Applications Security

OWASP Top 10

PyCon Argentina 2018

Objectives

- Generate **awareness** and visibility on web-apps security
- Set a **baseline** of shared knowledge across the company
- Trigger security-improving **tasks** in the projects

Why are we here /

OWASP / www.owasp.org

Open Web Application Security Project

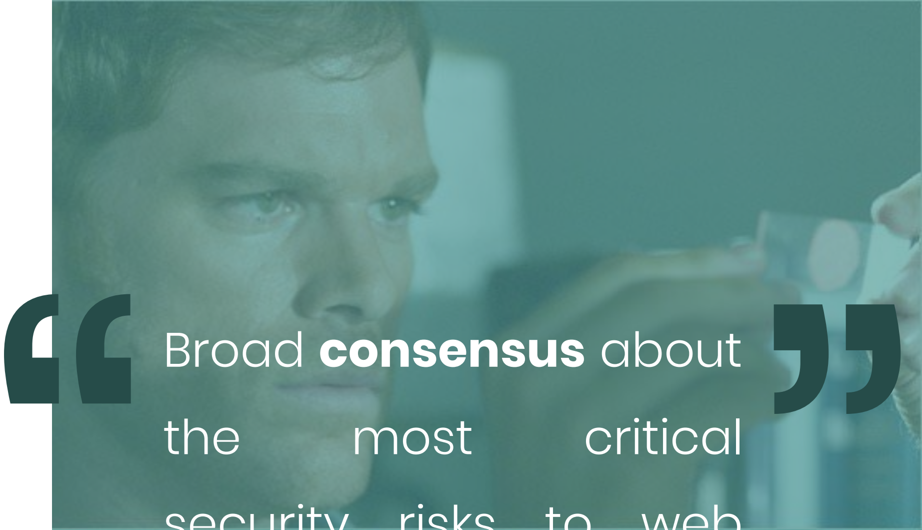
- NPO focused on improving the security of software
- make software security **visible**
- individuals and organizations are able to make **informed decisions**

- A **community** that issues software **tools** and **knowledge**-based documentation.

OWASP Top 10

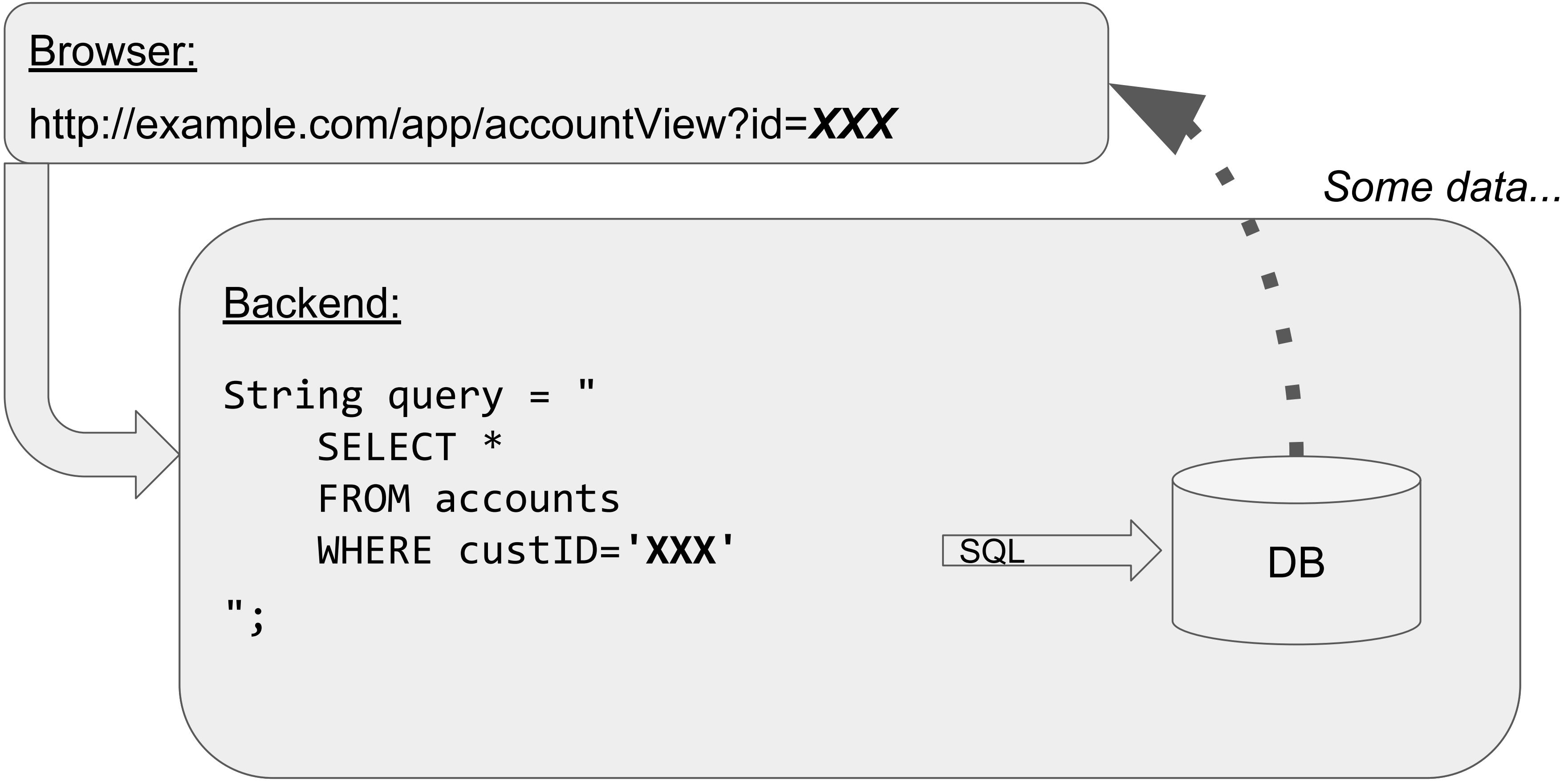
- PDFs
- cheatsheets
- translations
- tools
- etc

Los más buscados



> “Broad **consensus** about the most critical security risks to web applications.”

1- Injection *A1:2017-Injection*



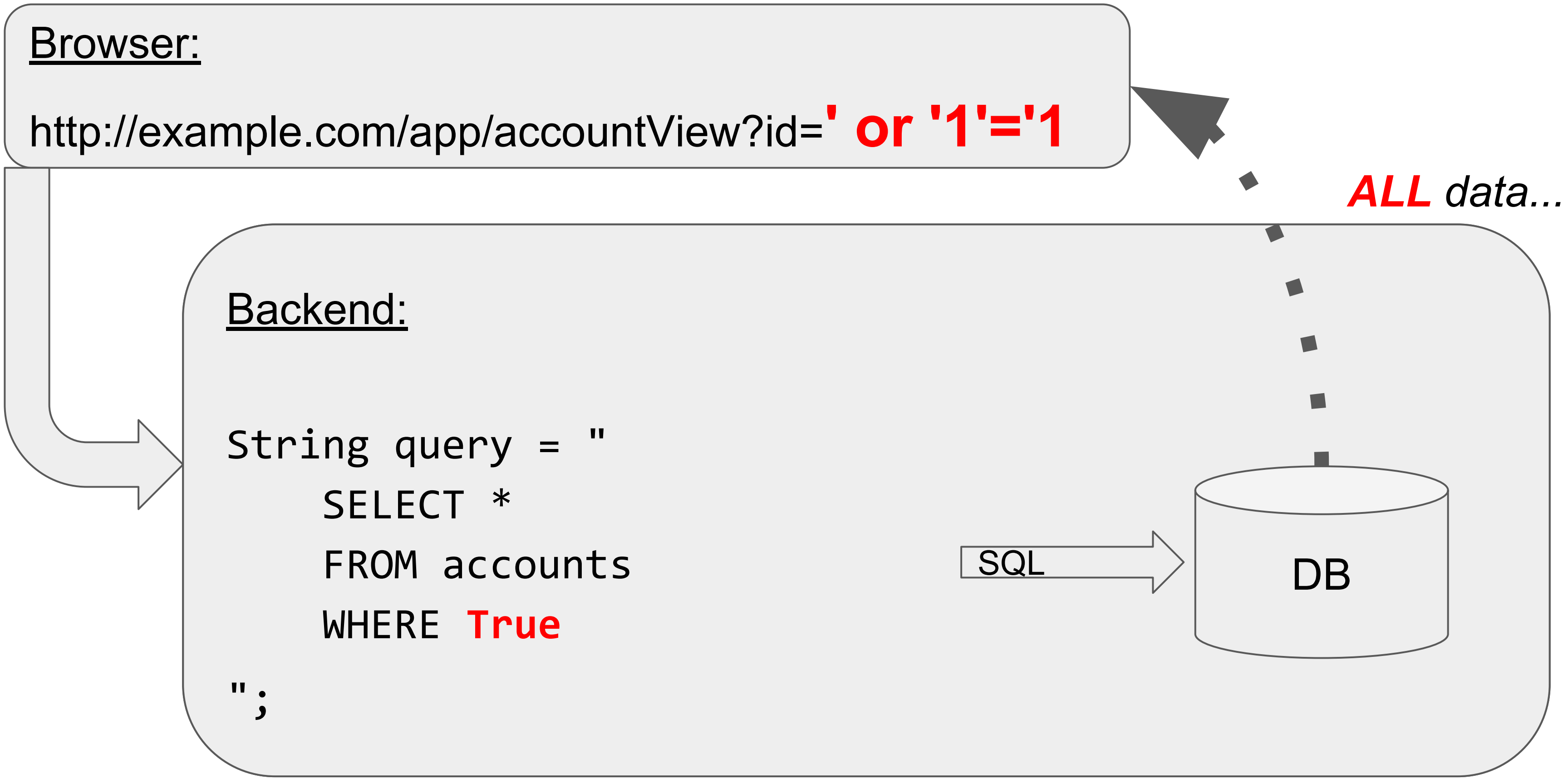
Browser:

http://example.com/app/accountView?id=***XXX***

Backend:

```
String query = "
    SELECT *
    FROM accounts
    WHERE custID='XXX'
";
```

1- Injection *A1:2017-Injection*



Browser:

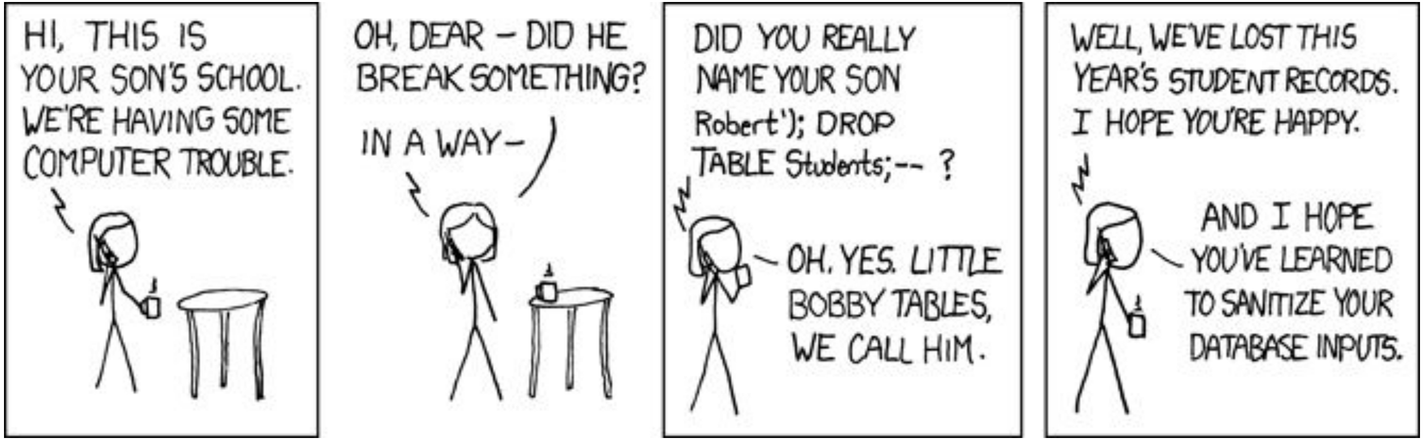
http://example.com/app/accountView?id=**' or '1'='1**

ALL data...

Backend:

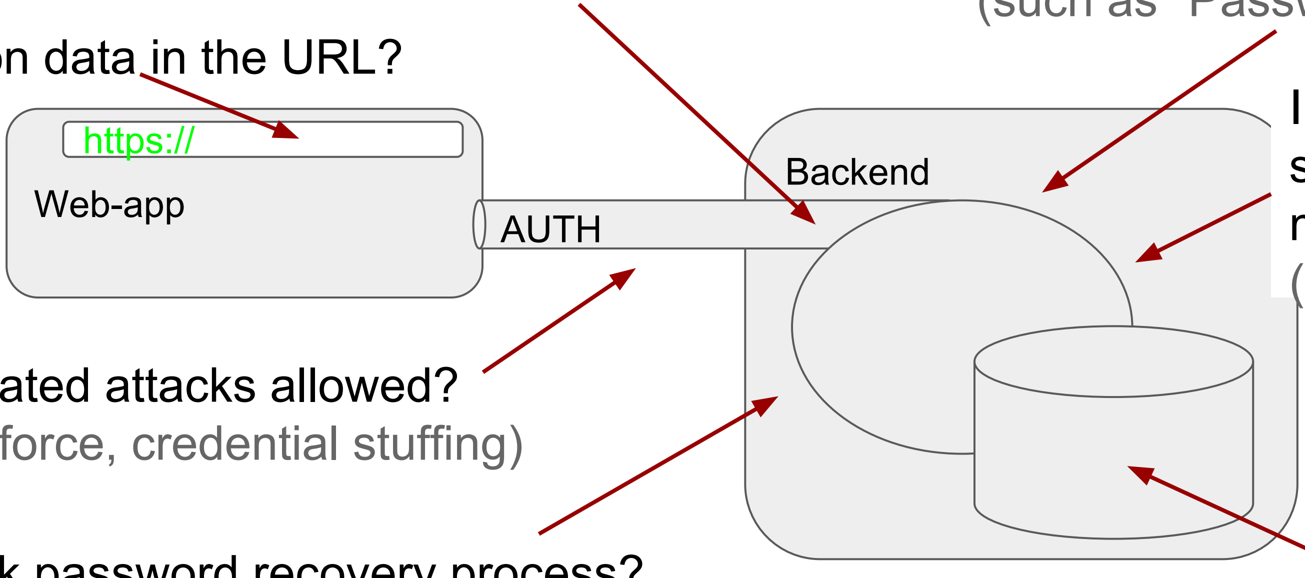
```
String query = "
     SELECT *
     FROM accounts
     WHERE True
";
```

1- Injection *A1:2017-Injection*


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

2 – Broken Authentication

A2:2017-Broken Authentication



Multi-factor authentication?

Weak passwords allowed?
(such as "Password1" or "123456“)

Session data in the URL?

Ineffective session/token management?
(rotation, invalidation)

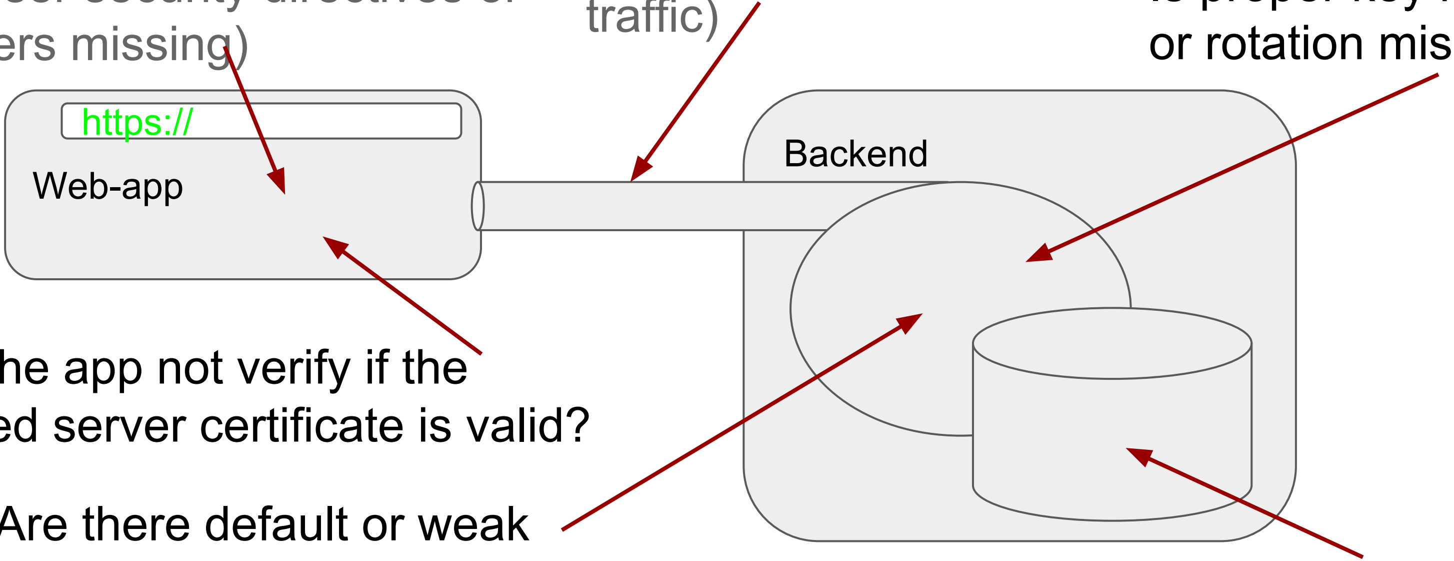
Automated attacks allowed?
(brute force, credential stuffing)

Weak password recovery process?
(such as "knowledge-based answers")

Weakly encrypted/hashed passwords?
(see A3:2017-Sensitive Data Exposure).

3 – Sensitive Data Exposure

A3:2017-Sensitive Data Exposure



Is encryption not enforced?
(browser security directives or headers missing)

data transmitted in clear text?
(Verify internal & external traffic)

Is proper key management or rotation missing?

Does the app not verify if the received server certificate is valid?

Are there default or weak cryptographic algorithms used?
(by default or in older code)

Is sensitive data stored in clear text?
(including backups and logs)

4 – XML External Entities A4:2017-XXE

Extract data from the server:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
  <!DOCTYPE foo [
  <!ELEMENT foo ANY >
  <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
  <foo>&xxe;</foo>
```

Probe the server's private network:

```
  <!ENTITY xxe SYSTEM "https://192.168.1.1/private" >]>
```

Attempt a denial-of-service attack:

```
    <!ENTITY xxe SYSTEM "file:///dev/random" >]>
```

5 – Broken Access Control

A5:2017-Broken Access Control

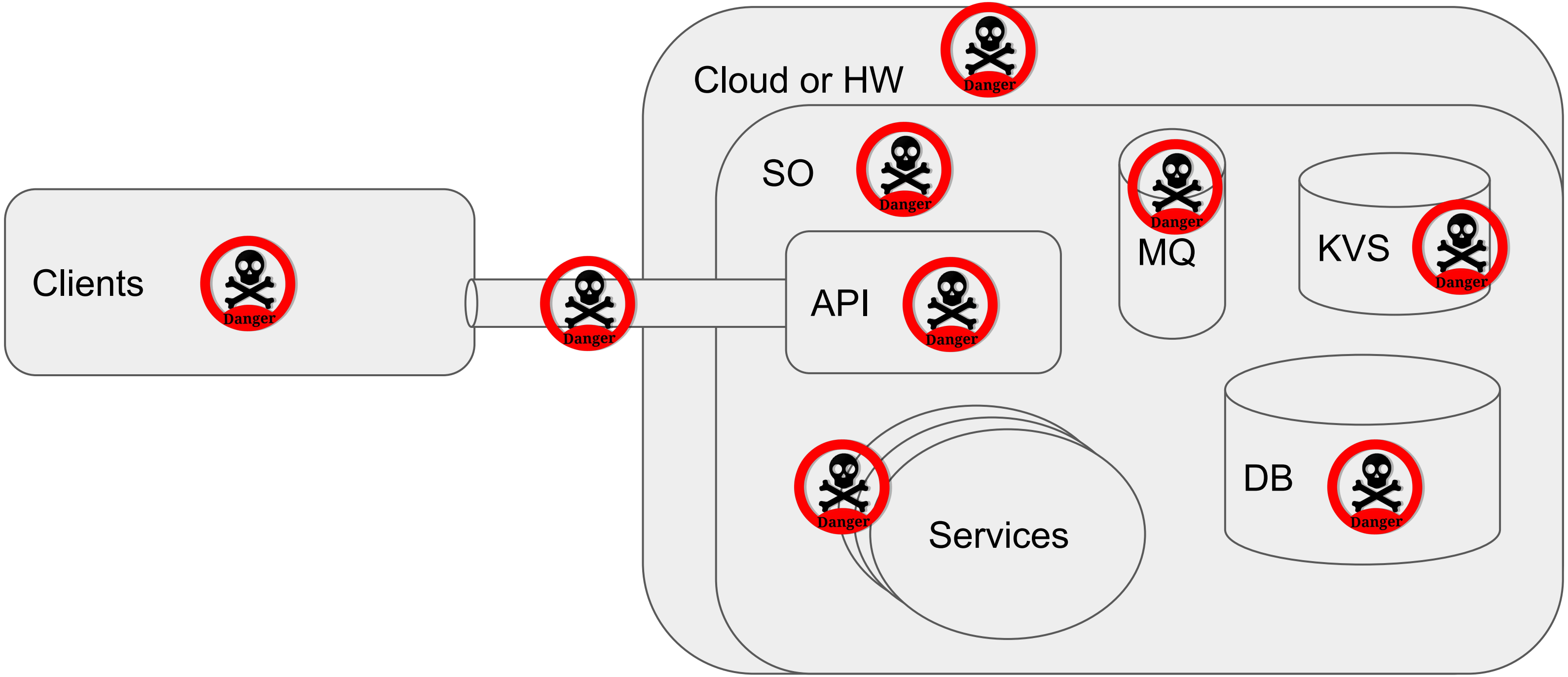
```
import django.contrib.auth
```

The main threat to a Django application is between the monitor and keyword

(it’s you, the developer)

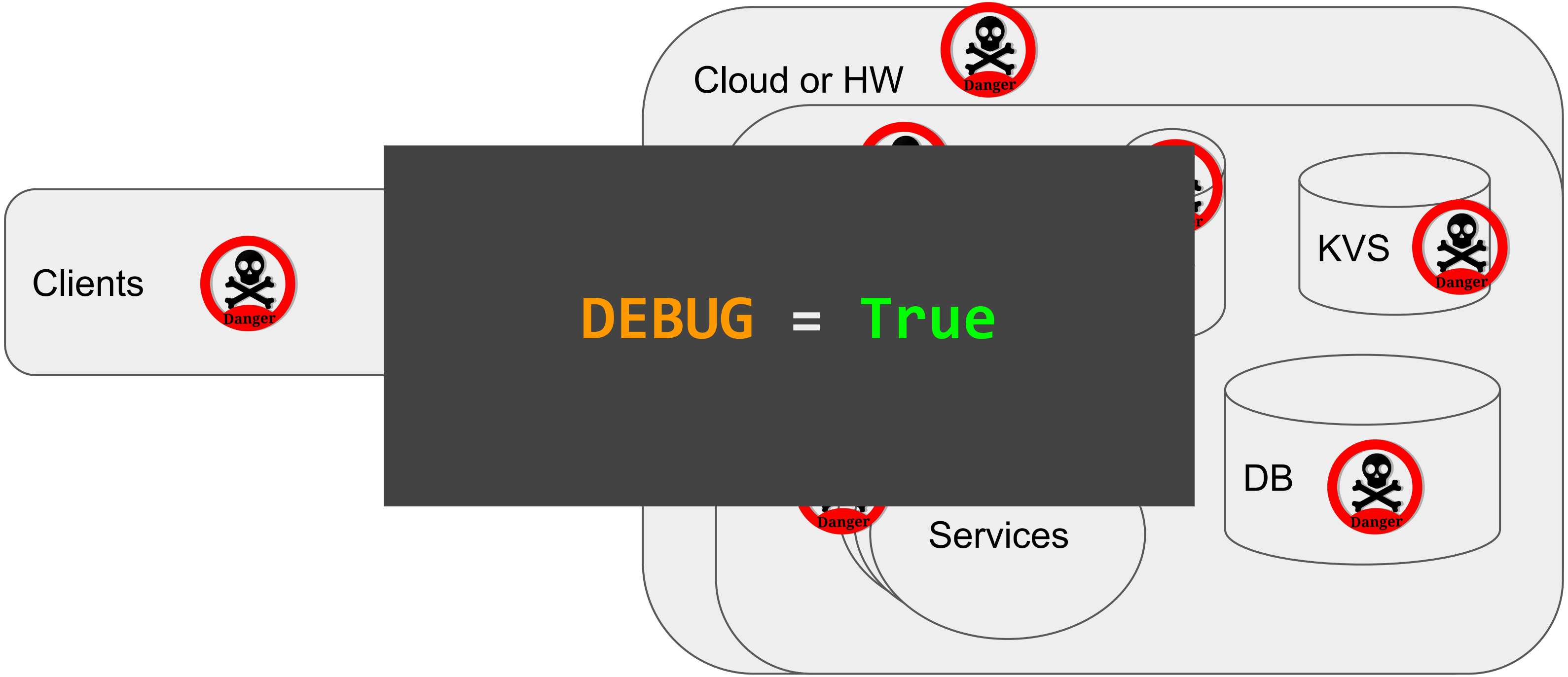
6 – Security Misconfiguration

A6:2017-Security Misconf.



6 – Security Misconfiguration

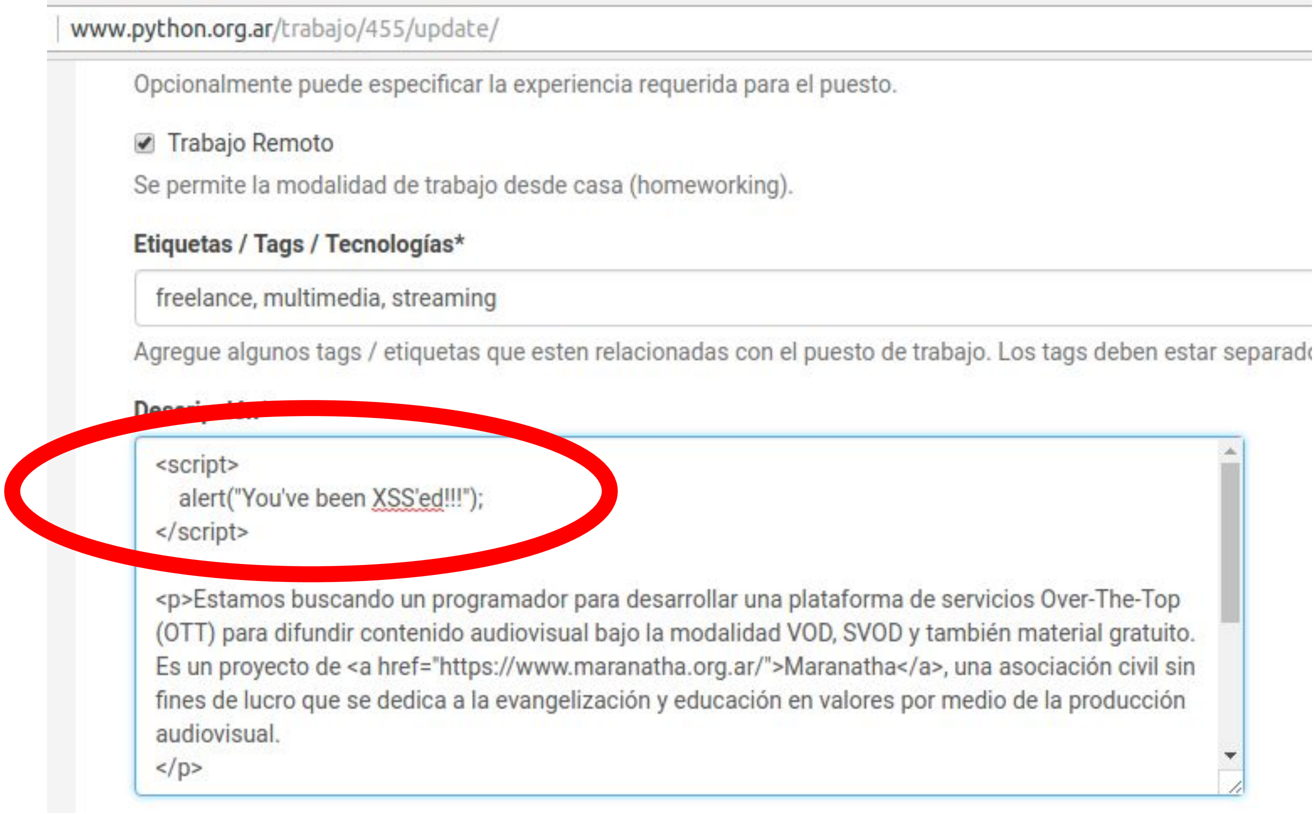
A6:2017-Security Misconf.



```
DEBUG = True
```

7 - Cross-Site Scripting (XSS)

A7:2017-XSS



www.python.org.ar/trabajo/455/update/

Opcionalmente puede especificar la experiencia requerida para el puesto.

☑ Trabajo Remoto

Se permite la modalidad de trabajo desde casa (homeworking).

Etiquetas / Tags / Tecnologías*

freelance, multimedia, streaming

Agregue algunos tags / etiquetas que esten relacionadas con el puesto de trabajo. Los tags deben estar separad

Descripción*

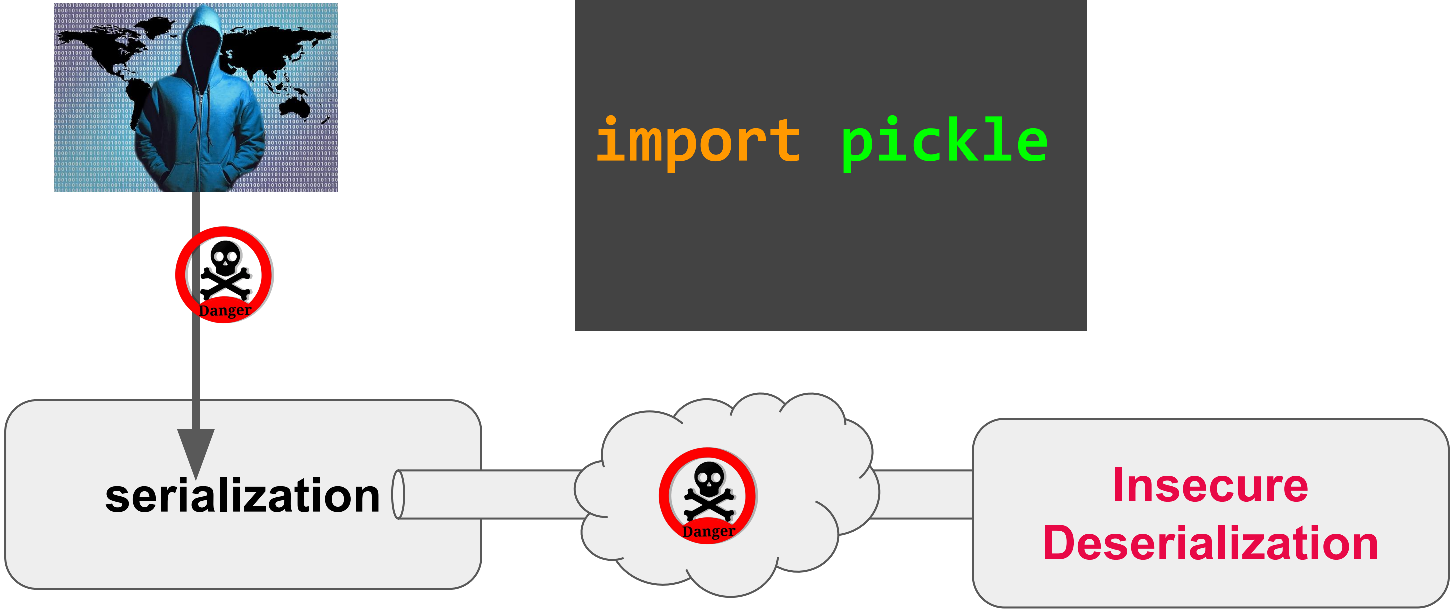
```
<script>
   alert("You've been XSS'ed!!!");
</script>

<p>Estamos buscando un programador para desarrollar una plataforma de servicios Over-The-Top
(OTT) para difundir contenido audiovisual bajo la modalidad VOD, SVOD y también material gratuito.
Es un proyecto de <a href="https://www.maranatha.org.ar/">Maranatha</a>, una asociación civil sin
fines de lucro que se dedica a la evangelización y educación en valores por medio de la producción
audiovisual.
</p>
```

8 – Insecure Deserialization

A8:2017-Insecure Deserialization

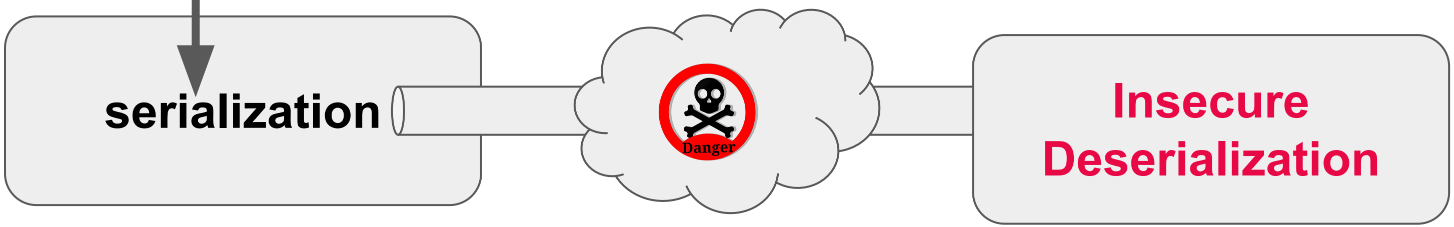
```
import pickle
```



8 – Insecure Deserialization

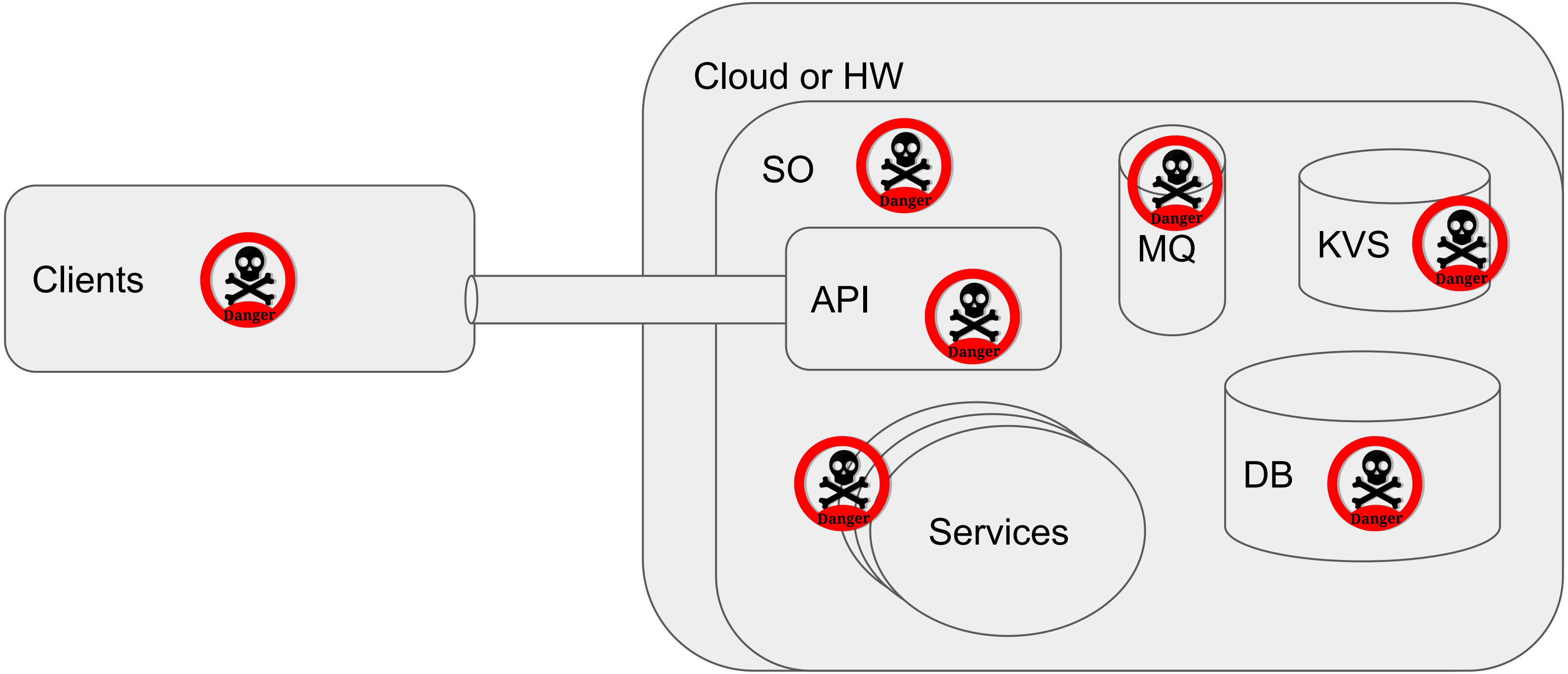
A8:2017-Insecure Deserialization

```
# don't import pickle
```



9 – Using Components With Known Vulnerabilities

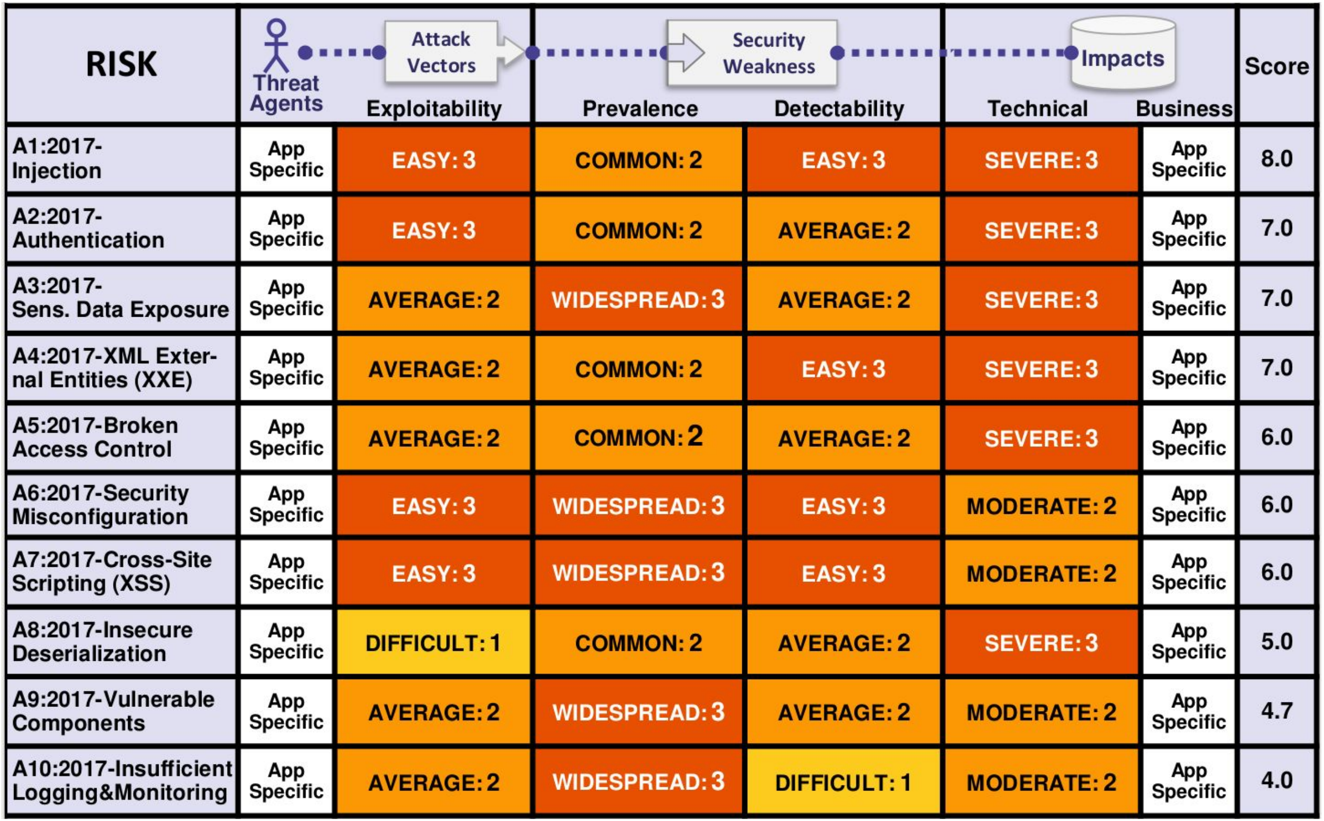
A9:2017-Using Components with Known Vulnerabilities



10 – Insufficient Logging & Monitoring

A10:2017-Insufficient Logging & Monitoring

Risk Factor based on statistics and experience

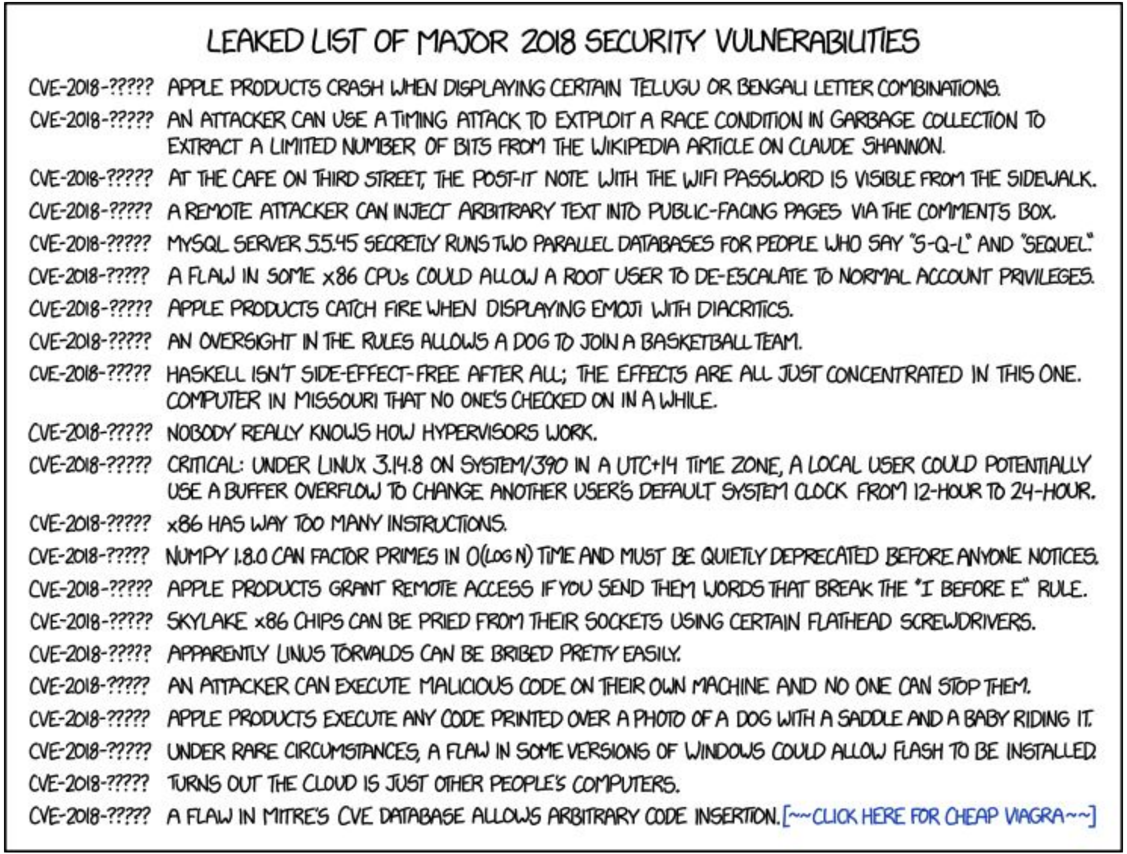


RISK	Threat Agents	Attack Vectors	Security Weakness		Impacts		Score
		Exploitability	Prevalence	Detectability	Technical	Business	
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

> Other not in the top-10

- Cross-Site Request Forgery (CSRF)
- Uncontrolled Resource Consumption ('Resource Exhaustion', 'AppDoS')
- Unrestricted Upload of File with Dangerous Type
- User Interface (UI) Misrepresentation of Critical Information (Clickjacking and others)
- Unvalidated Forward and Redirects
- Improper Control of Interaction Frequency (Anti-Automation)
- Inclusion of Functionality from Untrusted Control Sphere (3rd Party Content)
- Server-Side Request Forgery (SSRF)

› And more https://imgs.xkcd.com/comics/2018_cve_list.png



LEAKED LIST OF MAJOR 2018 SECURITY VULNERABILITIES

CVE-2018-????? APPLE PRODUCTS CRASH WHEN DISPLAYING CERTAIN TELUGU OR BENGALI LETTER COMBINATIONS.

CVE-2018-????? AN ATTACKER CAN USE A TIMING ATTACK TO EXPLOIT A RACE CONDITION IN GARBAGE COLLECTION TO EXTRACT A LIMITED NUMBER OF BITS FROM THE WIKIPEDIA ARTICLE ON CLAUDE SHANNON.

CVE-2018-????? AT THE CAFE ON THIRD STREET, THE POST-IT NOTE WITH THE WIFI PASSWORD IS VISIBLE FROM THE SIDEWALK.

CVE-2018-????? A REMOTE ATTACKER CAN INJECT ARBITRARY TEXT INTO PUBLIC-FACING PAGES VIA THE COMMENTS BOX.

CVE-2018-????? MYSQL SERVER 5.5.45 SECRETLY RUNS TWO PARALLEL DATABASES FOR PEOPLE WHO SAY "S-Q-L" AND "SEQUEL."

CVE-2018-????? A FLAW IN SOME x86 CPUs COULD ALLOW A ROOT USER TO DE-ESCALATE TO NORMAL ACCOUNT PRIVILEGES.

CVE-2018-????? APPLE PRODUCTS CATCH FIRE WHEN DISPLAYING EMOJI WITH DIACRITICS.

CVE-2018-????? AN OVERSIGHT IN THE RULES ALLOWS A DOG TO JOIN A BASKETBALL TEAM.

CVE-2018-????? HASKELL ISN'T SIDE-EFFECT-FREE AFTER ALL; THE EFFECTS ARE ALL JUST CONCENTRATED IN THIS ONE COMPUTER IN MISSOURI THAT NO ONE'S CHECKED ON IN A WHILE.

CVE-2018-????? NOBODY REALLY KNOWS HOW HYPERVISORS WORK.

CVE-2018-????? CRITICAL: UNDER LINUX 3.14.8 ON SYSTEM/390 IN A UTC+14 TIME ZONE, A LOCAL USER COULD POTENTIALLY USE A BUFFER OVERFLOW TO CHANGE ANOTHER USER'S DEFAULT SYSTEM CLOCK FROM 12-HOUR TO 24-HOUR.

CVE-2018-????? x86 HAS WAY TOO MANY INSTRUCTIONS.

CVE-2018-????? NUMPY 1.8.0 CAN FACTOR PRIMES IN O(LOG N) TIME AND MUST BE QUIETLY DEPRECATED BEFORE ANYONE NOTICES.

CVE-2018-????? APPLE PRODUCTS GRANT REMOTE ACCESS IF YOU SEND THEM WORDS THAT BREAK THE "I BEFORE E" RULE.

CVE-2018-????? SKYLAKE x86 CHIPS CAN BE PRIED FROM THEIR SOCKETS USING CERTAIN FLATHEAD SCREWDRIVERS.

CVE-2018-????? APPARENTLY LINUS TORVALDS CAN BE BRIBED PRETTY EASILY.

CVE-2018-????? AN ATTACKER CAN EXECUTE MALICIOUS CODE ON THEIR OWN MACHINE AND NO ONE CAN STOP THEM.

CVE-2018-????? APPLE PRODUCTS EXECUTE ANY CODE PRINTED OVER A PHOTO OF A DOG WITH A SADDLE AND A BABY RIDING IT.

CVE-2018-????? UNDER RARE CIRCUMSTANCES, A FLAW IN SOME VERSIONS OF WINDOWS COULD ALLOW FLASH TO BE INSTALLED.

CVE-2018-????? TURNS OUT THE CLOUD IS JUST OTHER PEOPLE'S COMPUTERS.

CVE-2018-????? A FLAW IN MITRE'S CVE DATABASE ALLOWS ARBITRARY CODE INSERTION. [~~CLICK HERE FOR CHEAP VIAGRA~~]

› Preguntas?

Francisco Capdevila
francisco.capdevila@mercadolibre.com
@pancho_jay

Carlos Matías de la Torre
carlos.delatorre@mercadolibre.com
@py_litox

Muchas Gracias

mercado libre

machinalis