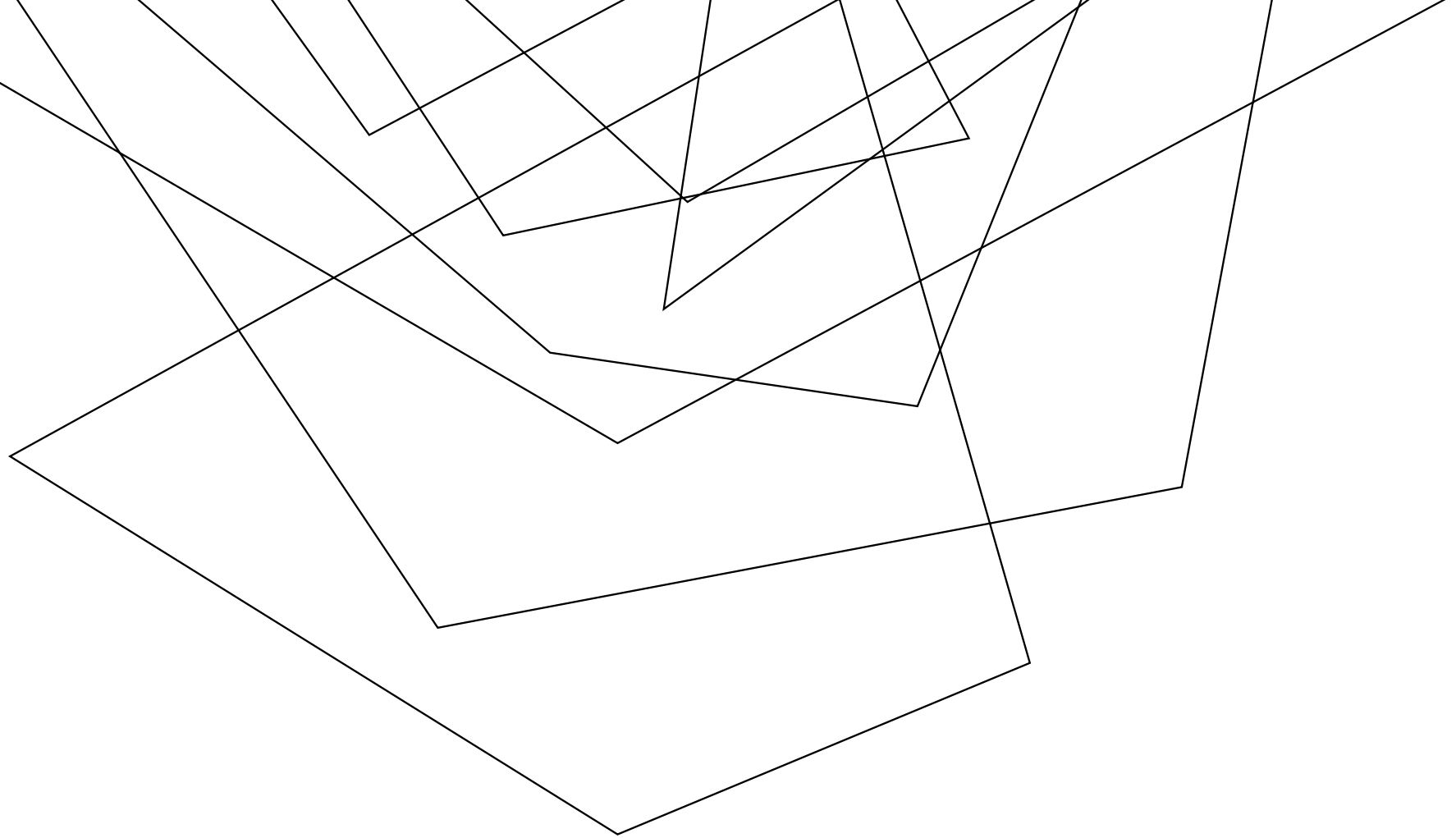
EXERCISE

WEB SECURITY REVIEW

What is an XSS? What is the threat model?

ADMINISTRIVIA AND ANNOUNCEMENTS

Remember! Quiz 3 is Monday



WEB FRONTENDS

EECS 677: Software Security Evaluation

Drew Davidson

LAST TIME

REVIEW: WEB RESOURCES

Basic web endpoint

- Handles user input
- Sanitizes input

```
import express from "express";
import validator from "validator";

const app = express();
app.get("/page", (req, res) => {
  let v = req.query.v ? req.query.v : "world";
  v = validator.escape(v);
  let c = `<h1>Hello ${v}!</h1>`;
  c += "<img src='https://drew.davidson.cool/drew.png'></img>";
  res.send(`${c}`);
});
app.listen(3001);
```

TODAY

WEB FRONTENDS

Frontend Security

- Elaborate the UI and create more of the web “stack”
- Create a frontend with react
- Secure a third-party resource
- Interact with the data endpoint

A REACT FRONTEND

WEB FRONTENDS

PROTECTING RESOURCES

WEB PROTECTIONS

Scripts come from 3rd parties!

- We should protect clients from those parties being compromised

SUB-RESOURCE INTEGRITY

WEB PROTECTIONS

Ensuring script integrity

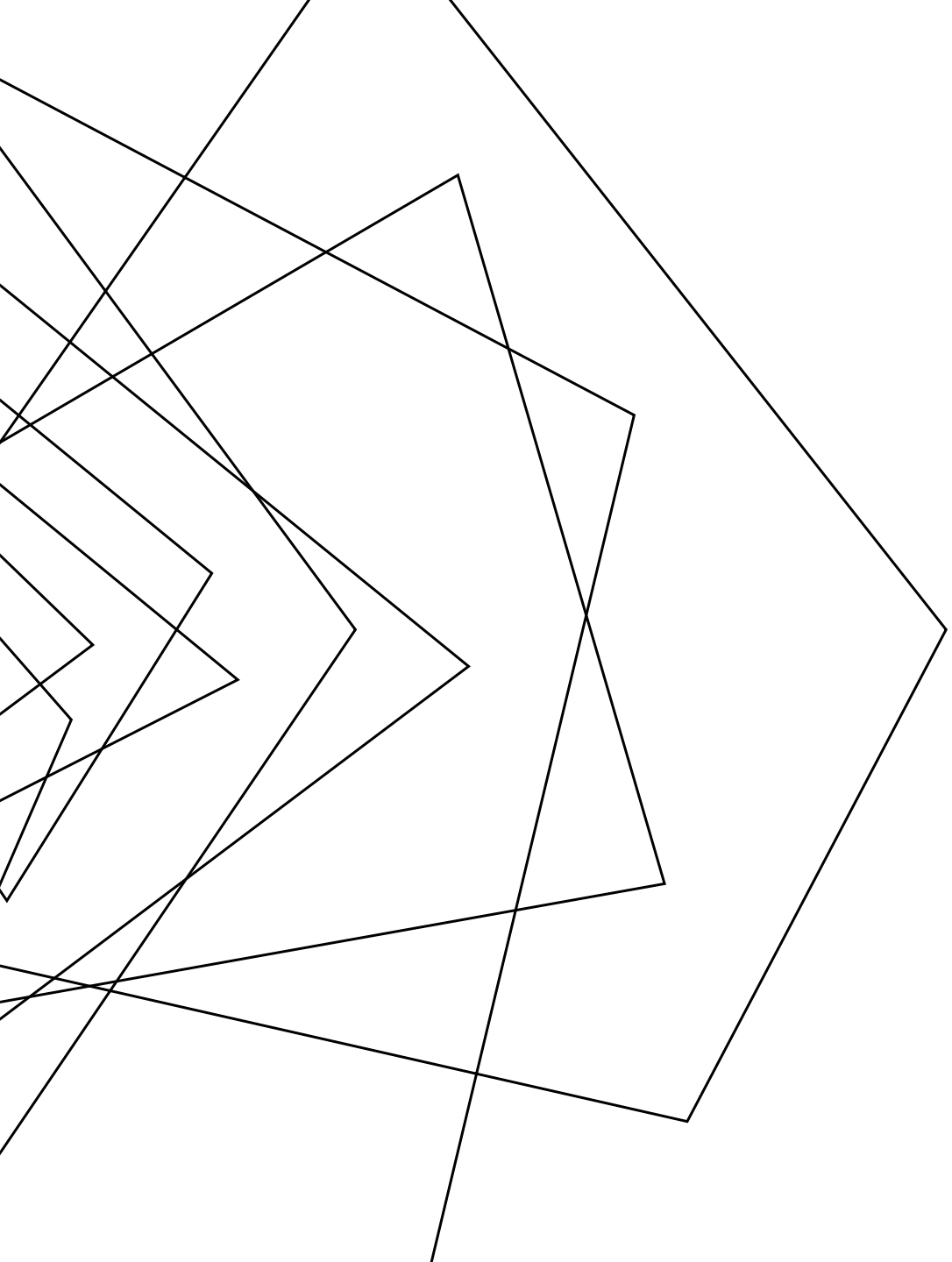
```
<script
   src="https://example.com/example-framework.js"
   integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
   crossorigin="anonymous"></script>
```

Generating the hash

```
cat FILENAME.js | openssl dgst -sha384 -binary | openssl base64 -A
```

A REACT FRONTEND

WEB FRONTENDS



LECTURE END!

Considering persistence