# Automating Almost All Application Security Things with CI/CD

Even Honeypots!

Mick Douglas and Andy Douglas



Continuous Integration

### Continuous Integration

```
🔃 ua-parser-js@0.7.5 - Regular Expres...
                                                       const mime = require('mime');
                                                                                                                                Code flow
                                                        function sendFile(filename, response) {
                                                          response.setHeader('Content-Type', mime.lookup(filenam
                                                                                                                                        scripts/bench/server.js
                                                                                                                                                                                            line #24

✓ app.js - 2 issues

                                                          response.writeHead(200);
         Timing Attack
                                                          const fileStream = createReadStream(filename);
                                                                                                                                        scripts/bench/server.js
                                                                                                                                                                                             line 20

☐ Cross-Site Scripting attack

                                                          fileStream.pipe(response);
                                                                                                                                        scripts/bench/server.js
                                                          fileStream.on('finish', response.end);

✓ server.is - 1 issue

         H Path Transversal Vulnerability
function createHTTP2Server(benchmark) {
                                                                                                                                External example fixes
                                                          const server = http2Server.createServer({}), (request,
                                                                                                                                This issue was fixed by 708 projects. Here are 3 example fixes.
                                                             const filename = join(
                                                                dirname.
                                                                                                                                 georgi/grant

✓ standalone.is - 2 issues

                                                                benchmarks'.
         Using component state to comput ...
                                                               benchmark,
                                                                                                                                    function static_file(route, p, req, res) {
         http (used in require) is an insecure..
                                                               request.url
                                                                                                                                       var uri = url.parse(req.url).pathname

	✓ Header.is - 1 issue

                                                                                                                                     function dump static file(route, p, req, res) {
                                                             ) replace(/\?.*/g, '');
                                                                                                                                      var uri = url.parse(this.reg.url).pathname;
         Unsanitized input flows from the H...
                                                                                                                                      var filename = path.join(process.cwd(), 'public', uri);
                                                             if (existsSync(filename) && statSync(filename).isFil

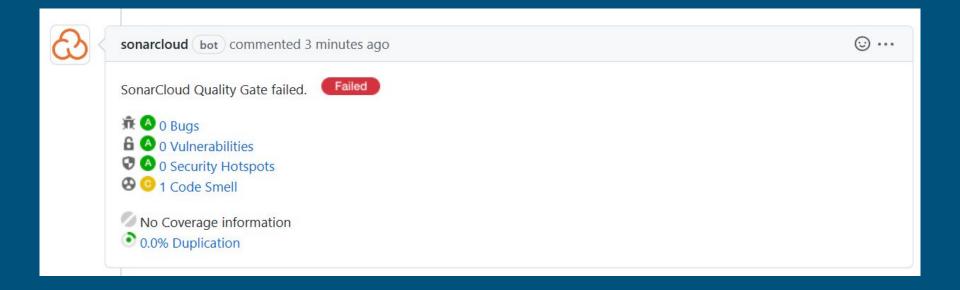
		✓ Code.js - 1 issue

                                                                                                                                      fs.exists(filename, function(exists) {
                                                               sendFile(filename, response);
         Testing a collection size for >= 0 wi...
                                                                                                                                        if(!exists) {
                                                             } else {
                                                                                                                                      var fileStream = fs.createReadStream(filename);

✓ contentScript.is - 1 issue

                                                               const indexHtmlPath = join(filename, 'index.html')
                                                                                                                                      fileStream.pipe(res);
         Setting targetOrigin to "*" in postM.
                                                                                                                                      fileStream.pipe(this.res);
                                                               if (existsSync(indexHtmlPath))
      ➤ standalone.js - 1 issue
                                                                  sendFile(indexHtmlPath, response);
         III Signature mismatch: the implement...
                                                                } else {
                                                                  response.writeHead(404);
                                                                                                                                                                                          Feedback
                                                                                                                                  Share issue
                                                                                                                                                 Ignore issue
                                                                  response.end();
```

Continuous Integration



### Continuous Integration

```
PS C:\Users\AndyDouglas> docker run --rm -t --network host owasp/zap2docker-stable:2.12.0
zap-baseline.py -t http://localhost:3000 -s_
```

Continuous Integration

Continuous Delivery or Deployment

#### **Active Defense**

# Automate Application Security with CI/CD

Part 1: Dynamic Scans for <u>prevention</u>

#### Part 2: Active Defense for <u>detection</u>

# Goal: Actionable Security Improvement

#### Hi, my name is Andy Douglas

- Long-time CodeMash attendee, first-time speaking
- Full Stack Software Dev/Engineer > Architect > Engineering Manager
- Security...meh

#### Hi, my name is Mick Douglas

- First time CodeMash attendee
- Passionate about security
- Infosec Innovations, SANS Principle Instructor, IANS Research Faculty

## Part 1: Dynamic Scans for <u>prevention</u>





# SAST - quick word

mendati

#### Integrate SAST w/ IDE + CI

Popular Tools: Snyk, Checkmarx, SonarQube/SonarCloud

# Dynamic Application Security Testing (DAST)

Merge into main

CI build runs
(hopefully with SAST)

CD build runs
to deploy to env X

Smoke tests
and DAST

#### 4 Labs

#### DAST Lab

# DAST Lab: deploy vulnerable web app

DAST Lab: Automate a leading DAST tool

# DAST Lab: Learn how to include DAST in your pipelines

## DAST Strengths

#### DAST Weaknesses

nendatio.

#### DAST: CD and/or scheduled

Popular Tools: ZAP, StackHawk, Burp Suite, Astra Pentest, etc.

#### Part 2: Active Defense for detection





#### Part 2: Active Defense for detection FTW!!







Traditional Defense == Passive

Traditional Defense == KNOWN

Active Defense == Passive & Active

# Shift focus/effort to higher reward

Attackers have predictable paths

Active Defence at each phase

#### Recon: Ports

## Honey Port

#### DEMO: Honey Port

# Privilege Escalation: session tokens

#### Honey Tokens

#### Demo: Honey Tokens

#### Strategy: Defense Options

Watch and learn?

## Random error response?

#### Firewall

#### QoS

#### Demo response options

### Security != Hard/Expensive

## Security as Functional Requirement

#### Security + CI/CD is good

#### LAB IT UP!!