

# Pen Testing: Reporting

---

## Documenting Vulnerabilities



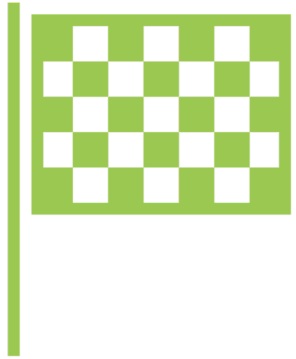
**Gavin Johnson-Lynn**

Software Developer, Offensive Security Specialist

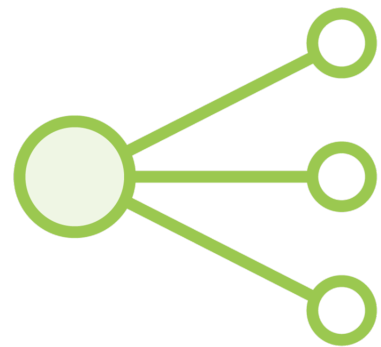
@gav\_jl   [www.gavinjl.me](http://www.gavinjl.me)



# In This Course



**The goal: a good pen test report**



**Report efficiently**



**Covers various test types – web, infrastructure, mobile etc.**



# Overview



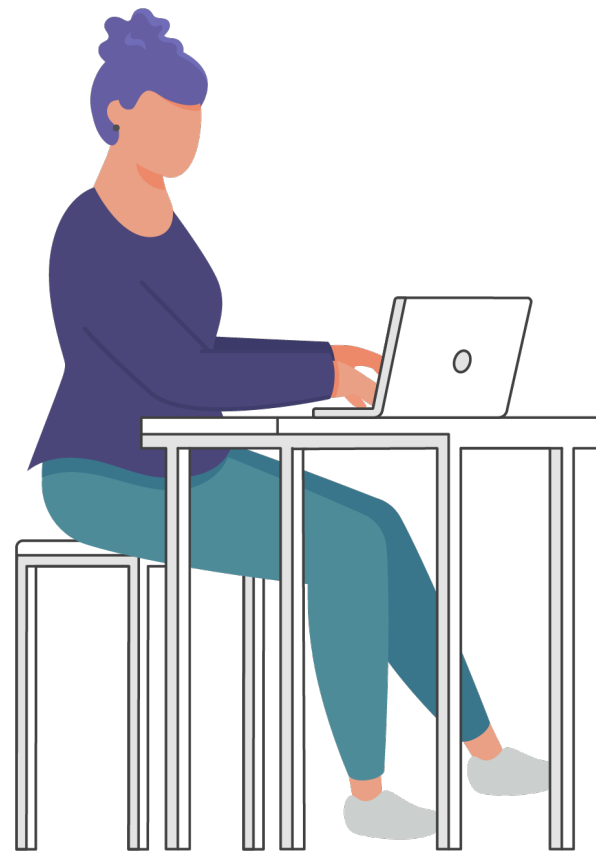
## **Document vulnerabilities**

- Main part of a report

**What information do we get across?**

**Who are we talking to?**





**Kim: Pen Tester**



**Chris: I.T.  
Manager**



**Vincent: Senior  
Security Engineer**



# I.T. Manager: Chris



**Assess network security posture**

**Do we need more security focus?**

**How difficult is it to fix this?**

**What is the risk if it isn't fixed?**



# Vincent: Senior Security Engineer



**Understand technical vulnerabilities**

**How do the vulnerabilities work?**

**How do we replay attacks?**

**How do we know when something is fixed?**



# Stakeholder Viewpoints



## **Non (or less) technical**

- Assess business impact
- How much risk?
- High level mitigations

## **Technical**

- Detail vulnerabilities
- Fix or mitigate

# High Level Goals

**Detail the  
vulnerabilities**  
**Mostly technical**

**State the  
mitigations**  
**What should the  
response be,  
mostly technical**

**Highlight the risks**  
**Aimed at the  
business,  
non-technical**





# Kim: Pen Tester



**Writes reports her way**

**Keeps within Globomantics guidelines**

**Meets high level report goals**

**Works to communicate effectively**

**There is no single way to do this**



# Report Structure



## **Details about the test**

- What's tested and why

## **Useful information**

- How the report works

## **Summaries**

- Executive summary
- Finding summary

## **Findings**

## **Appendices**

- Additional information

# Findings / Vulnerabilities

**Documented vulnerability is a finding**

**Enough information to fix the vulnerability**

**Targets the technical team**

Don't assume level of security knowledge

More detail is good

Use web links

**How important is each finding?**





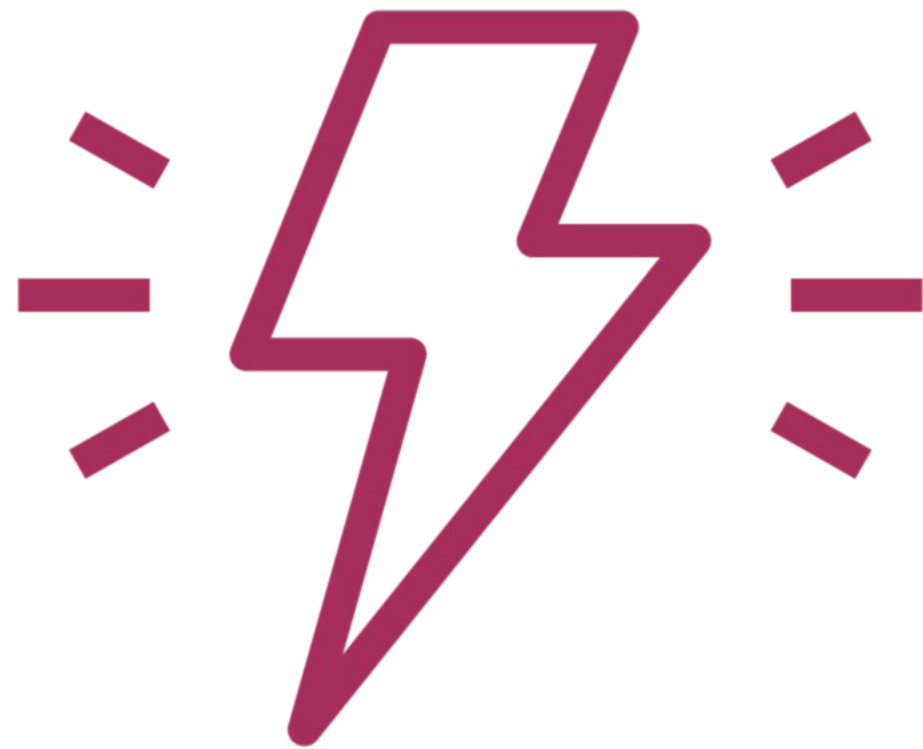
# What Goes into a Finding?

Think “High level goals”:

- Detail the vulnerabilities
- State the mitigations
- Highlight the risks



# Non-technical Details



## Title

- Less technical is better
- “Weak Stream Ciphers in Use”
- “Weak Cryptography in Use”

## Severity rating

- CVSS, DREAD
- Assists with transparency

## Risk score

- Likelihood \* impact

# Technical Details

## Description

Understand the vulnerability class

## Detail

How a vulnerability presented

How to find and exploit

Could you repeat this?

## Remediation

One or more fixes

## Further reading

Think education as well as remediation



# Summary



## High level goals

- Detail vulnerabilities
- State mitigations
- Highlight risks

## Transparency

- Helps with trust

## Readability

No single “best” way to do this

