Security Issues in Web Programming (Part 4)

Robert M. Dondero, Ph.D.
Princeton University

Objectives

- We will cover:
  - Data comm attacks
  - Third-party authentication (briefly):
    - CAS
    - Google authentication

Agenda

- **Data comm attacks**
- Third-party authentication (briefly)
  - CAS
  - Google authentication

Data Comm Attacks

- **Problem:**
  - Attacker may access data during comm between PennyAdmin app and browser
- **Solution:**
  - ***Hypertext Transfer Protocol Secure (HTTPS)***

Data Comm Attacks

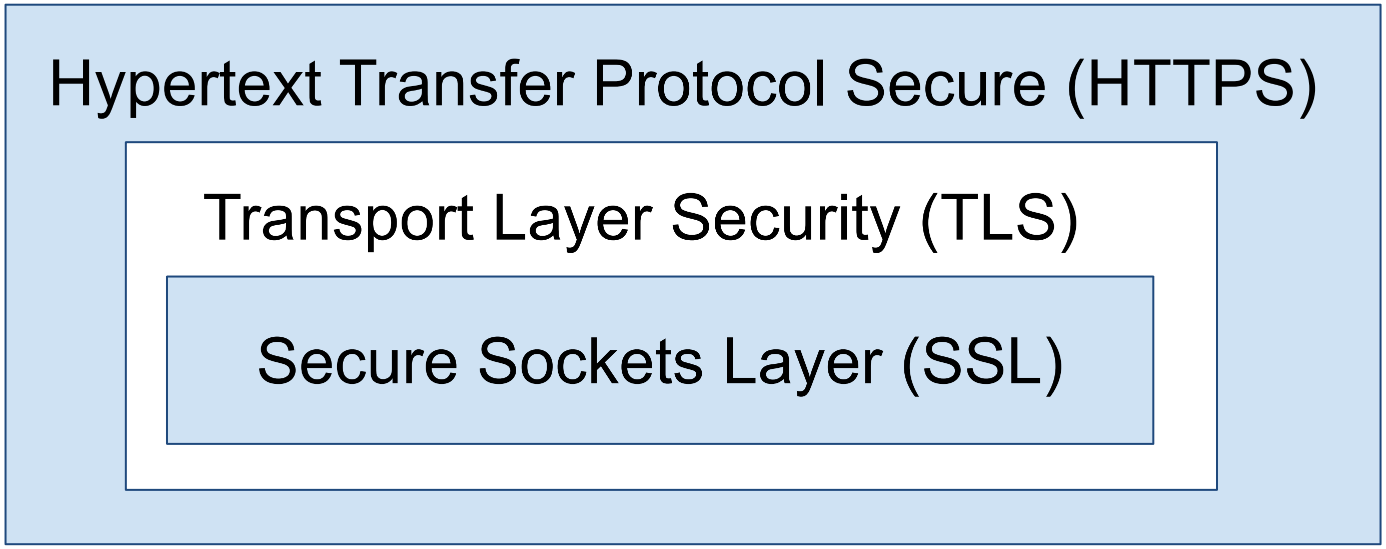
- **Technical** advantages of using HTTPS
  - Confidentiality
    - Prohibits ***message eavesdropping attacks***
  - Integrity
    - Prohibits ***message tampering attacks***
  - Authentication
    - Prohibits ***message forgery attacks***

Data Comm Attacks

- **Business** advantages of using HTTPS
  - Increases user confidence/trust in website
  - Increases Google search rank of website

Data Comm Attacks

- How HTTPS works:


Hypertext Transfer Protocol Secure (HTTPS)
Transport Layer Security (TLS)
Secure Sockets Layer (SSL)

Data Comm Attacks

- How to use HTTPS:
  - Configure server & app to use (& require use of) HTTPS
  - Command browser to send request specifying HTTPS as protocol
    - `https://…`

Data Comm Attacks

- How to configure server & app to use (& require use of) HTTPS:
  - Depends upon server…

Data Comm Attacks

- **Render server**
  - Already configured to use (& require use of) HTTPS
    - When server receives **`http:`**`//`*`something`* request, it sends redirect for **`https:`**`//`*`something`* request
  - So:
    - **Server**: Do nothing!
    - **App**: Do nothing!

Data Comm Attacks

- **Heroku server**
  - Already configured to use (but not require use of) HTTPS
    - When server receives **`https:`**`//`*`something`* request, it uses HTTPS
    - When server receives **`http:`**`//`*`something`* request, it uses HTTP
  - So
    - **Server**: (Regrettably) Do nothing!
    - **App**: Small change…

Data Comm Attacks

- **Solution 1:**
  - App explicitly performs redirects

Data Comm Attacks

- See **PennyAdmin13Https** app
  - runserver.py
  - penny.sql, penny.sqlite
  - database.py
  - header.html, footer.html
  - index.html, show.html,
  - add.html, delete.html, reportresults.html
  - login.html, signup.html, loggedout.html
  - top.py, **penny.py**, auth.py

Data Comm Attacks

- **Solution 2:**
  - `flask_talisman` module

Data Comm Attacks

- See **PennyAdmin14Https** app
  - runserver.py
  - penny.sql, penny.sqlite
  - database.py
  - header.html, footer.html
  - index.html, show.html,
  - add.html, delete.html, reportresults.html
  - login.html, signup.html, loggedout.html
  - **top.py**, **penny.py**, auth.py

Data Comm Attacks

- Notes:
  - Good to design your app to require use of HTTPS even when the app server already forces use of HTTPS
  - flask_talisman implements some additional security measures
  - Need not configure Flask test server to use (or require use of) HTTPS
    - But if you want to…
    - Or if you're using Google authentication…

Data Comm Attacks

- How to configure Flask test server & app to use (& require use of) HTTPS:

Data Comm Attacks

- **Preliminary step**: Get a ***certificate*** for your app

- **Option 1**: Get a certificate that is signed by a ***certificate authority***

Data Comm Attacks

Certificate authorities:

Rank	Authority	Market Share
1	IdenTrust	49%
2	DigiCert	19%
3	Sectigo	16%
4	Let’s Encrypt	8%
5	GoDaddy	6%
6	GlobalSign	3%

https://en.wikipedia.org/wiki/Certificate_authority#Providers
(as of Aug 2022)

Data Comm Attacks

- **Preliminary step**: Get a certificate for your app
- **Option 1**: Buy a certificate that is signed by a certificate authority
- **Option 2**: Create a ***self-signed certificate***

Data Comm Attacks

Linux, Mac, MS Windows Git Bash:

```
$ openssl req -x509 -newkey rsa:4096 -nodes -out cert.pem -keyout key.pem -days 365
Generating a RSA private key
...........................................................++++
.......++++
writing new private key to 'key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: US
State or Province Name (full name) [Some-State]: NJ
Locality Name (eg, city) []: Princeton
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Princeton University
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []: localhost
Email Address []:
$
```

Output: cert.pem, key.pem

Data Comm Attacks

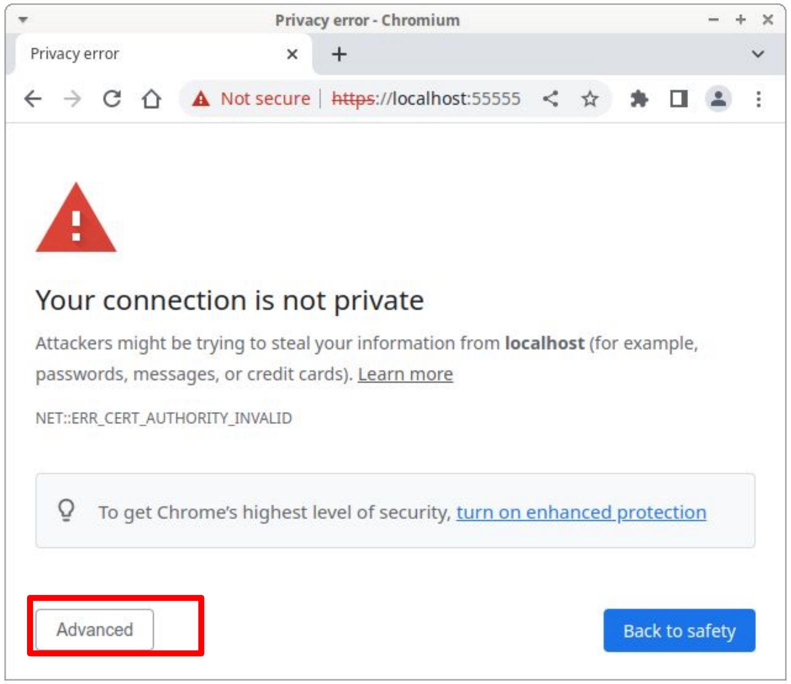
- Self-signed certificate
  - Confidentiality: yes
  - Integrity: yes
  - Authentication: no

Data Comm Attacks

- See **<u>PennyAdmin15HttpsLocal</u>** app
  - **runserver.py**
  - penny.sql, penny.sqlite
  - database.py
  - header.html, footer.html
  - index.html, show.html,
  - add.html, delete.html, reportresults.html
  - login.html, signup.html, loggedout.html
  - top.py, penny.py, auth.py

Data Comm Attacks

- See **<u>PennyAdmin15HttpsLocal</u>** app
  - On local computer with Flask test server (using self-signed certif)



Privacy error - Chromium

Privacy error

Not secure | ~~https~~://localhost:55555

Your connection is not private

Attackers might be trying to steal your information from **localhost** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

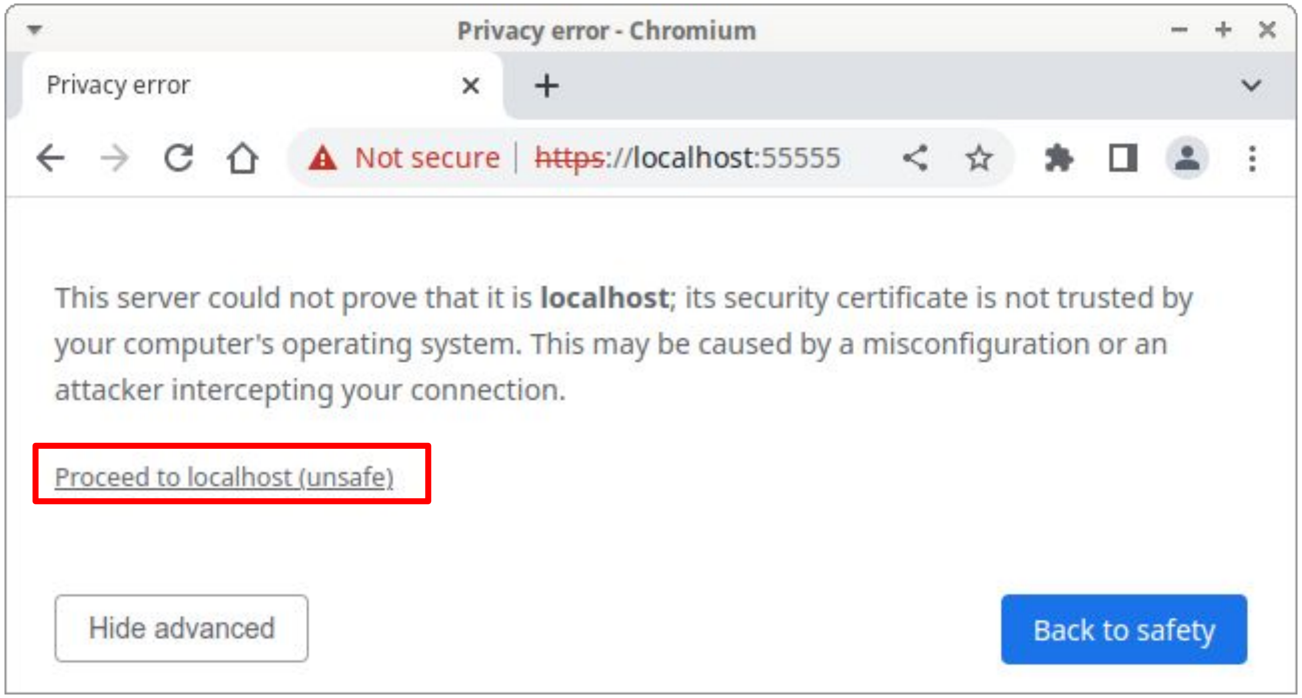
To get Chrome's highest level of security, turn on enhanced protection

Advanced

Back to safety

Data Comm Attacks

- See **<u>PennyAdmin15HttpsLocal</u>** app
  - On local computer with Flask test server (using self-signed certif)



Privacy error - Chromium

Privacy error

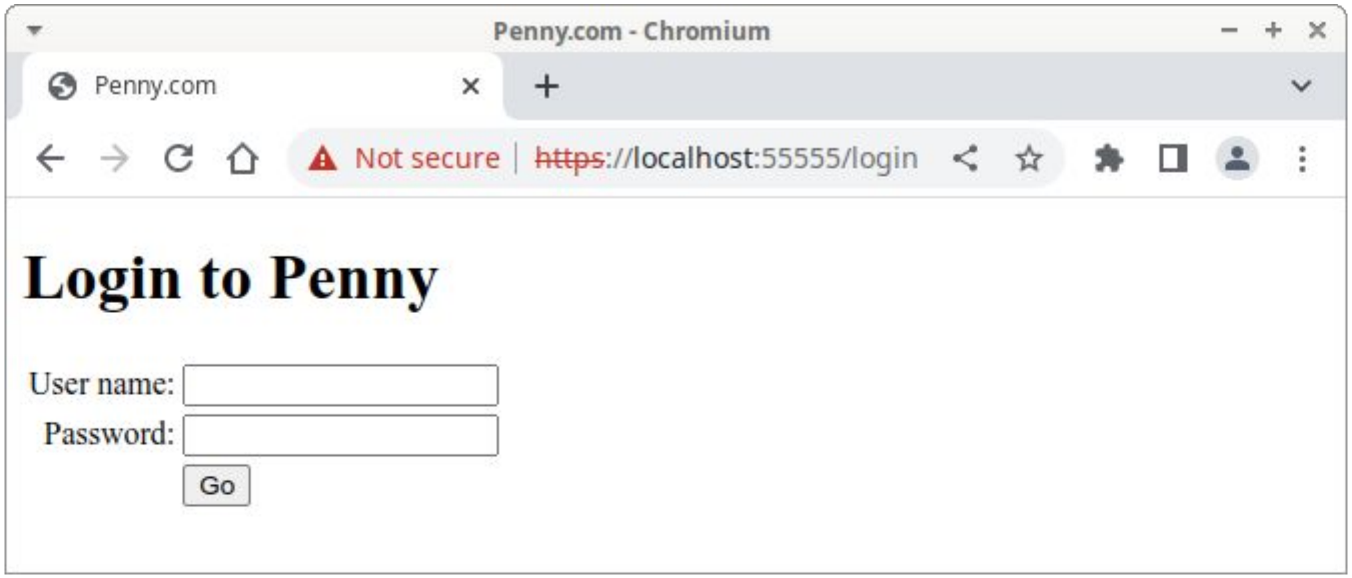
Not secure | ~~https~~://localhost:55555

This server could not prove that it is **localhost**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to localhost (unsafe)

Data Comm Attacks

- See **PennyAdmin15HttpsLocal** app
  - On local computer with Flask test server (using self-signed certif)



Penny.com - Chromium

Penny.com

Not secure | ~~https~~://localhost:55555/login

Login to Penny

User name:

Password:

Go

Data Comm Attacks

- Q: Project concern?
- A: **Yes**

Agenda

- Data comm attacks
- **Third-party authentication (briefly)**
  - CAS
  - Google authentication

Agenda

- Data comm attacks
- Third-party authentication (briefly)
  - **CAS**
  - Google authentication

CAS

- *Central Authentication Service (CAS)*

“The **Central Authentication Service (CAS)** is a single sign-on protocol for the web. **Its purpose is to permit a user to access multiple applications while providing their credentials (such as userid and password) only once. It also allows web applications to authenticate users without gaining access to a user’s security credentials, such as a password.**”

– https://en.wikipedia.org/wiki/Central_Authentication_Service

CAS

- See **PennyAdmin16Cas** app (cont.)
  - **Part 1**: User logs into CAS server
    - Unnecessary if user is already logged into CAS server
    - User must provide credentials
  - **Part 2**: User logs into PennyAdmin
    - User need not provide credentials

CAS

- See **PennyAdmin16Cas** app (cont.)
  - How to run it on your local computer…

CAS

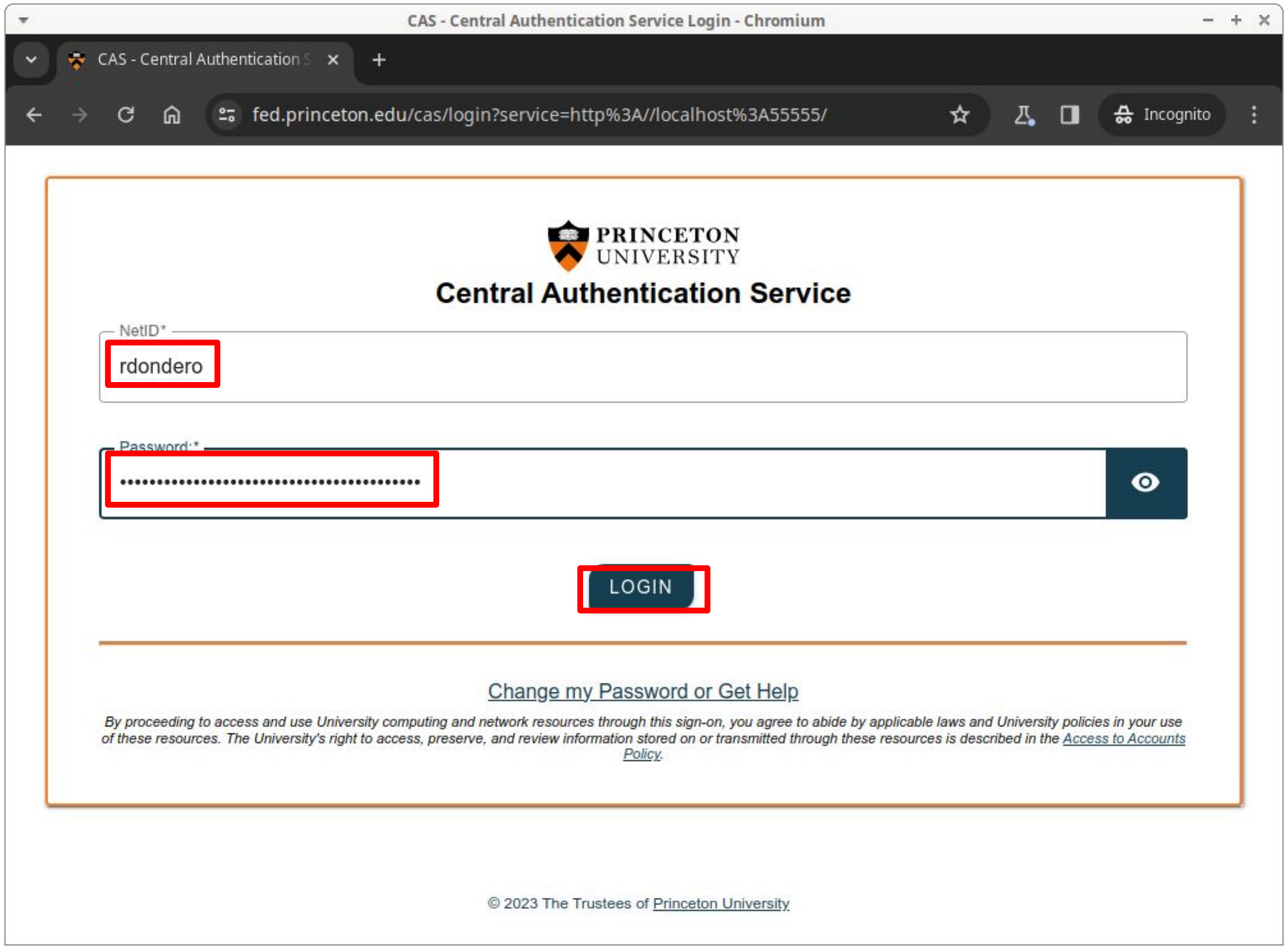
- See **PennyAdmin16Cas** app (cont.)
  - In terminal, enter this command:

```
$ python runserver.py 55555
```

  - In browser, enter URL:
    - http://localhost:55555
      - Must use `localhost` (and not `127.0.0.1`, and not the real IP address of your computer)

CAS

- See **PennyAdmin16Cas** app (cont.)


CAS - Central Authentication Service Login - Chromium

fed.princeton.edu/cas/login?service=http%3A//localhost%3A55555/

PRINCETON UNIVERSITY

Central Authentication Service

NetID*: rdondero

Password:*: ••

LOGIN

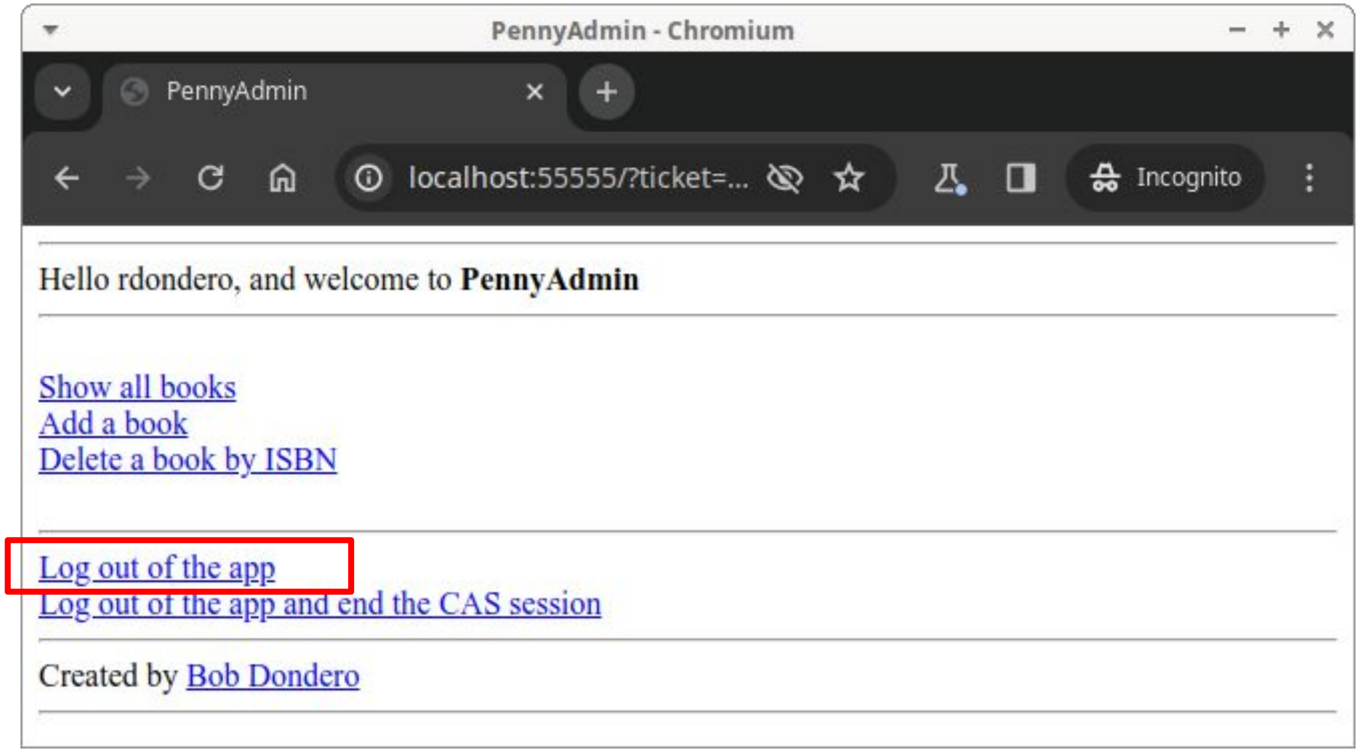
Change my Password or Get Help

By proceeding to access and use University computing and network resources through this sign-on, you agree to abide by applicable laws and University policies in your use of these resources. The University's right to access, preserve, and review information stored on or transmitted through these resources is described in the Access to Accounts Policy.

© 2023 The Trustees of Princeton University

CAS

- See **PennyAdmin16Cas** app (cont.)



Hello rdondero, and welcome to **PennyAdmin**

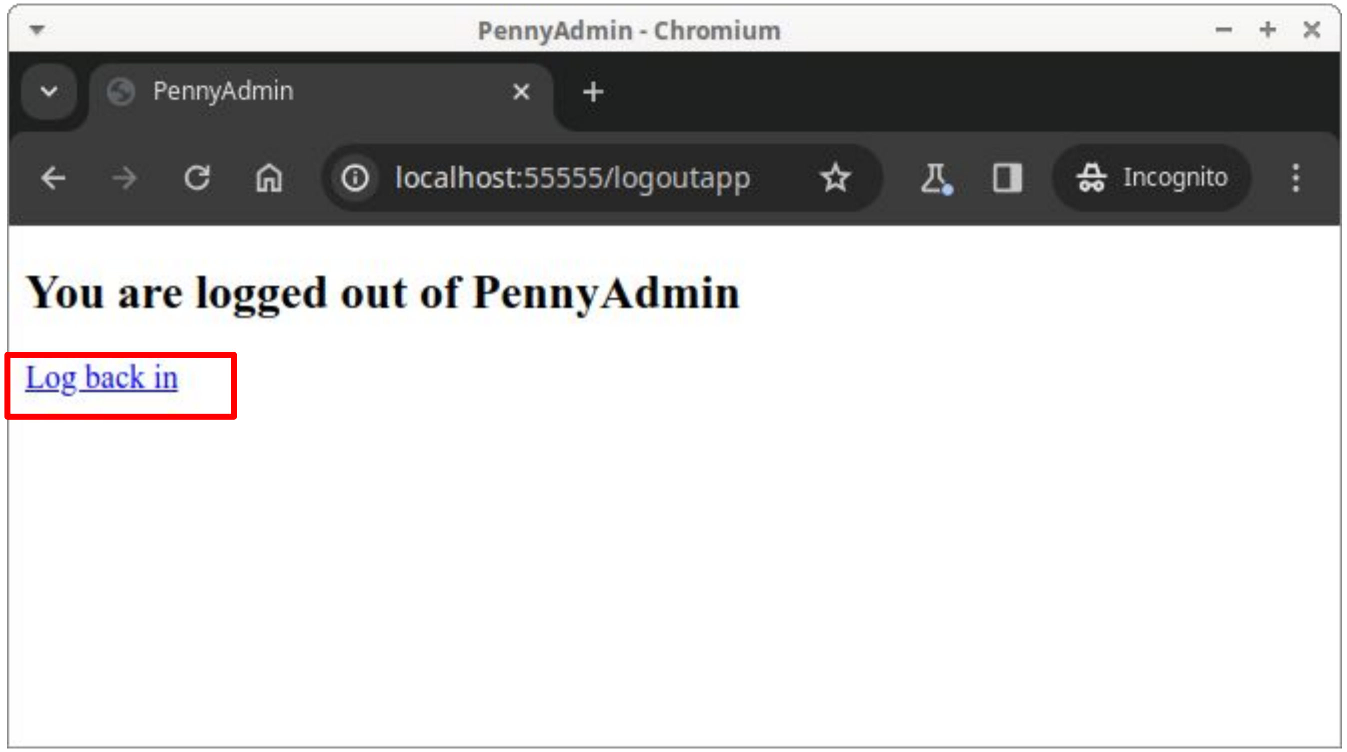
Show all books
Add a book
Delete a book by ISBN

Log out of the app
Log out of the app and end the CAS session

Created by Bob Dondero

CAS

- See **PennyAdmin16Cas** app (cont.)

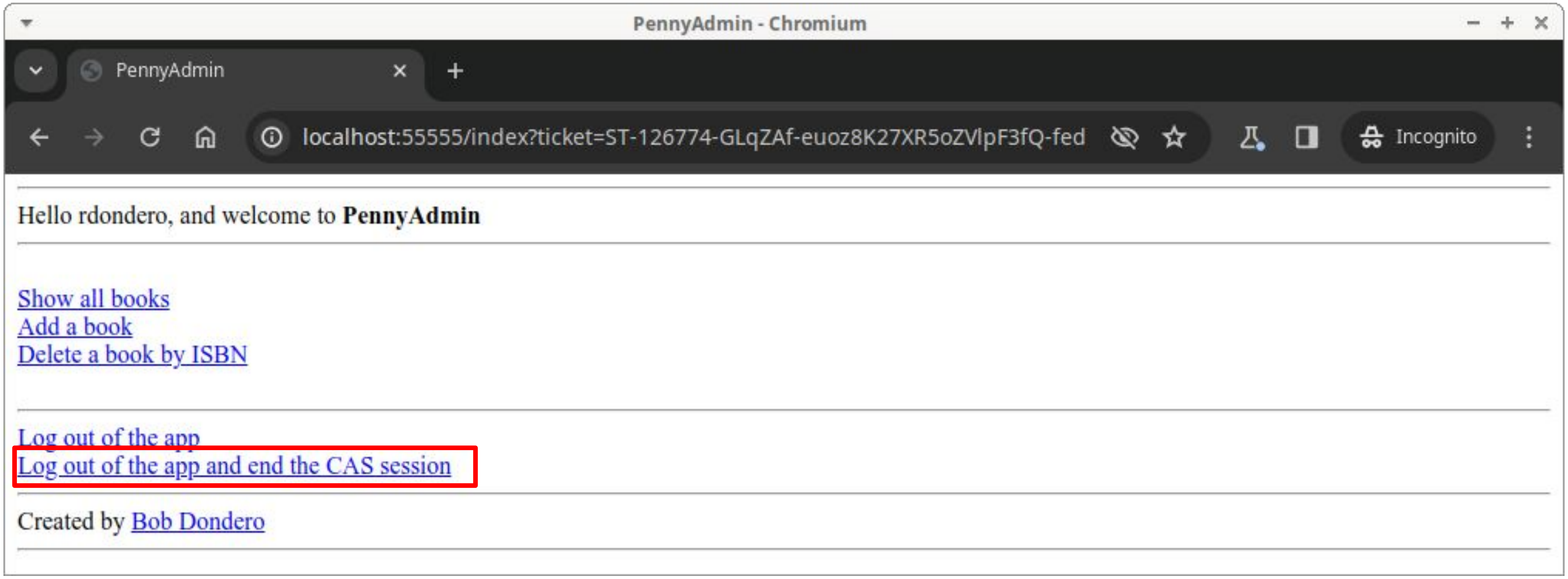


You are logged out of PennyAdmin

Log back in

CAS

- See **PennyAdmin16Cas** app (cont.)


PennyAdmin - Chromium

localhost:55555/index?ticket=ST-126774-GLqZAf-euoz8K27XR5oZVlpF3fQ-fed

Hello rdondero, and welcome to **PennyAdmin**

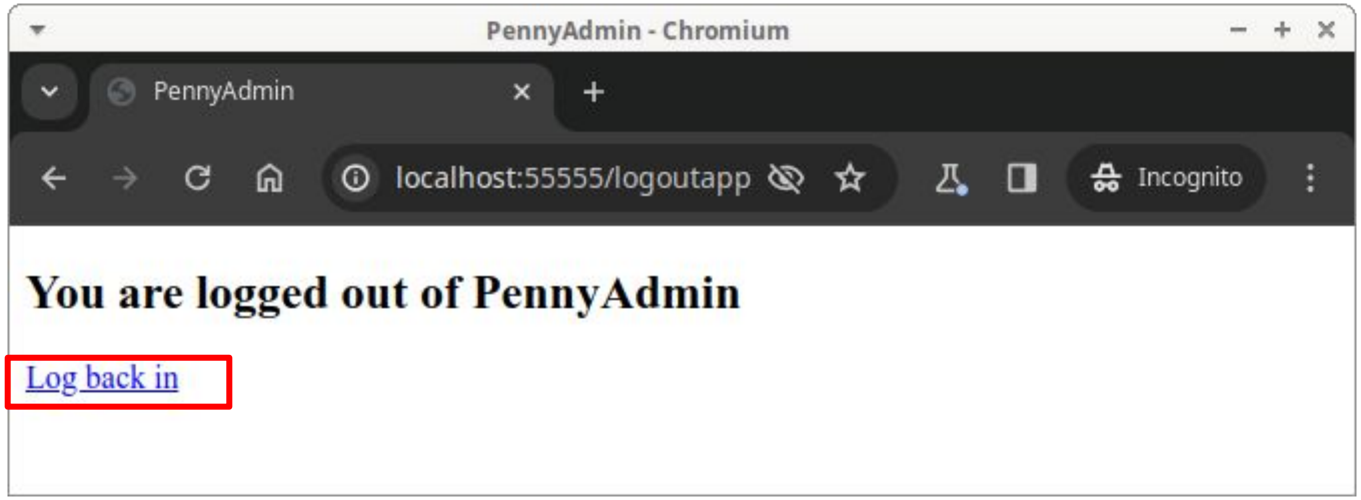
Show all books
Add a book
Delete a book by ISBN

Log out of the app
Log out of the app and end the CAS session

Created by Bob Dondero

CAS

- See **PennyAdmin16Cas** app (cont.)

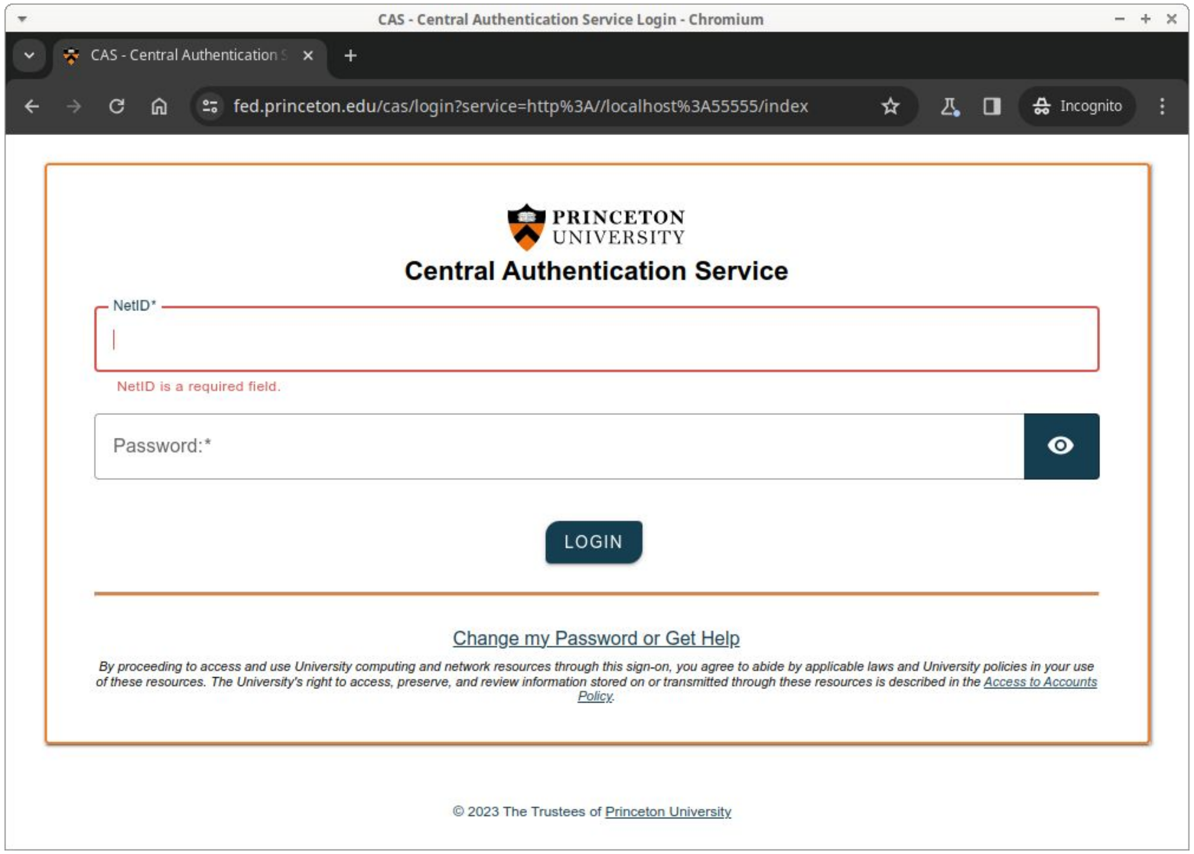


You are logged out of PennyAdmin

Log back in

CAS

- See **PennyAdmin16Cas** app (cont.)



CAS - Central Authentication Service Login - Chromium

CAS - Central Authentication S

fed.princeton.edu/cas/login?service=http%3A//localhost%3A55555/index

PRINCETON UNIVERSITY

Central Authentication Service

NetID*

NetID is a required field.

Password:*

LOGIN

Change my Password or Get Help

By proceeding to access and use University computing and network resources through this sign-on, you agree to abide by applicable laws and University policies in your use of these resources. The University's right to access, preserve, and review information stored on or transmitted through these resources is described in the Access to Accounts Policy.

© 2023 The Trustees of Princeton University

CAS

- See **PennyAdmin16Cas** app (cont.)
  - How to run it on Render (or Heroku, or any cloud service) …

CAS

- See **<u>PennyAdmin16Cas</u>** app (cont.)
  - Ask OIT to place the URL of the app on the ***Princeton CAS white list***
    - Instructions are provided in the COS 333 *Princeton Data Sources* web page
  - In browser, enter URL:
    - https://*ipaddress*

CAS

- See **PennyAdmin16Cas** app (cont.)
  - runserver.py
  - **penny.sql**, penny.sqlite
  - **database.py**
  - header.html, **footer.html**
  - index.html, show.html,
  - add.html, delete.html, reportresults.html
  - loggedout.html
  - top.py, **penny.py**, **auth.py**

CAS

- See **PennyAdmin16Cas** app (cont.)

  - How it works…
  - See **Appendix 1**

CAS

- **Pros**
  - Application need not manage usernames or passwords
  - Application ***cannot*** access passwords!
  - Application is constrained to one user community

CAS

- **Cons**
  - Complex
  - Adds overhead, but only during user’s first visit to the app per browser session
  - Application is constrained to one user community!

Agenda

- Data comm attacks
- Third-party authentication (briefly)
  - CAS
  - **Google authentication**

Google Authentication

- See **PennyAdmin17Google** app
  - **Part 1**: User logs into Google server
    - Unnecessary if user is already logged into Google server
    - User must provide credentials
  - **Part 2**: User logs into PennyAdmin
    - User need not provide credentials

Google Authentication

- See **PennyAdmin17Google** app (cont.)
  - How to run it on your local computer…

Google Authentication

- **Preliminary**
  - Make sure these packages are installed (via `pip`) in your Python virtual environment

```
Flask
python-dotenv
oauthlib
requests
```

Google Authentication

- **Preliminary**
  - Create a self-signed certificate (as described previously in this lecture)

```
$ openssl req -x509 -newkey rsa:4096 -nodes -out cert.pem -keyout key.pem -days 365
…
Country Name (2 letter code) [AU]: US
State or Province Name (full name) [Some-State]: NJ
Locality Name (eg, city) []: Princeton
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Princeton University
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []: localhost
Email Address []:
$
```

Google Authentication

- **Preliminary**
  - Strongly suggested…
  - Create a ***project Google account*** (i.e., a gmail address) for your project team
    - Use your project Google account exclusively for Google authentication setup and subsequent app testing

Google Authentication

- **Preliminary**
  - Register app (https://localhost:5000) as a client of Google
    - Log into Google using your project Google account
    - Browse to https://console.developers.google.com/apis/credentials
    - Click *CREATE PROJECT*
    - For *Project name* enter `Penny`
    - Click *CREATE*

Google Authentication

- **Preliminary**
  - Register app (https://localhost:5000) as a client of Google (cont.)
    - Click CONFIGURE CONSENT SCREEN
    - For User Type choose *External*
    - Click *CREATE*
    - For *App name* enter `Penny`
    - For *User support email* enter your your project gmail address
    - For *Developer contact information* enter your project gmail address
    - Click *SAVE AND CONTINUE* a few times to finish the consent

Google Authentication

- **Preliminary**
  - Register app (https://localhost:5000) as a client of Google (cont.)
    - Click Credentials
    - Click *Create Credentials*, *OAuth client ID*, *Web Application*
    - In Authorized JavaScript origins:
      - Click ADD URI
      - Enter https://localhost:5000
    - In Authorized redirect URIs:
      - Click ADD URI
      - Add Authorized Redirect URI: https://localhost:5000/login/callback

Google Authentication

- **Preliminary**
  - Register app (https://localhost:5000) as a client of Google (cont.)
    - Google provides **`GOOGLE_CLIENT_ID`** and **`GOOGLE_CLIENT_SECRET`**
      - Take note of them!

Google Authentication

Create environment variables:

```
APP_SECRET_KEY=yourappsecretkey
GOOGLE_CLIENT_ID=yourgoogleclientid
GOOGLE_CLIENT_SECRET=yourgoogleclientsecret
```

Google Authentication

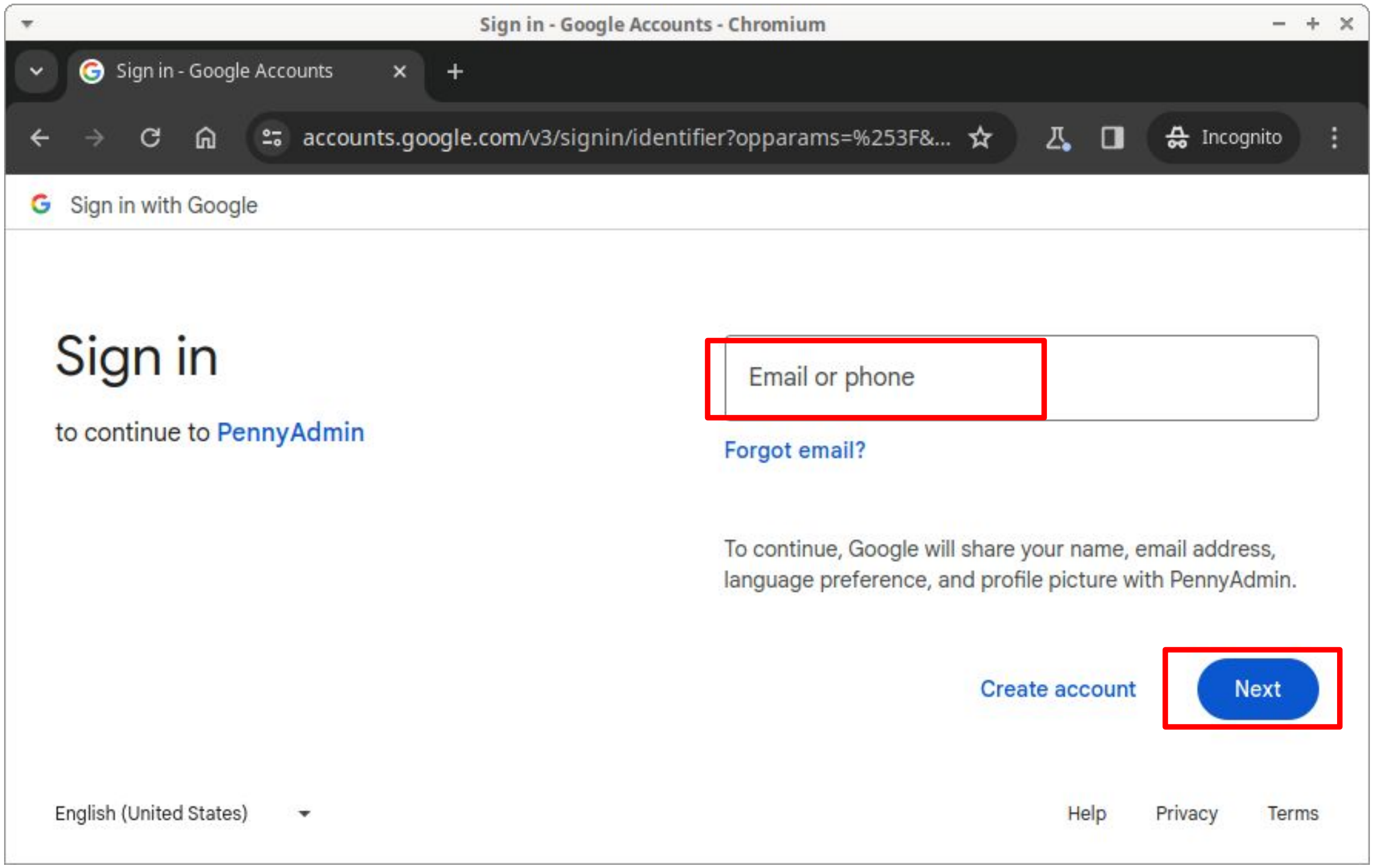
- See **PennyAdmin17Google** app (cont.)
  - In terminal, enter this command:

```
$ python runserver.py
```

    - Runs Flask test server on port 5000
    - Runs Flask test server using HTTPS
  - In browser, enter URL:
    - https://localhost:5000

Google Authentication

- See **<u>PennyAdmin17Google</u>** app (cont.)


Sign in - Google Accounts - Chromium

Sign in - Google Accounts

accounts.google.com/v3/signin/identifier?opparams=%253F&...

Incognito

Sign in with Google

Sign in

to continue to PennyAdmin

Email or phone

Forgot email?

To continue, Google will share your name, email address, language preference, and profile picture with PennyAdmin.

Create account

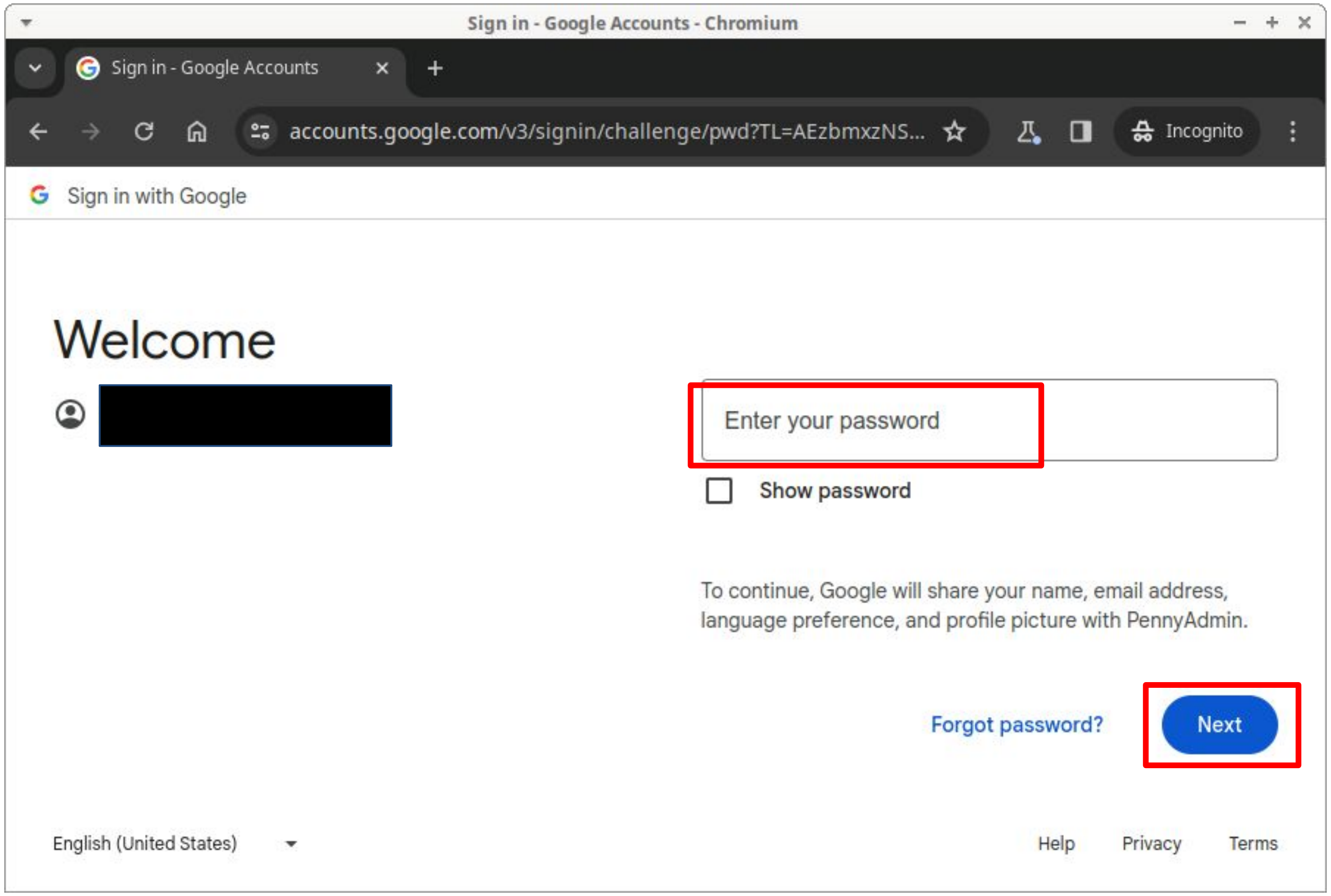
Next

English (United States)

Help Privacy Terms

Google Authentication

- See **PennyAdmin17Google** app (cont.)


Sign in - Google Accounts - Chromium

Sign in - Google Accounts

accounts.google.com/v3/signin/challenge/pwd?TL=AEzbmxzNS...

Incognito

Sign in with Google

Welcome

[redacted]

Enter your password

Show password

To continue, Google will share your name, email address, language preference, and profile picture with PennyAdmin.

Forgot password?

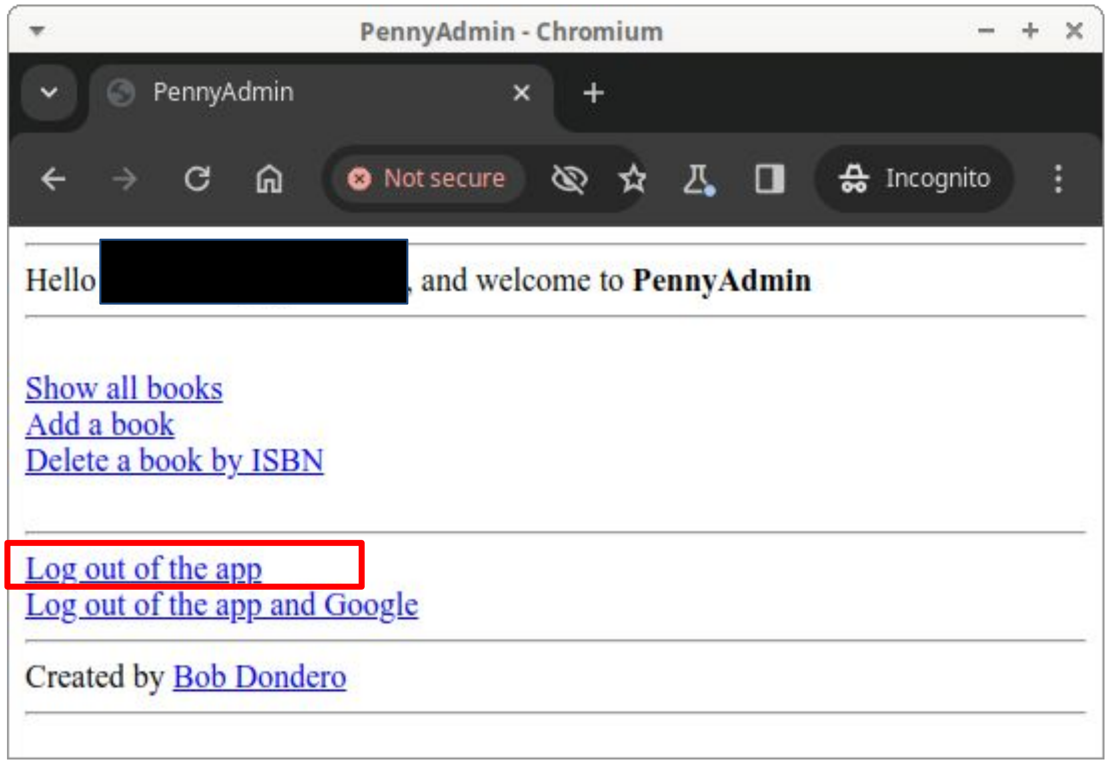
Next

English (United States)

Help Privacy Terms

Google Authentication

- See **PennyAdmin17Google** app (cont.)



Hello [redacted], and welcome to **PennyAdmin**

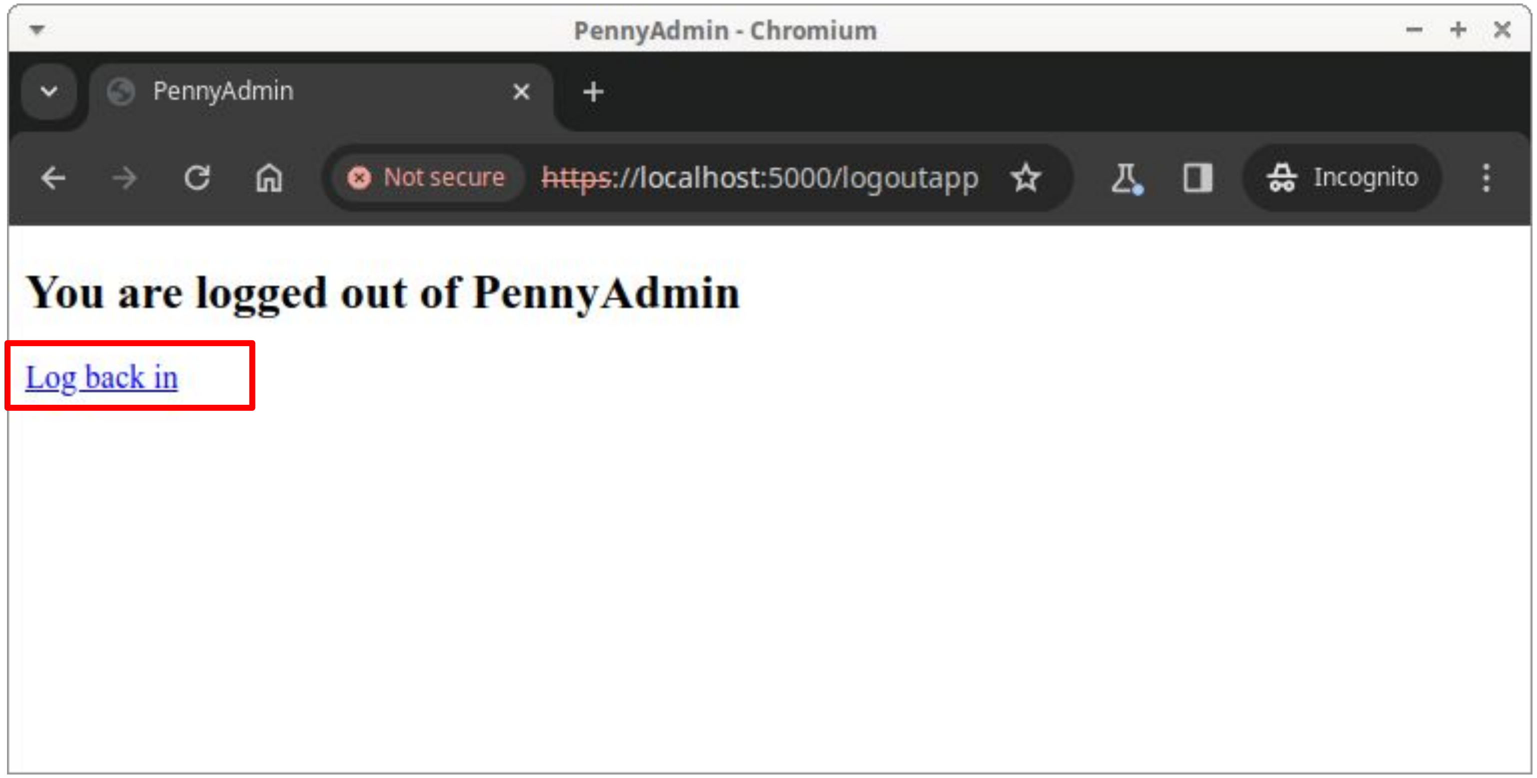
Show all books
Add a book
Delete a book by ISBN

Log out of the app
Log out of the app and Google

Created by Bob Dondero

Google Authentication

- See **PennyAdmin17Google** app (cont.)

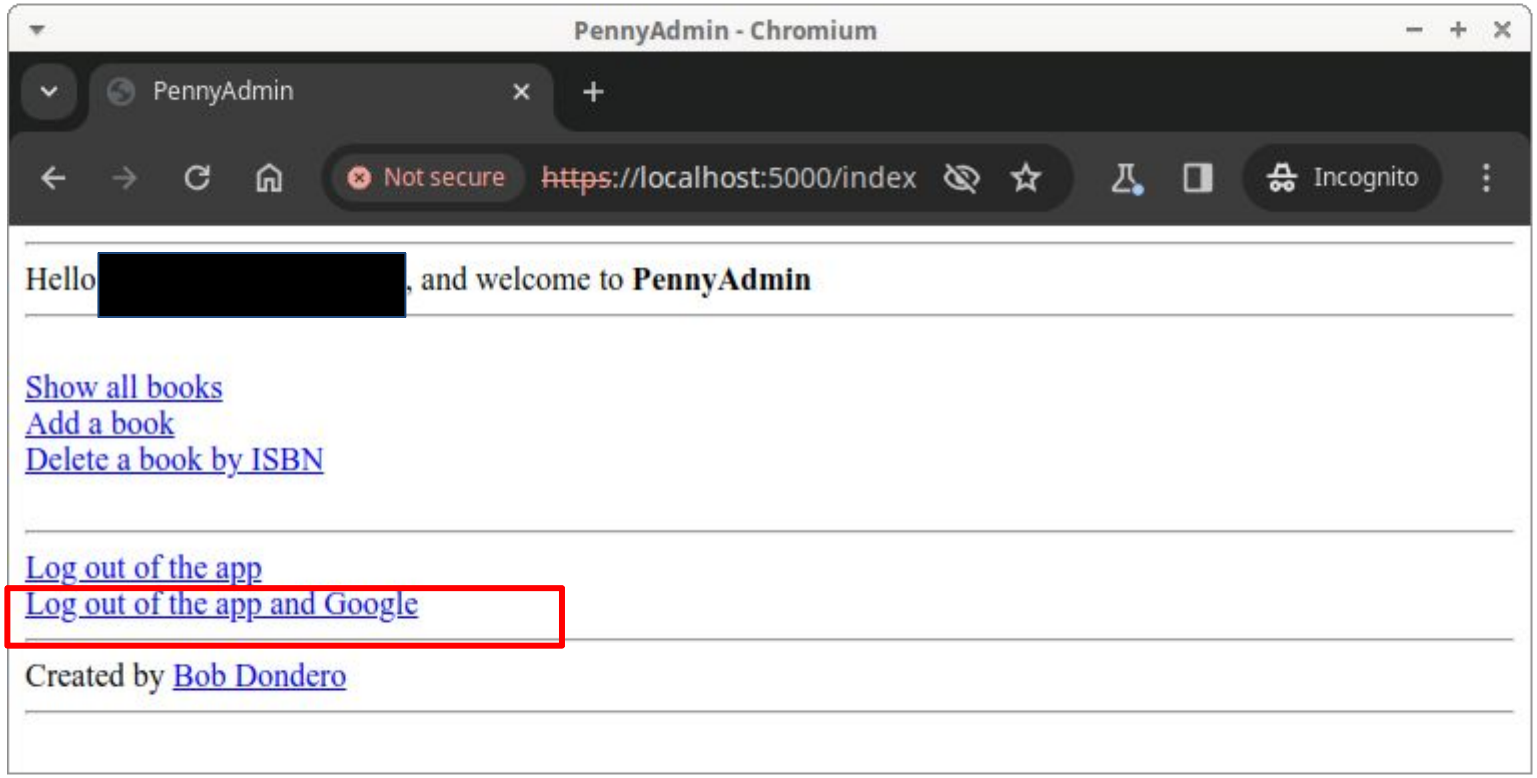


You are logged out of PennyAdmin

Log back in

Google Authentication

- See **PennyAdmin17Google** app (cont.)



Hello [redacted], and welcome to **PennyAdmin**

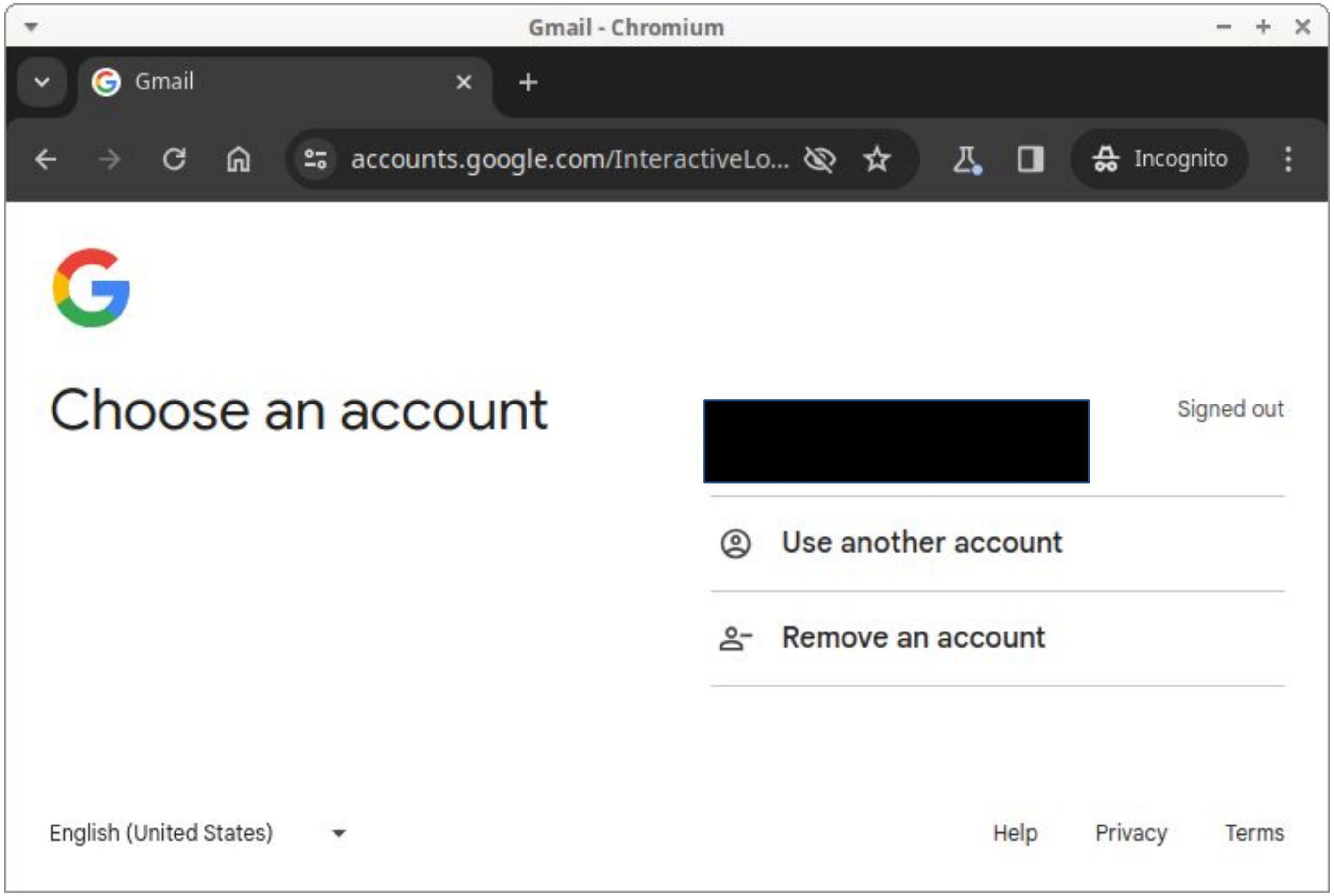
Show all books
Add a book
Delete a book by ISBN

Log out of the app
Log out of the app and Google

Created by Bob Dondero

Google Authentication

- See **PennyAdmin17Google** app (cont.)



Gmail - Chromium

Gmail

accounts.google.com/InteractiveLo...

Incognito

Choose an account

[redacted]

Signed out

Use another account

Remove an account

English (United States)

Help Privacy Terms

How to show loggedout page?

Google Authentication

- See **PennyAdmin17Google** (cont.)
  - How to run it on Render (or Heroku, or any cloud service)…

Google Authentication

- Preliminary
  - Deploy the app to Render
    - Push the app to a GitHub repo
    - Create a new Render app linked to the GitHub repo
    - Deploy the application from GitHub to Render
  - Configure the Render app
    - Create env vars APP_SECRET_KEY, GOOGLE_CLIENT_ID, GOOGLE_CLIENT_SECRET

Google Authentication

- Preliminary (cont.)
  - All preliminaries are the same, except:
    - For *Authorized JavaScript origins* enter the URL of your deployed application
    - For *Authorized redirect URIs* enter the callback URL of your deployed application
- In browser, enter URL:
    - https://*ipaddressofrenderapp*

Google Authentication

- See **PennyAdmin17Google** app (cont.)
  - How it works…
  - See **Appendix 2**

Google Authentication

- See **PennyAdmin17Google** app (cont.)
  - **runserver.py**
  - **penny.sql**, penny.sqlite
  - **database.py**
  - header.html, **footer.html**
  - index.html, show.html,
  - add.html, delete.html, reportresults.html
  - top.py, **penny.py**, **auth.py**

Google Authentication

- **Pros**
  - Users need not remember (yet another) password
  - Application need not manage usernames or passwords
  - Application ***cannot*** access passwords
  - Application can access profile info that user provided to Google
    - Given name, family name, picture, …

Google Authentication

- **Cons**
  - Complex
  - Adds overhead, but mostly only during first user visit per browser session
  - Application is constrained to users who have Google accounts
  - If attacker learns user's password for **Google**, then attacker learns user's password for **your app**

Google Authentication

- For more information...
- https://realpython.com/flask-google-login/

Summary

- We have covered:
  - Data comm attacks
  - Third-party authentication (briefly)
    - CAS
    - Google authentication

Summary

- We have covered:
  - SQL injection attacks
  - Cross-site scripting (XSS) attacks
  - Authentication & authorization
  - Cookie forgery attacks
  - Cross-site request forgery (CSRF) attacks
  - Data storage attacks
  - Data comm attacks
  - Third-party authentication (briefly)

Appendix 1:
How CAS Works

How CAS Works

- Procedure
  - **Part 1**: User logs into CAS server
    - User must provide credentials
  - **Part 2**: User logs into PennyAdmin
    - User need not provide credentials

How CAS Works

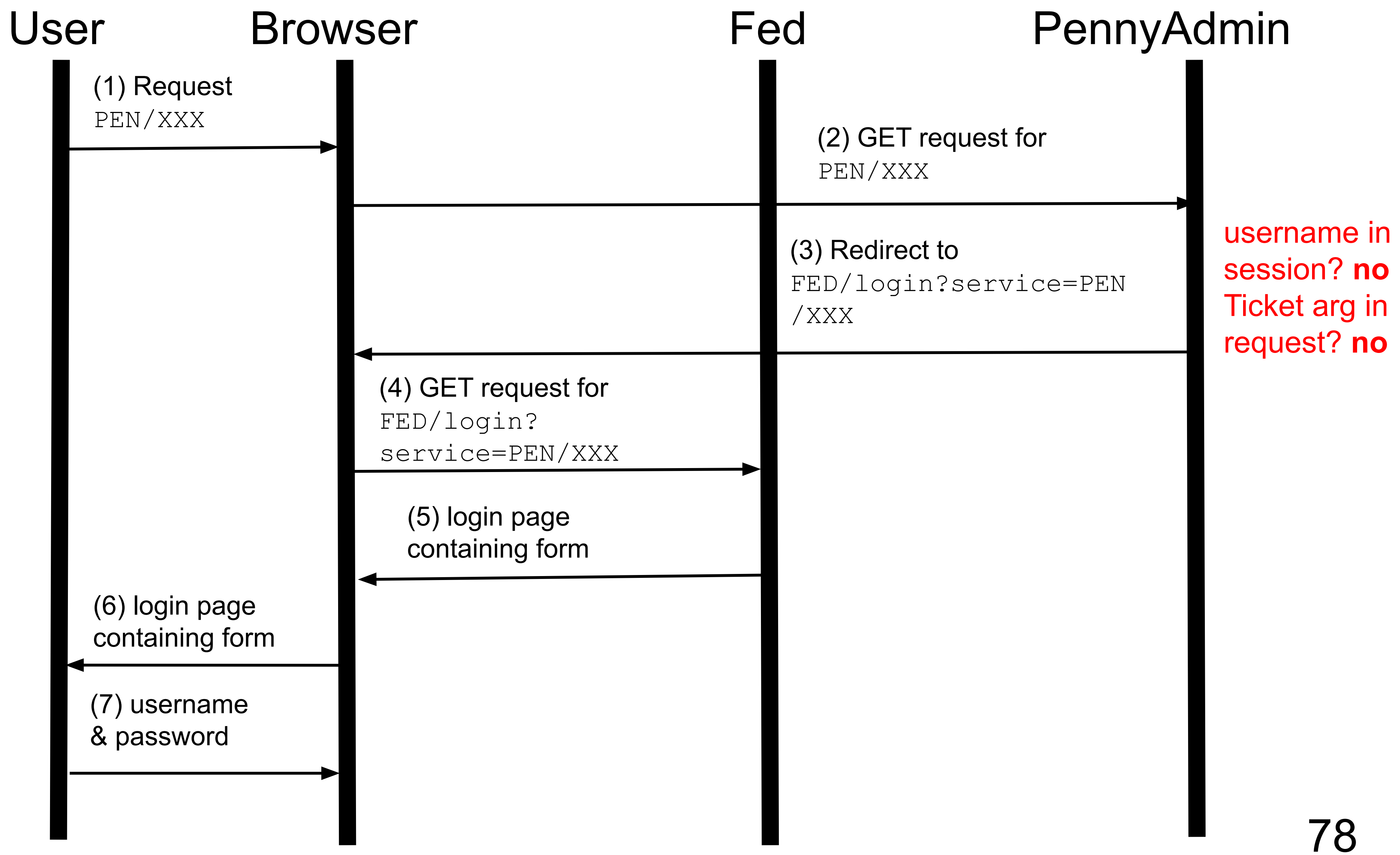
- See **PennyAdmin16Cas** app (cont.)
  - The flow…

Abbreviations:
  FED = https://fed.princeton.edu/cas
  PEN = https://localhost:55555

How CAS Works

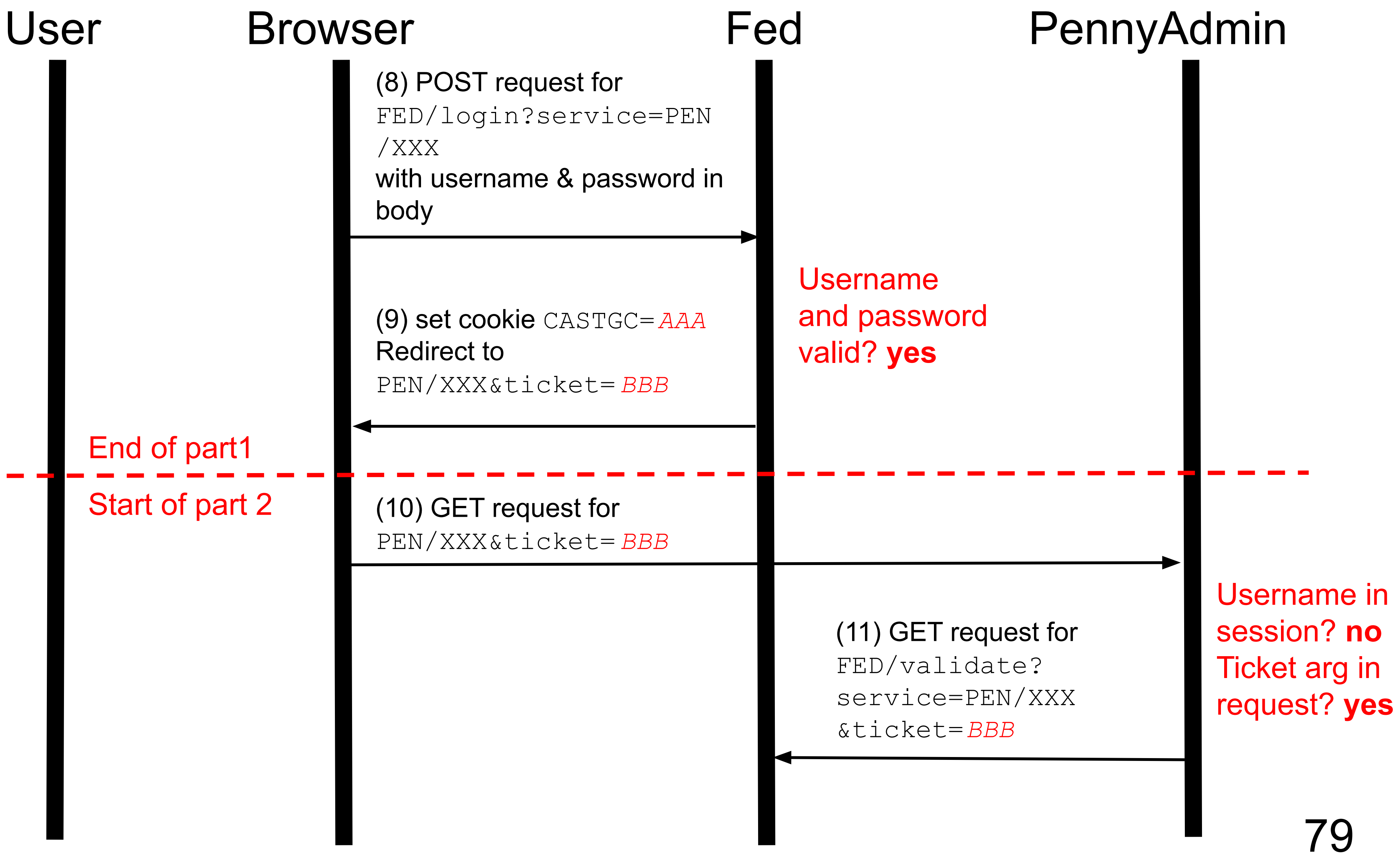
First use of PennyAdmin in browser session, browser session not CAS authenticated…

How CAS Works

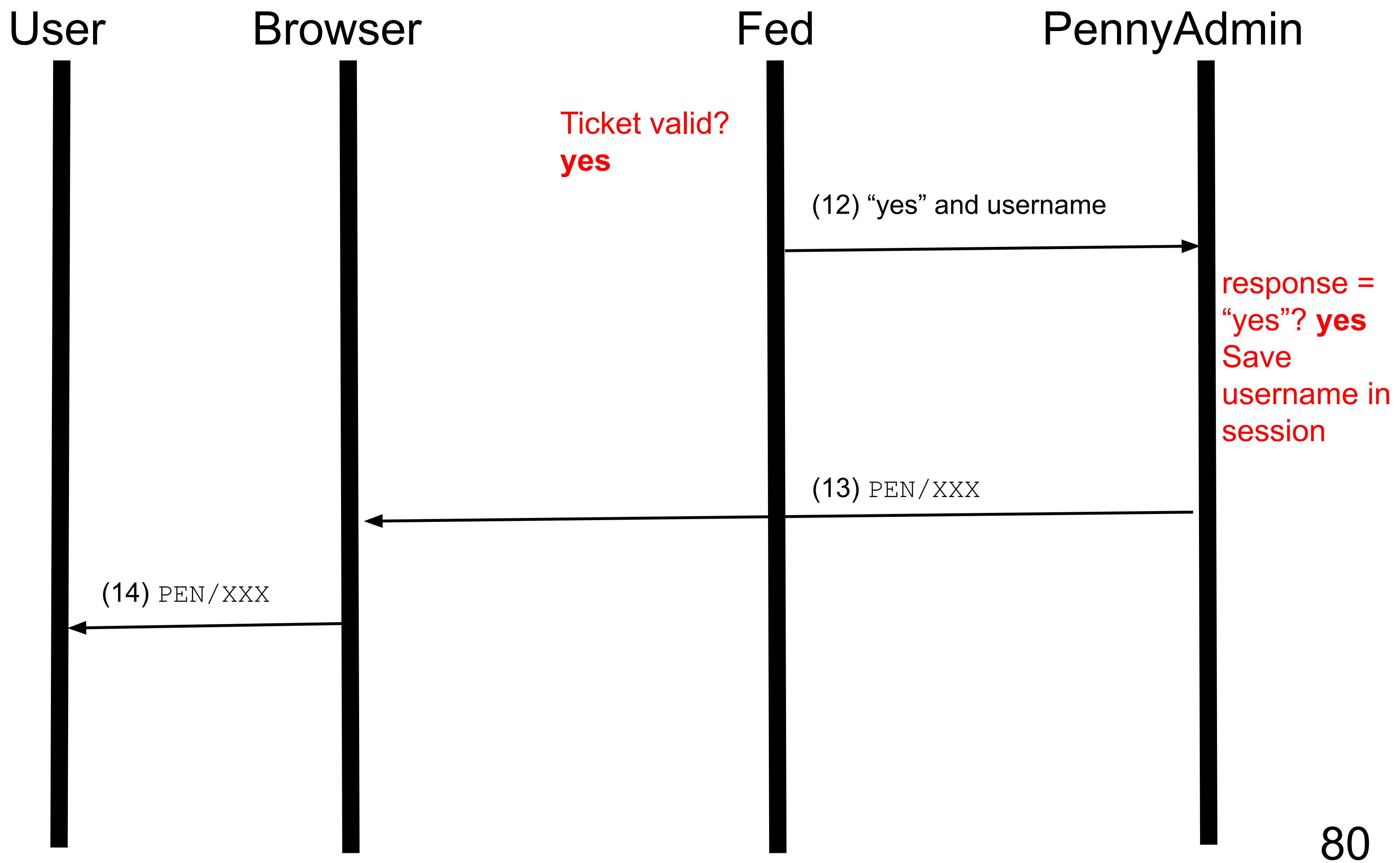


User
Browser
Fed
PennyAdmin
(1) Request PEN/XXX
(2) GET request for PEN/XXX
(3) Redirect to FED/login?service=PEN/XXX
username in session? **no**
Ticket arg in request? **no**
(4) GET request for FED/login?service=PEN/XXX
(5) login page containing form
(6) login page containing form
(7) username & password

How CAS Works



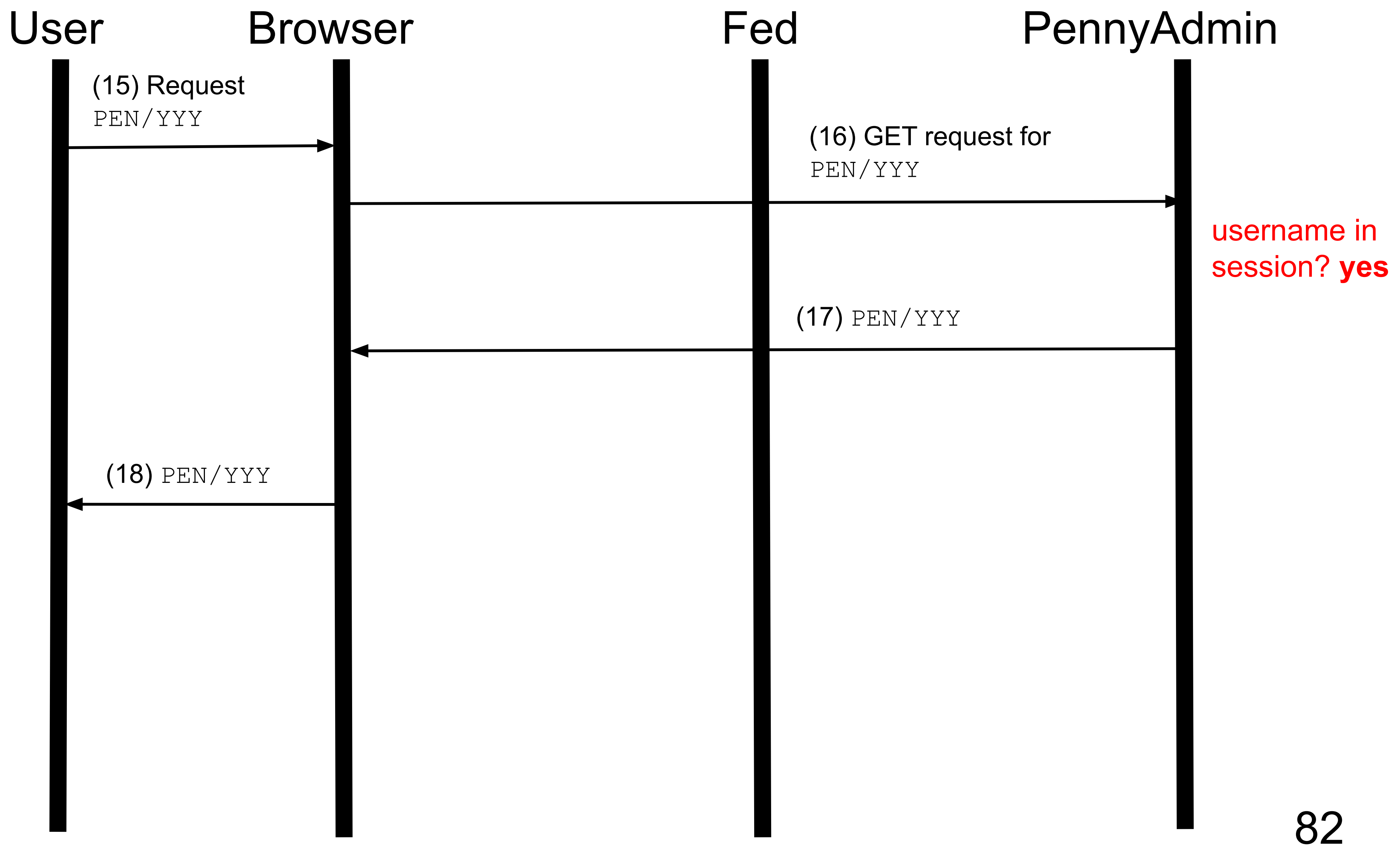
How CAS Works



How CAS Works

Second use of PennyAdmin in same browser session…

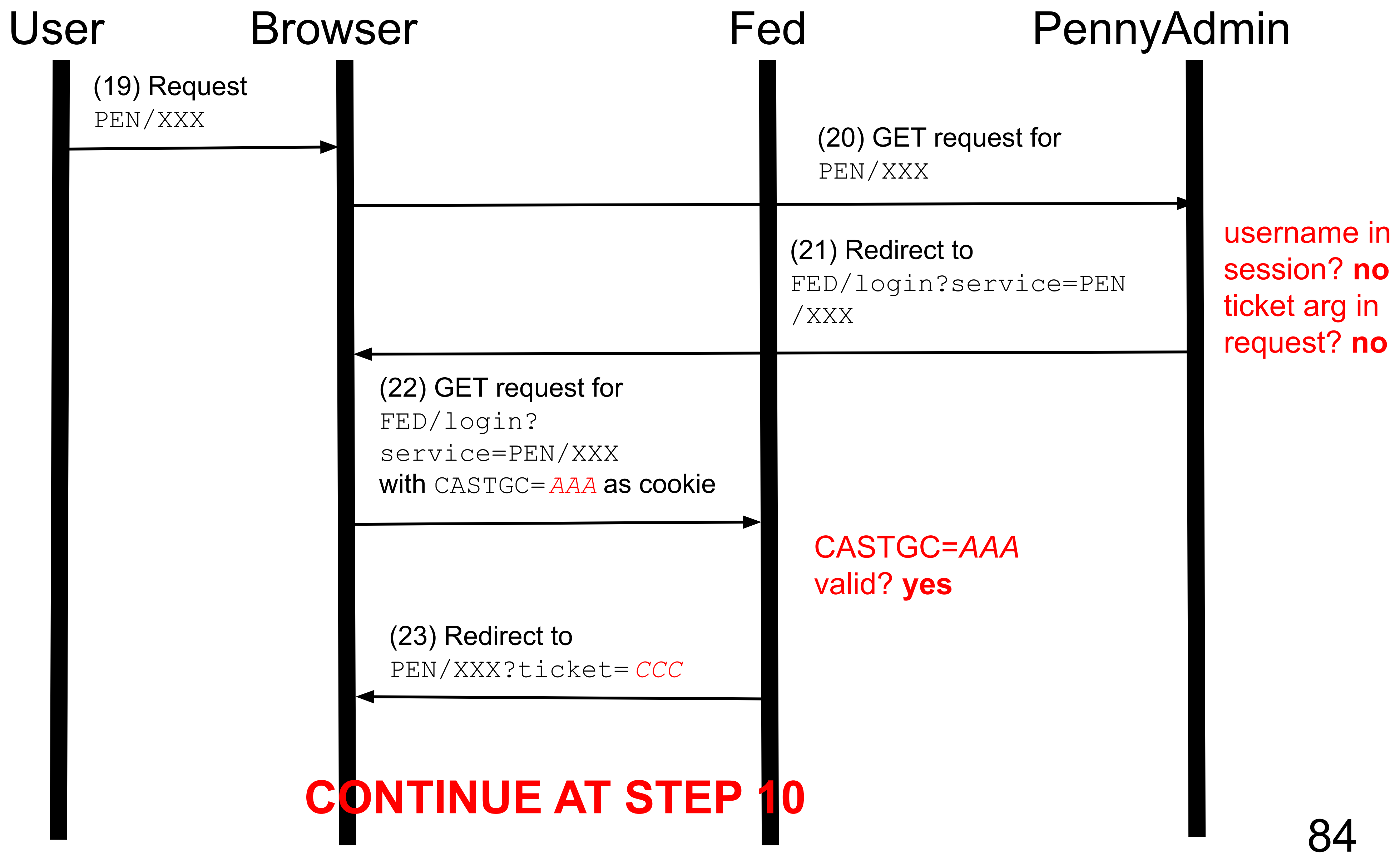
How CAS Works



How CAS Works

First use of PennyAdmin in browser session, browser session already CAS authenticated…

How CAS Works



How CAS Works

- For more information…
- https://apereo.github.io/cas/6.5.x/protocol/CAS-Protocol.html

Appendix 2:
How Google Authentication Works

How Google Auth Works

- Procedure

  - **Part 1**: User logs into Google
    - User must provide credentials
  - **Part 2**: User logs into PennyAdmin
    - User need not provide credentials

How Google Auth Works

- ***OAuth2***

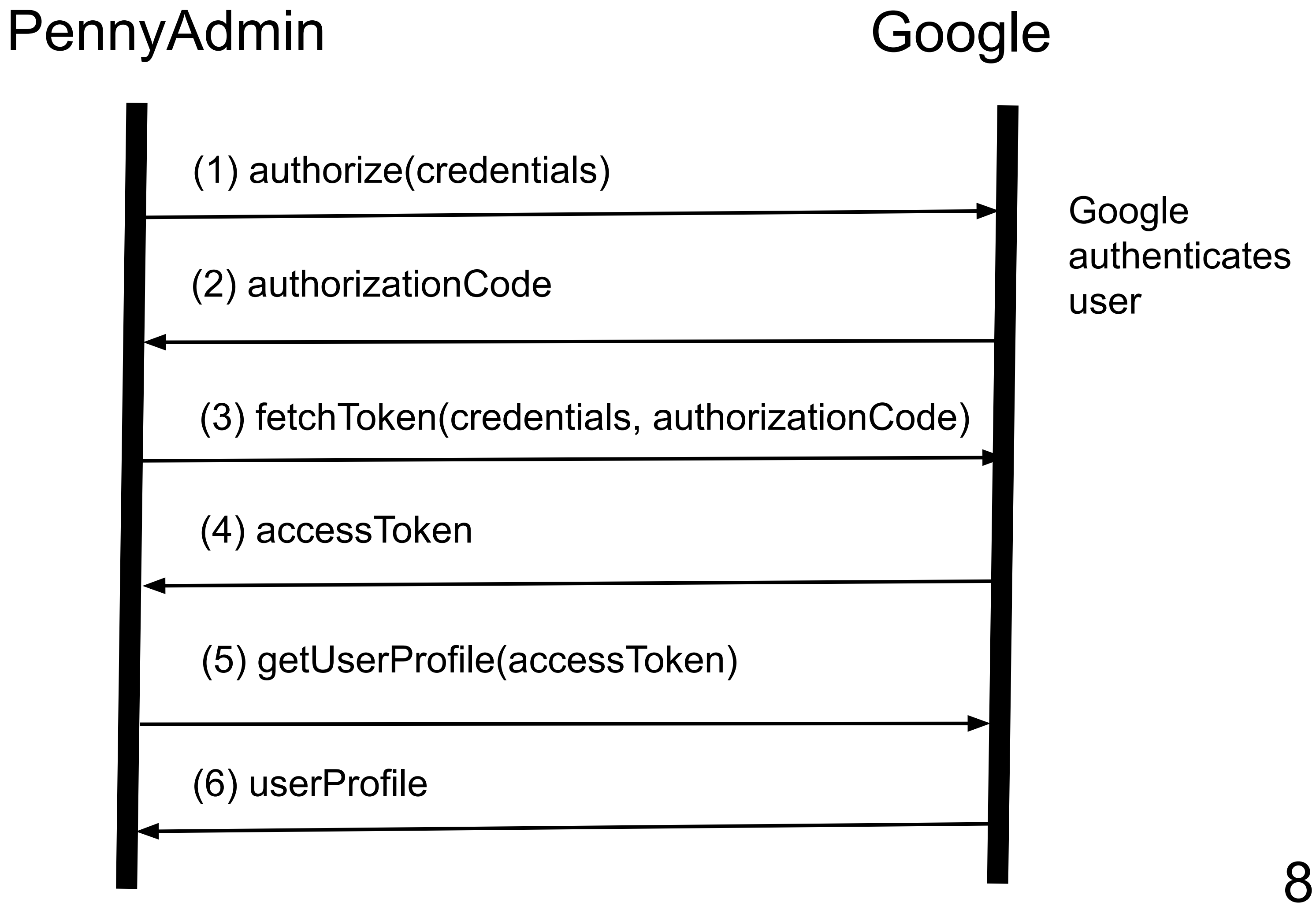
OAuth ("Open Authorization") is an open standard for access delegation, commonly used as a way for internet users to grant websites or applications access to their information on other websites but without giving them the passwords. This mechanism is used by companies such as Amazon, **Google**, Facebook, Microsoft, and Twitter to permit the users to share information about their accounts with third-party applications or websites.

– https://en.wikipedia.org/wiki/OAuth

How Google Auth Works

OAuth2 Flow Overview:

Ahead of time: register PennyAdmin with Google; get credentials


PennyAdmin
Google
(1) authorize(credentials)
Google authenticates user
(2) authorizationCode
(3) fetchToken(credentials, authorizationCode)
(4) accessToken
(5) getUserProfile(accessToken)
(6) userProfile

How Google Auth Works

- See **PennyAdmin17Google** app (cont.)
  - The flow:

How Google Auth Works

First use of PennyAdmin in browser session, browser session not Google authenticated…

How Google Auth Works

(1) User
Type: `https://localhost:5000/index`

(2) Browser
Send GET request: `https://localhost:5000/index`

(3) PennyAdmin (in /index endpoint)
Email in session? **No**
Return redirect: `https://localhost:5000/login`

(4) Browser
Send GET request: `https://localhost:5000/login`

(5) PennyAdmin (in /login endpoint)
Return redirect to the Google authorization endpoint, passing `GOOGLE_CLIENT_ID` and `https://localhost:5000/login/callback` as parameters

(6) Browser
Send request to the Google authorization endpoint, passing `GOOGLE_CLIENT_ID` and `https://localhost:5000/login/callback`as parameters

How Google Auth Works

(7) Google

Are the application (identified by `GOOGLE_CLIENT_ID`) and the given callback (`https://localhost:5000/login/callback`) registered? **Yes**.

Do cookies indicate that the browser session is already Google authenticated? **No**.

Return Google login page to browser

(8) Browser

Render Google login page

(9) User

Enter Google email and password and submit form

(10) Browser

Send POST request to Google, with email and password in body

(11) Google

Does the user authenticate? **Yes**.

Return redirect:

`https://localhost:5000/login/callback?code=`*`authorizationcode`*

END OF PART 1; BEGINNING OF PART 2

How Google Auth Works

(12) Browser

Send GET request:

`https://localhost:5000/login/callback?code=`*`authorizationcode`*

(13) PennyAdmin (in login/callback endpoint)

Send POST request to Google with the *authorizationcode*, `GOOGLE_CLIENT_ID`, and `GOOGLE_CLIENT_SECRET` in the body

(14) Google

Return access token

(15) PennyAdmin (in login/callback endpoint)

Send GET request to Google with the access token as a header

(16) Google

Return user’s profile data

(17) PennyAdmin (in login/callback endpoint)

Add user’s profile data (notably email) to the session

Return redirect: `https://localhost:5000/index`

How Google Auth Works

(18) Browser
Send GET request: `https://localhost:5000/index`

(19) PennyAdmin
Email in session? **Yes**
Return index page

(20) Browser
Render index page

How Google Auth Works

Second use of PennyAdmin in browser session…

How Google Auth Works

(21) User
In index page, click on `https://localhost:5000/show` link

(22) Browser
Send GET request: `https://localhost:5000/show`

(23) PennyAdmin
Email in session? **Yes**
Return show page

(24) Browser
Render show page

How Google Auth Works

First use of PennyAdmin in browser session, browser session already Google authenticated…

How Google Auth Works

(25) User
Type: `https://localhost:5000/index`

(26) Browser
Send GET request: `https://localhost:5000/index`

(27) PennyAdmin (in /index endpoint)
Email in session? **No**
Return redirect: `https://localhost:5000/login`

(28) Browser
Send GET request: `https://localhost:5000/login`

(29) PennyAdmin (in /login endpoint)
Return redirect to the Google authorization endpoint, passing `GOOGLE_CLIENT_ID`and `https://localhost:5000/login/callback`as parameters

How Google Auth Works

(30) Browser

Send request to the Google authorization endpoint, passing `GOOGLE_CLIENT_ID` and `https://localhost:5000/login/callback` as parameters

(32) Google

Are the application (identified by `GOOGLE_CLIENT_ID`) and the given callback (`https://localhost:5000/login/callback`) registered? **Yes**

Do cookies indicate that the browser session is already Google authenticated? **Yes**

Return redirect:

`https://localhost:5000/login/callback?code=`*`authorizationcode`*

CONTINUE AT STEP 12