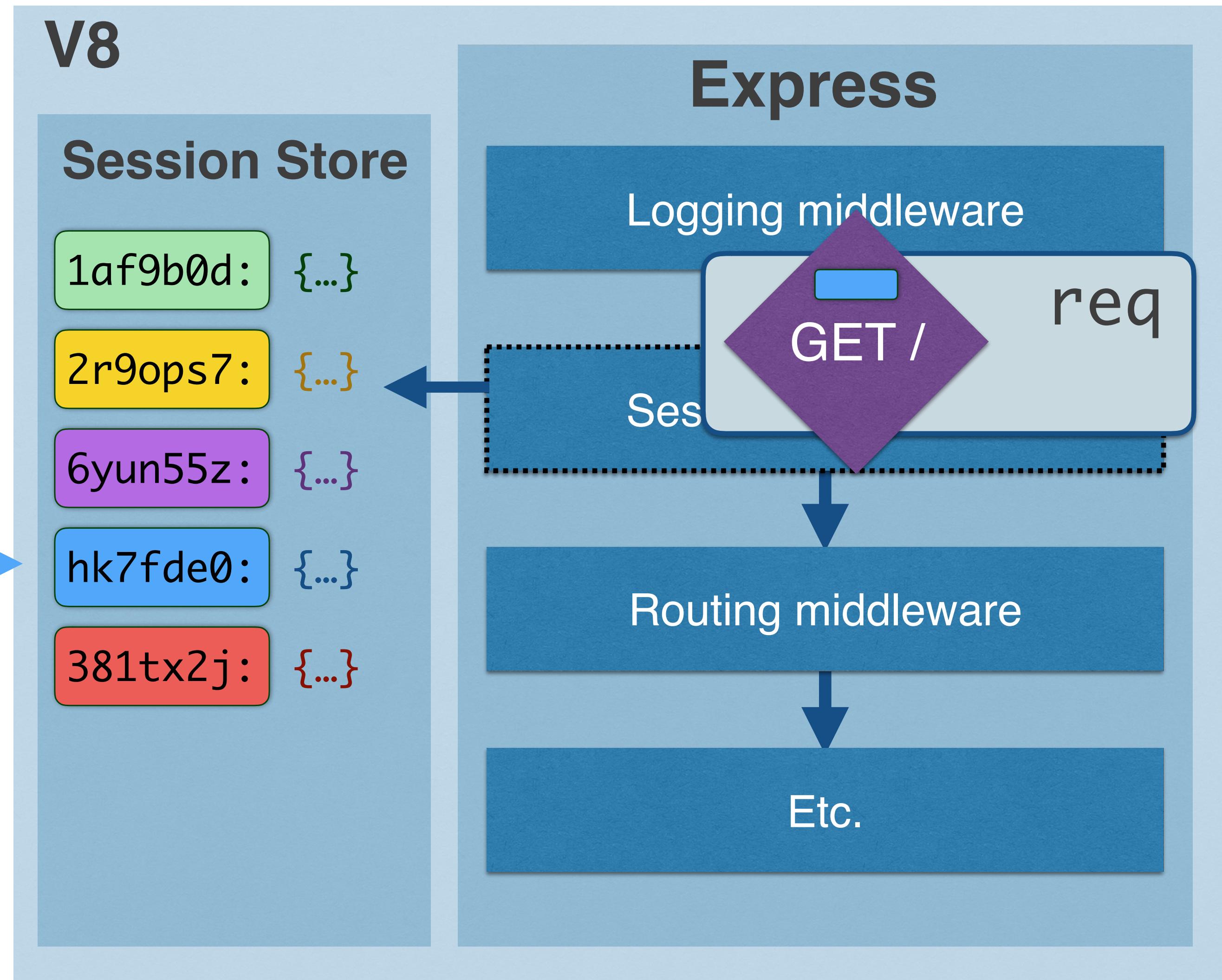


Client 2 (Browser)

Server (Backend)

Internet (HTTP)

Client 1 (Browser)



<http://yourapp.com>

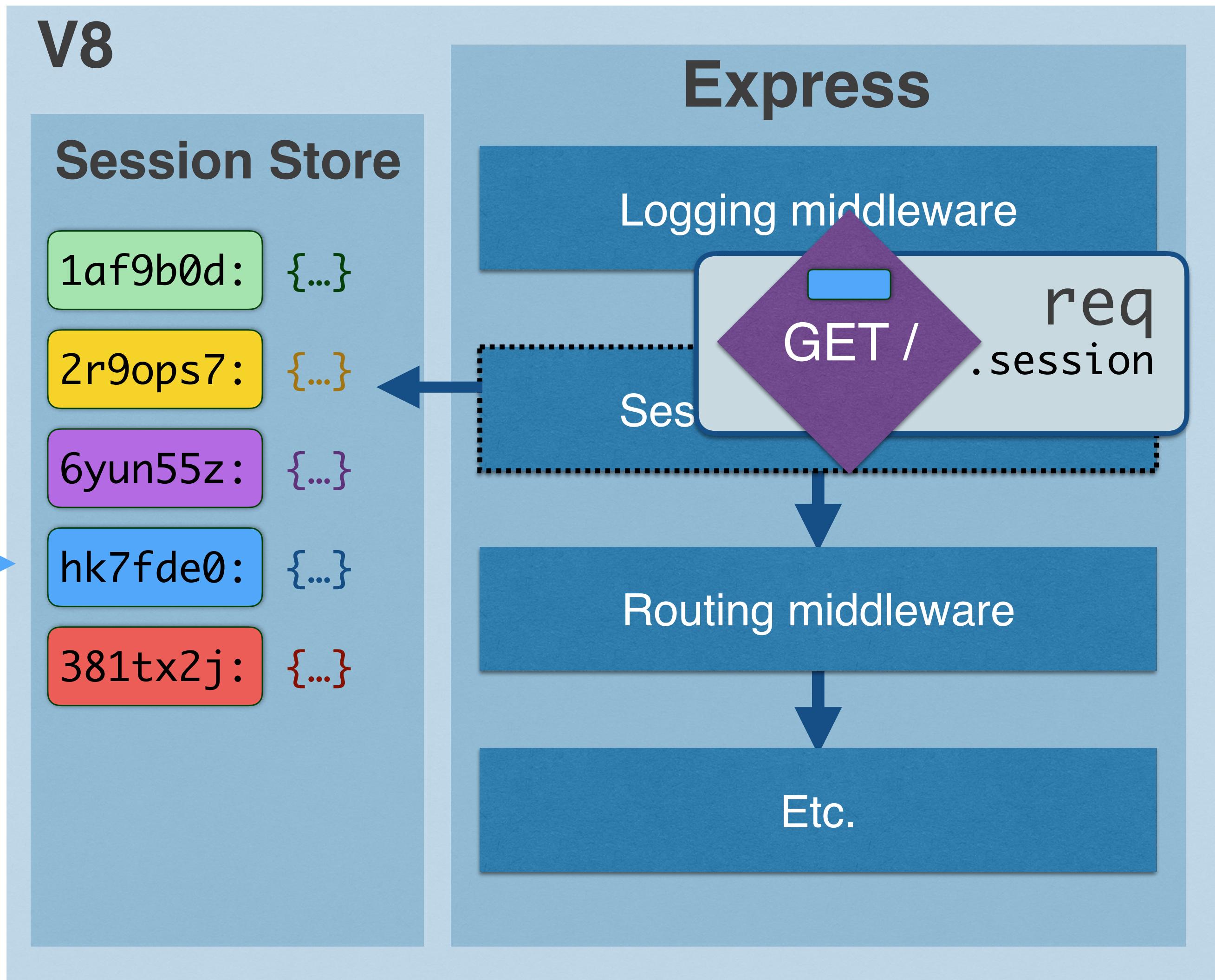


Client 2 (Browser)

Server (Backend)

Internet (HTTP)

Client 1 (Browser)



<http://yourapp.com>

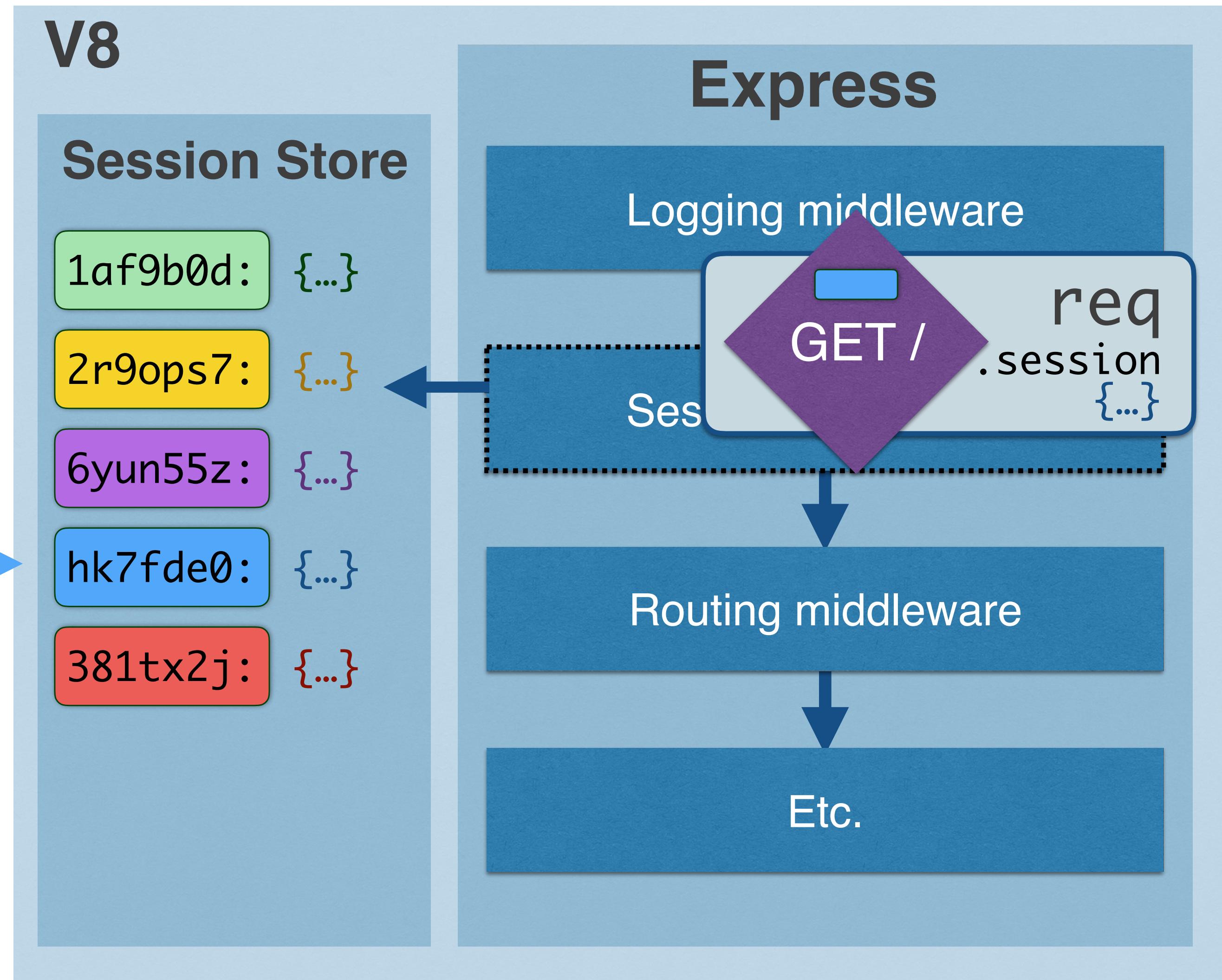


Client 2 (Browser)

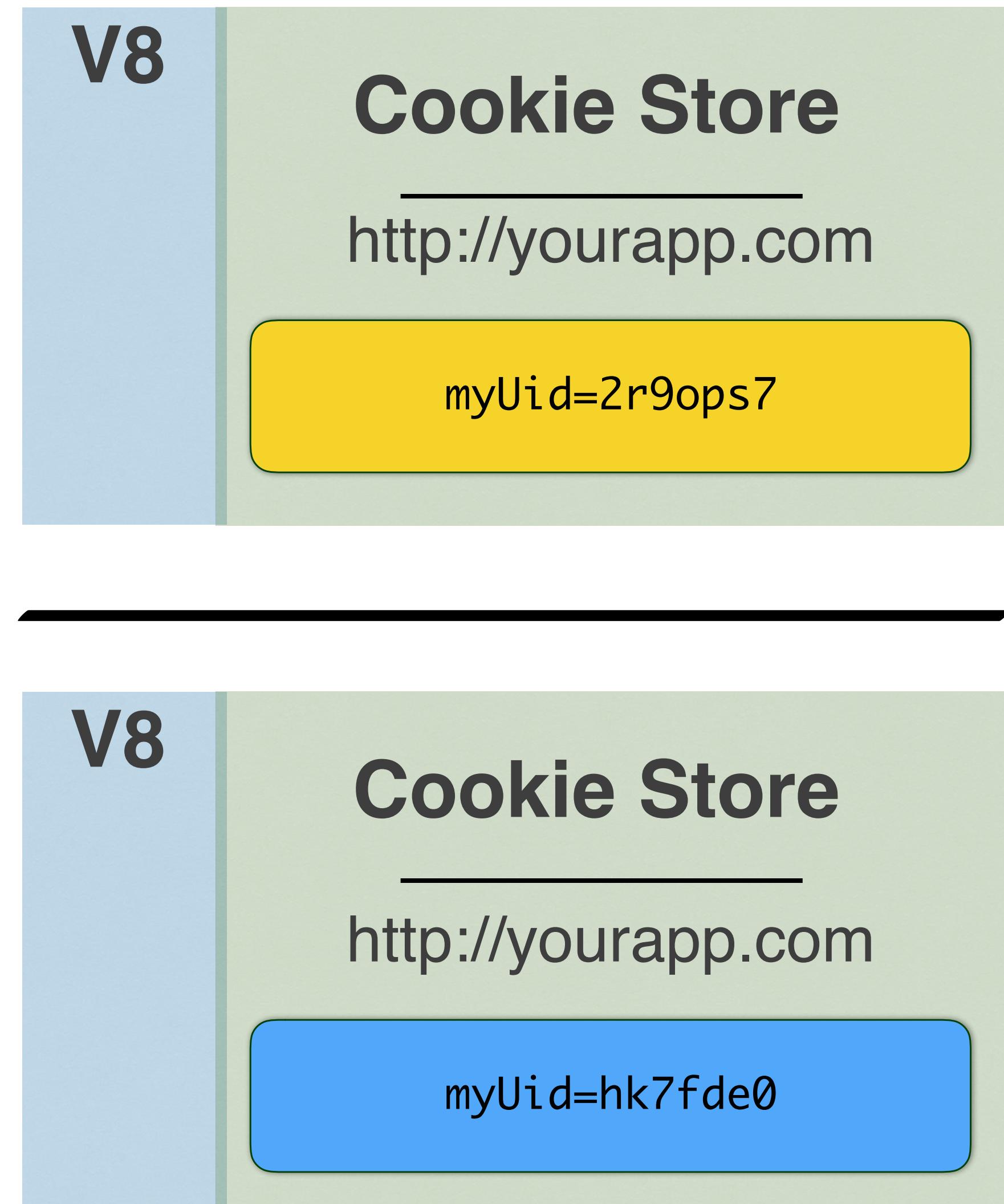
Server (Backend)

Internet (HTTP)

Client 1 (Browser)



<http://yourapp.com>



Client 2 (Browser)

*“You get a session, you get a session,
everybody gets a session!”*

-NOT OPRAH