

# Ensuring Quality

---



**Gavin Johnson-Lynn**

Software Developer, Offensive Security Specialist

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



# Overview



**Done what and why**

**Now look at how**

**Common mistakes**



# Kim: Pen Tester Viewpoint



**Enjoys the technical challenge**

**Few people enjoy writing reports**

**Get vulnerabilities fixed!**

**Communication is important to pen testing!**

**The report conveys something about you**

**Mistakes in the report = mistakes in the test?**



People will make assumptions  
based on what they read in  
your report!



# Quality Assurance (QA)



**Does it meet specific requirements?**

**Performed by another person**

**You will make mistakes**

**Aim for very few issues**

**QA requirements**

- High-level goals
- Accuracy
- Clarity
- Conciseness

# Accuracy

**Technically correct**

**Evidence shown**

**False positives?**

Wasted remediation

**Risk scores?**

Should reflect this instance  
of the finding (not the worst case)

Evidence!





# Accuracy

## **Typos**

- Spell check

## **Hyperlinks**

- Do links still work?

**Mention version numbers where appropriate**

# Clarity



## **Convey unambiguous messages**

- What are the vulnerabilities?
- How do we fix them?
- What are the risks?

## **Don't assume a high level of knowledge**



# Improving Clarity

## **Explain abbreviations**

“Denial of Service (DoS)”  
“(DoS)” after the first time

## **Explain domain specific words**

Explain and use links

## **Step by step walkthroughs**

Include images  
Copy and paste commands

## **Write consistently**

Important if more than 1 tester



# Conciseness



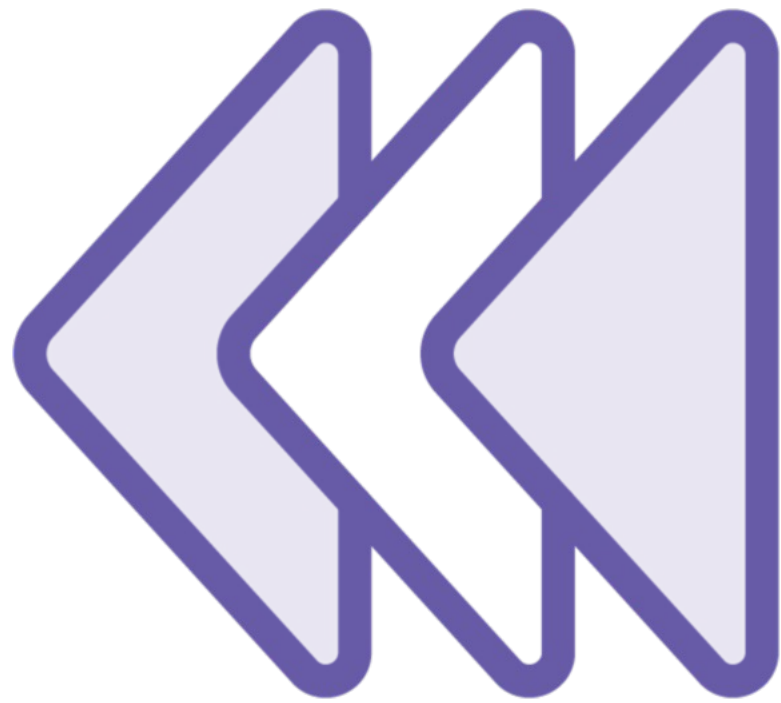
**Readers want a concise report**

**Accuracy, clarity and detail = lots of words**

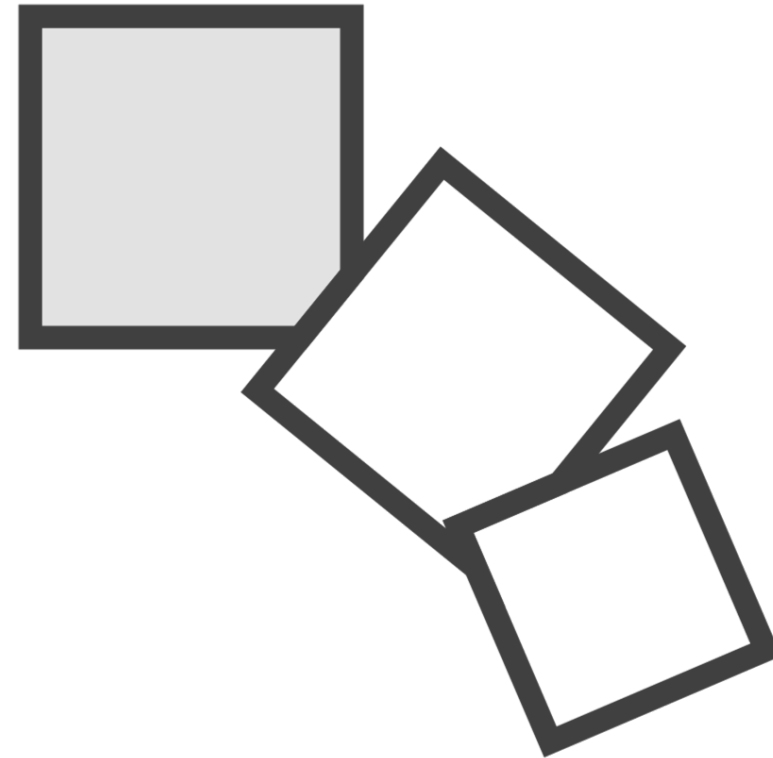
**Needs a balance**

- Enough information
- Not too much text

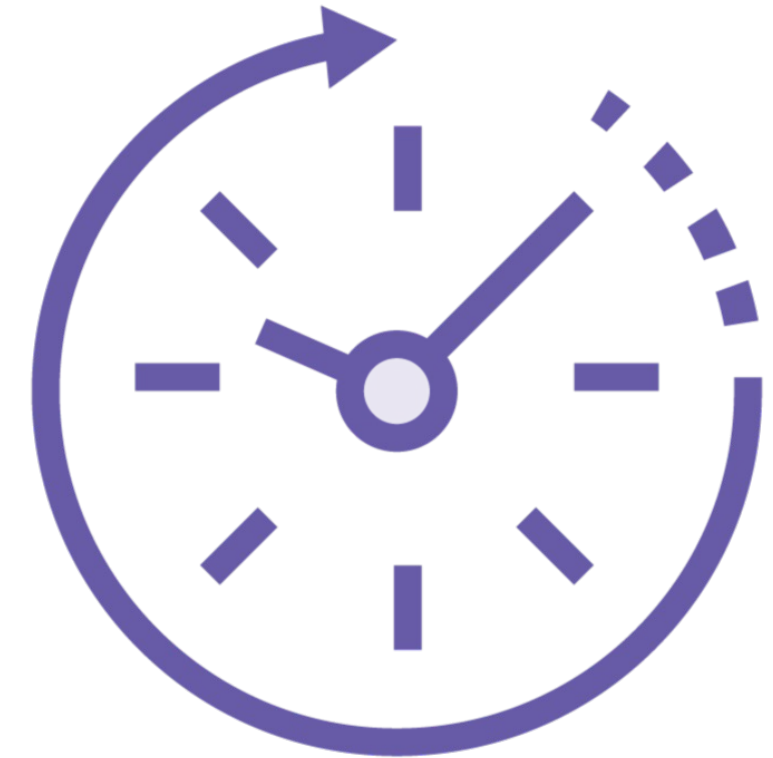
# Use Past Tense



**A report describes  
the past**



**Things could change  
since the report**



**The report is for a  
point in time**

“A port scan on 192.168.88.18  
shows port 445 **is** open...”

“A port scan on 192.168.88.18  
shows port 445 **was** open...”



# Avoid Personal Pronouns



**Avoid references to people**

**Acceptable when naming test team**

**Avoid I, we, you, he, she, us...**

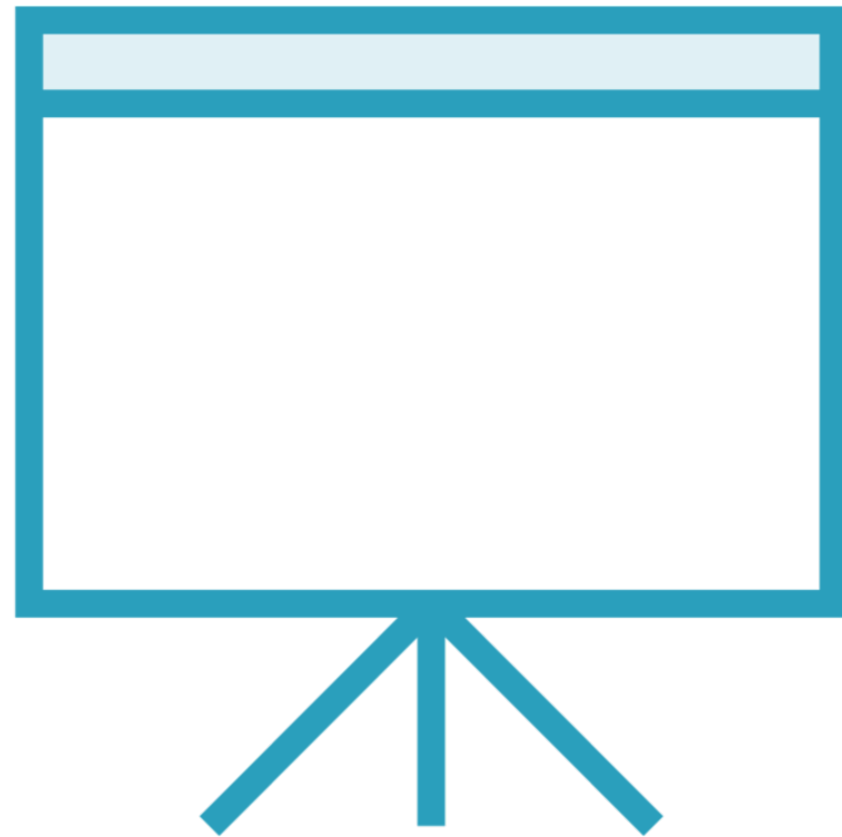
“**We** found a vulnerability...”

“The **team** found a vulnerability...”

“A vulnerability was found...”



# Report Presentation



## **Assists knowledge transfer**

- Different medium
- May be more useful to some people
- Allow questions

## **Not all testers will like presentations**

- It is a learning opportunity
- Helps to improve future reports

# Presentation Structure

**Often a report walkthrough with questions**

**What does the customer want?**

Focus on specific findings?

Non-technical focus?

Help the case for more budget?

**Include both stakeholders?**

Non-technical first

Benefits both stakeholders

Allows non-technical people to leave early





# Presentation Goals

**Same as report goals**

**Detail vulnerabilities**

Talking can be better than hyperlinks

**State mitigations**

Which are best for us?

**Highlight risks**

Interpret scores



# Common Problems: Conciseness

**How long should a report be?**

It depends!

Short report is perhaps 20 pages

**Don't go too short either!**

Use detail where important

**Templates help**



# Common Problems: Accuracy



## Lack of QA

- False Positives
- Wrong company name!
- Out of scope findings
- Wildly inaccurate risk / severity
- Incorrectly state attacker abilities
- Duplicate findings
- Typos and spelling mistakes

# Common Problems: Clarity

**Screenshots where text is better**

**Difficult to repeat findings**

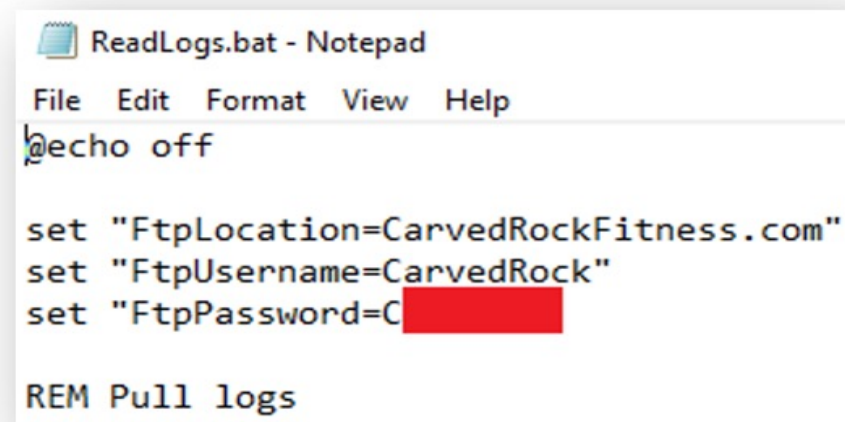
**No attempt to chain  
vulnerabilities**

**Missing image borders**



# Using Borders on Images

The file contained clear text credentials. The internal team confirmed that these were credentials for the production website. This allowed read access to logs, which could contain further sensitive information and be useful to an attacker.



```
ReadLogs.bat - Notepad
File Edit Format View Help
echo off

set "FtpLocation=CarvedRockFitness.com"
set "FtpUsername=CarvedRock"
set "FtpPassword=C[REDACTED]"

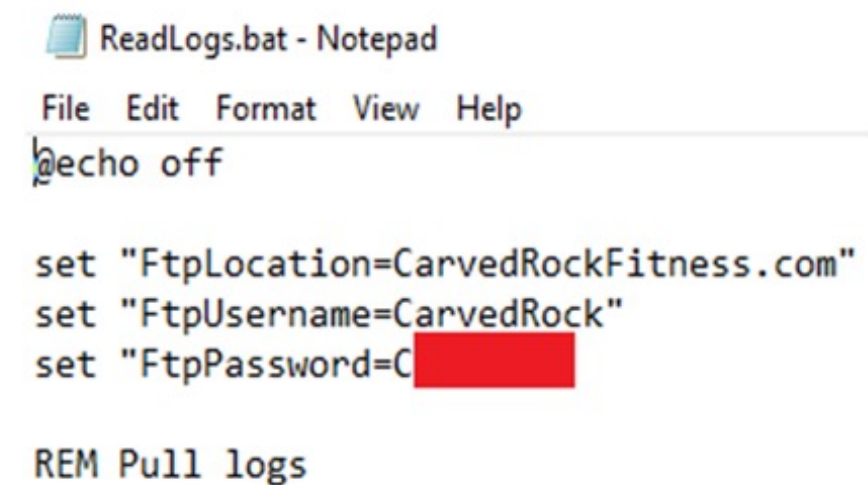
REM Pull logs
```

*Figure 5 Exposed Credentials in File Share*

As this was out of scope, no further testing was performed using those credentials.

## Border Shadow

The file contained clear text credentials. The internal team confirmed that these were credentials for the production website. This allowed read access to logs, which could contain further sensitive information and be useful to an attacker.



```
ReadLogs.bat - Notepad
File Edit Format View Help
echo off

set "FtpLocation=CarvedRockFitness.com"
set "FtpUsername=CarvedRock"
set "FtpPassword=C[REDACTED]"

REM Pull logs
```

*Figure 5 Exposed Credentials in File Share*

As this was out of scope, no further testing was performed using those credentials.

## No Border



# Summary



## Creating quality reports:

- It's tough!
- Lots to consider
- Time consuming
- Critical to a good pen test

