

DEV
SEC
OPS
DAYS

Building a culture of security in a developer's company

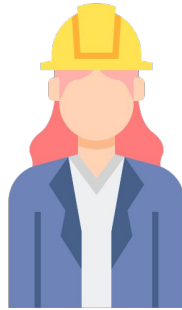
16.12.2021



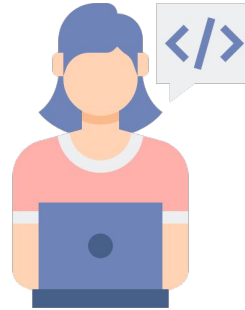
What is Theodo?



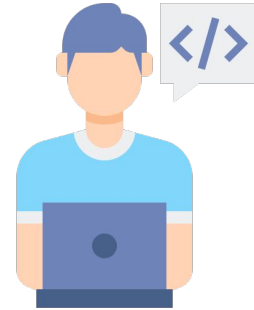
Tech lead



Product Owner



**Software
engineer**



**Software
engineer**



Short story time

How I joined a developer's company



```
...keywords_info_bar">
style="float: left;" for="keywords
class="field_information_container
...keywords_count_info" class="field_infor
...margin-top: 3px;"></a>
...keywords_log" class="field_infor
leted</a>

style="float: right; padding-top: 10px;
...clear: both;"</div>
area id="keywords" class="tag-editor ui-sortable"
class="tag-editor ui-sortable">
style="width:1px"></li>
class="placeholder">
</div>Enter keywords or paste via clipboard
</li>

area id="keywords_for_clipboard" style="width: 100%; height: 100%; border: 1px solid #ccc; border-radius: 4px; margin-bottom: 10px;" class="btn_keywords_container" style="width: 100%; height: 100%; border: 1px solid #ccc; border-radius: 4px; margin-bottom: 10px;"
class="has-feedback has-clear" style="width: 100%; height: 100%; border: 1px solid #ccc; border-radius: 4px; margin-bottom: 10px;"
body div div keywords add


```

"You want to be a Web Developer?"

*"You can do security by doing web
development!"*



That's why I'm especially happy to be here today!





**Do you need to build a
security culture?**



Do *you* need to build a security culture?

01

You might not be convinced yourself

02

You might need to convince your management

03

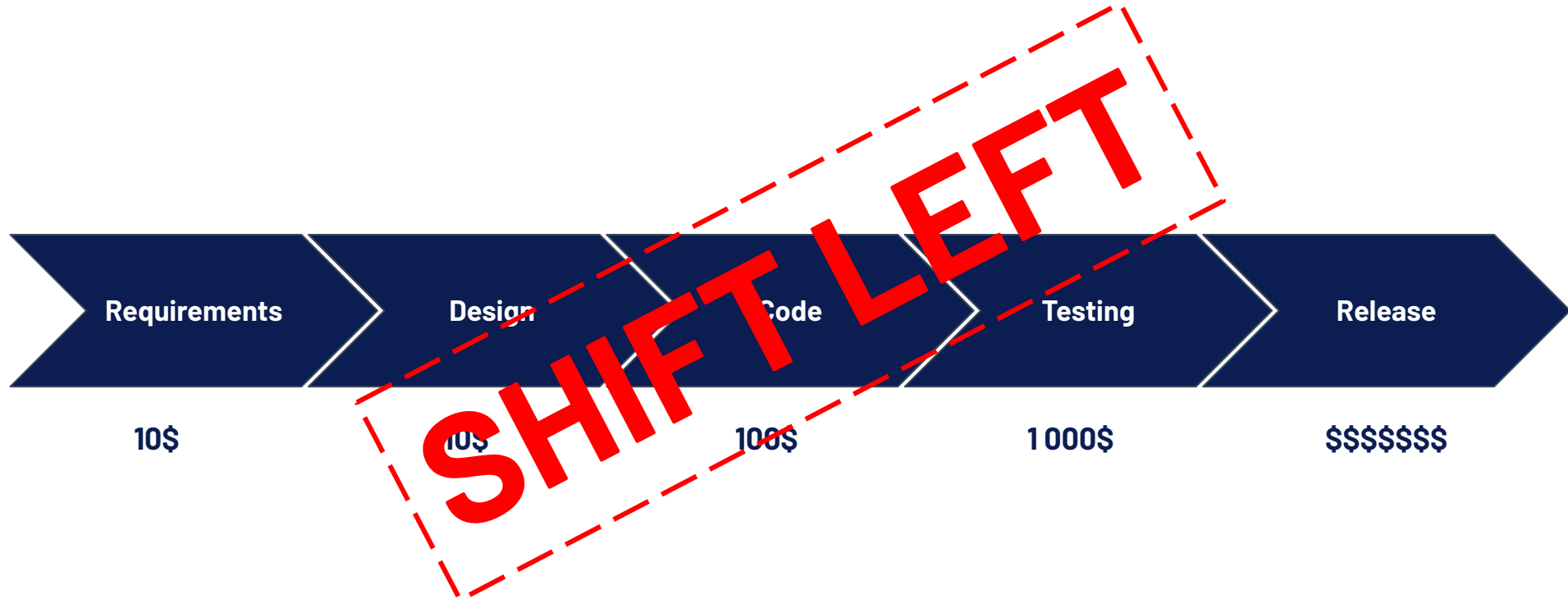
You might need to convince your colleagues





Avoid rework, avoid waste

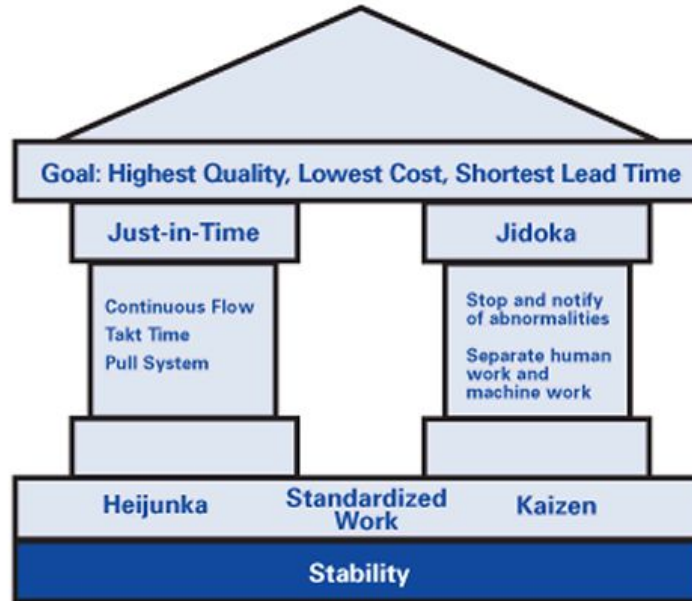
How much does a security flaw cost?





Avoid rework, avoid waste

Toyota Production System



Toyota Production System "House."

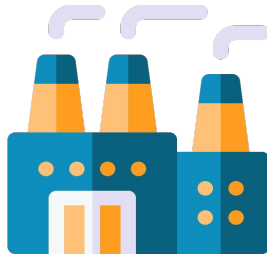


Avoid rework, avoid waste

Flux SDLC, coût de correction



Defects



Overproduction



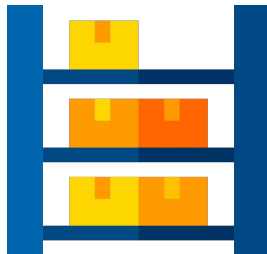
Waiting



Unused talent



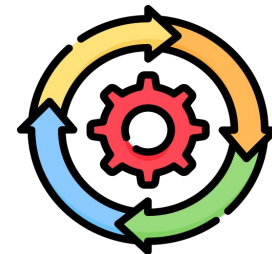
Transportation



Inventory



Motion



Extra processing

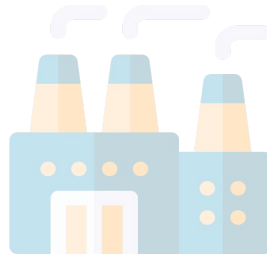


Avoid rework, avoid waste

Flux SDLC, coût de correction



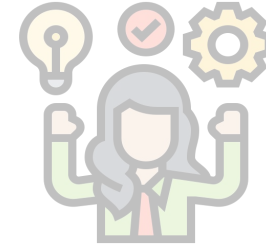
Defects



Overproduction



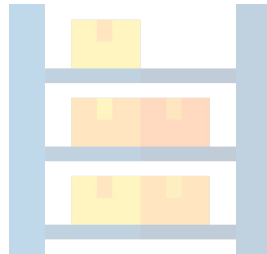
Waiting



Unused talent



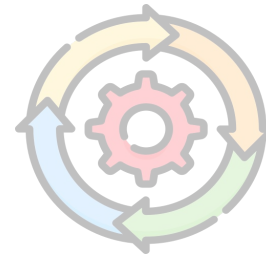
Transportation



Inventory



Motion

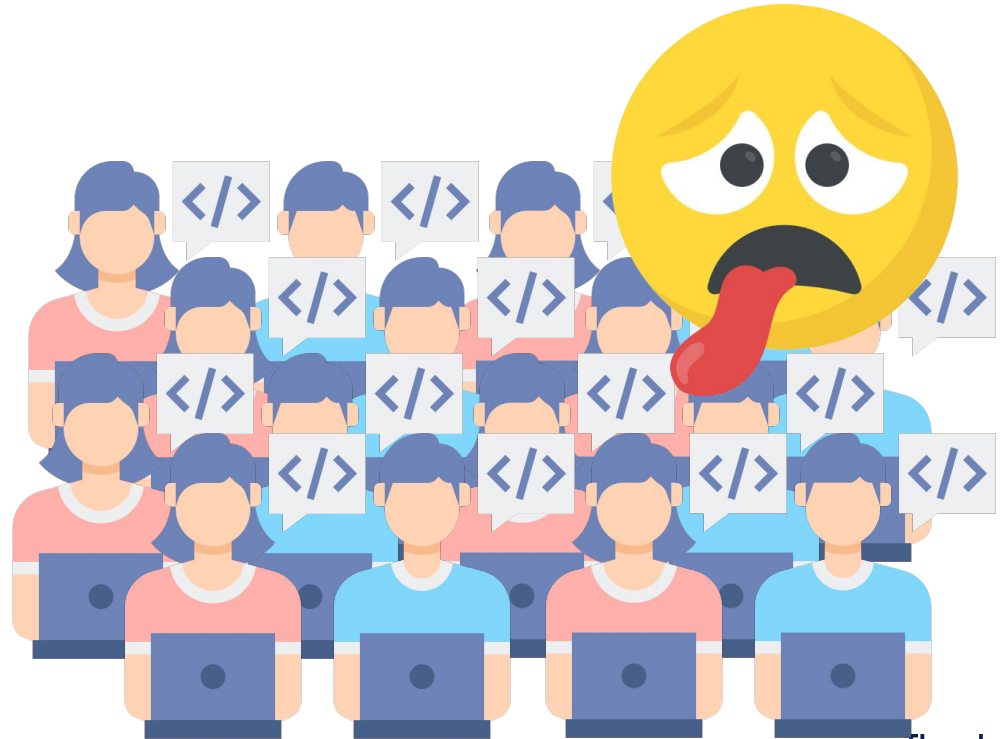


Extra processing



Scale efficiently

Can you keep up with your development team?





Focus on creating value

Do you really want to spend all your time finding the same flaws?



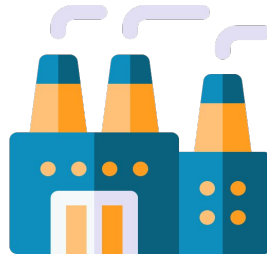


Focus on creating value

Do you really want to spend all your time finding the same flaws?



Defects



Overproduction



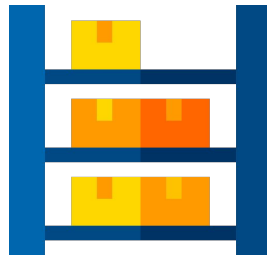
Waiting



Unused talent



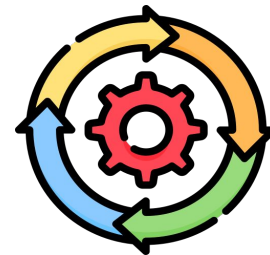
Transportation



Inventory



Motion



**Extra
processing**

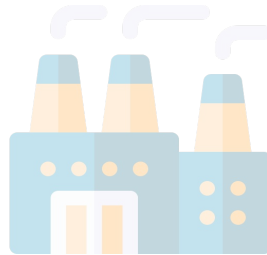


Focus on creating value

Do you really want to spend all your time finding the same flaws?



Defects



Overproduction



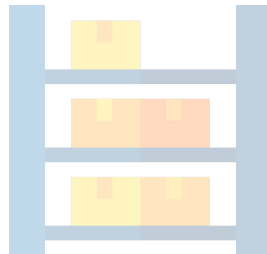
Waiting



Unused talent



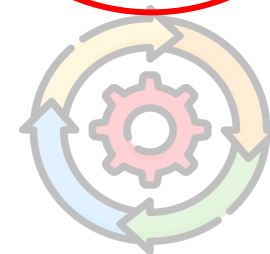
Transportation



Inventory



Motion



**Extra
processing**



Developers already use quality tools

It is much easier to plug in an existing system than to redesign one





How?



A few challenges

It only happens to other people/companies/...

We don't want other tools / there are too many false positives

Security is not as interesting as other things

We didn't think of security this one time!

Let's not tell security about this, they will only block us.

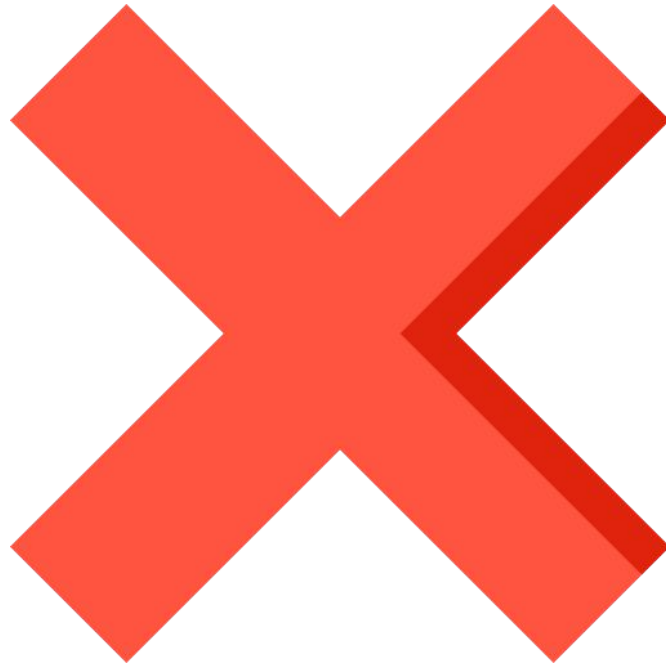
Security doesn't understand anything





Let's not tell security about this, they will only block us.

You have a problem





Let's not tell security about this, they will only block us.

First dysfunction of a team





Security doesn't understand anything





Security doesn't understand anything

Name	Value	Domain	Path	Expires / Max-Age	Size	▲	HttpOnly	Secure	SameSite
lang	FR	www.theodo.fr	/	Session	6				
session	c9785d5e276...	www.theodo.fr	/	Session	47				



We don't want other tools ; there are too many false positives

They may be right





We don't want other tools ; there are too many false positives

Developers love building & improving things





We don't want other tools ; there are too many false positives

RisXSS, an ESLint rule to detect XSS in React and Vue





We don't want other tools ; there are too many false positives

RisXSS, an ESLint rule to detect XSS in React and Vue

```
export const BlogPost = ({ post }) => {  
  return (  
    <div dangerouslySetInnerHTML={post} />  
  );  
};
```



We don't want other tools ; there are too many false positives

RisXSS, an ESLint rule to detect XSS in React and Vue

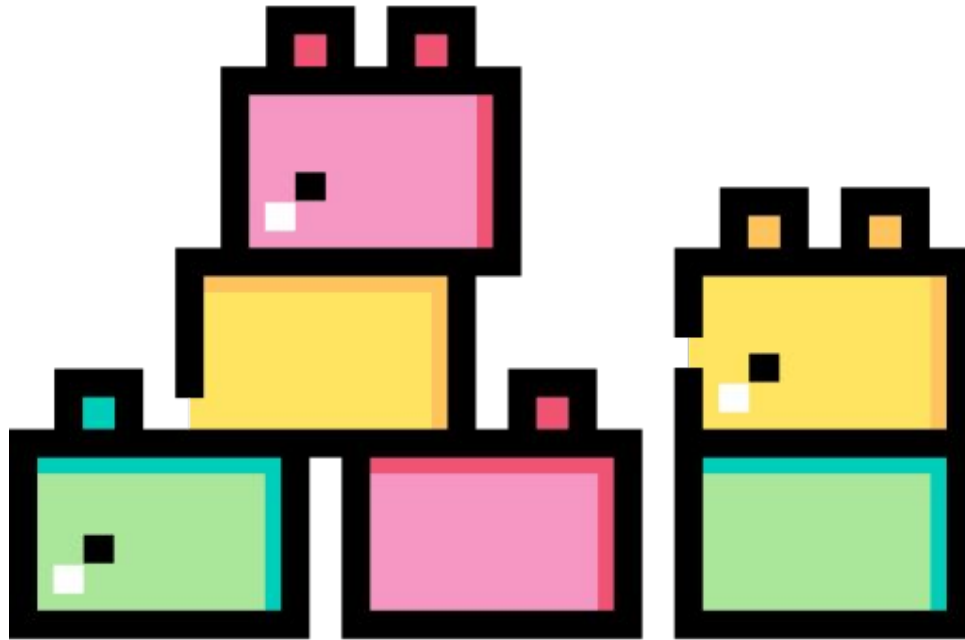
```
import { sanitize } from 'dompurify';

export const BlogPost = ({ post }) => {
  return (
    <div dangerouslySetInnerHTML={{ __html: sanitize(post) }} />
  );
};
```




Security is boring ; I want to build things

Or is it?





Security is boring ; I want to build things

Improving in security has made me a better developer





Security is boring ; I want to build things

Or is it?

Find a LFI	
There's an upload feature	
Manage to upload a PHP reverse shell	
Launch linpeas.sh	
vim is allowed to run as sudo	



What's a cookie?

1

A file containing information about the user stored on the user's computer

3

A file containing information about the user stored on the server

2

A string sent by the server and stored in the browser

4

A delicious shortbread cake with chocolate chips



What's a cookie?

1

A file containing information about the user stored on the user's computer

2

A string sent by the server and stored in the browser

3

A file containing information about the user stored on the server

4

A delicious shortbread cake with chocolate chips



When is a pre-flight request sent to the server? _____

1

Always

4

For form-based POST requests

2

For DELETE, PUT, PATCH requests

5

For GET requests

3

It's a trap

6

For AJAX-based POST requests



When is a pre-flight request sent to the server? _____

1

Always

4

For form-based POST requests

2

For DELETE, PUT, PATCH requests

5

For GET requests

3

It's a trap

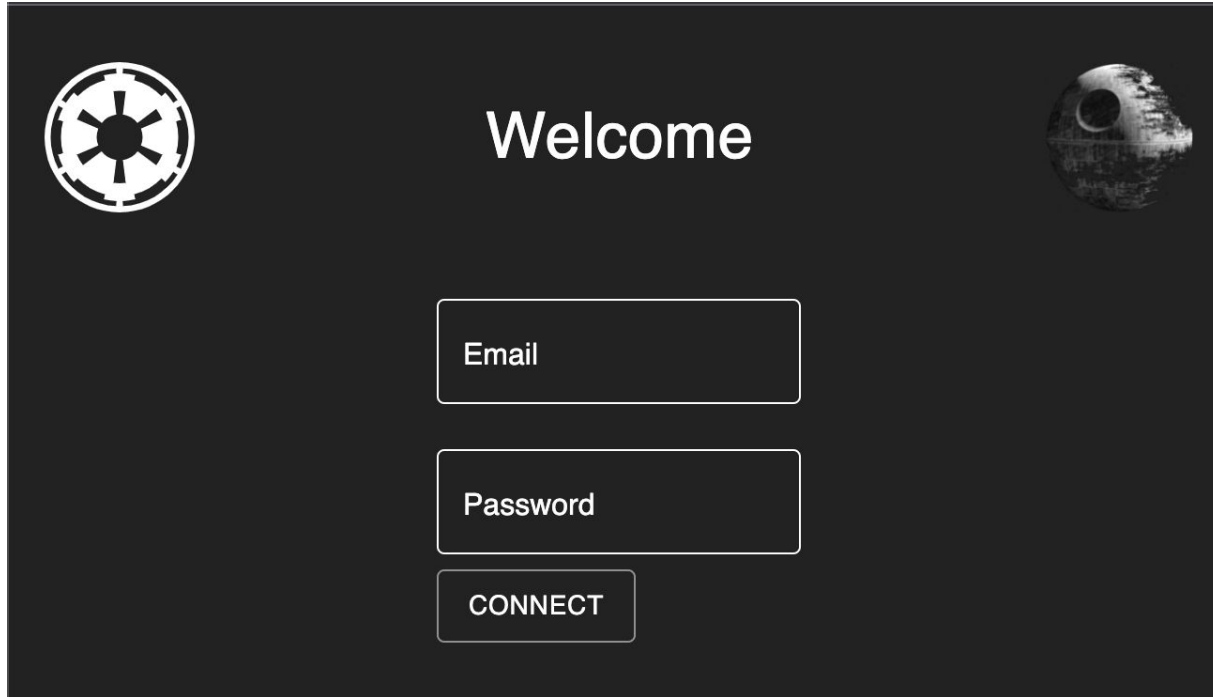
6

For AJAX-based POST requests



Security is boring ; I want to build things

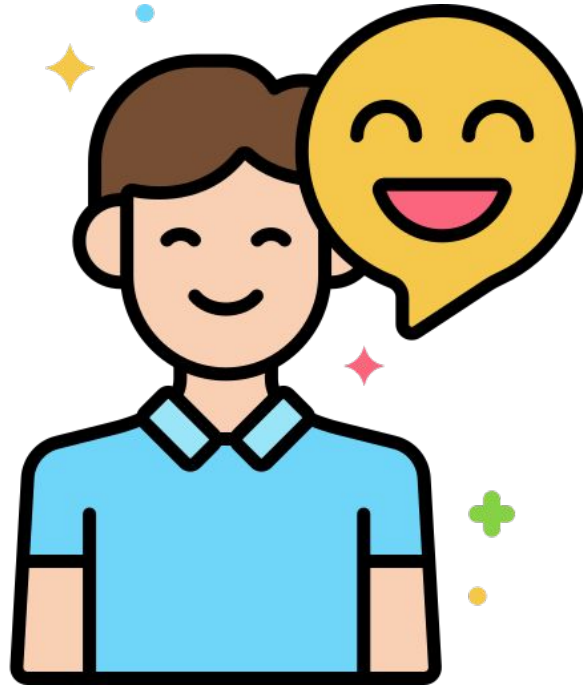
Or is it?





It only happens to other people/companies

Newsletter / storytelling





It only happens to other people/companies

Newsletter / storytelling





It only happens to other people/companies

Newsletter Sécurité #16

Bonjour à toutes et à tous,

En août dernier, un expert en sécurité travaillant chez GitHub a découvert [une faille](#) dans l'application Slack, la célèbre messagerie collaborative utilisée par plus de 12 millions d'utilisateurs. Cette faille montre que même les entreprises stars du digital ne sont pas immunisées contre certaines failles élémentaires. Que s'est-il passé ?

Récupérer les frappes de l'utilisateur grâce à du CSS ?

L'interface de Slack permet à l'utilisateur de choisir la couleur utilisée pour les différents éléments du design. Ainsi il est par exemple possible de spécifier une couleur de fond pour la page sous format hexadécimal : #FFFFFF par exemple pour du blanc.

L'expert a cependant remarqué une anomalie : l'intégralité du champ renseigné pour la couleur est injecté tel quel dans le CSS de la page. Utiliser cette chaîne de caractère : `#FFFFFF; } html {display:none;}` à la place d'une simple couleur a pour effet de faire disparaître tout le contenu de la page.

L'expert a ensuite souhaité vérifier si des données pouvaient fuiter grâce à cette faille. Il a pensé à utiliser une propriété CSS permettant de styliser un élément lorsqu'une certaine valeur (ici la lettre a) est entrée dans un champ input : `input[type="text"][value$="a"]`. En l'associant au chargement d'une image de fond il était capable de créer un début de





It only happens to other people/companies

Escaping is not enough for SQLi...

...Look at what happened to Magento

XSS don't really happen...

...Tell that to Google

No one would actually log the user's passwords in cleartext...

...Well... do you know a company named Facebook

It's not **that** useful to update your dependencies...

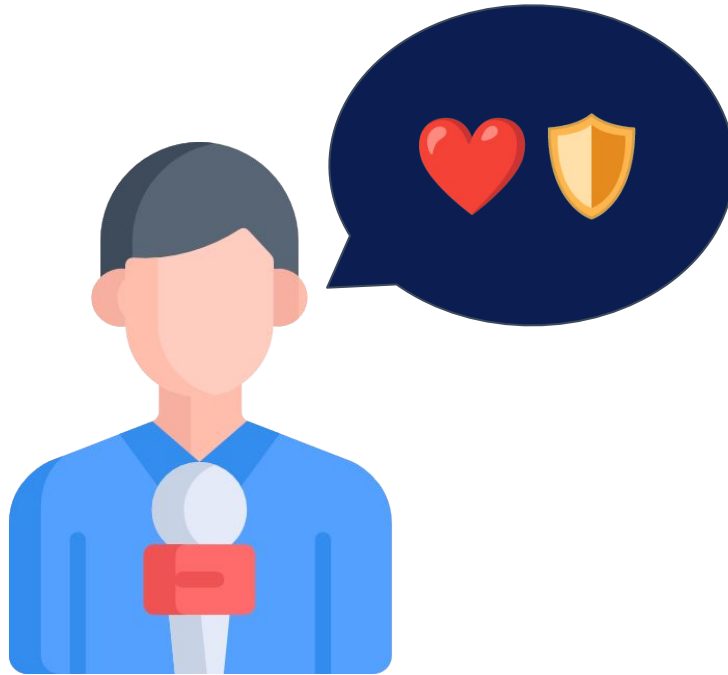
...Do you remember Log4j?





I know security ; my framework protects me

A question for my first talk





I know security ; my framework protects me

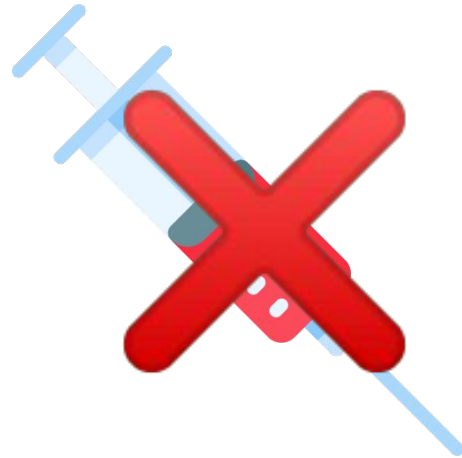
4 levels of competence





I know security ; my framework protects me

SQLi in Symfony





I know security ; my framework protects me

SQLi in Symfony

```
$qb = $this->createQueryBuilder( string: 'user')  
->select('user.name')  
->andWhere('user.id = '.$id);
```



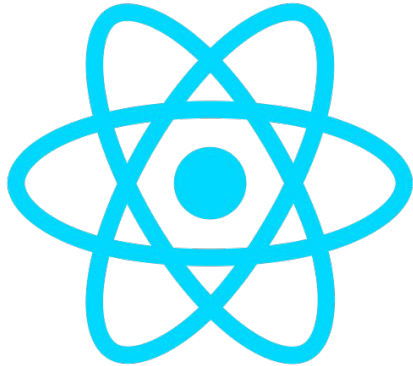
```
$qb = $this->createQueryBuilder( string: 'user')  
->select('user.name')  
->andWhere('user.id = :id')  
->setParameter('id', $id);
```





I know security ; my framework protects me

XSS in React.js



```
return <a href={userUrl}>My personal website</a>;
```



```
javascript:alert('XSS')
```





We didn't think of security this one time!





We didn't think of security this one time!






We didn't think of security this one time!

Projet - Client

- | | | | | | | |
|------------------------------|----------------------------|---------------------|--------------------|-----------|-----------|------|
| 1. Server Injection ✓ | Param. Queries ✓ | Whitelist ✓ | Input validation ✓ | | | |
| 2. Authentication ✗ | User logout ✗ | | | | | |
| 3. Sensible Data ✓ | HTTPS ✓ | Private resources ✓ | | | | |
| 4. XXE ✓ | XXE prevented ✓ | | | | | |
| 5. Access control ✓ | Vertical ✓ | Horizontal ✓ | CSRF ✓ | | | |
| 6. Misconfiguration ✗ | SSH ✓ | Closed ports ✓ | Secrets ✓ | Headers ✓ | Cookies ✗ | DB ✗ |
| 7. XSS ✓ | Design ✓ | URLs ✓ | WYSIWYGs ✓ | | | |
| 8. Insecure deserialization | | | | | | |
| 9. Vulnerable dependencies ✓ | No known vulnerabilities ✓ | | | | | |
| 10. Monitoring | | | | | | |




We didn't think of security this one time!

6 / 8 | Security Report 

- A1. Server Injection** ✓
 - Param. Queries ✓
 - Whitelist ✓
 - Input validation ✓
- A2. Authentication** ✗
 - User logout ✗
 - Passwords encryption ✓
 - Token in URL ✓
 - Forgotten passwords ✓
- A3. Sensible Data** ✓
 - HTTPS ✓
 - Private resources ✓
- A4. XXE** ✓
 - XXE prevented ✓
- A5. Access Control** ✓
 - Vertical ✓
 - Horizontal ✓
 - CSRF ✓
- A6. Misconfiguration** ✗
 - SSH ✓
 - Closed ports ✓
 - Secrets ✓
 - Headers ✓
 - Cookies ✗
 - DB ✗
- A7. XSS** ✓
 - Design ✓
 - URLs ✓
 - WYSIWYGs ✓
- A9. Vulnerable dependencies** ✓
 - No known vulnerabilities ✓

MAJ : 27/06/2018

We didn't think of security this one time!

Company Name YOUR LOGO HERE Nom du projet 

8/10 catégories OK Django / React MAJ le 07/08/2019

A1. Server Injection <ul style="list-style-type: none">✓ Parameterized Queries✓ Whitelisted Inputs✓ Input Validation✓ XXE prevented	A2. Authentication <ul style="list-style-type: none">✓ User logout✓ No token in URLs✓ Forgotten password	A3. Sensitive Data <ul style="list-style-type: none">✓ Forced HTTPS✓ All resources protected✓ Data stored in front
A5. Access Control <ul style="list-style-type: none">✗ Vertical✗ Horizontal✓ CSRF✓ CORS✗ Anti spam system	A6. Misconfiguration <ul style="list-style-type: none">✓ SSH✓ Closed ports✓ Secrets✓ Headers✓ Cookies	A7. XSS (Javascript Injection) <ul style="list-style-type: none">✓ By design✓ In URLs✓ WYSIWYGs
A9. Vulnerable dependencies <ul style="list-style-type: none">✗ Frontend✓ Backend	T1. File Upload <ul style="list-style-type: none">✓ Renamed file✓ Limited File size✓ Whitelist of accepted file type✓ Anti-virus analysis✓ Upload directory	T2. Architecture <ul style="list-style-type: none">✓ Secure communication

✗

AX. Not audited
AX. Not OK
AX. OK

```
id="keywords_info_bar">
  style="float: left;" for="keywords
  class="field_information_container
  id="keywords_count_info" class="field
  style="margin-top: -3px;"></a>
  id="keywords_log" class="field_inform
  teted</a>
  style="float: right; padding-top: 10px;
  style="clear: both;"</div>
  area id="keywords" class="tag_editor
  class="tag-editor ui-sortable">
  style="width:1px"></li>
  class="placeholder">
  <div>Enter keywords or paste via clipboard
  </div>
  area id="keywords_for_clipboard"
  class="btn_keywords_container" style="width:
  class="has-feedback has-clear" style="width:
  body > div > div keywords add...
```



"The definition of quality MUST include security"

Tanya Janca





Add security to *your* definition of quality










3S Framework

Stability Speed Security



Add security to your definition of quality

3S Framework

3S 	Performance	Part	Strengths 🍌	Next steps 🚀
 Stable	 0 1 2 3 4 5 6 7 8 9 10 	Code	Workflow CI + architecture PR Analyse statique / Sonar Tests unitaires + Code coverage + Tests E2E Score SonarCloud / SonarQube / Typemobius Modèle de données	Sentry + analyse régulière logs SEO ?
		Infra	Procd stable à la cible Validation en Préprod (CD) Prod Déploiement auto + rollback + durée Infra professionnalisée	Onboarding facile (installation + doc + makefile)
 Secure	 0 1 2 3 4 5 6 7 8 9 10 =	Code	Dependencies checked and updated automatically Injections are prevented by design	Add re-auth for sensitive actions
		Infra	All components communicate with TLS	Add an AV scanner for uploaded files
 Speed	 0 1 2 3 4 5 6 7 8 9 10 	Code	Score Lighthouse sur Firefox % pages se chargent == 10 Respects clients éventuels	
		Infra	Test inutile au change	



The long run



How to keep up-to-date?

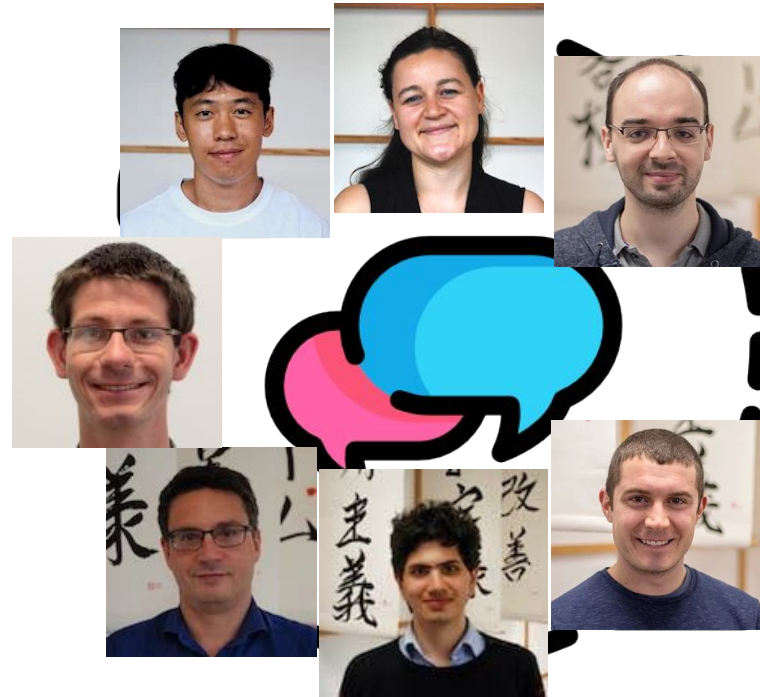
Create a community of practice





How to keep up-to-date?

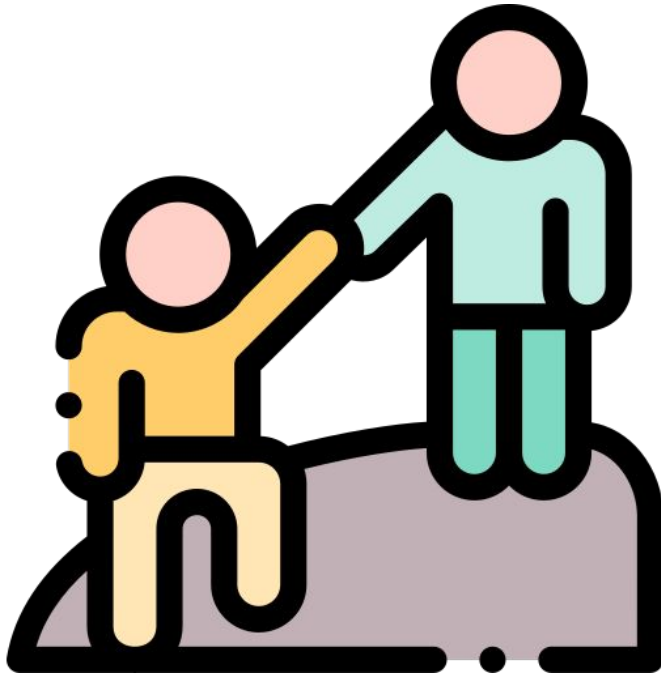
Create a community of practice



@theodo @paulmolin42



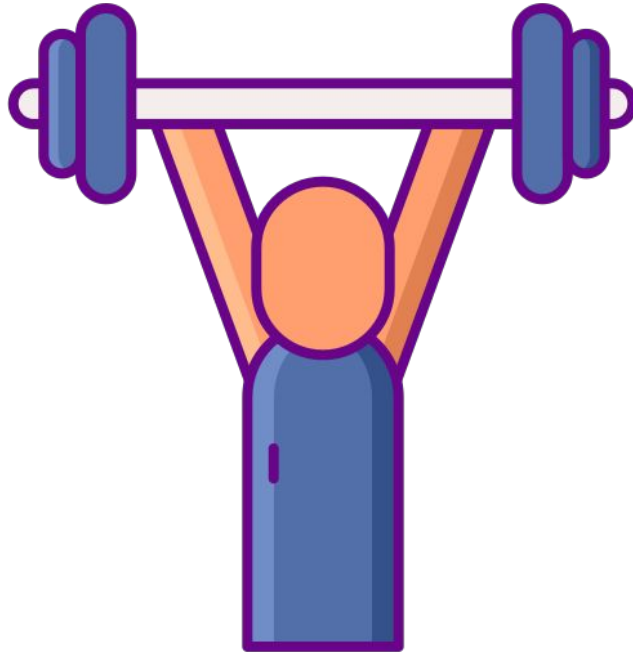
Create communication channels for help





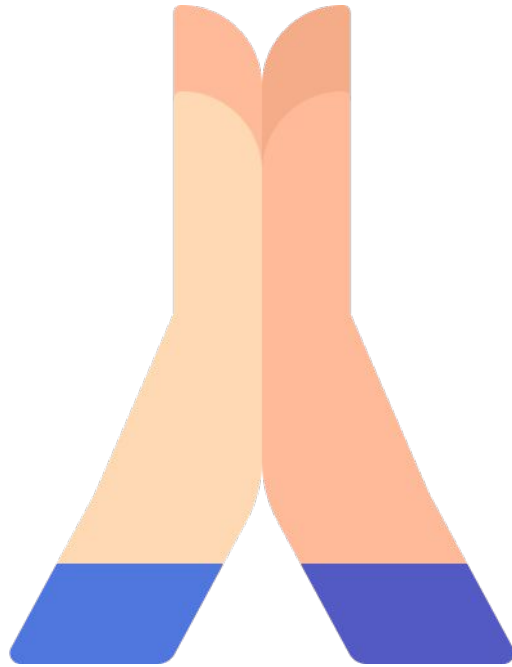
How to keep up-to-date?

Keep training





Thank you for your attention





Questions?

