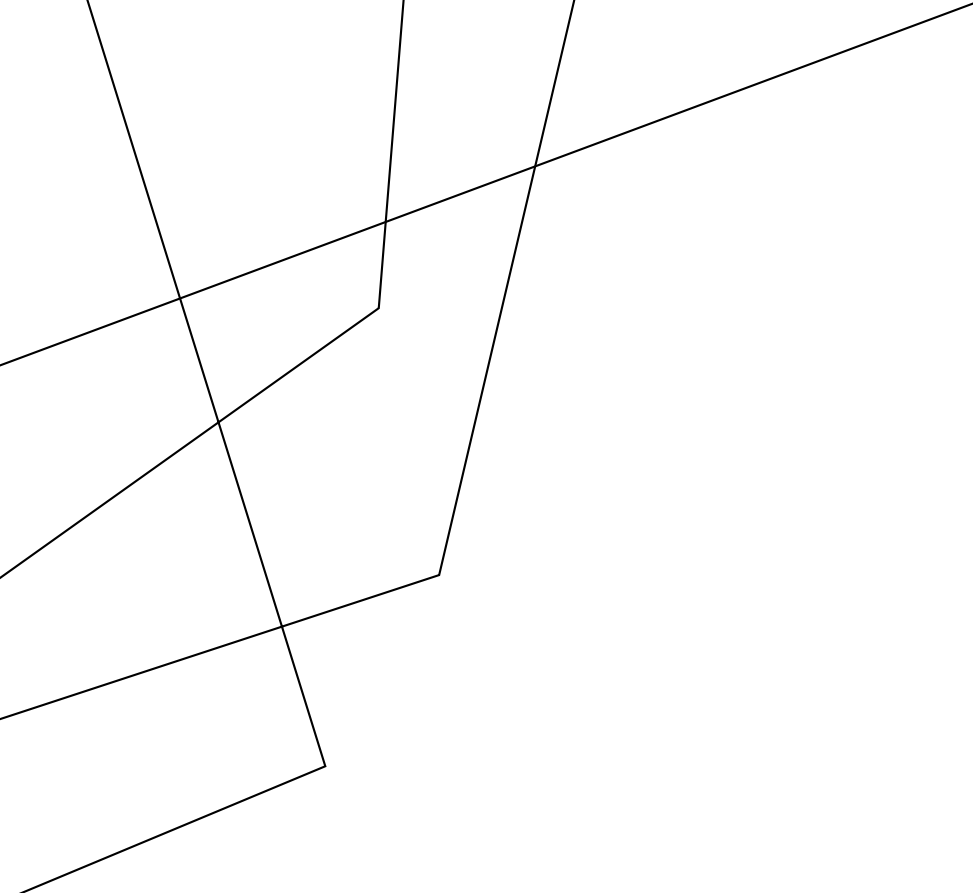


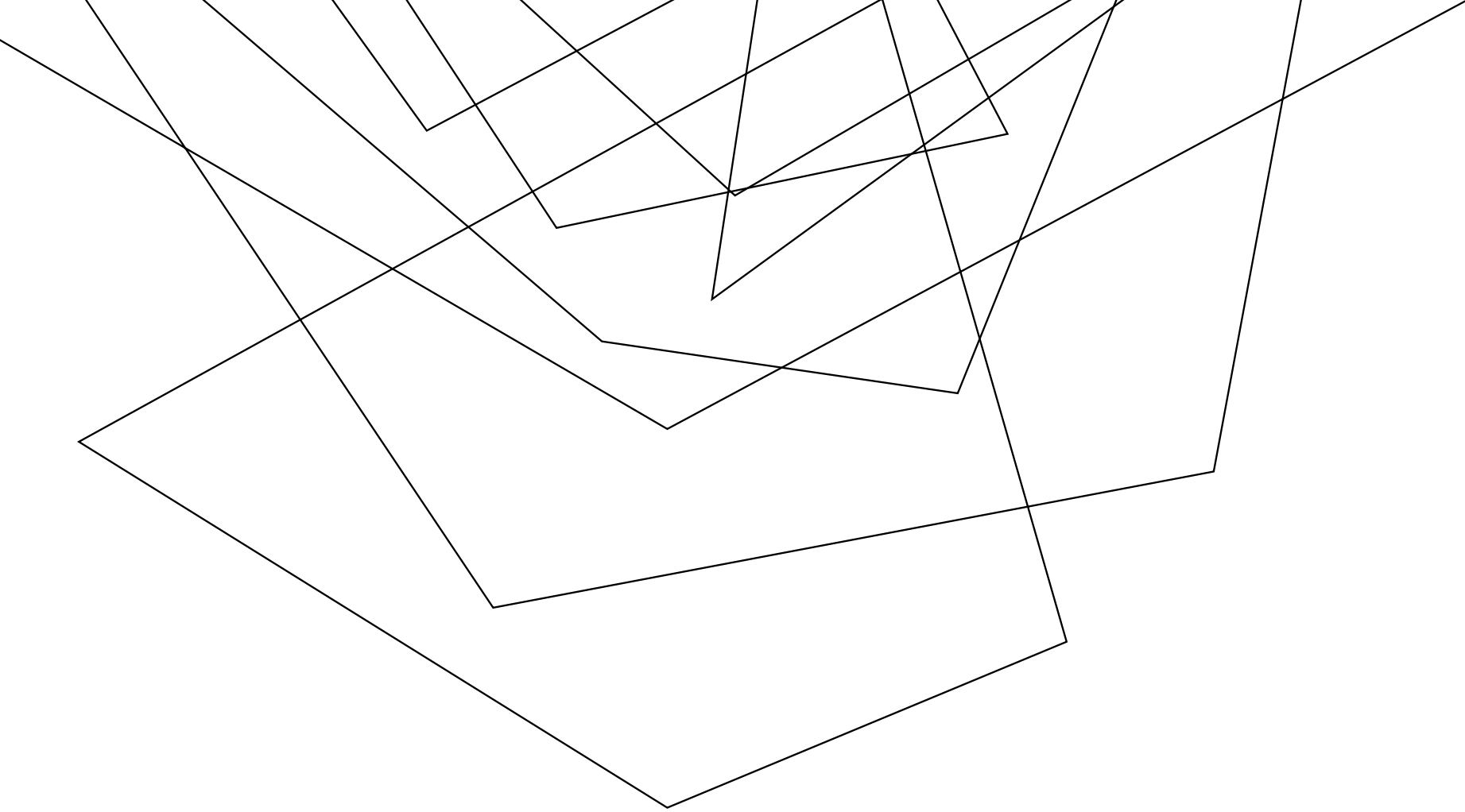
EXERCISE 35

WEB AUTHENTICATION REVIEW

What are the disadvantages of sending passwords in a GET parameter? What is the advantage of using JWT?

Abstract geometric lines in the top left corner, consisting of several thin black lines forming a series of overlapping, tilted rectangular shapes.

ADMINISTRIVIA AND ANNOUNCEMENTS

Abstract geometric lines in the top-left corner of the slide, consisting of several thin black lines forming various polygons and intersecting at different points.

WEB APPS

EECS 677: Software Security Evaluation

Drew Davidson

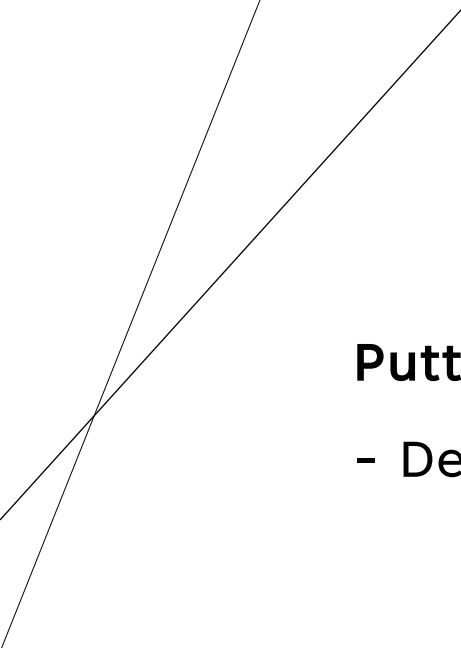


LAST TIME

REVIEW: WEB RESOURCES

Authentication Security

- Ensuring Database Integrity
- Ensuring Credential Integrity

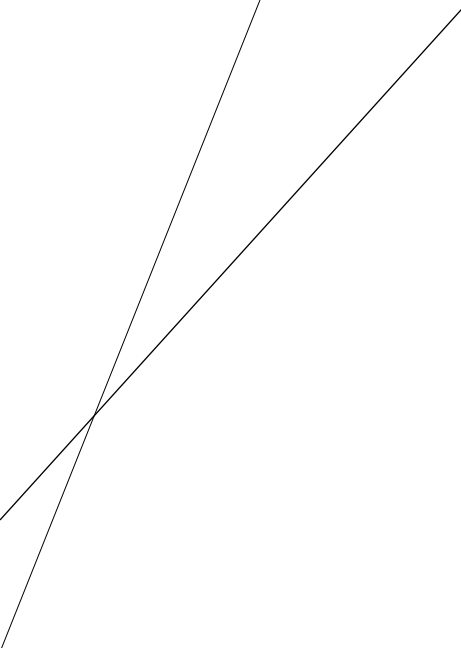


TODAY

WEB PROTECTIONS

Putting it all together

- Developing a react app and examining security aspects



A MODERN WEB-APP

FULL STACK SECURITY

frontend

react

api

node

database

sqlite

REACT FRONTEND

WEB PROTECTIONS

npm create vite@latest
cd frontend
npm install axios
npm run dev

```
import { useState } from 'react'
import './App.css'
import { Login } from './Login.jsx'

export default function App() {
  const [token, setToken] =
    useState(window.sessionStorage.getItem("token"));

  if (token === undefined || token === null){
    return <Login tokenSetter={setToken} />
  }
  return (<p>{"I'm some content!!!!"}</p>)
}
```

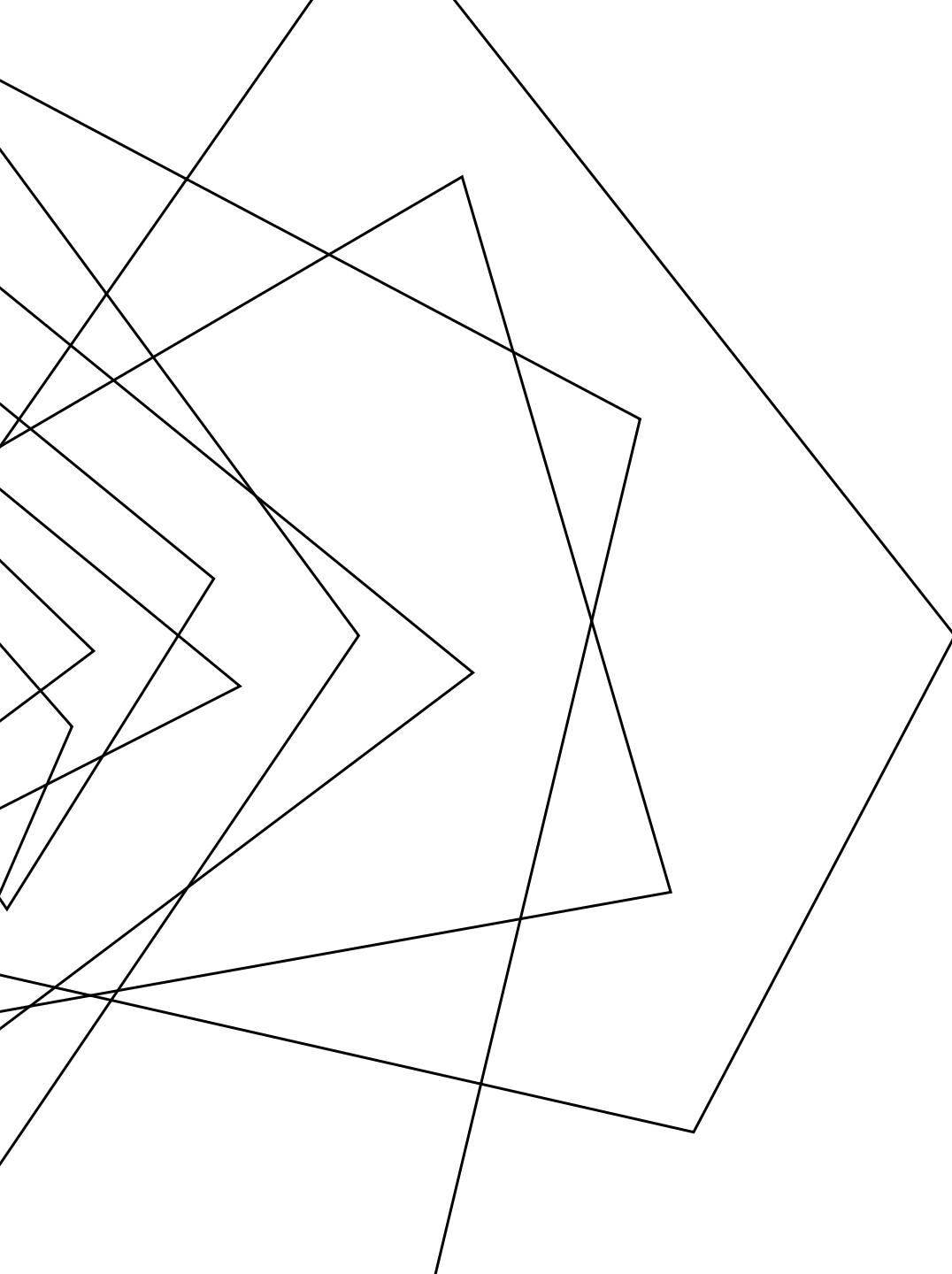
NODE BACKEND API

WEB PROTECTIONS

npm create
npm install express sqlite3

```
app.post('/login', (req, resp) => {
  const name = req.body.name;
  const pw = req.body.pw;

  const Q = "SELECT name,id FROM accounts"
    + " WHERE pw = '" + pw
    + "' AND name = '" + name + "'";
  db.get(Q, function(err, row) {
    if (!row) {
      resp.send(JSON.stringify({ok:false}));
      return;
    }
    const creds = { "name":row['name'], "id":row['id']}
    const token = encodeJWT(creds, SECRET);
    const res = {'ok':true,'token':token};
    resp.send(JSON.stringify(res));
  });
});
```



LECTURE END!

BASIC END-TO-END SCHEME

NEXT TIME: FILLING OUT FUNCTIONALITY