Testing or Hacking: Real Advice on Effective Security Testing Strategies

Daniel Billing
Medidata, UK

@thetestdoctor

EuroSTAR Software Testing CONFERENCE
STOCKHOLM
31.10 - 03.11
2 0 1 6

WE HAVE A PROBLEM

OUR APPLICATIONS AND SYSTEMS ARE BEING HACKED

Source: hackmageddon.com

eurostarsoftwaretesting.com


LinkedIn


myspace

TESTING CAN HELP

WE NEED TO LEARN FROM THE HACKERS

Keren Elazari

"Hackers...they might just be the immune system for the Information Age"

WHY DO WE NEED TO DO SECURITY TESTING?

THAT'S OUT OF SCOPE

WE ARE OUTSOURCING THAT

THAT'S A NON FUNCTIONAL REQUIREMENT

WE DON'T HAVE THE SKILLS

WE NEED TO DELIVER FAST, NOT SLOW THINGS DOWN

I THINK WE NEED TO DO SOME SECURITY TESTING

WHERE DO WE START?

HOW DO WE DO IT?

WE NEED SOME TRAINING

WHAT TOOLS DO WE NEED?

HOW DO WE KNOW IF WE ARE SECURE?


1.CONSIDER THE
SCOPE

FUNCTIONAL FLOW

REGISTER

SEARCH

RESULTS

PURCHASE

STOCK

ADMIN

UNREGISTERED USERS

REGISTER

SEARCH

RESULTS

REGISTERED/ADMIN USERS

PURCHASE

STOCK

ADMIN

2. KNOW YOUR STACK

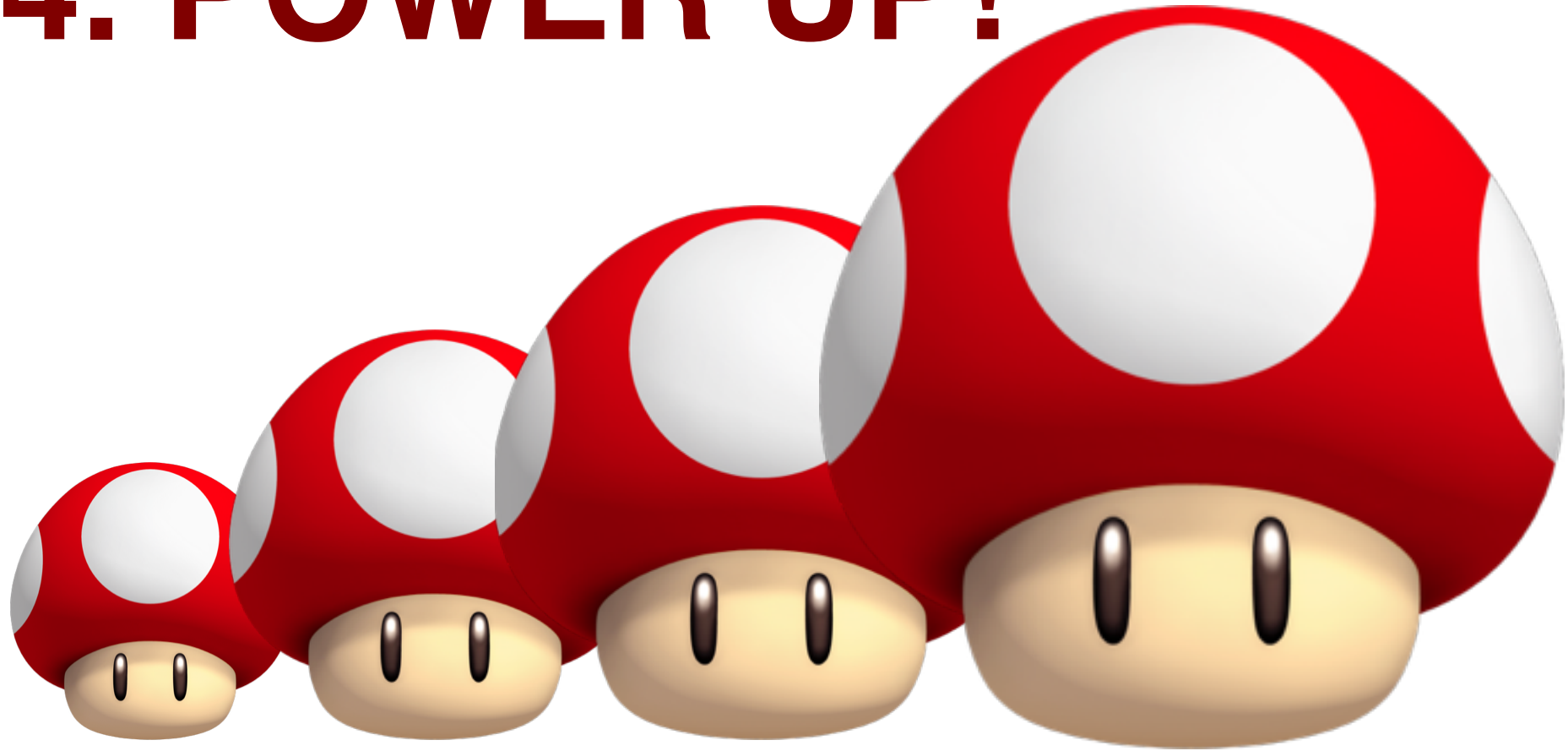
ALL COMPONENTS HAVE POTENTIAL VULNERABILITIES

POOR IMPLEMENTATIONS OF ANY COMPONENT CAN LEAD TO FLAWS

DEEP, INTIMATE KNOWLEDGE OF YOUR ENVIRONMENT WILL SUPPORT YOUR TESTING

3. UNDERSTAND YOUR WEAKNESSES

4. POWER UP!

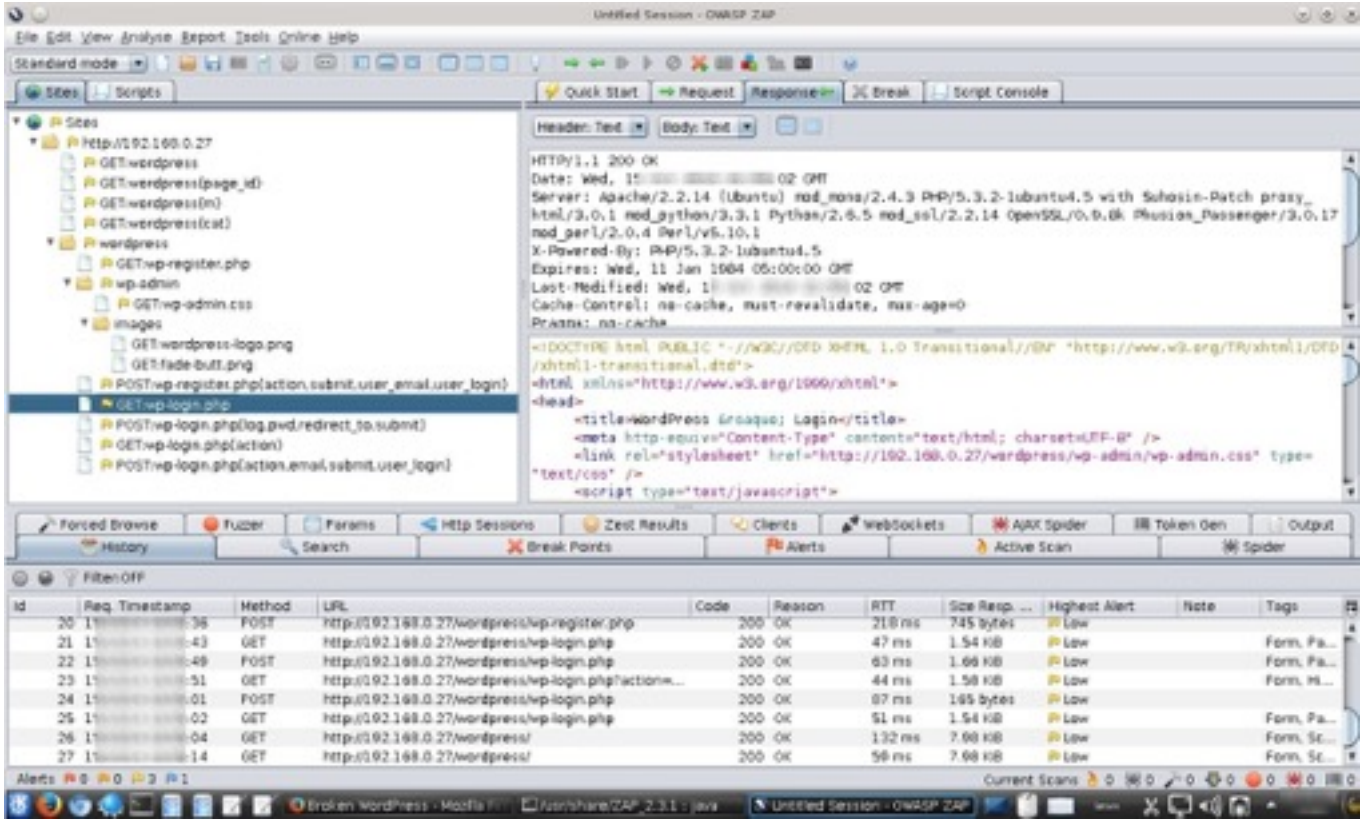


5. USE TOOLS EFFECTIVELY


Applications
Places
Thu 11:59
Favorites
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - System Services
Usual applications
Activities Overview
cewl
crunch
hashcat
john
johnny
medusa
ncrack
ophcrack
pyrit
rainbowcrack
rcracki_mt
wordlists

KALI

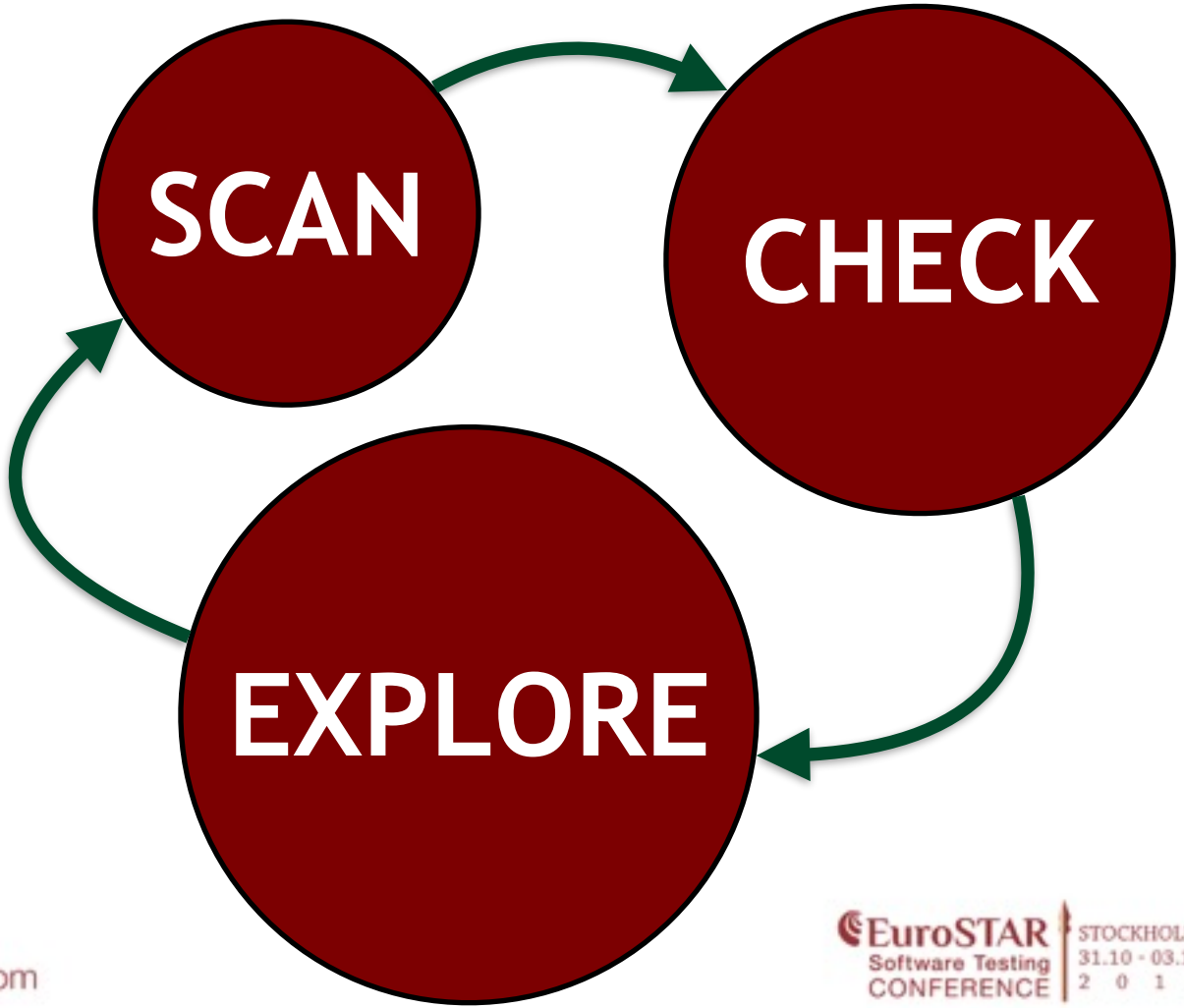
ZED ATTACK PROXY



```
$ python sqlmap.py -u "http://target/vuln.php?id=1" --batch

                         {1.0-dev-4512258}
                         http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 15:02:07

[15:02:07] [INFO] testing connection to the target URL
[15:02:07] [INFO] heuristics detected web page charset 'ascii'
[15:02:07] [INFO] testing if the target URL is stable. This can take a couple of
 seconds
[15:02:08] [INFO] target URL is stable
[15:02:08] [INFO] testing if GET parameter 'id' is dynamic
[15:02:08] [INFO] confirming that GET parameter 'id' is dynamic
[15:02:08] [INFO] GET parameter 'id' is dynamic
[15:02:08] [INFO] heuristic (basic) test shows that GET parameter 'id' might be
injectable (possible DBMS: 'MySQL')
```

SQLMAP

6.




7. BE
OCCASIONALLY
EVIL

As a hacker, I can

- send bad data in URLs, so I can access data and functions for which I am not authorised
- send bad data in the content of requests…
- send bad data in HTTP headers…
- read and even modify all data that is input/ output by your application

8. DON'T DO IT ALONE

9. BE CLEAR, BE HEARD

Creative Commons: Eden, Janine and Jim https://flic.kr/p/ajC5WF

10. BE DETERMINED

1. CONSIDER YOUR SCOPE
2. KNOW YOUR STACK
3. UNDERSTAND YOUR WEAKNESSES
4. POWER UP!
5. USE TOOLS EFFECTIVELY
6. SCAN > CHECK > EXPLORE
7. BE OCCASIONALLY EVIL
8. DON'T DO IT ALONE
9. BE CLEAR, BE HEARD
10. BE DETERMINED

ANY QUESTIONS?

Daniel Billing
Medidata, UK

@thetestdoctor

EuroSTAR Software Testing CONFERENCE
STOCKHOLM
31.10 - 03.11
2 0 1 6