Hello and welcome!

#VismaAClabs @ligaac_labs

will begin shortly....

Thursday, 22nd of April

VISMA

Introduction to
Application Security

What will we learn

Attackers and targets

The software development life-cycle

Application security

Database security and data privacy

OWASP

CTF

VISMA

Sessions

Week 16 (22nd April)	Session 1
Week 17	Vacation
Week 18 (6th May)	Session 2
Week 19 (13th May)	Session 3
Week 20 (19th,20th May)	Session 4 (2h each day) 08 AM - 10 AM
Week 21 (27th May)	CTF
Week 22 (3rd June)	Session 5 / CTI, Monitoring
Week 23 (10th June)	Session 6 - final session

VISMA

A typical day

4 hour day

08:00 - 09:00	**Work**
09:00 - 09:10	Break
09:10 - 10:30	**Work**
10:30 - 11:00	Long break
11:00 - 12:00	**Work**

Let’s begin our journey

22nd April

VISMA

Agenda

Attackers and targets

The software development life-cycle

Introduction to OWASP

OWASP - Injection

Targets and attackers

For many years security was understood as IT infrastructure security.

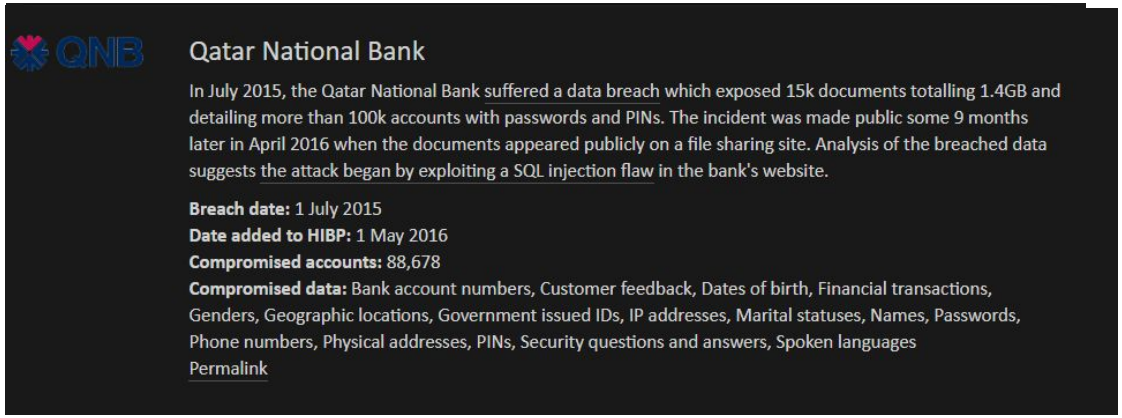
Cloud changed this. Today DevSecOps teams are responsible for everything.

Expectations are high, roles are combined , responsibility is shared.

Most breaches are because of poor software security.

Many breaches come from internal unhappy employees.

Who has been hacked - data breaches



And many others...

VISMA

Have you been pwned?

Who is behind Have I Been Pwned (HIBP)

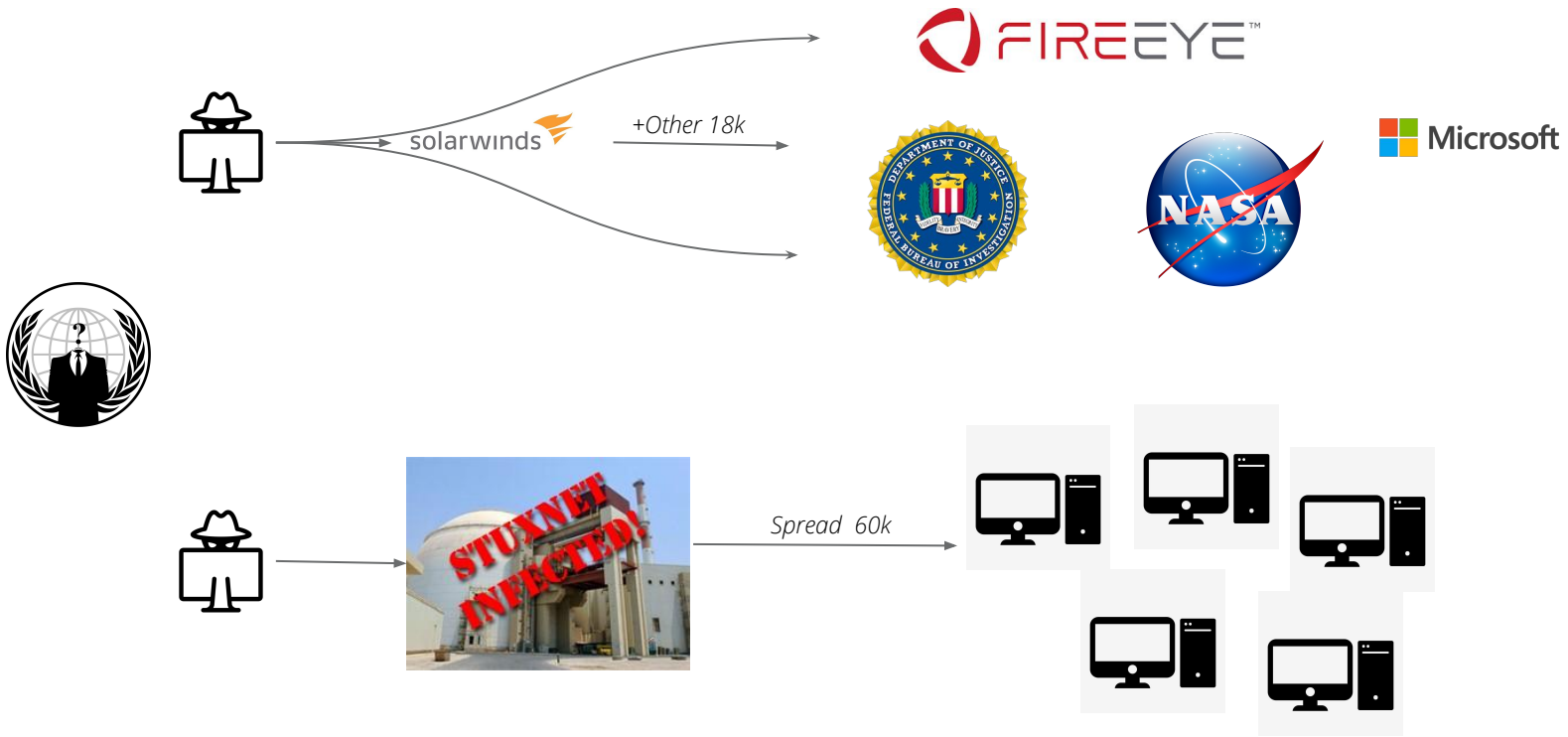
I'm Troy Hunt, a Microsoft Regional Director and Most Valuable Professional awardee for Developer Security, blogger at troyhunt.com, international speaker on web security and the author of many top-rating security courses for web developers on Pluralsight.

I created HIBP as a free resource for anyone to quickly assess if they may have been put at risk due to an online account of theirs having been compromised or "pwned" in a data breach. I wanted to keep it dead simple to use and entirely free so that it could be of maximum benefit to the community.

Short of the odd donation, all costs for building, running and keeping the service currently come directly out of my own pocket. Fortunately, today's modern cloud services like Microsoft Azure make it possible to do this without breaking the bank!

HaveIBeenPwned

Who has been hacked - cyber attacks

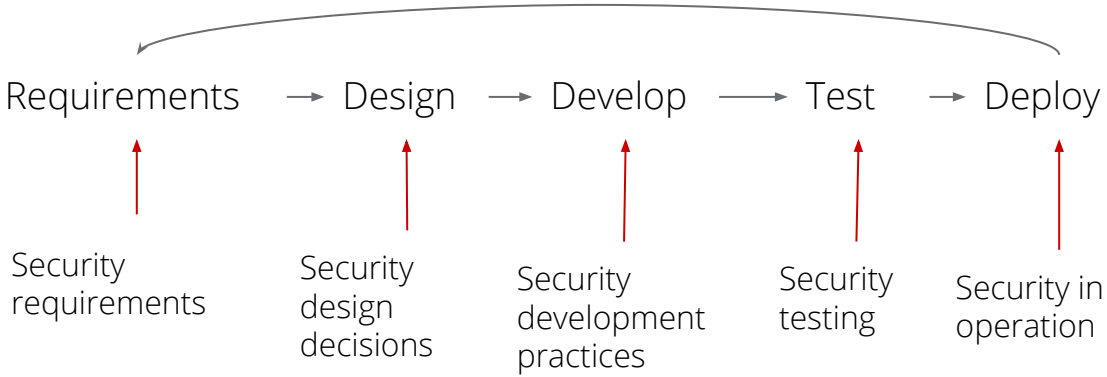


Who are the attackers

- Hacktivists
  - motivated by civil disobedience to promote a political agenda or social change
  - poorly funded
- Online criminals
  - financial data
  - motivated by cash
- Nation states
  - cyber warfare
  - national or political interests
  - unlimited funded

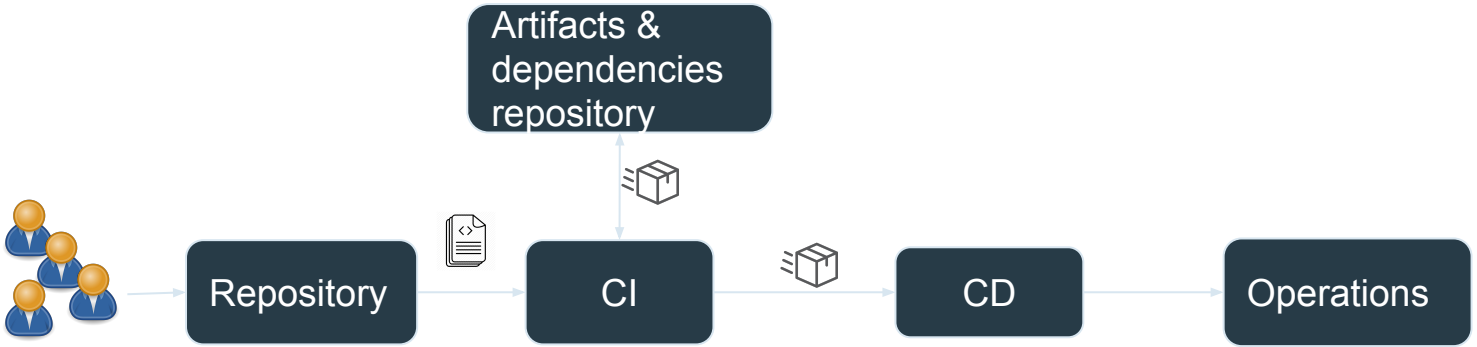
VISMA

Security in the SDLC



VISMA

Security in the delivery pipeline



Secure coding standards
Code reviews
Pre-commit hooks
IDE Security plugins
Threat modeling

Code analysis
Dependencies vuln. analysis
Secured build environment

Infrastructure as code
Secure credentials management
Security scanning
Security testing
Penetration testing

Hosting configuration checks
Monitoring
Detection
Threat intelligence
Penetration testing

VISMA

OWASP

Introduction

Our experience taught us that the current level of security of web-applications is not sufficient enough to ensure security. This is mainly because web-developers simply aren't aware of the risks and dangers that are lurking, waiting to be exploited by hackers.

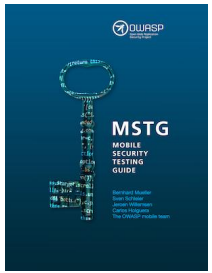
Open Web Application Security Project

A nonprofit foundation that works to improve the security of software.

They run different projects helping the IT industry to learn how to strengthen application security.

Their projects expand to all the software delivery pipeline from security knowledge framework, to testing guidelines, training applications and testing tools.

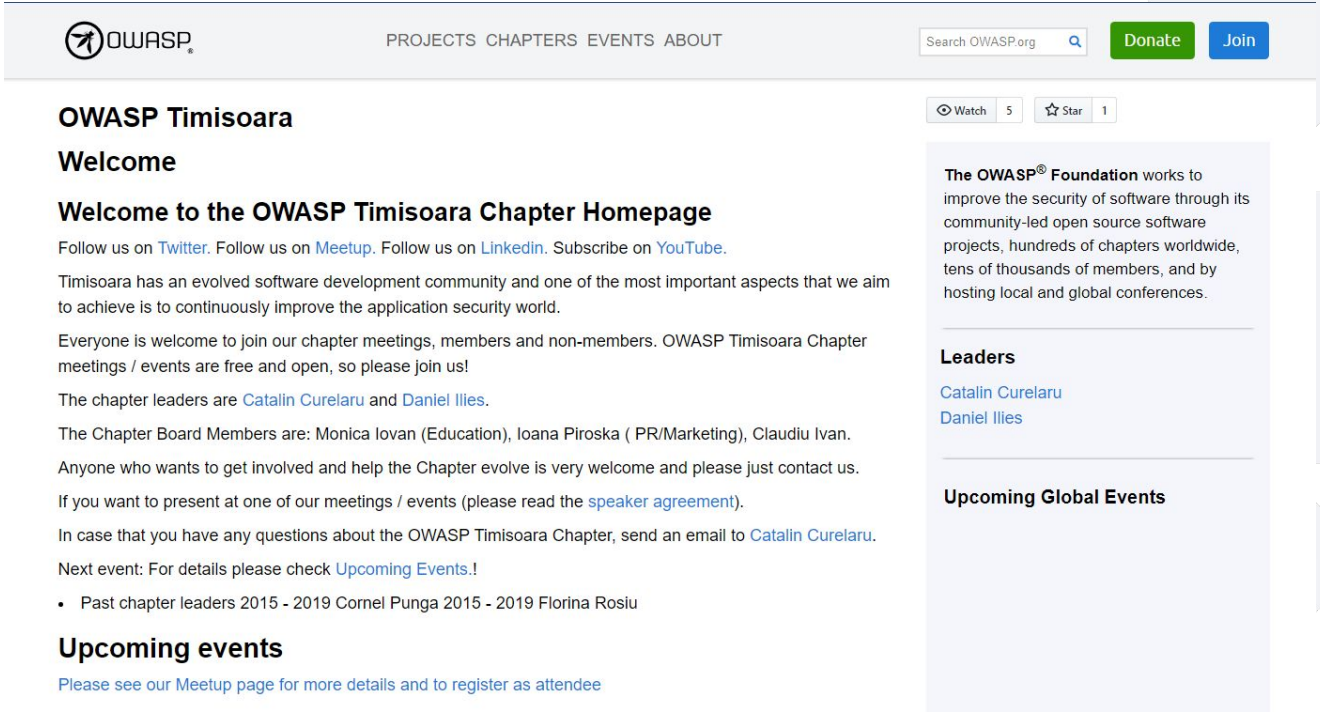
dependency track



ZAP

VISMA

OWASP local meet-ups



VISMA

Overview OWASP Top 10

- **Injection**

  Untrusted data is sent to an interpreter and tricks it to execute unintended commands.

- **Broken Authentication**

  The attacker is able to assume other users identities.

- **Sensitive data exposure**

  Sensitive data should be handled with case with exchanged with the browser.

- **XML External Entities**

  XML processors evaluating external entities URI during XML document parsing.

- **Broken Access Control**

  The attacker is able to access unauthorized functions, view sensitive data, change user data.

- **Security misconfiguration**

  Insecure default configurations, unprotected storage and databases, verbose logging, misconfigured HTTP headers.

VISMA

OWASP Top 10

- **Cross-site scripting (XSS)**

  Execute scripts in victim's browser to hijack user session, redirect to malicious sites, crypto mining

- **Insecure deserialization**

  Untrusted data defines the data type of the object that the stream will be deserialized to.

- **Using components with known vulnerabilities**

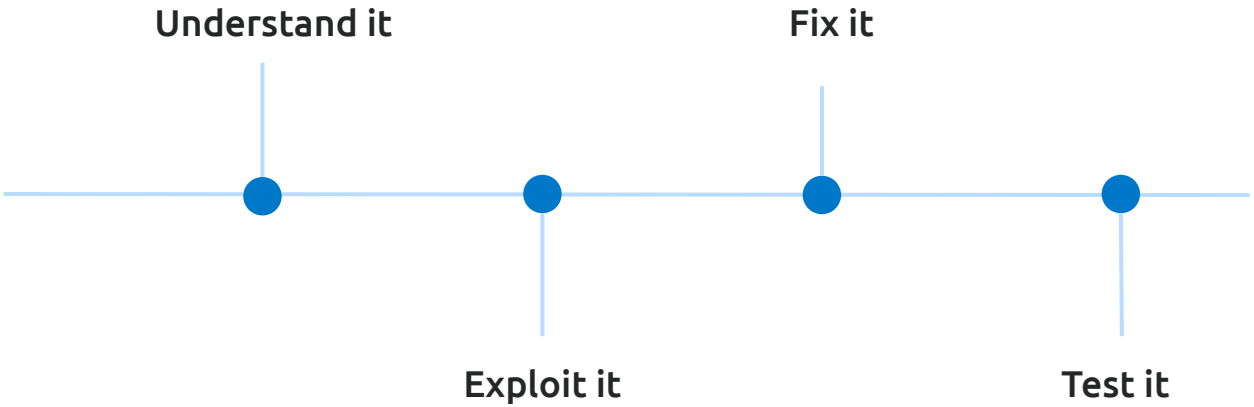
  External libraries, packages, frameworks run with the same privileges as the application. Attackers exploit known vulnerabilities.

- **Insufficient logging and monitoring**

  Helps attackers achieve their goals without being detected in time.

VISMA

Working model



VISMA

Injection

What ?

A user is allowed to send code to an application and that code gets executed by the application.

Multiple types of injection : Sql, NoSql, LDAP, OS

Code or command injection.

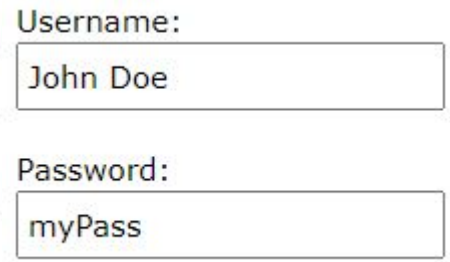
Why ?

Lack or poor user input or output validation. Lack of input encoding.

VISMA

Sql Injection

How ?




```
SELECT * FROM Users WHERE Name ="John Doe" AND Pass ="myPass"
```

VISMA

Injection

Demo

Injection

```
select name from sysobjects where id=(
    select top 1 id from (
        select top 3 id from sysobjects where xtype=char(85) order by id asc
    ) sq order by id desc
)
```

What do you think the query does?
What represents *char(85)* ?
What can we do with this information that we found? Are we able to further exploit the application?

VISMA

Injection - let’s fix it

- Database; least privilege
- Parameterized queries
- Stored procedures*
  - when written correctly
- ORM Framework
- Data validation and whitelisting
  - Get away from strings
  - Use regular expressions to validate emails, phone numbers

What about blacklisting ?

VISMA

Respect

Reliability

Innovation

Competence

Team spirit