EXERCISE 34

WEB SECURITY REVIEW

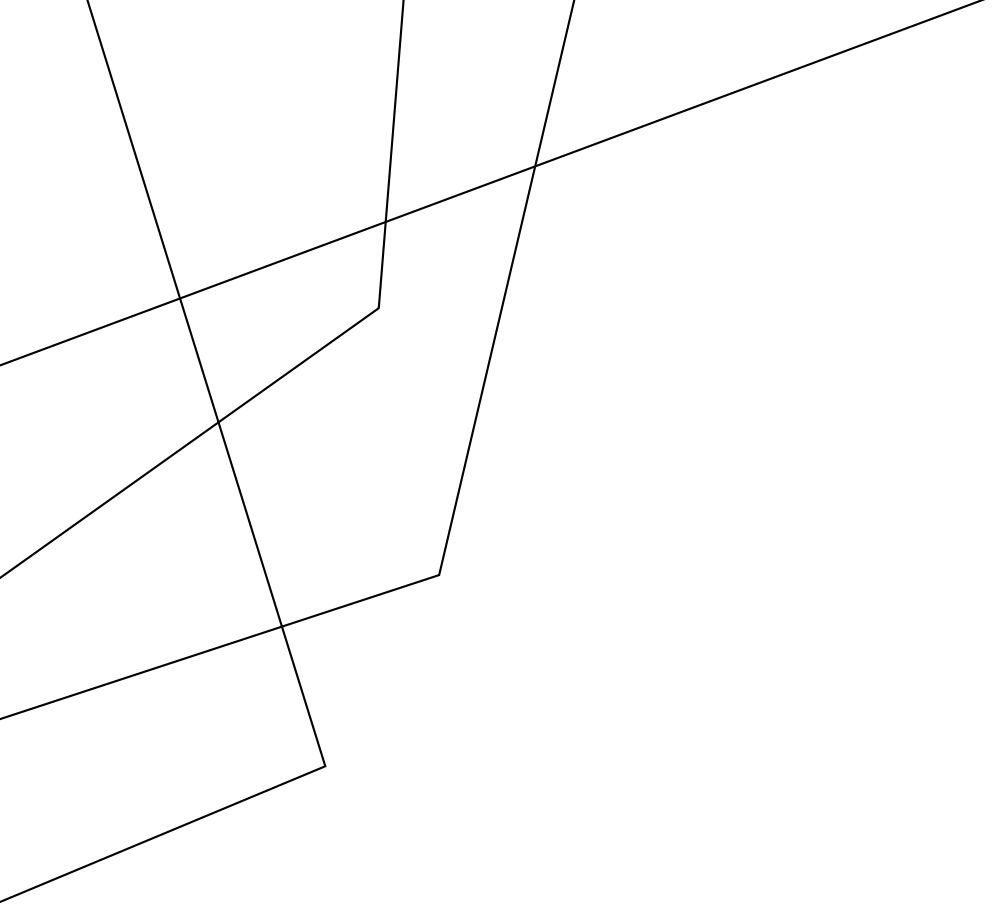
What is the definition of an XSS attack? How does an XSS attack happen?

EXERCISE 34 SOLUTION

WEB SECURITY REVIEW

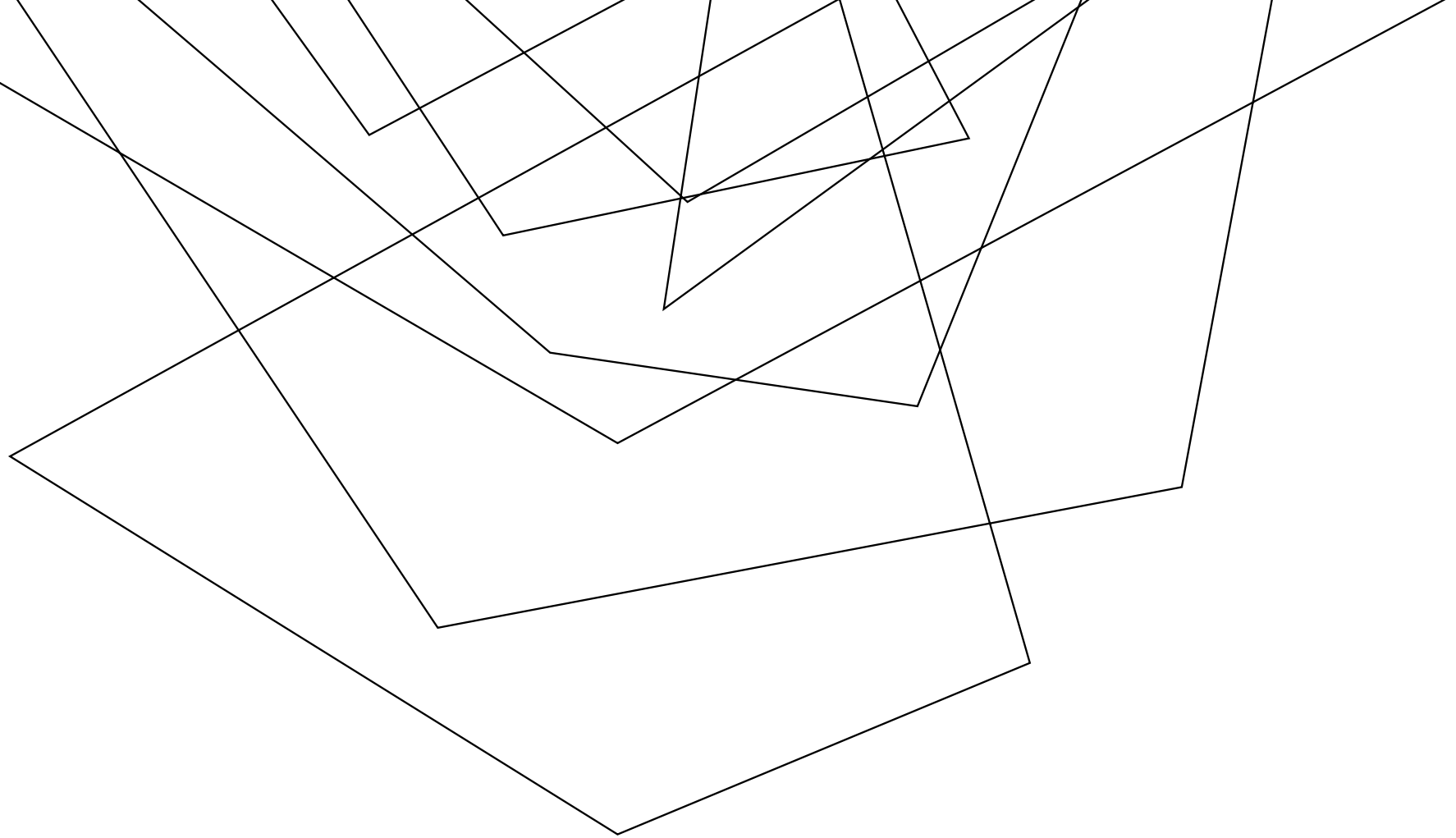
ADMINISTRIVIA AND ANNOUNCEMENTS

Quiz 3 Info (including review session:
https://analysis.cool/quiz3.php



ADMINISTRIVIA AND ANNOUNCEMENTS

When is Quiz 3?



WEB PROTECTIONS

EECS 677: Software Security Evaluation

Drew Davidson

LAST TIME

REVIEW: WEB SECURITY

High-level overview of dynamic behavior

Dynamic server via nodejs

Dynamic client via javascript browser

Classic Vulnerability

XSS – Cross-site Scripting

TODAY

WEB PROTECTIONS

Prevent the attack described last lecture (simple reflected XSS)

Sample some of the other issues in a client-server relationship

THE PROBLEM

WEB PROTECTIONS: XSS

Content (data) being (mis)interpreted as code

SANITIZATION

WEB PROTECTIONS: XSS

```
import express from 'express'
import validator from 'validator'

const app = express()

app.get('/', (req, res) => {
    let name = "(nameless)";
    if ('v' in req.query){
       name = req.query['v'];
       name = validator.escape(name);
    }
    res.send("Hello " + name);
})

app.listen(3000)
```

RESOURCES

WEB PROTECTIONS

```
import express from 'express'
import fs from 'node:fs';

const app = express()

app.get('/', (req, res) => {
        const data = fs.readFileSync('content.html', 'utf8');
        res.send(data);
})

app.listen(3000)
```

SUB-RESOURCES

WEB PROTECTIONS

A modular approach to web development

THE SAME ORIGIN POLICY

WEB PROTECTIONS

SUB-RESOURCE INTEGRITY

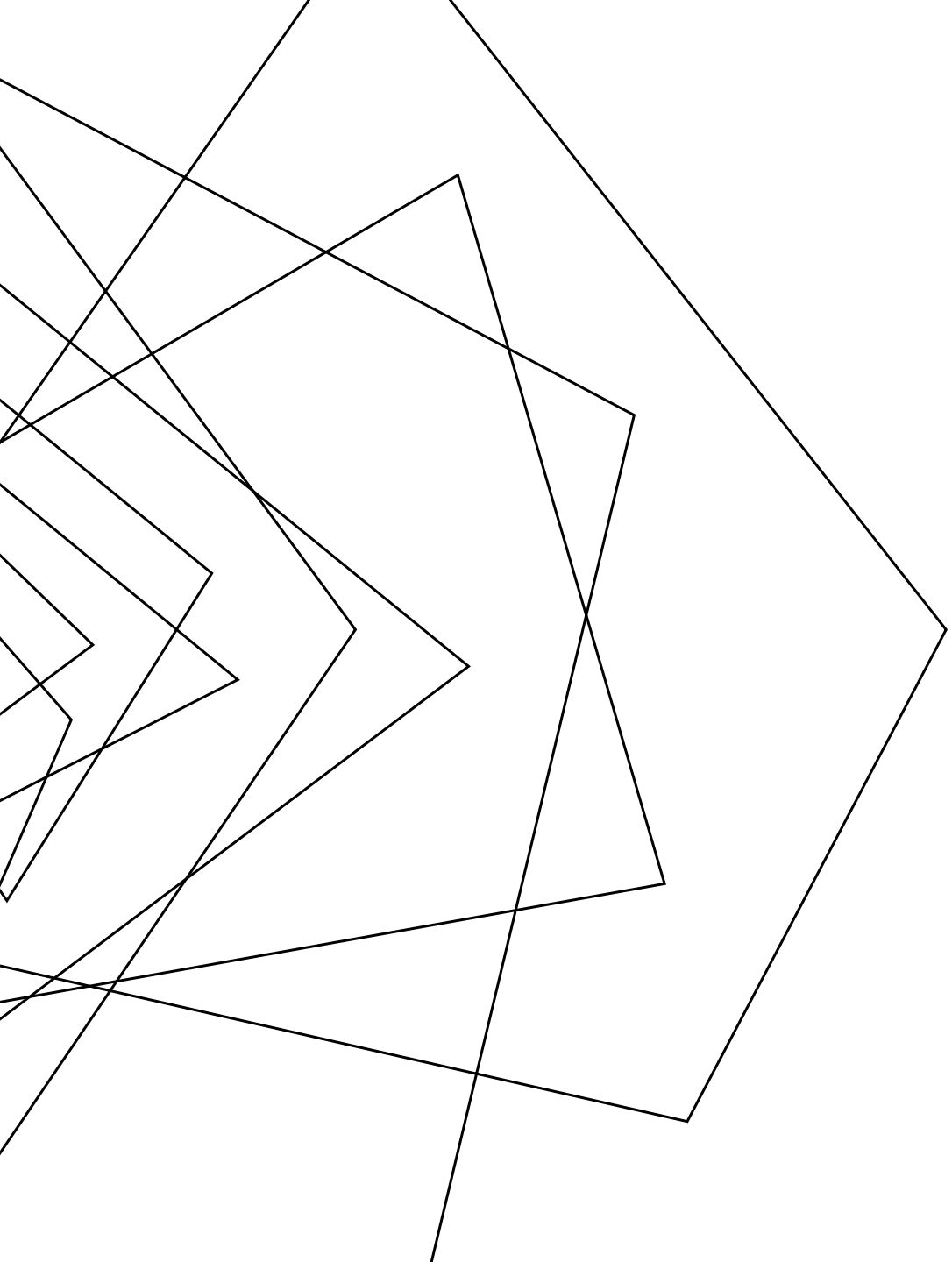
WEB PROTECTIONS

```
<script src="https://example.com/example-framework.js"
integrity="sha384-
oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPz
Qho1wx4JwY8wC" crossorigin="anonymous"></script>
```

SUB-RESOURCE INTEGRITY

WEB PROTECTIONS

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



LECTURE END!

Preventing XSS and looking beyond