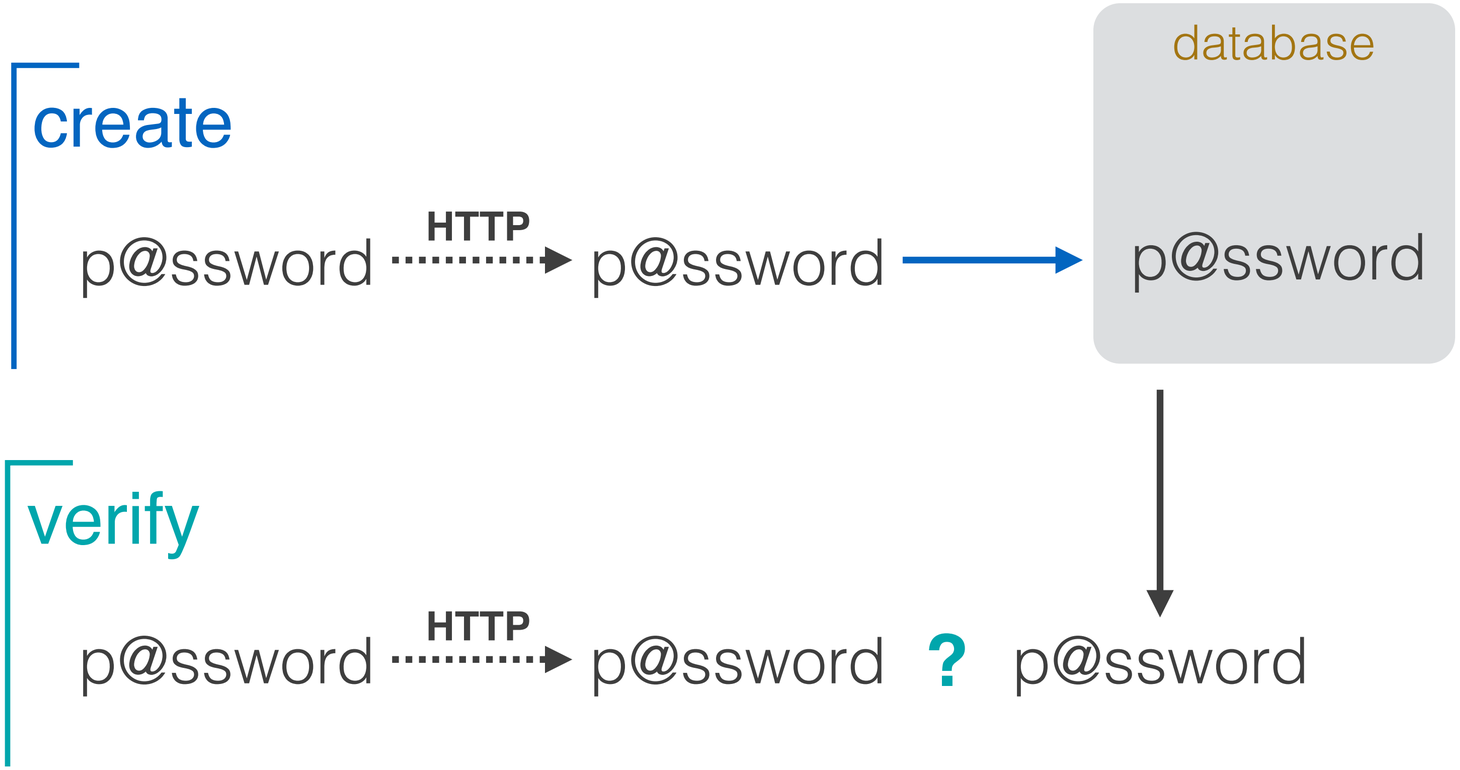
SESSIONS AND AUTH DATA FLOW

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?”

LOGIN/SIGNUP



STAYING LOGGED IN

THE PROBLEM

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

IDEAS?

- script variables
- database documents

SCRIPT VARIABLES?

Data will not persist across browser pages

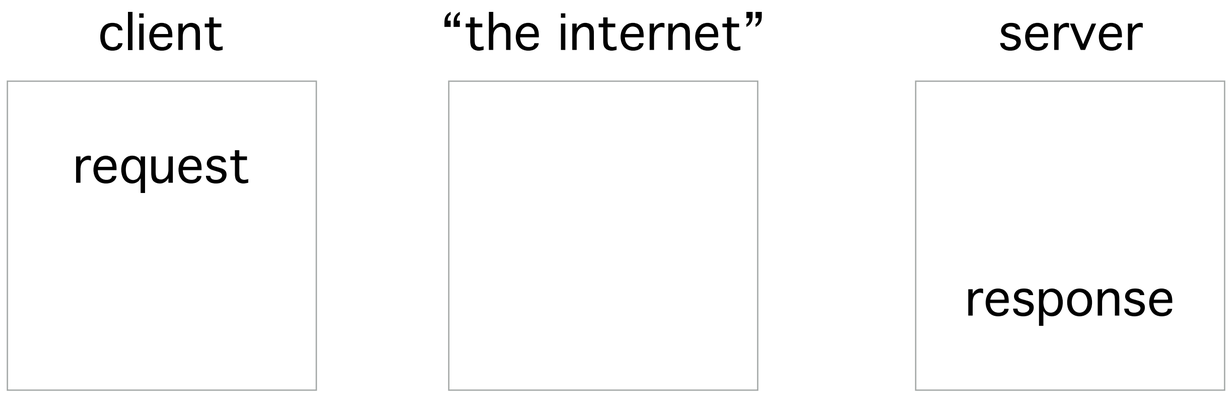
DATABASE DOCUMENTS?

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

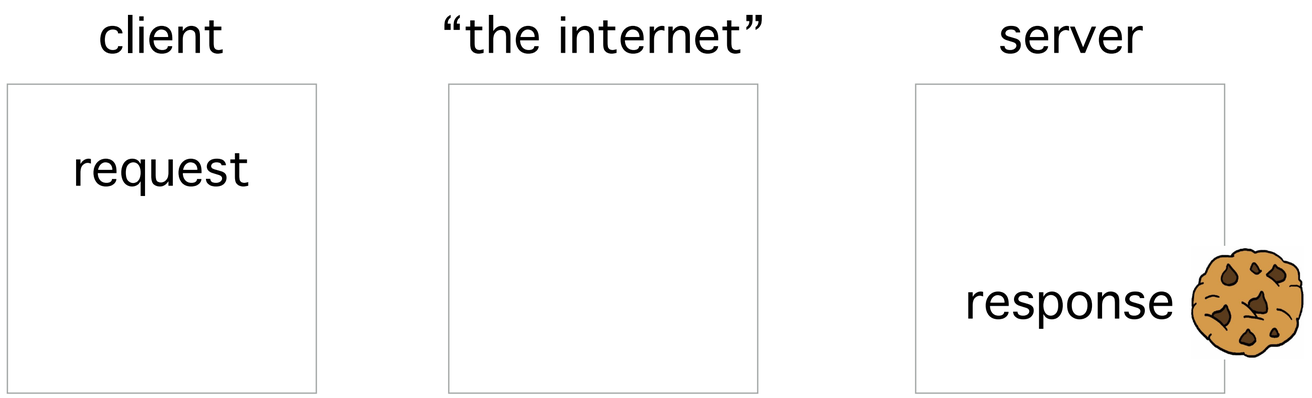

COOKIE!

= small text file

HTTP



WITH COOKIES



WITH COOKIES

client

“the internet”

server

WITH COOKIES

client

request

“the internet”

server

response

Do something with cookie

COOKIES & SESSIONS

No need to authenticate for every request

SESSIONS

client

request

“the internet”

server

response

Make server session

sessions[id] = {}

SESSIONS

client

“the internet”

server

SESSIONS

client

request

“the internet”

server

response

Look up session

req.session = sessions[id]

COOKIES & SESSIONS

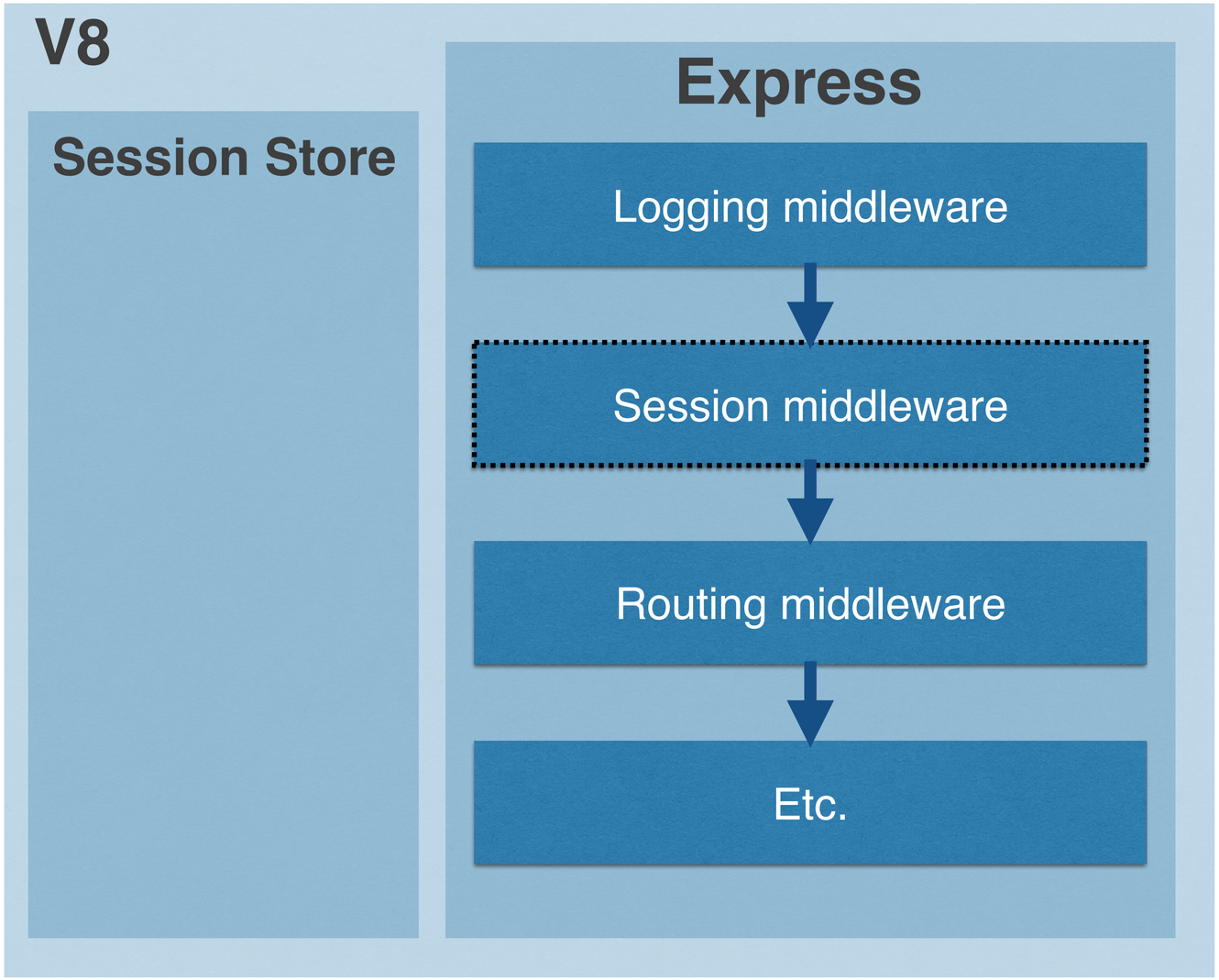
- Server gives client a cookie with ID only
- Client keeps cookie and sends with all requests
- Server loads request-specific session (stored in RAM)

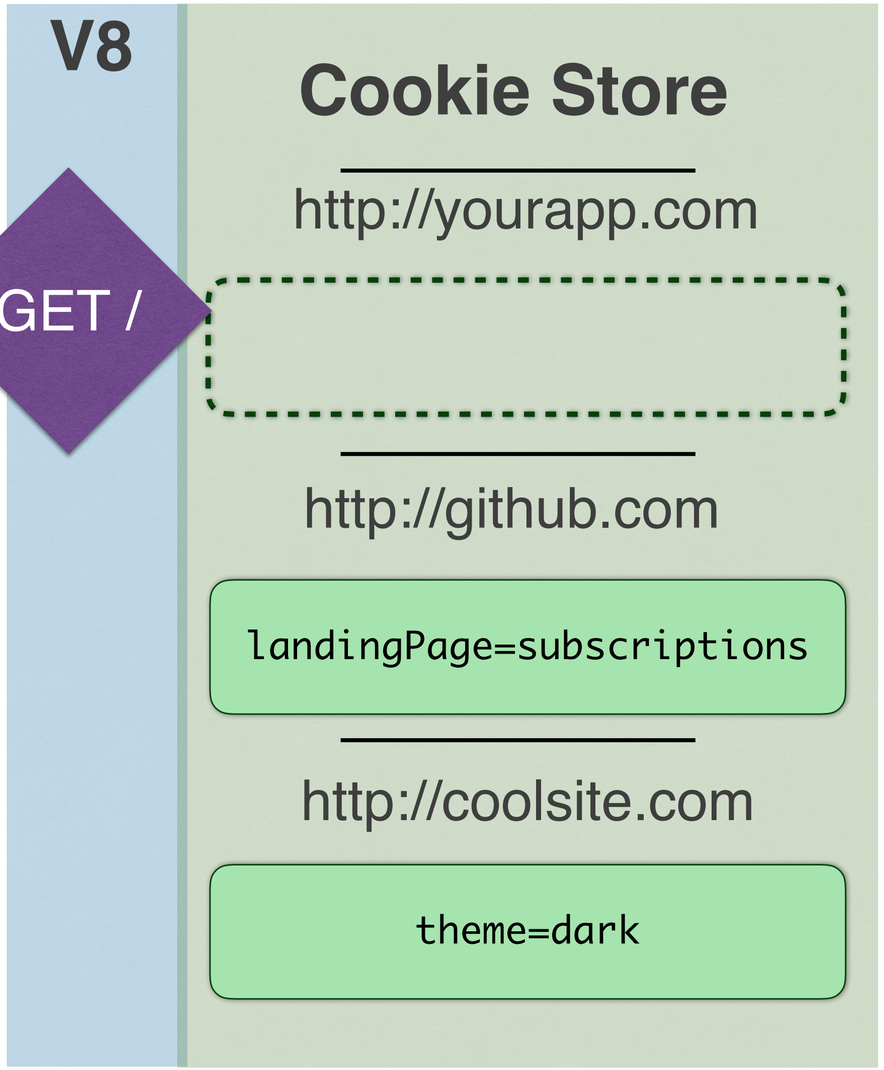

SESSIONS
IN
DETAIL

Server (Backend)

Internet (HTTP)

Client (Browser)





http://yourapp.com

HTTP REQUEST

```
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)!

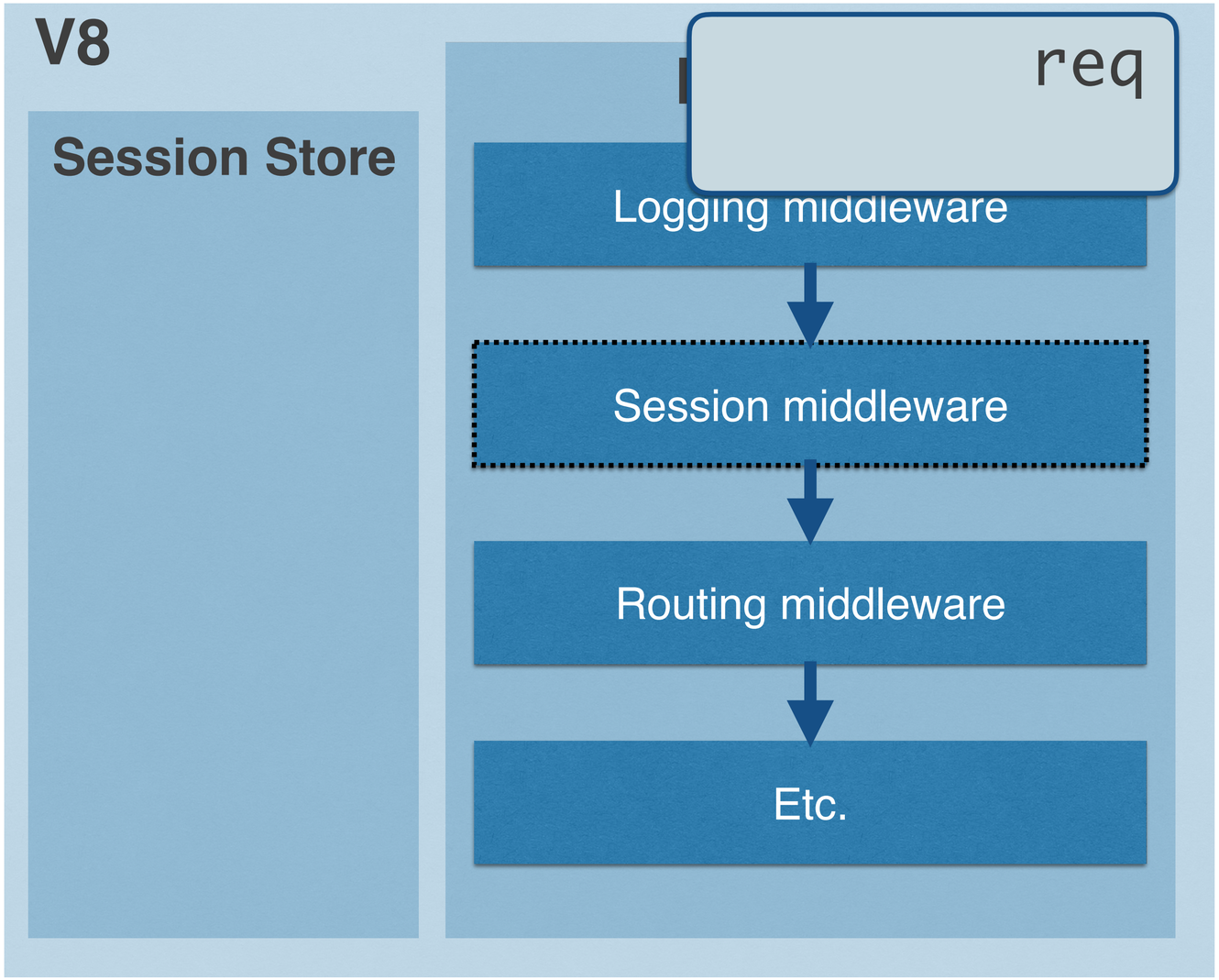
(headers)

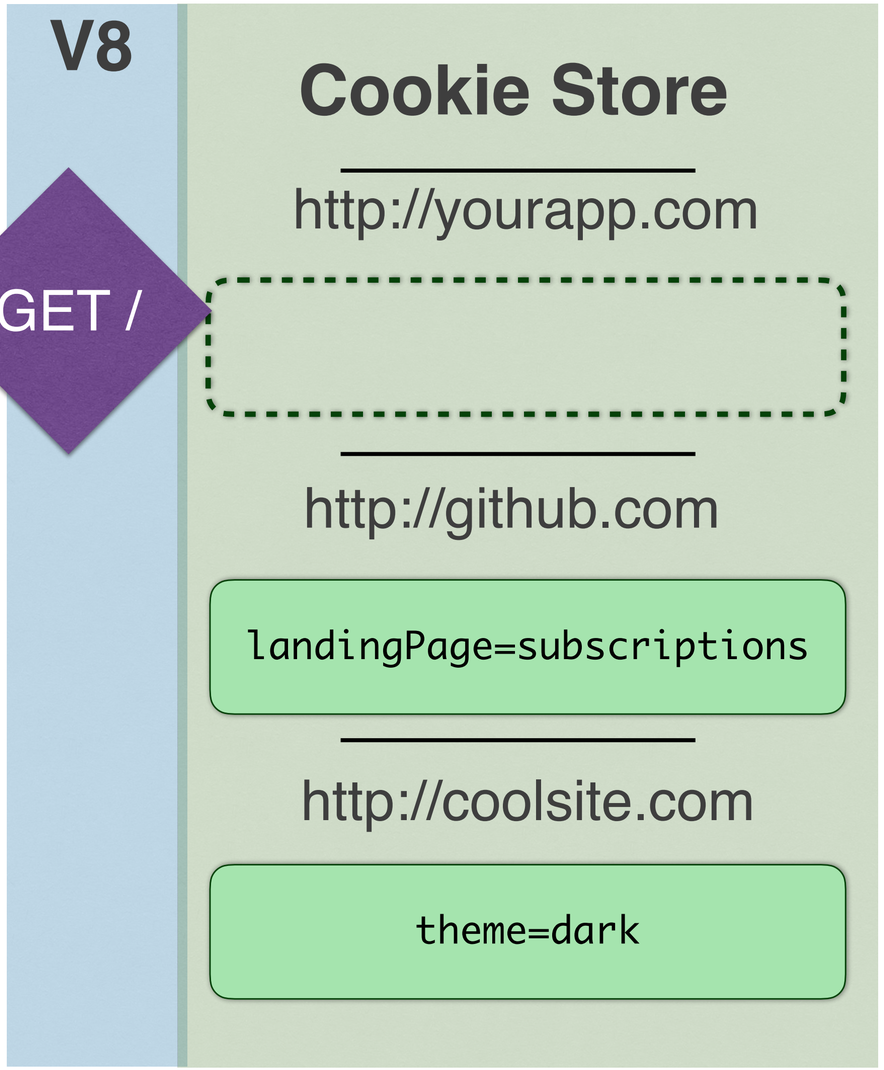
(body)

Server (Backend)

Internet (HTTP)

Client (Browser)





http://yourapp.com

HTTP REQUEST

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

(headers)

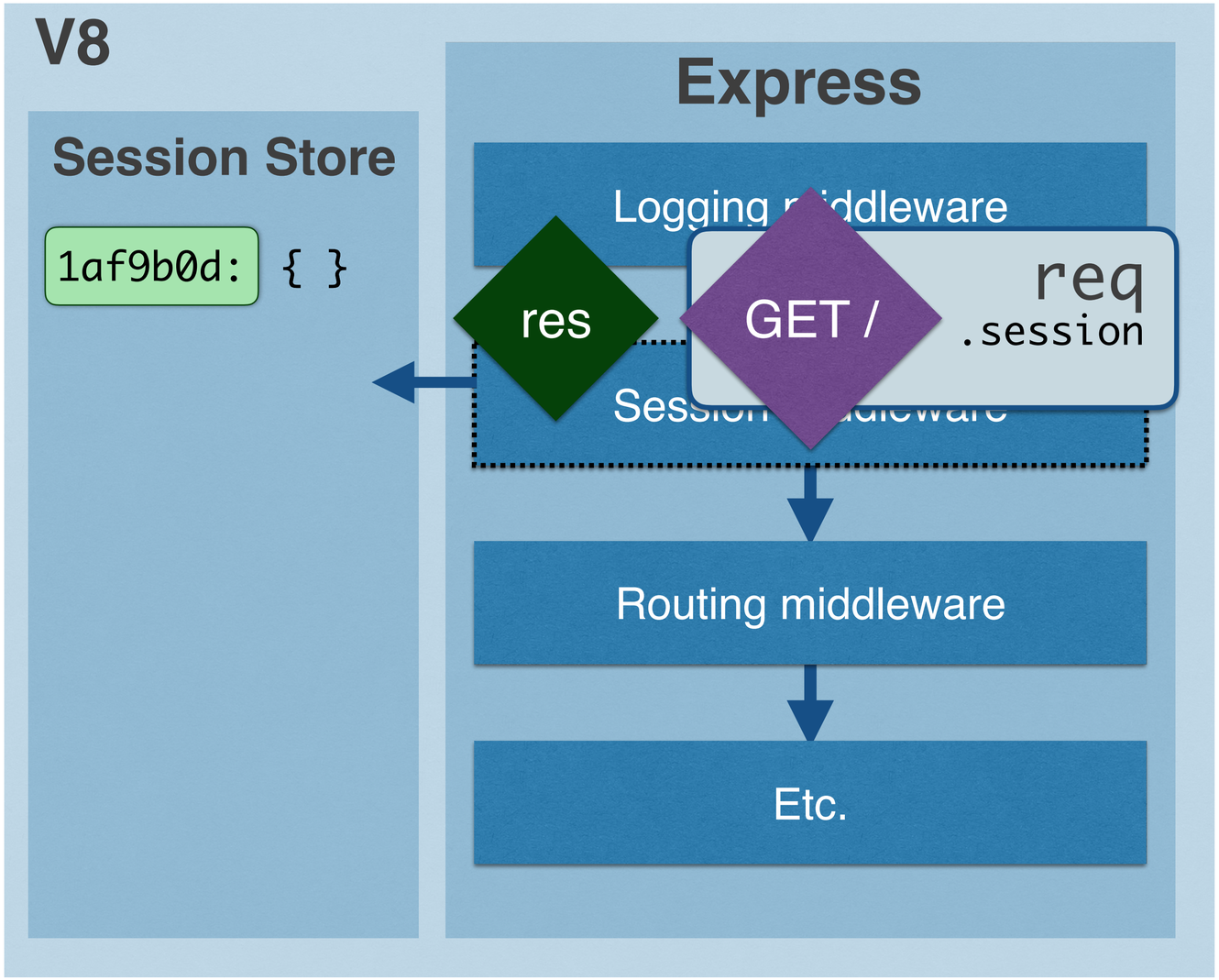
(body)

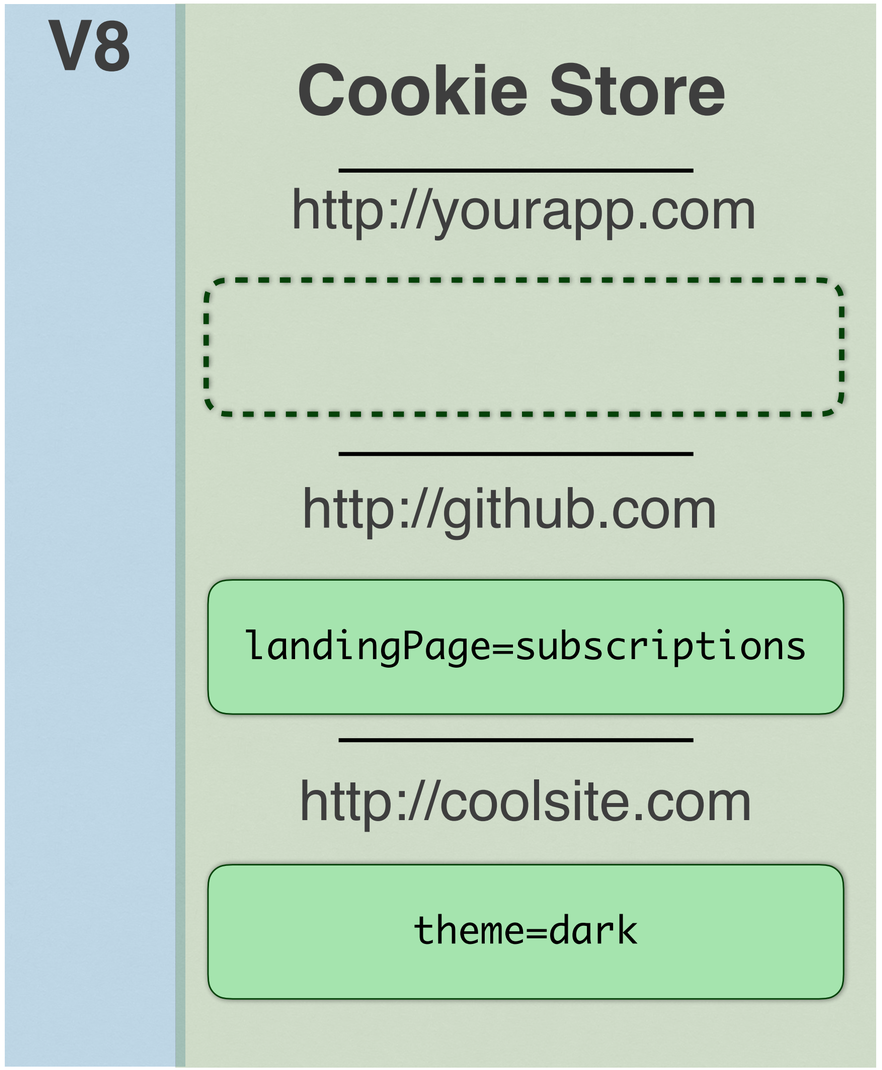
still no cookie info…
session middleware:
"let's make a session!"

Server (Backend)

Internet (HTTP)

Client (Browser)





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
```

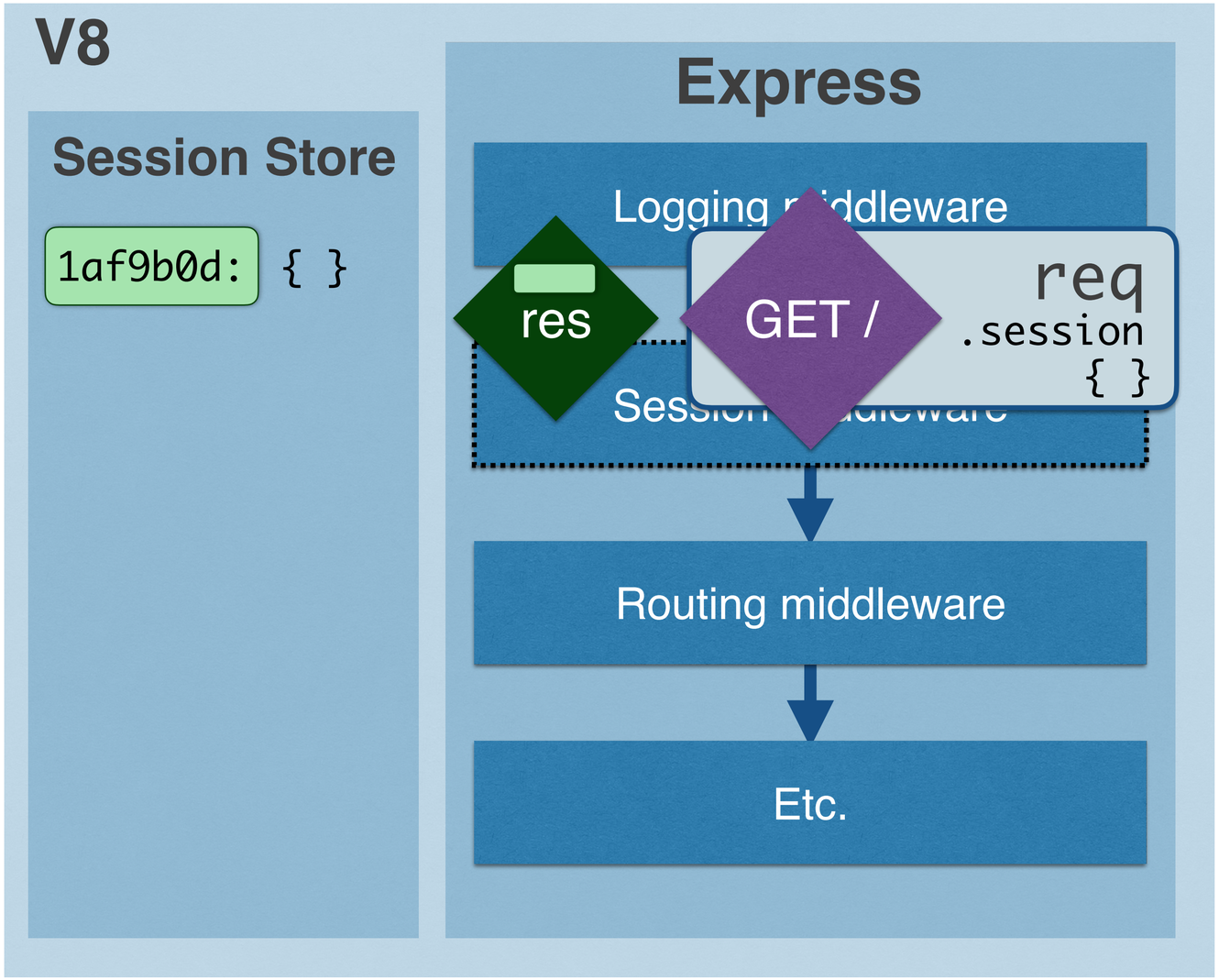
(body, after routing is done)

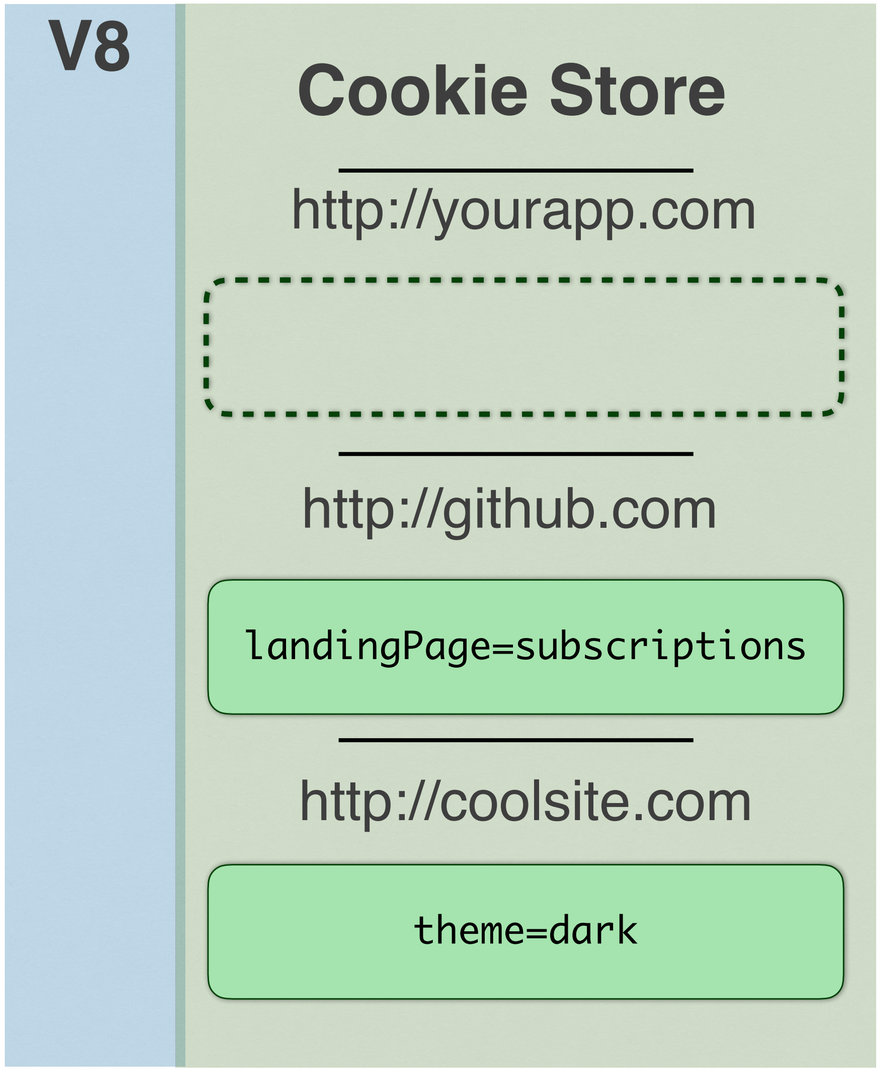
```
<!DOCTYPE html>
<html>
  <head>
    <title>Your Sweet App</title>
    <script src="/js/main.js"></script>
  </head> …etc.
```

Server (Backend)

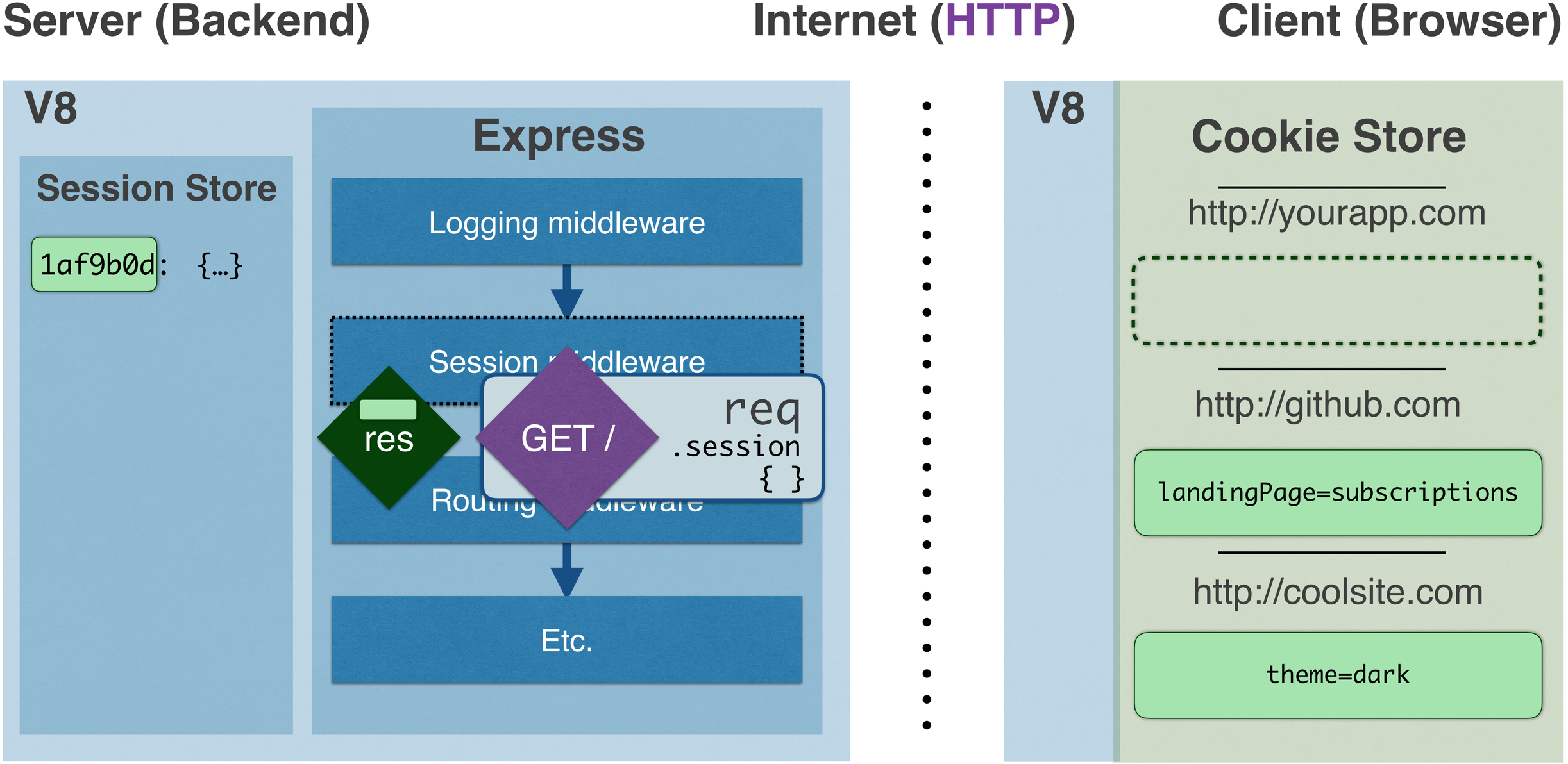
Internet (HTTP)

Client (Browser)





http://yourapp.com


Server (Backend)
Internet (HTTP)
Client (Browser)
V8
Session Store
1af9b0d: {…}
Express
Logging middleware
Session middleware
res
GET /
req
.session
{ }
Routing middleware
Etc.
http://yourapp.com
V8
Cookie Store
http://yourapp.com
http://github.com
landingPage=subscriptions
http://coolsite.com
theme=dark

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
```

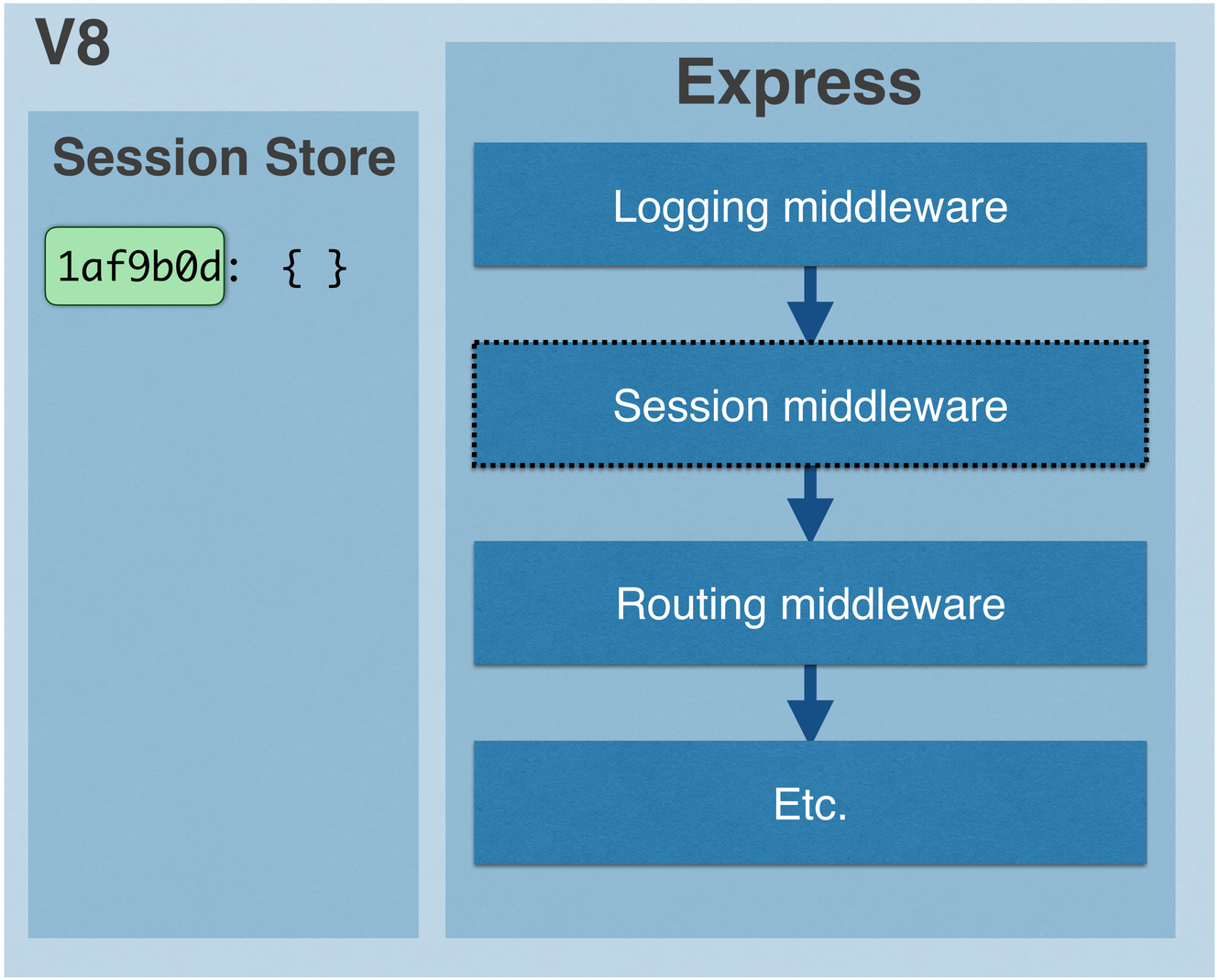
(body, after routing is done)

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

Server (Backend)

Internet (HTTP)

Client (Browser)

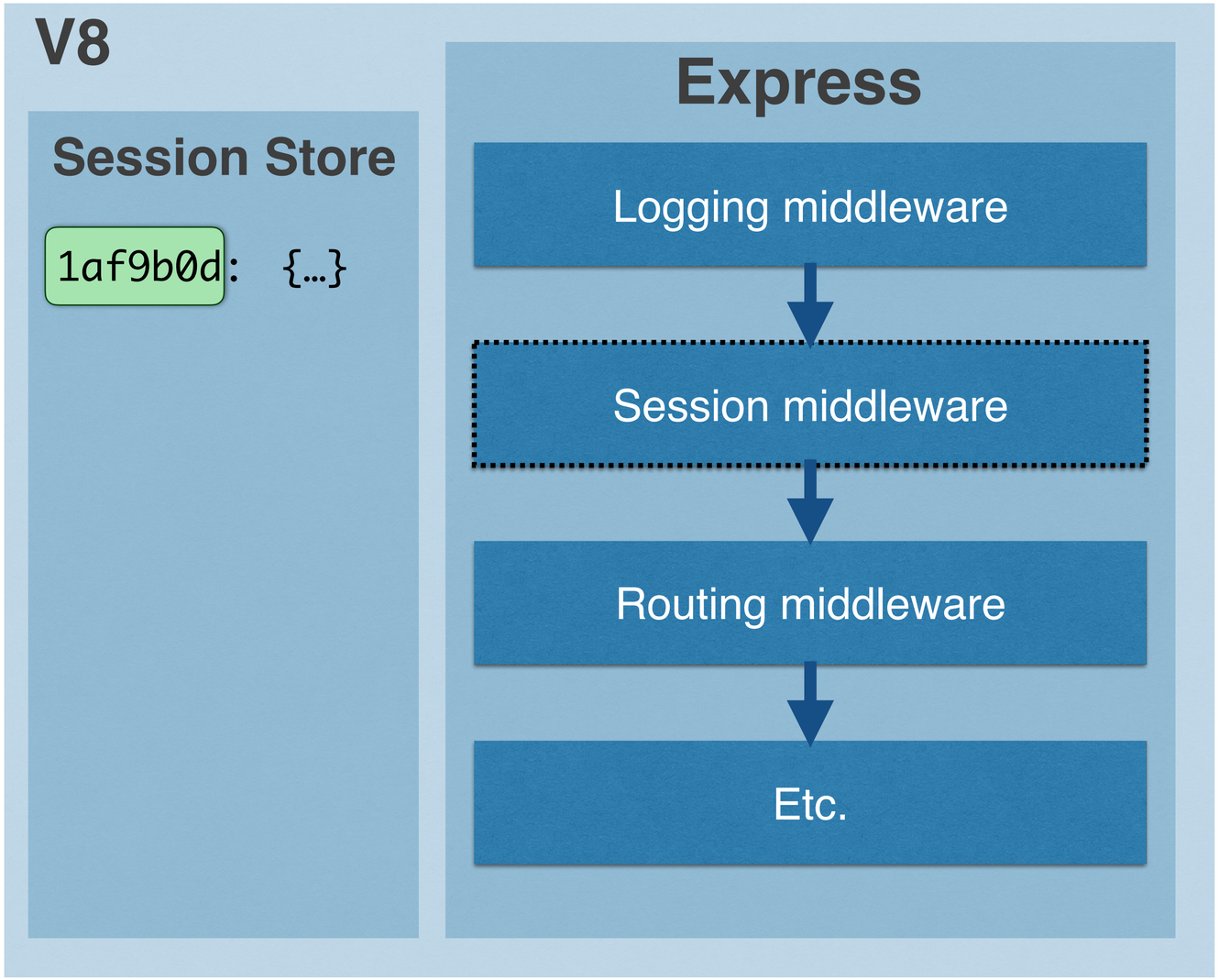


http://yourapp.com

Server (Backend)

Internet (HTTP)

Client (Browser)



http://yourapp.com

HTTP REQUEST

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

(headers)

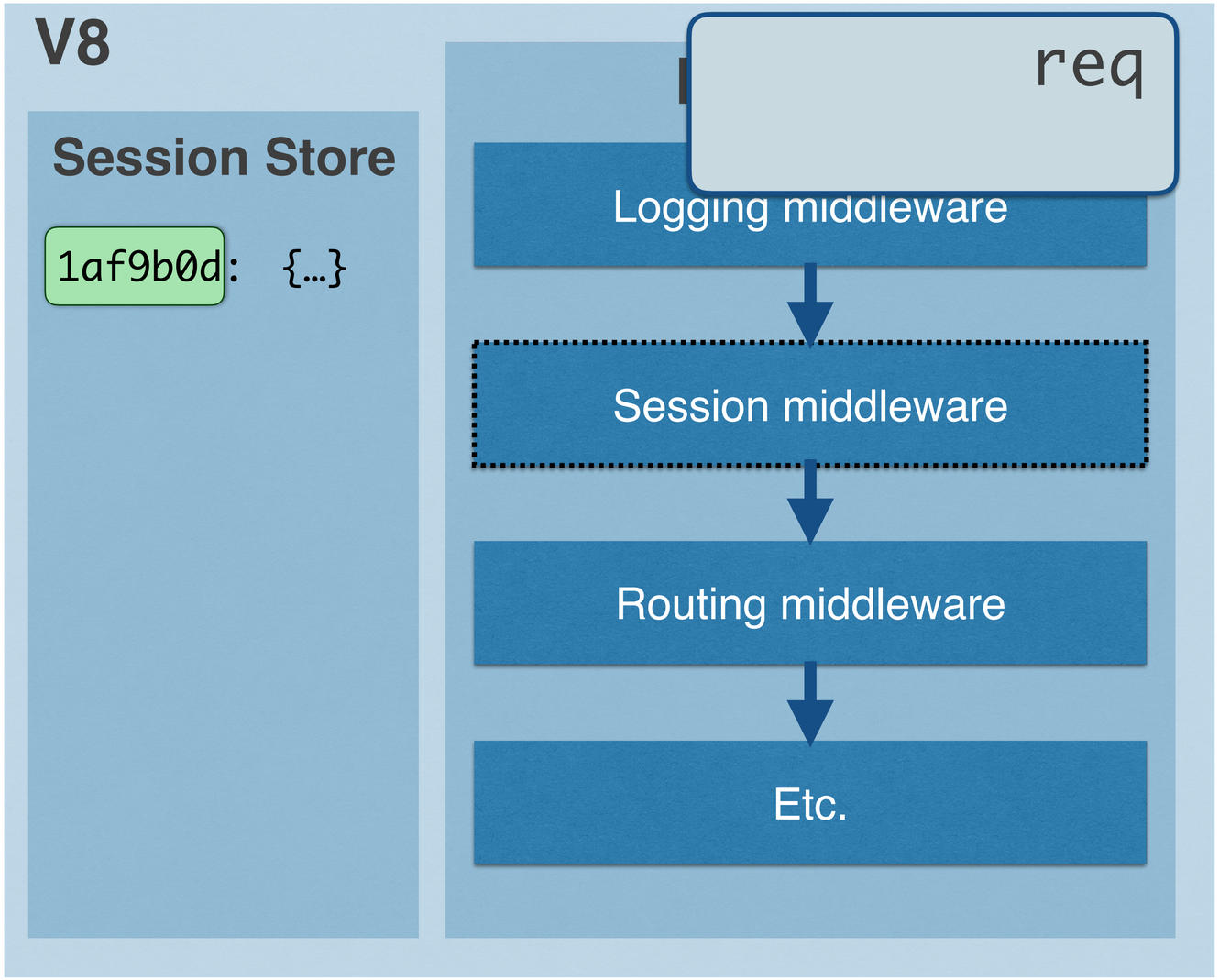
(body)

…attached cookie!

Server (Backend)

Internet (HTTP)

Client (Browser)



http://yourapp.com

HTTP REQUEST

```
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!

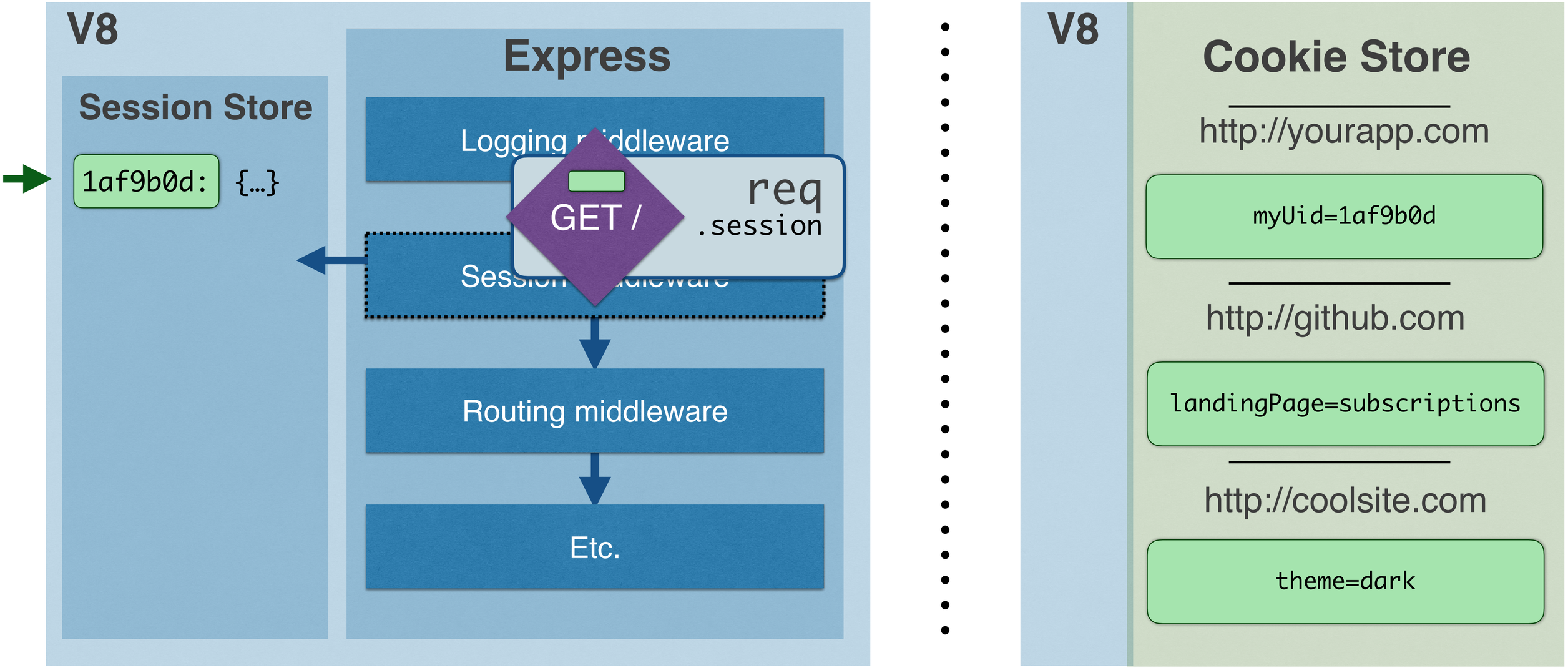
(headers)

(body)

Server (Backend)

Internet (HTTP)

Client (Browser)

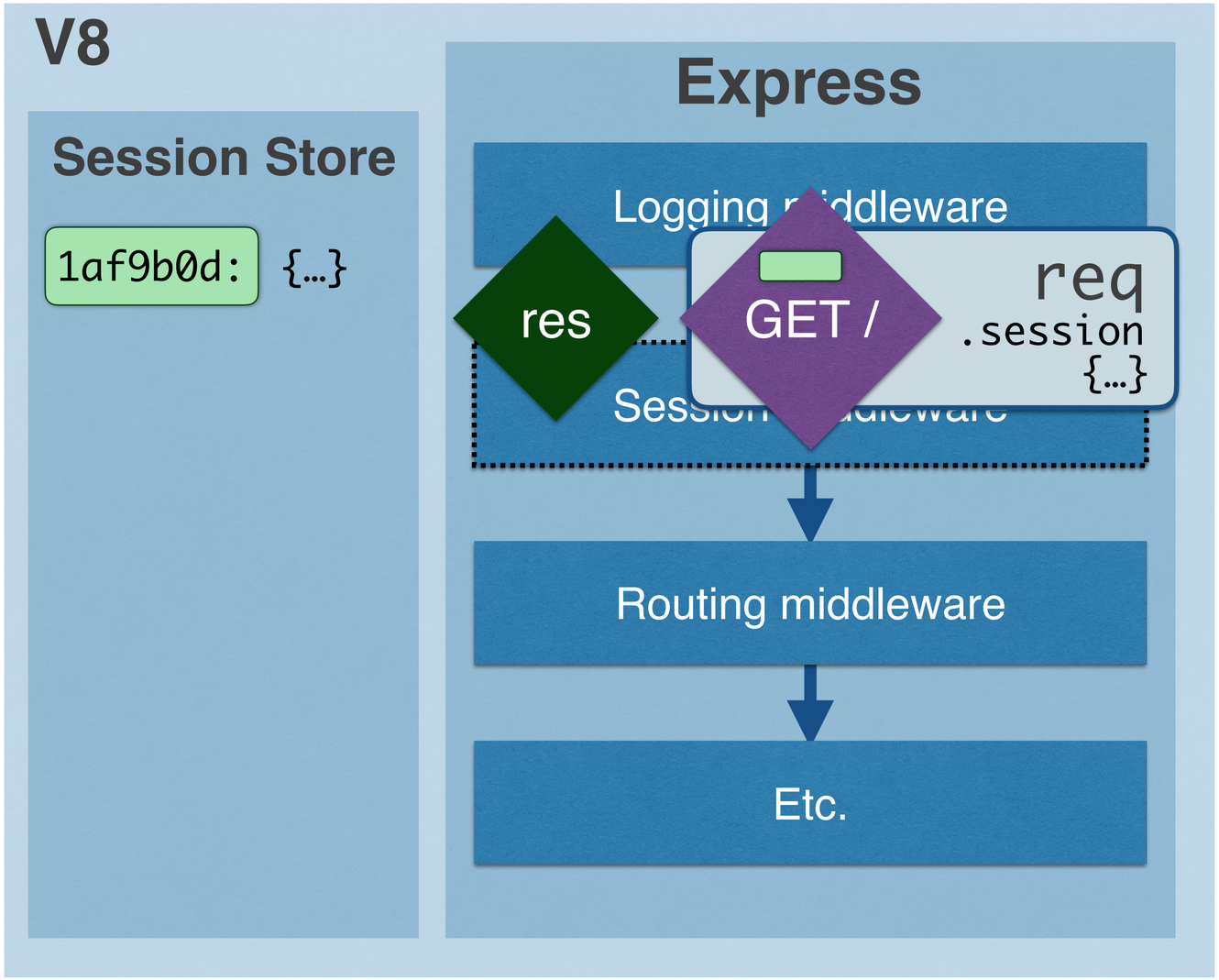


http://yourapp.com

Server (Backend)

Internet (HTTP)

Client (Browser)



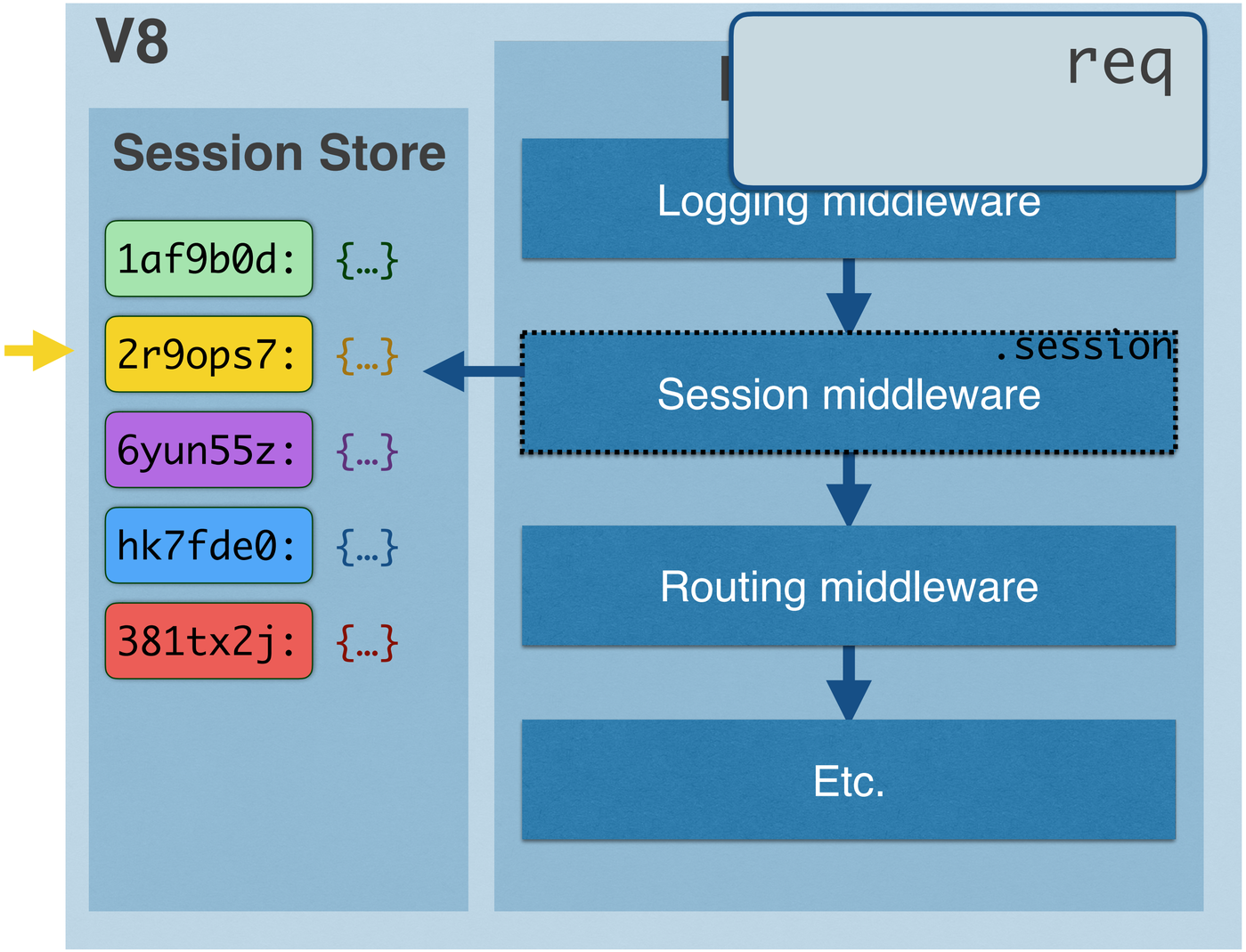
http://yourapp.com

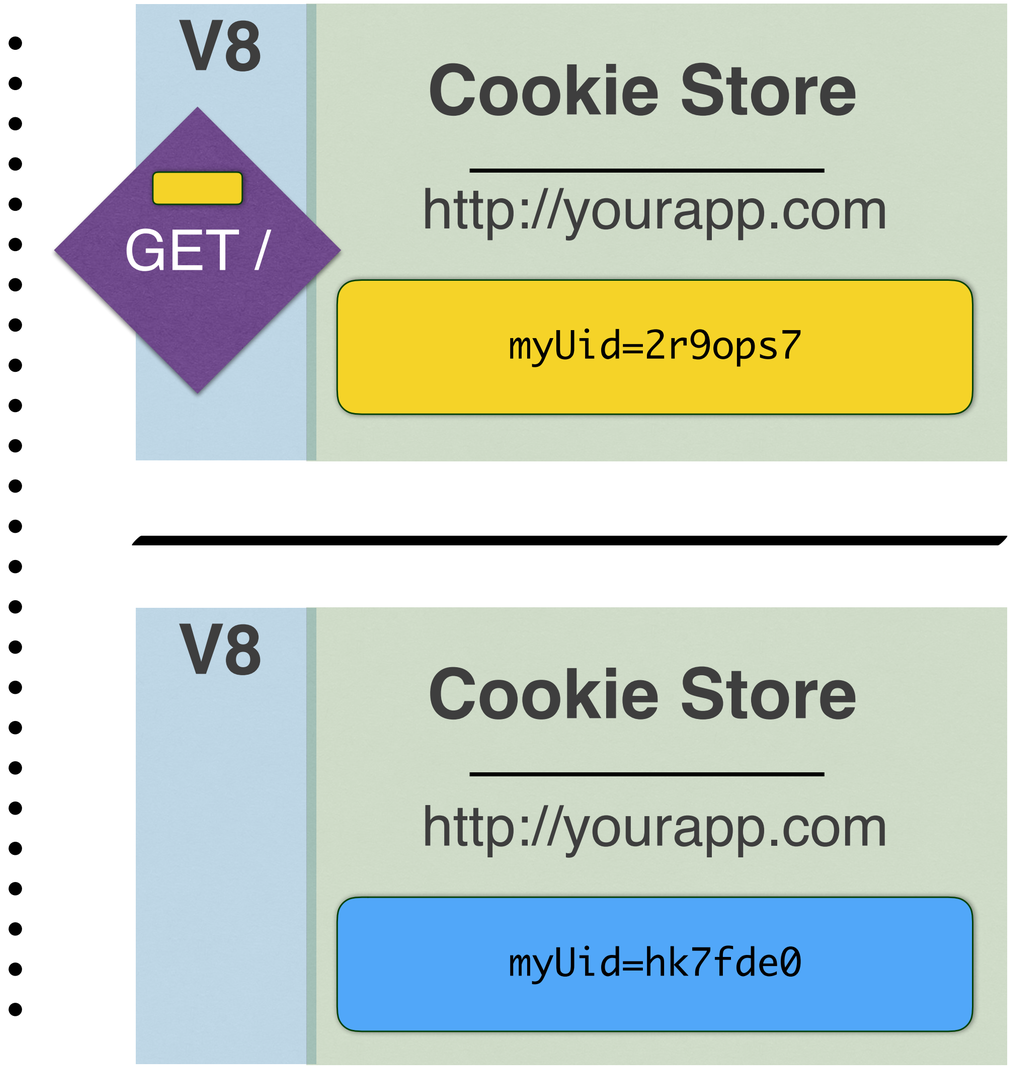
Multiple Sessions

Server (Backend)

Internet (HTTP)

Client 1 (Browser)





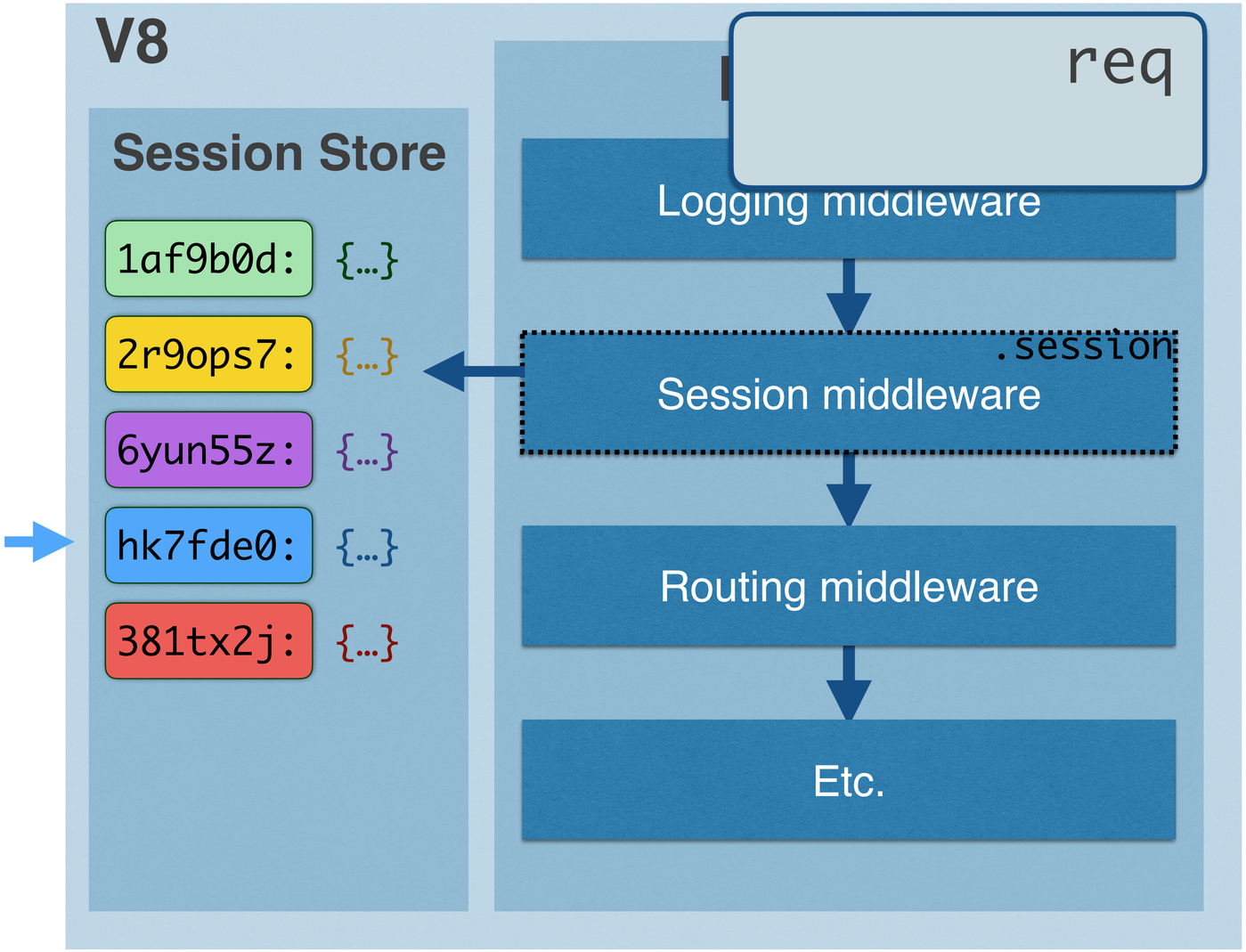
http://yourapp.com

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