Hack for Show Report for Dough

Part II

You do want to get paid for this, right?

1

Brian “BB” King

- Pentester at Black Hills Infosec, 6 yrs.
- Pentester at other places since 2008.

- Artist by education

- Part One is here: https://www.youtube.com/watch?v=NUueNT1svb8
  - But we’ll start with a recap

2

Your
Report
Matters MORE*
Than Your Hacking

* waaaay more.

3

How Can I Become a Better Tester?

- Certifications?
- Classes?
- CTFs?
- Set up scenarios in my labs?
- Write tools?
- Help others?

4

What does “Better” Mean?

- “Better” means, “closer to some ideal”

- So, what’s the ideal?
  - “That depends: what’s your goal?”
  - Why do you do this?

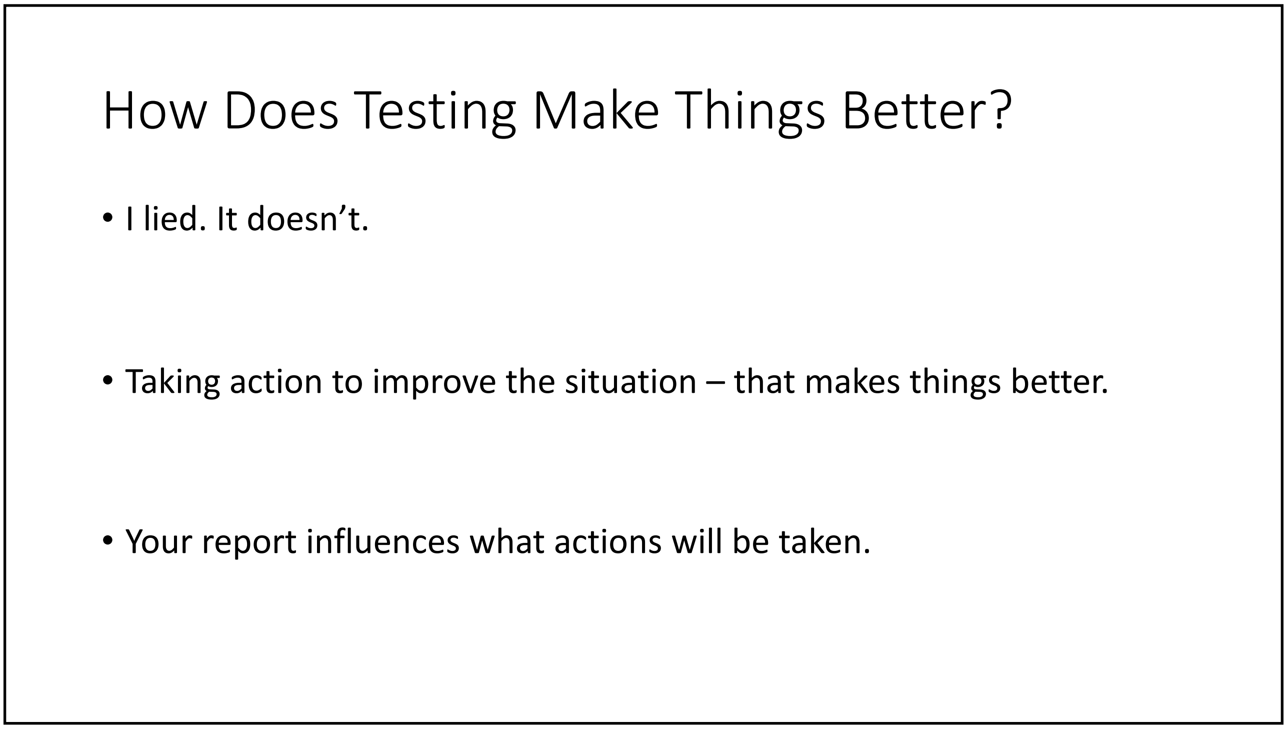
5

Testing Makes Things Better

“To make things better. Closer to the ideal.”

That’s why we do it.

6



How Does Testing Make Things Better?

- I lied. It doesn't.
- Taking action to improve the situation – that makes things better.
- Your report influences what actions will be taken.

7

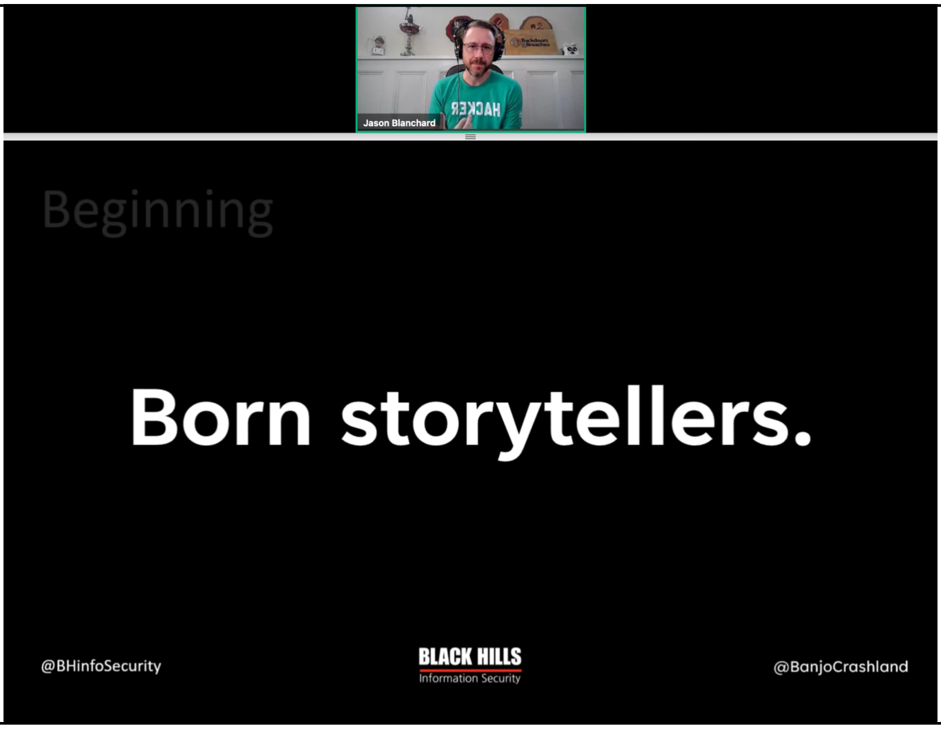
Your Report
is
Your Product

It's what you produce. It's what clients pay for. It's why they came to you.

Your test is a series of actions over time – dust in the wind.

What you *make* is *reports*.

8



Beginning

Born storytellers.

@BHinfoSecurity

BLACK HILLS
Information Security

@BanjoCrashland

9

Your Report is Your Product

- You are a storyteller.
  - (because you are human)
- But your report is not a novel. Not a short story, even.
- It’s scenes. Vignettes.
- A mystery, maybe, but not a crime story.
- There’s no central conflict, no rising action, no resolution, no villain.
- A series of side quests, maybe.
- You are a storyteller. Tell the story.

10

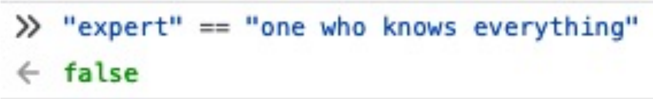
Never Just Copy-paste Scanner Output

- Believing that is halfway to seeing how important your report really is.
- How you present your information is MORE IMPORTANT than the information itself.
- You’re the expert, here.
  - Apply your expertise.
  - Be better than a scanner.

11

Scanners: There’s no Story There.

- Scanner output has no context.
  - Nothing but “severity” to distinguish any thing from any other thing.
- Your vuln scanner is not an expert. It’s very dumb.
  - Super-fast, amazingly thorough, and wonderfully helpful, but still … not smart.
- Your *perspective* brings the *context*, which brings the *value*.
- <u>You</u> are the security expert.
  - Stay with me, here…
  - Your perspective, your experience, your spidey sense, your ability to see patterns and intuitively group similar things. That’s what “expert” means.



```
» "expert" == "one who knows everything"
← false
```

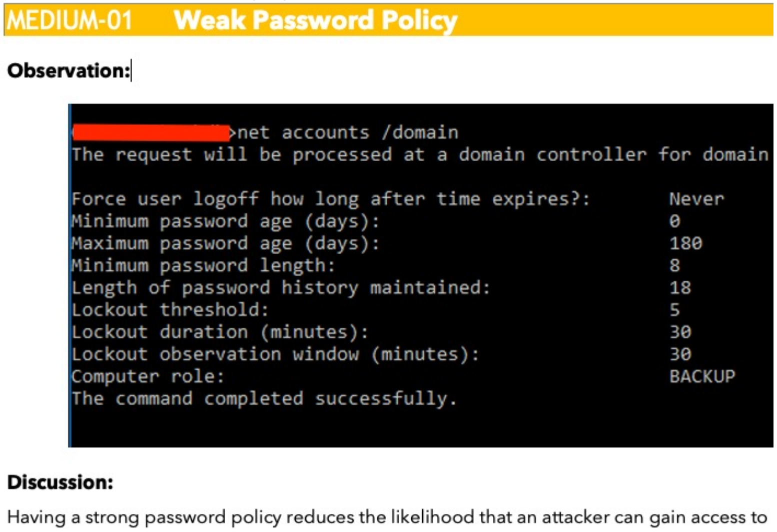
12

Things that are like copy-pasting from your scanner.

Facts without context are less helpful than facts with context.

13

2 Seconds: What Are You Supposed To Notice, Here?



MEDIUM-01 **Weak Password Policy**

Observation:

```
[redacted]>net accounts /domain
The request will be processed at a domain controller for domain

Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          180
Minimum password length:                              8
Length of password history maintained:                18
Lockout threshold:                                    5
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        BACKUP
The command completed successfully.
```

Discussion:

Having a strong password policy reduces the likelihood that an attacker can gain access to

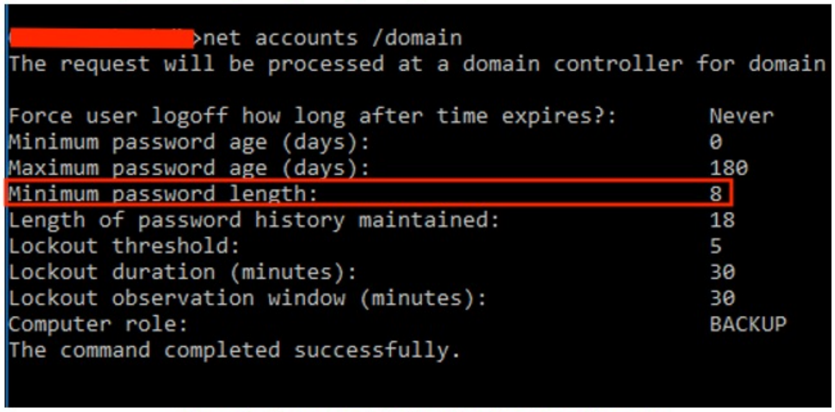
14

15

MEDIUM-01 Weak Password Policy

Observation:

The default password policy accepted passwords as short as 8 characters.



```
[redacted]>net accounts /domain
The request will be processed at a domain controller for domain

Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          180
Minimum password length:                              8
Length of password history maintained:                18
Lockout threshold:                                    5
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        BACKUP
The command completed successfully.
```

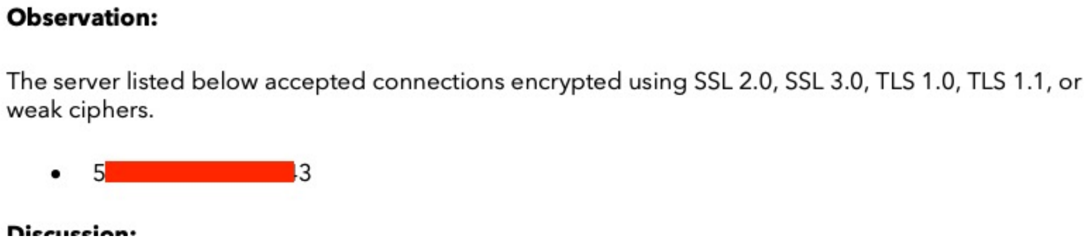
Domain Password Policy for Contoso Domain

Discussion:

Having a strong password policy reduces the likelihood that an attacker can gain access to

16

What Are You Supposed to Fix, Here?



Observation:

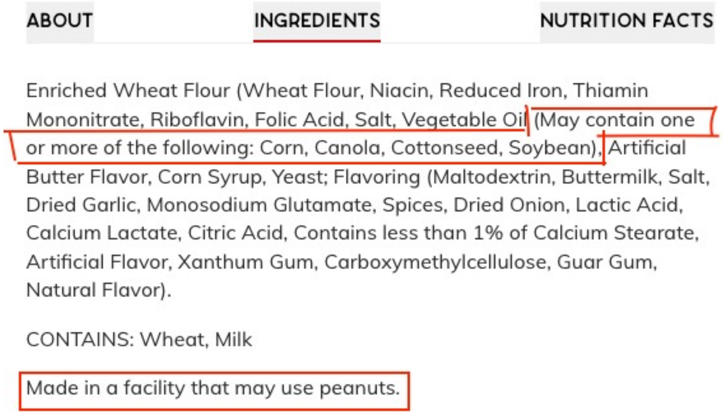
The server listed below accepted connections encrypted using SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, or weak ciphers.

- 5[redacted]3

Discussion:

17

May Contain One Or More of the Following



ABOUT INGREDIENTS NUTRITION FACTS

Enriched Wheat Flour (Wheat Flour, Niacin, Reduced Iron, Thiamin Mononitrate, Riboflavin, Folic Acid, Salt, Vegetable Oil (May contain one or more of the following: Corn, Canola, Cottonseed, Soybean), Artificial Butter Flavor, Corn Syrup, Yeast; Flavoring (Maltodextrin, Buttermilk, Salt, Dried Garlic, Monosodium Glutamate, Spices, Dried Onion, Lactic Acid, Calcium Lactate, Citric Acid, Contains less than 1% of Calcium Stearate, Artificial Flavor, Xanthum Gum, Carboxymethylcellulose, Guar Gum, Natural Flavor).

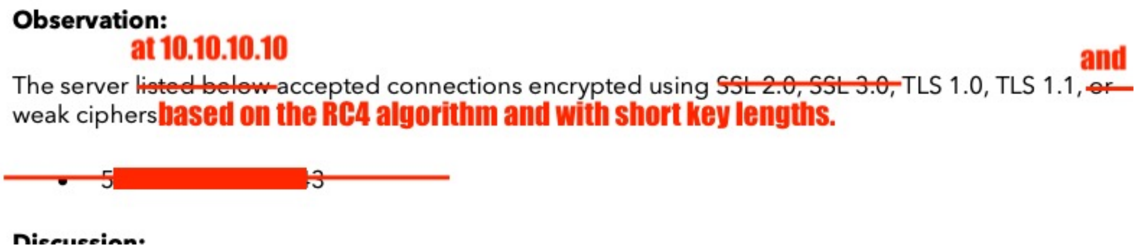
CONTAINS: Wheat, Milk

Made in a facility that may use peanuts.

https://dotspretzels.com/product/dots-homestyle-pretzels-16oz/

18

Say What You Saw.
Not What You Might Have Seen



Observation:

The server ~~listed below~~ at 10.10.10.10 accepted connections encrypted using ~~SSL 2.0, SSL 3.0,~~ TLS 1.0, TLS 1.1, ~~or~~ and weak ciphers based on the RC4 algorithm and with short key lengths.

- ~~5[redacted]3~~

Discussion:

19

Make It Obvious

Don’t just show: also tell.

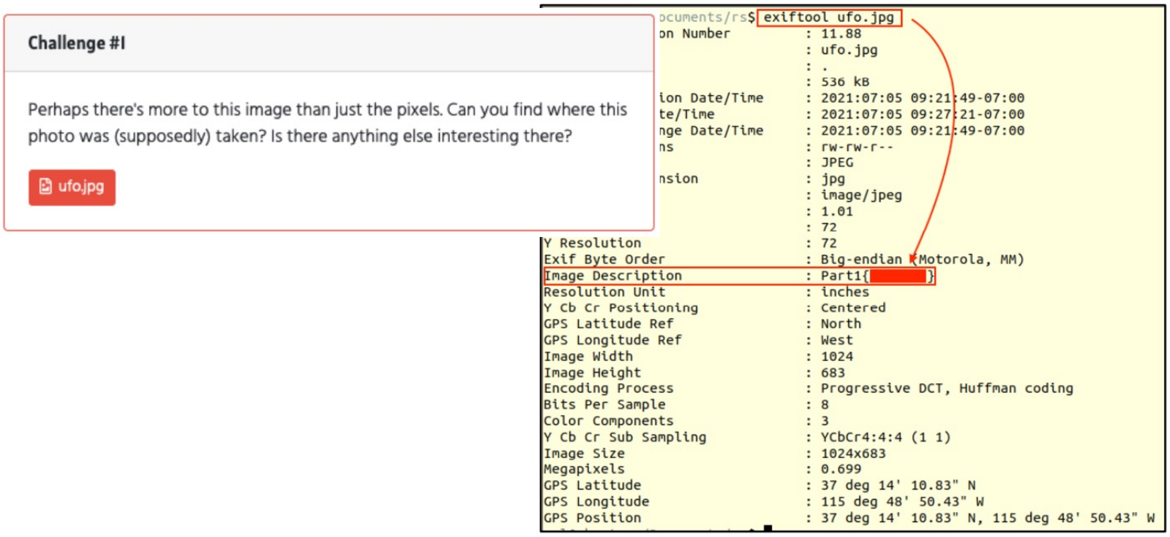
20

Not Mentioning Attacks that Failed

#2 most common failure in reporting.

“But how much should I write about a thing that didn’t work out?”

Show What Worked, Obviously



Challenge #1

Perhaps there's more to this image than just the pixels. Can you find where this photo was (supposedly) taken? Is there anything else interesting there?

```
ocuments/rs$ exiftool ufo.jpg
on Number                       : 11.88
                                : ufo.jpg
                                : .
                                : 536 kB
ion Date/Time                   : 2021:07:05 09:21:49-07:00
te/Time                         : 2021:07:05 09:27:21-07:00
nge Date/Time                   : 2021:07:05 09:21:49-07:00
ns                              : rw-rw-r--
                                : JPEG
nsion                           : jpg
                                : image/jpeg
                                : 1.01
                                : 72
Y Resolution                    : 72
Exif Byte Order                 : Big-endian (Motorola, MM)
Image Description               : Part1{[redacted]}
Resolution Unit                 : inches
Y Cb Cr Positioning             : Centered
GPS Latitude Ref                : North
GPS Longitude Ref               : West
Image Width                     : 1024
Image Height                    : 683
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:4:4 (1 1)
Image Size                      : 1024x683
Megapixels                      : 0.699
GPS Latitude                    : 37 deg 14' 10.83" N
GPS Longitude                   : 115 deg 48' 50.43" W
GPS Position                    : 37 deg 14' 10.83" N, 115 deg 48' 50.43" W
```

Alternative Part1 Solution (Redacted)

Less Obviously, Include What Did Not Work

- What if you have no serious findings after two weeks' work?
- Are you going to submit a report that just says, "Hey, good job."

"The tester analyzed the image
with `strings` and with `exiftool`
but found no sensitive information."

23

Use Your Words

- Two Audiences. Technical and Business.
- Technical Folks: "your friend, the smart sysadmin"
  - Knows computers & networks. Doesn't do pentesting.
  - They have to fix this stuff.
    - Help them DO THE FIX.
- Business Folks: smart people like you except they say "cyber" unironically because sometimes there's really not a better word.
  - Talk Policies and Procedures and Conflicting Priorities and Limited Resources.
  - They have to allocate resources to fix this stuff.
    - Help them PRIORITIZE and ASSIGN.

24

Being Too Technical In The Executive Summary

#1 most common mistake.

…because you must get out of your own head to do this well.

And that’s hard to do.

Good Testing! Exec Summary Needs Work

- A … device was found to be vulnerable to unauthenticated command line access. Successful exploitation of this vulnerability could lead to root access to the device.

- Maybe something like…
  - The testers found a device that allowed anyone on the ”lab” network to obtain administrative access with no password. Anyone on the lab network could trivially take full control of this device and any system attached to it.

Good Testing! Make it Actionable

- BHIS was able to obtain lsass.exe dump files from a number of systems and take the files offline to retrieve the plaintext passwords of logged-in users with Mimikatz.

- BHIS gained administrator-level access to five systems based on their use of a very weak, shared password. Using that access, the tester exported a sensitive portion of the systems’ RAM to an offline BHIS device. Running Mimikatz on this BHIS device revealed the cleartext password for every user who was logged in to those systems at the time, regardless of how long or random those passwords were.

27

How Would YOU Re-phrase This for Execs?

- **SMB Message Signing Disabled:** Systems were discovered that did not validate the integrity of authentication requests against file share related services.

28

Assume Competence

- Implement policies that require the use of strong network protocols. These vulnerabilities can be addressed easily and with appropriate directive, quickly.
- Review policies, procedures, and baseline configurations to ensure that unnecessary or insecure features and protocols are prohibited. Review business needs and current network architecture to ensure that exceptions are justified, documented, and set for periodic review.
  - Never say *just* or *simple* or *easily…*

29

So, How Does One *Get Better* At This?

- Are there tricks? Shortcuts? Automation?

30

How many therapists does it take to change a lightbulb?

yeah.

"It's *simple*: you can *easily* get better if you *just* practice."

31

Screenshots: Illustrate, Don't Decorate

- Accurate ("conforming to fact")
- Precise ("strictly distinguished from others")

- Accurate means it's helpful.
  - It adds something the words left out.
- Precise means it's clear.
  - It's hard to miss the intended meaning
  - It's also hard to draw an incorrect conclusion

32

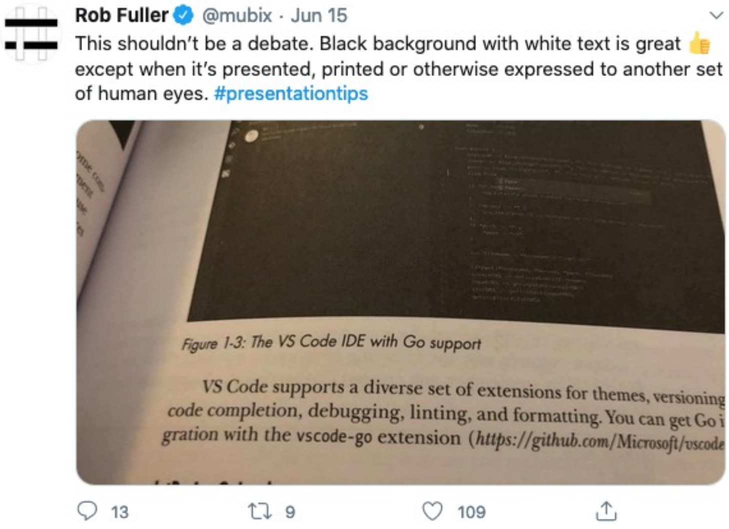
Screenshots: Illustrate, Don’t Decorate

- Crop to the relevant portion.
  - Grabbing the full window is usually a mistake.
- Direct the viewer’s attention.
  - Boxes and Arrows to highlight the important parts
- Make it harmonious.
  - Important text in image should be the same size as the text around the image.
- Dark Mode Is Bad.
  - …for screenshots.

33

Screenshots: Illustrate, Don’t Decorate

- Live examples soon
- but first, Dark Mode



Rob Fuller @mubix · Jun 15

This shouldn’t be a debate. Black background with white text is great 👍 except when it’s presented, printed or otherwise expressed to another set of human eyes. #presentationtips

Figure 1-3: The VS Code IDE with Go support

VS Code supports a diverse set of extensions for themes, versioning
code completion, debugging, linting, and formatting. You can get Go i
gration with the vscode-go extension (*https://github.com/Microsoft/vscode*

https://twitter.com/mubix/status/1272657499917815808

34

Words: Hacking winword.exe

- Insert Screenshot (Insert Ribbon)
- Autocorrect
  - Win: File > Options > Proofing
  - Mac: Word > Preferences > Autocorrect
- Quick Parts and Auto Text
  - Win: Insert Ribbon > Quick Parts
  - Mac: Insert MENU > Autotext…
- Split View / New Window (View Ribbon / Quick Access Toolbar)
- Insert Table (Insert Ribbon)
- Layout > Columns
- Macros

35

How Do I Become A Better Tester?

Dig deep into something. Anything. Write about it and get feedback.

Blog posts, CTF writeups, how-to guides.

Also get good with the tools, but you already know that.

36

Your Report Matters MORE* Than Your Hacking

* waaaay more.

37