

# Streamlining the Process

---



**Gavin Johnson-Lynn**

Software Developer, Offensive Security Specialist

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



# Overview



**Using templates**

**Using automated solutions**

**Further reducing effort**



# Kim: Templates



**Minimum mistakes**

**Minimum time / effort**



# Template Areas

**Complete report structure**

**Individual findings**



# Templates: Static and Dynamic

## **Areas that stay the same (static)**

Rarely change between pen tests

Generic information

## **Areas that change (dynamic)**

Specific to a pen test



# Static and Dynamic Areas



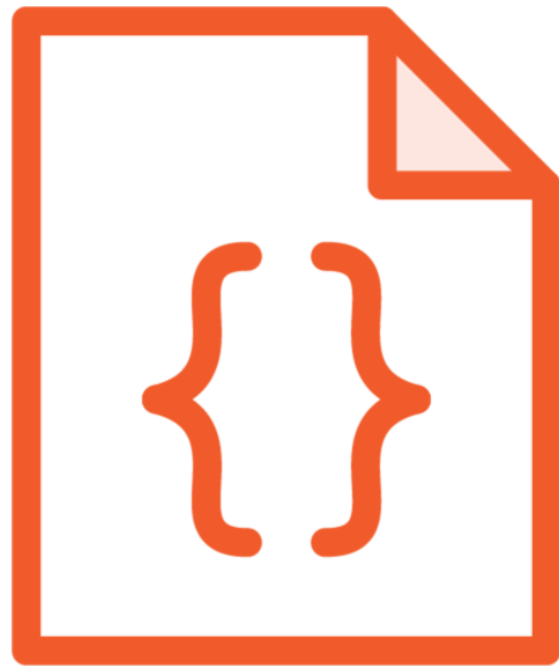
**Static / placeholders**

**Dynamic areas:**

- Customer name
- Scope
- Executive summary
- Appendices

**Be very clear which areas are dynamic!**

# Templating: Important Points



## Placeholders

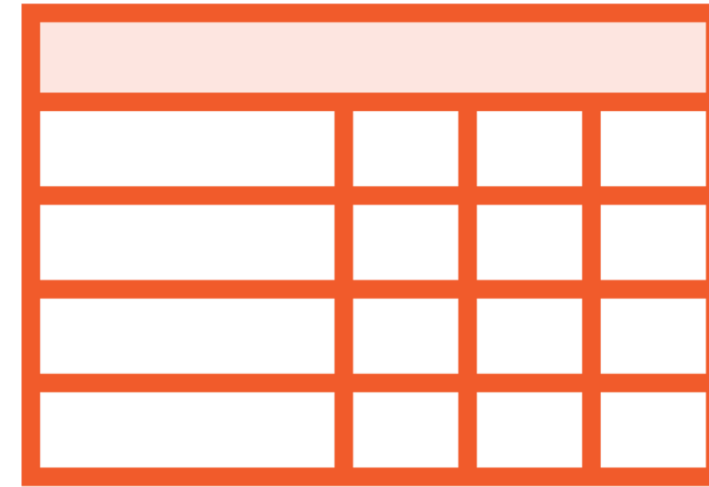
{{Braces}}

Highlighting

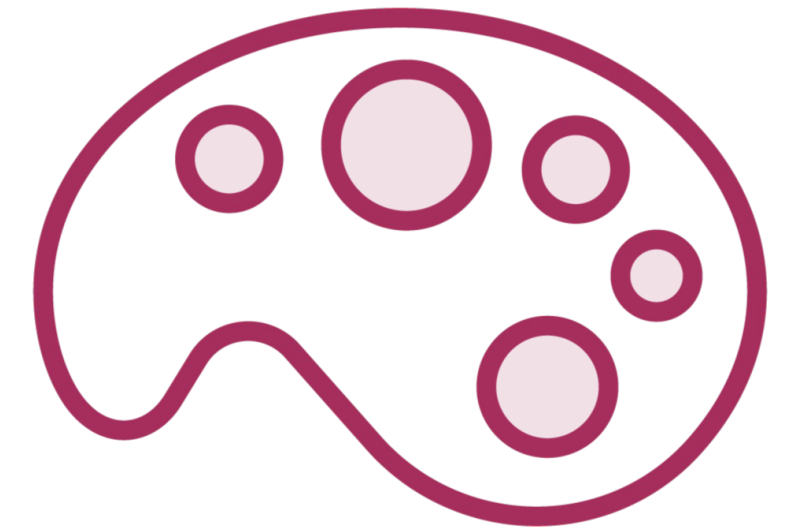


## Stock phrases

Accurate, clear and  
concise takes time



## Graphs



## Colors



# Templating: Findings



**Give thought to arranging templates**

**Templates in the format you'll use them**

- Better for copy and paste

**Use folders**

**Naming conventions on file names**



# Using Templates Wisely

**Save time /  
reduce errors**

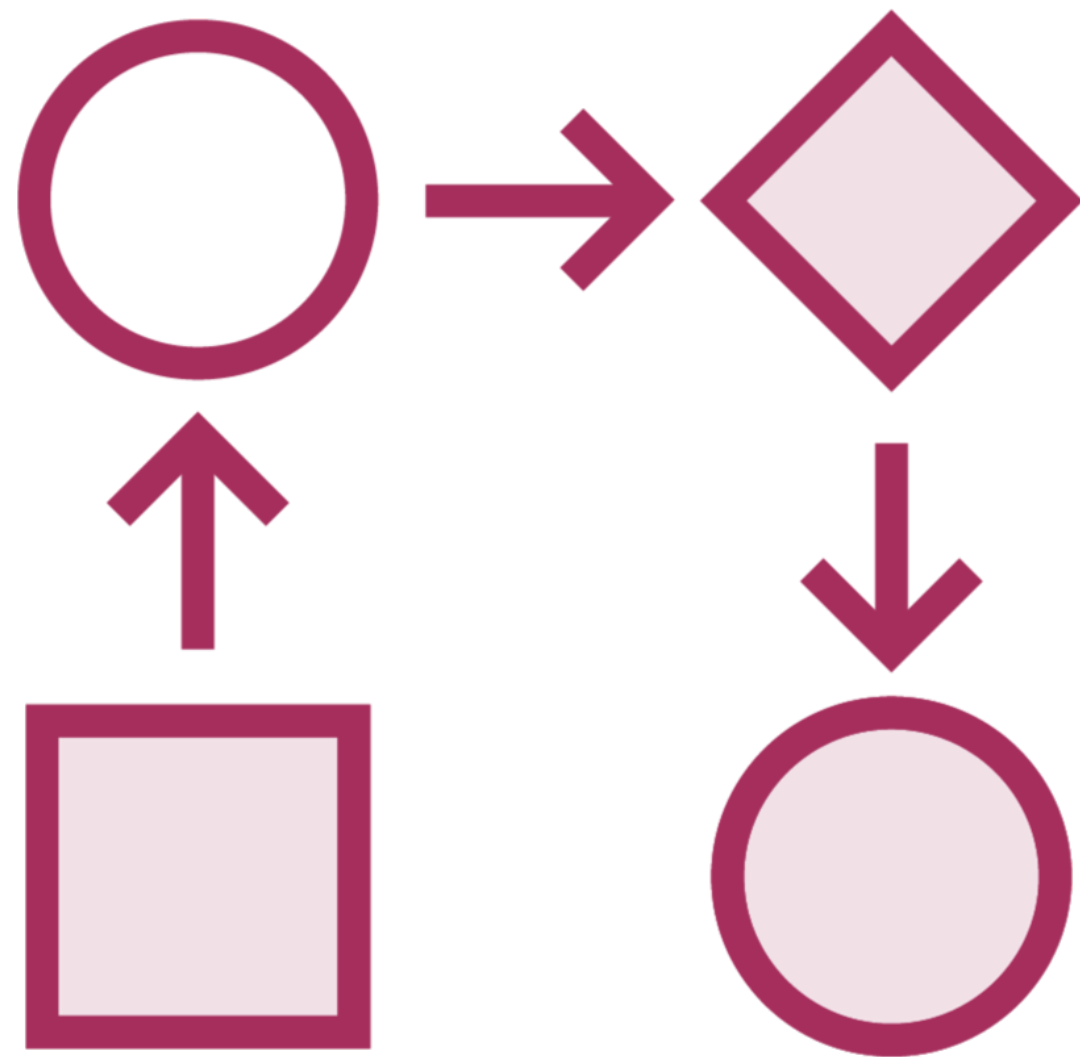
Be sure to do both!

**Easy to see where  
to do things**

**Hard to forget to  
do things**



# Automated Solutions



**Both free and paid solutions available**

## **PwnDoc**

- Open source
- Arrange templates
- Produce report

# Demo



**Using PwnDoc**

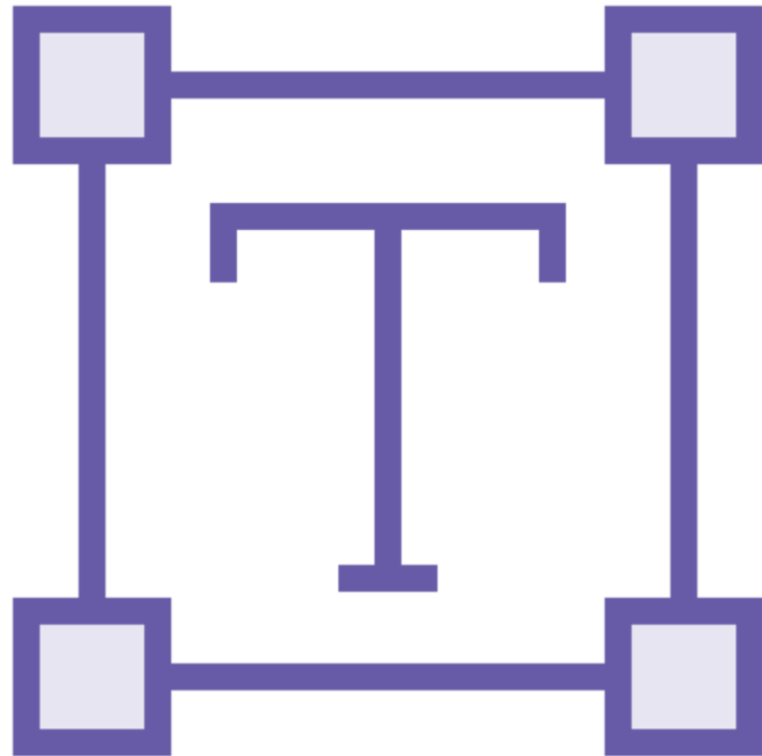
**Carved Rock pen test report**

**Report and finding templates**

- Use of placeholders



# Avoid Complicated



**Complicated  
formatting / fonts etc.**



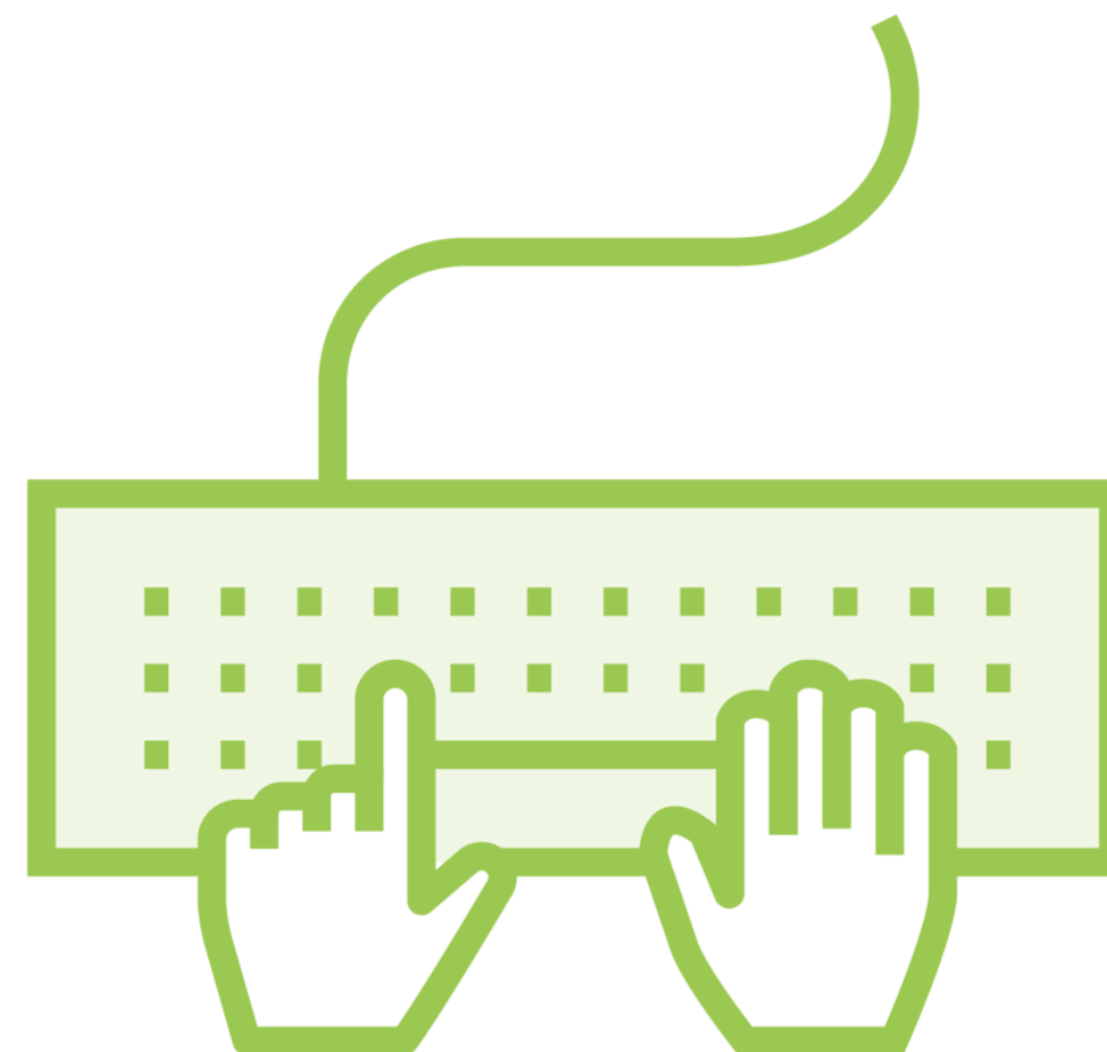
**Saves time**



**Less mistakes**

# Documenting Vulnerabilities

**Document as you find them**  
**Resist the urge to document vaguely!**  
**Get details as you find things**  
**You won't regret it!**



# Multiple Testers



**Adds complication**

**Documenting findings as you go**

- Helps other testers

**Good communication is difficult**

- Takes effort
- Worth it

**Automation like PwnDoc helps**

# Module Summary



**Refine the reporting process**

**Re-use wording**

**Automation doesn't fix all problems**



# Course Summary



## **Reporting in depth**

### **Reporting goals**

- Detail vulnerabilities
- State mitigations
- Highlight risks

### **Consider stakeholders**

- Technical
- Non-technical





## More Information

### Communications for Technologists

Learning Path



# Questions or Comments



**Course Discussion**



**Twitter: @Gav\_JL**

