

# Usable Security

## Current research areas



PV226 Seminar LaSArIS later  
Thursday 30th of December 2023

Katarína Galanská, [galanska@mail.muni.cz](mailto:galanska@mail.muni.cz)



# Error on line 42

```
41      });  
42  
43      if (includ
```

imgflip.com



Birthday\*:

January ▾ 1 ▾ 2017 ▾

Primary phone number\*:

0 ▾ 0 ▾ 0 ▾ 0 ▾ 0 ▾ 0 ▾ 0 ▾ 0 ▾

- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9

Secondary phone number:

0 ▾ 0 ▾ 0 ▾ 0 ▾ 0 ▾ 0 ▾

Fields with asterisks are required. Make sure your details are correct and review your application and will email you on the progress. Make sure you have read and understood the terms and agree to reject your application in cases outlined in terms and agree

Do you want  
to cancel it?

Yes

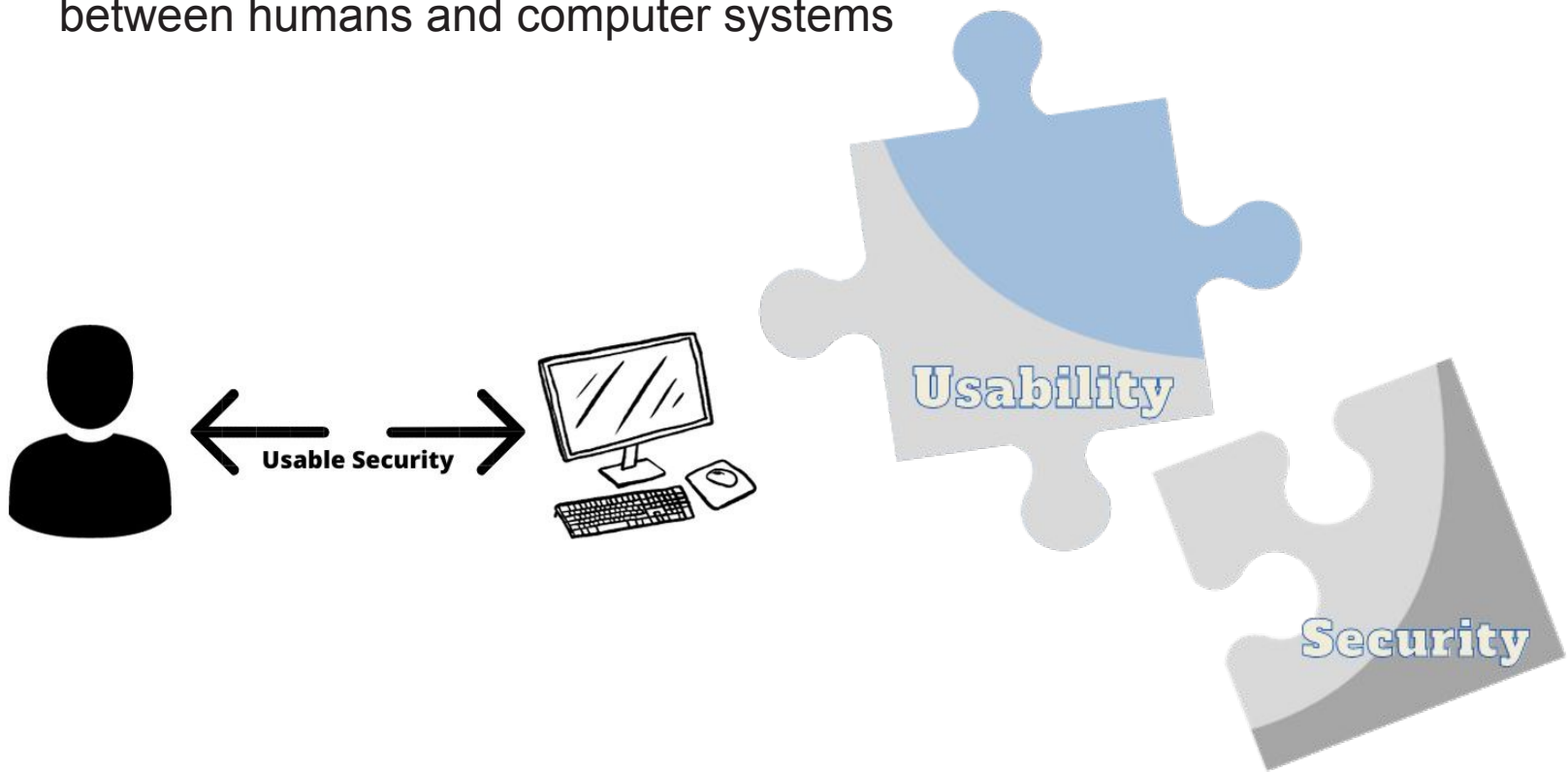
Cancel





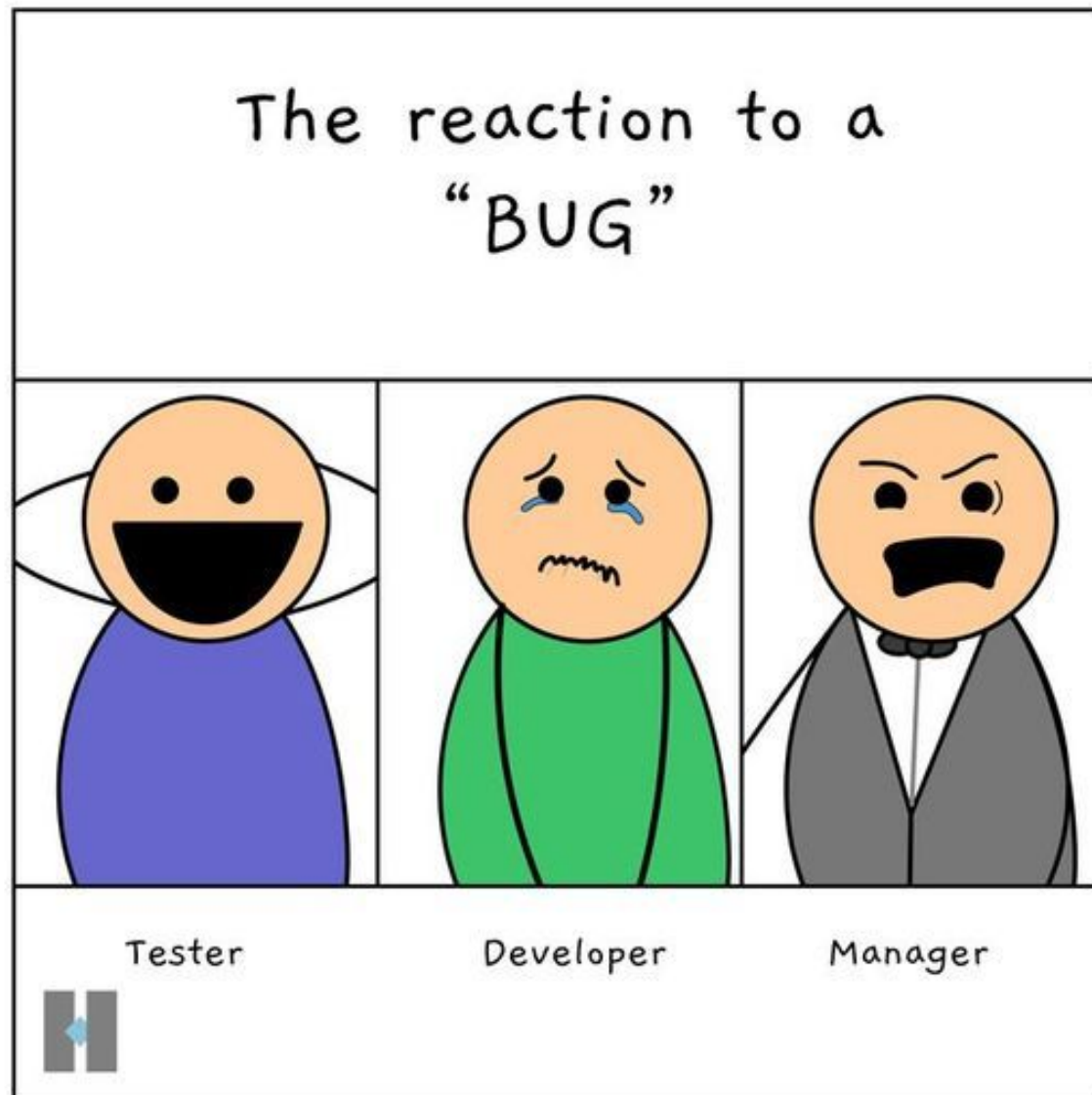
# Usable Security?

- a type of security that protects against threats arising from interactions between humans and computer systems



# Mastering penetration testing reports

Current state of the research





# Motivation

**Performing the test**



**Writing the report**



**Presenting the report**





# Research Questions

## RQ #1

What are IT professionals' perceptions of penetration testing reports?

## RQ #2

Where are the gaps in penetration testing report from the usability perspective of an IT professionals?

# Workshops (data collection)

## Prague

- Collaboration with AEC
- Workshop + Survey

## Tallinn

- Collaboration with Cybernetica
- CHESS Project
- Workshop + Survey + 1 Focus Group

## Tartu

- Collaboration with Cybernetica
- CHESS Project
- Workshop + Survey + 2 Focus Groups

# Demo

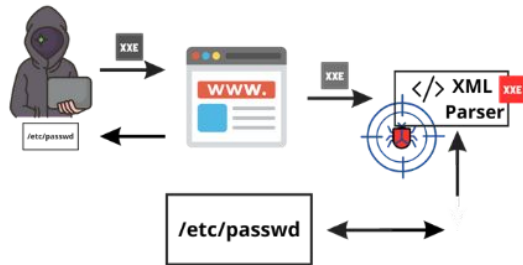
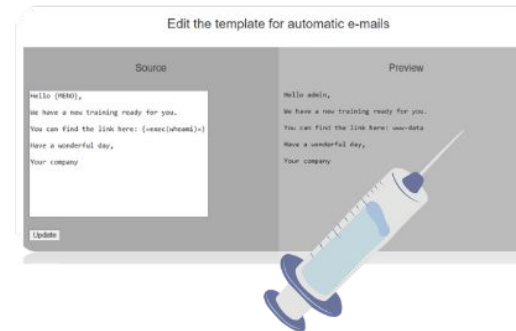


```




Stack Trace
Error Message:
An error occurred in their /var/www/html/trainings.php at line 15.
Stack Trace:
#0 /app/trainings.php(15): thirdFunction()
#1 /app/trainings.php(19): secondFunction()
#2 /app/trainings.php(23): firstFunction()
#3 {main}
    
```

```

Request  Response
[Raw] [Hex] [Render] [v] [≡]
1 HTTP/1.1 200 OK
2 Date: Sat, 20 May 2023 11:34:21 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 Last-Modified: Sat, 20 May 2023 07:50:22 GMT
5 ETag: "1e-5fcb66d399a"
6 Accept-Ranges: bytes
7 Content-Length: 30
8 Connection: close
9 Content-Type: text/plain
10
11 User-agent: *
12 Disallow: /log/
    
```



# Example finding

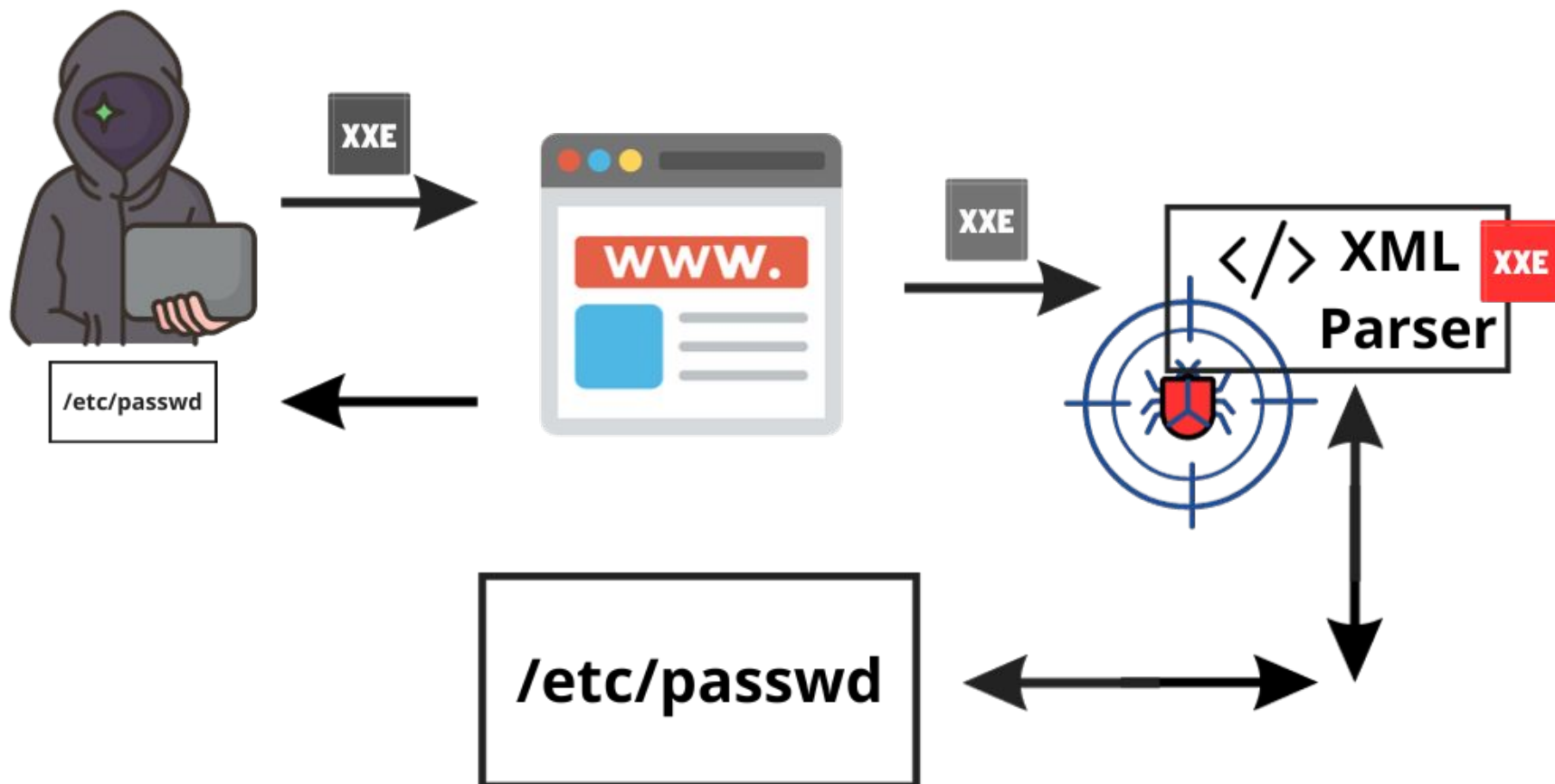
SEVERITY	PROBABILITY	REMEDIATION EFFORT
 HIGH	 MEDIUM	 MEDIUM
OWASP category:	OTG-INPVAL-008 - Testing for XML Injection	
Affected systems:	<a href="https://vulnerable.lms/process">https://vulnerable.lms/process</a>	
Attachments:	\Attachments\	

## Finding

XML External Entity arises when a user supplied input is processed with a weakly configured XML parser. This way an attacker might be able to introduce a crafted XML file in which way he could potentially:

- access resources on the server with privileges of the application user
- use application as a proxy server and retrieve sensitive content from any web server that the application can reach
- exploit vulnerabilities on back-end
- test for existing IP addresses (including internal IP addresses) and scan for open ports
- cause a denial of service

As a Proof-of-Concept we present following images that show inject location and then extracted data from the server.



# Data analysis



589,141

Views

78,791

CrossRef  
citations to date

413

Altmetric

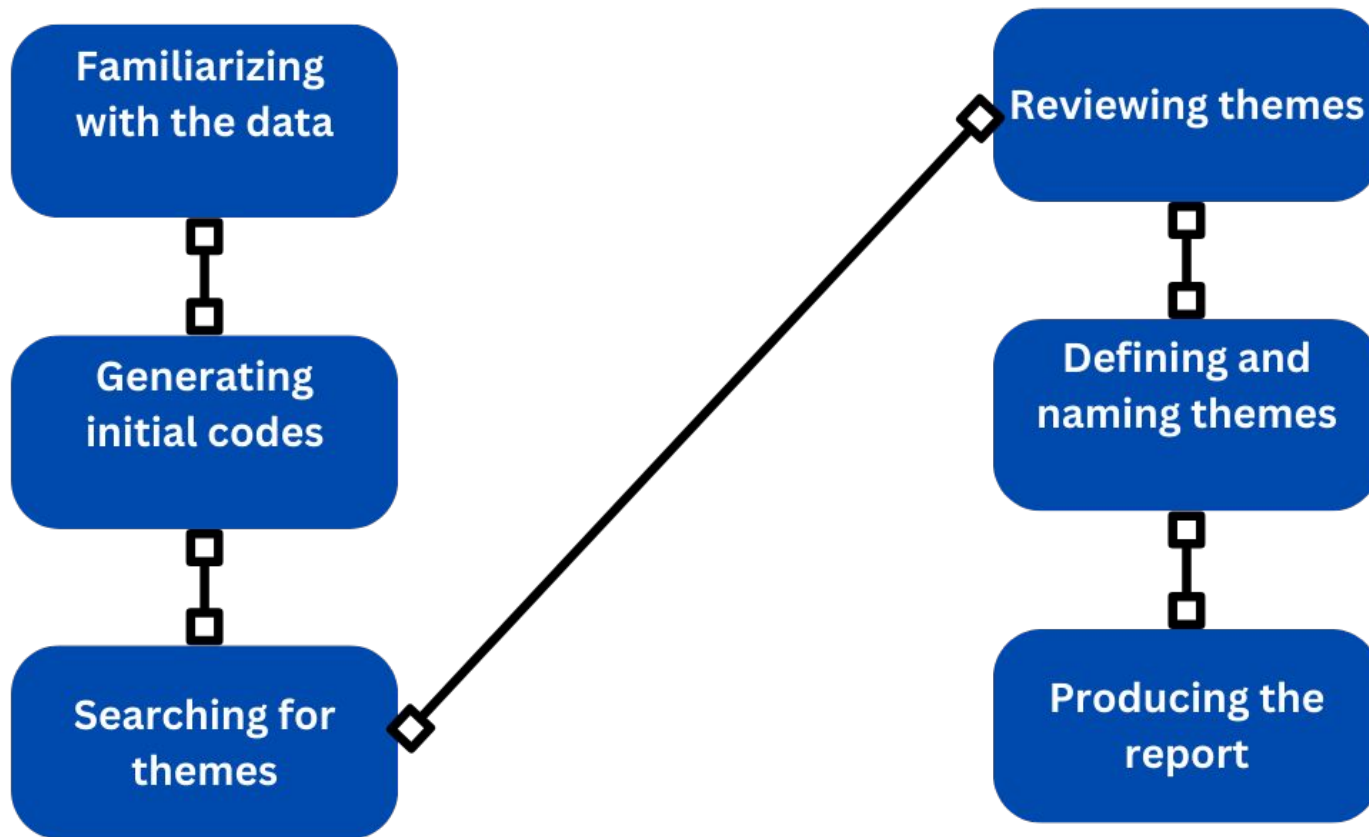
Original Articles

# Using thematic analysis in psychology

Virginia Braun & Victoria Clarke

Pages 77-101 | Published online: 21 Jul 2008

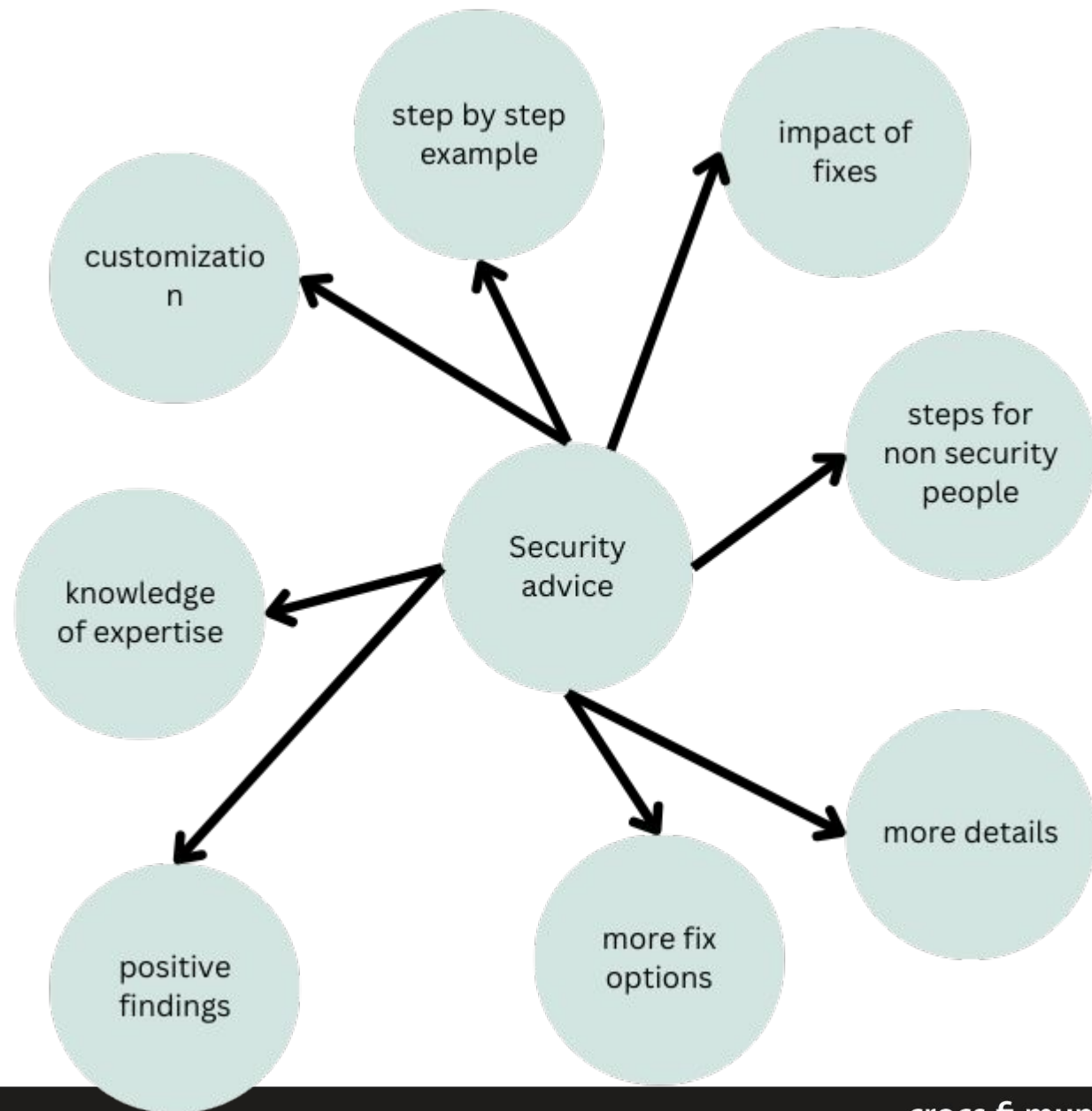
Quote Cite this article <https://doi.org/10.1191/1478088706qp063oa>



# Initial Codes

- **Initial list of ideas**
- **Most basic segments of raw data that can be assessed in meaningful way regarding the phenomenon**

# Security Advice



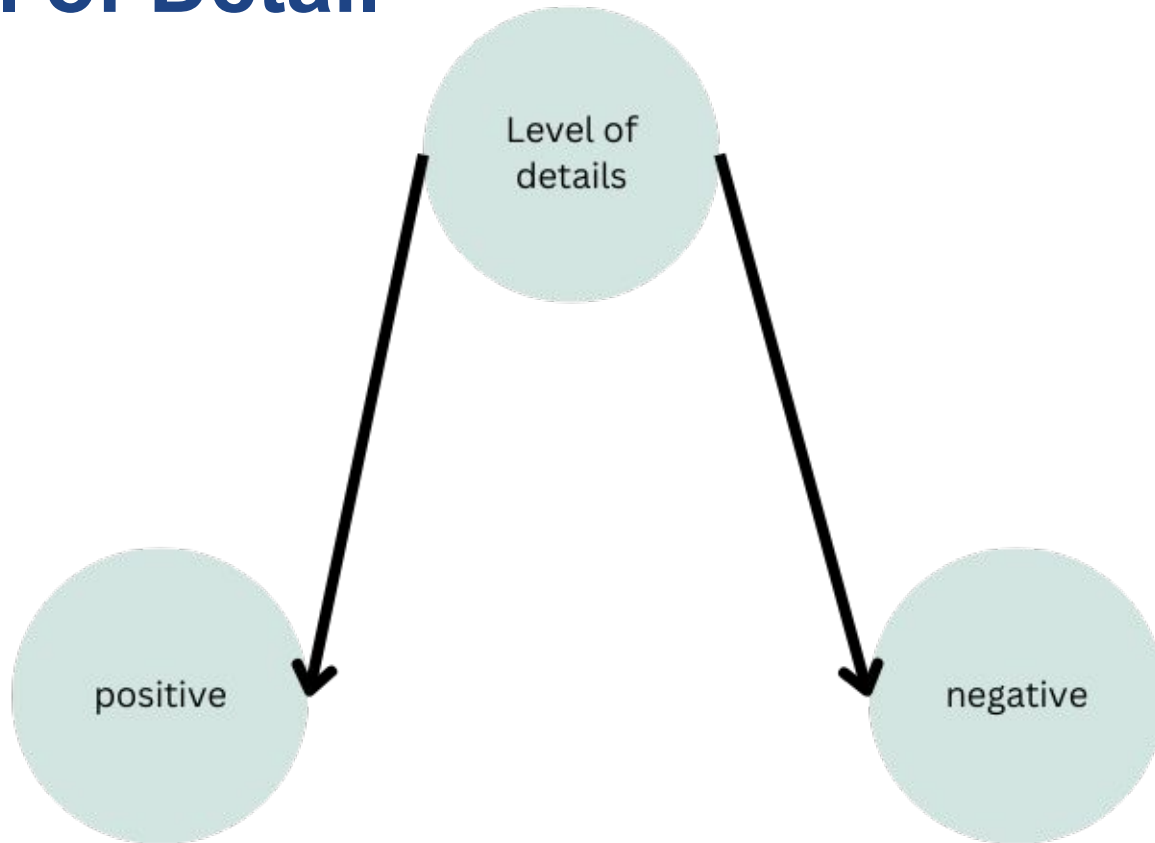
# Technical vs Managerial perspective

- *“Understand and Reproduce” .. said a technician*
- *“Do not put too much effort because you never know what's going to be the real solution” .. said a manager*
- *“Recommendations is just copy paste like common advice” .. said a former pentester, currently manager*
- *“Then the manager will say like, okay, we have to follow this, we have to do only this thing because our pen tester recommended it” .. said a technician*
- *“I can spend more effort on actually finding the vulnerabilities and not so much describing what the issues are.” .. said a technician*

# Risk

- “It should be well enough described that a company can... Like not a technical person can create a risk for the company. And mitigation”
- “But the pentesters, if they talk what they do, they just say that we are pentesters. We don't know how to defend. We know how to attack. And for me, it is a problem. Because I get the report and I have to defend my company, not to attack my company.”

# Level of Detail



# Level of Detail

- “I think details are good. If it can be detailed, that's better. But it needs more effort to put details down. “
- “Sometimes it is important to add also what were the preconditions before they started to do the test because it could differ somehow. And later you need to find the same situation to fix it. You can add something from the developer side. “
- “ Usually it's too little. This is not good. I think it depends on the organization. Organization has good quality of stuff like administrators, developers, network administrators. They can easily fix if they know their problem is. But if organization is small, they have only the outer support for their infrastructure. Then it's good to have a good explanation or...”
- “I think that depends on if the pen tester even knows how to fix it. So you can only recommend what you know. So if you're telling me, you know, of grid or something of fixing, the pen tester is not manufacturer or developed to software. “

# Positive Findings

- “I think they just would like to emphasize the positive findings of a scope just to have the repeatability ”
- “It is important for me how this pentesting has been done. Is it made manually or is made using you with some scanning tool, what is a method? “



## Remediation effort

- “I haven't seen in any reports the remediation effort. This is the first time I'm seeing this”
- “It's quite complicated actually because pentesters even don't know how to fix things. ”

# Importance of methodology

- These regulations that ask companies or organizations to do pen testing. They don't say what it means, and what they have to be, what a pen test has to find out. No, it's just, you need to have a tick that you have done it. Okay, which am I waiting? That's the weak point. “
- “I want to know if the testing methodology was changed or if I introduced a new vulnerability”

# Management needs n.1

- “How to translate them into my business process?” (findings)
- “Actually, the main problem is how to import these findings into our workflow management system. And if we get only the PDF file, then it's problematic. Because then there is a lot of hand work. ”
- “It should be machine readable. It doesn't have to be like PDF files, they can be sent, I don't know, through API or something”

## Management needs n.2

- “ And different regulatory markets have different requirements for penetration test risk assessments.”
- “ I want to have the reflection that he really understands what information I gave. That he draws himself some graph that is our threat model of our business process or something like that. ”

## Recommendation - negatives

- “We have had some examples that penetration report says that you need to fix this, like this. But it doesn't solve the problem, it creates another vulnerability.”
- “And so if I remove some feature, like this example, was remove this feature, I'm not the technical side. But if I remove this feature, how it affects my business process, again, it's a question. ”

## Obvious correlation

- People who usually work with PT reports and their understanding of recommendation in the workshop example

# Taking recommendation seriously



*“I have to prioritize putting together the criticality of the vulnerability and the resources we need for fixing that. Let's go with this, this, this. This one, we have to probably accept. For this one, just disconnect the f\*cking computer. And that's it. Problem solved.”*