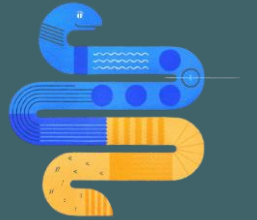
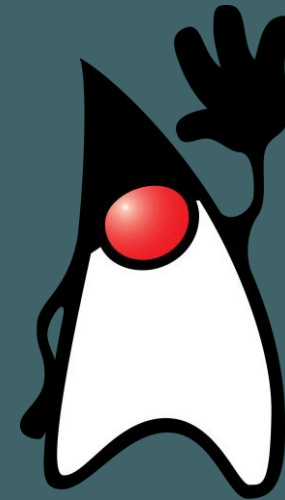


Développer des applications communicantes



SAE 32
27/01

GOMBERT Julien
BERTEAU Yoann
BAZIN Titouan
CAILLET Adrien

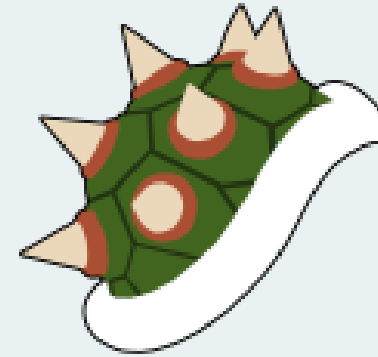
Ordre du jour



- Introduction
- Présentation du produit
- Les principaux problèmes rencontrés
- La gestion du planning
- Les pistes futures

=== SYNCHRONISATION (DIFF) ===

STATUS	SEVERITY	NOM	ENDPOINT
REOPEN	critical	Lighttpd 1.4.34 SQL Injection and P...	http://172.22.3.226
REOPEN	high	Apache 2.4.49 - Path Traversal and ...	http://172.22.3.226
REOPEN	high	Gradio < 2.5.0 - Arbitrary File Read	http://172.22.3.226
REOPEN	high	PHP Development Server <= 7.4.21 - ...	http://172.22.3.226
REOPEN	high	Generic Linux - Local File Inclusion	http://172.22.3.226
REOPEN	high	Bullwark Momentum Series JAWS 1.0 -...	http://172.22.3.226
REOPEN	high	gSOAP 2.8 - Local File Inclusion	http://172.22.3.226
REOPEN	critical	Pulse Connect Secure SSL VPN Arbitr...	http://172.22.3.226
REOPEN	high	Onkyo TX-NR585 Web Interface - Dire...	http://172.22.3.226
REOPEN	high	MagicFlow - Local File Inclusion	http://172.22.3.226
REOPEN	high	Nginx Server - Local File Inclusion	http://172.22.3.226
REOPEN	medium	MERCUSYS Mercury X18G 1.0.5 Router ...	http://172.22.3.226
REOPEN	high	Huawei HG255s - Local File Inclusion	http://172.22.3.226



Bowser Shell

Application Java (Linux) :
permettant de regrouper des
outils pour faire des audits de
sécurité

Scope : CVE Web

Application Web (Linux) :
Tableau dynamique
(recherche, tri, filtrage,
pagination côté serveur)

M2M : API REST

Application Android :
Visualisation des CVE

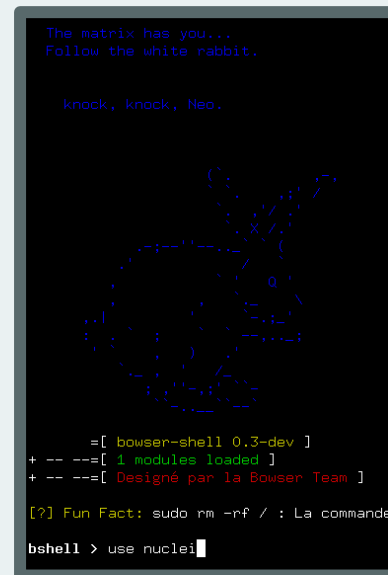
Gestion Failles

Faillies (CVE)

Recherche (name/target/state) Target exacte Tous états ID 1 25 / page Réinitialiser

58 résultat(s)

ID	Name	Target	State	Infos
1	Lighttpd 1.4.34 SQL Injection and Path Traversal	http://172.22.3.226	closed	Voir (3 clés)
2	Apache 2.4.49 - Path Traversal and Remote Code Execution	http://172.22.3.226	closed	Voir (3 clés)
3	Gradio < 2.5.0 - Arbitrary File Read	http://172.22.3.226	closed	Voir (3 clés)
4	PHP Development Server <= 7.4.21 - Remote Source Disclosure	http://172.22.3.226	closed	Voir (3 clés)
5	Generic Linux - Local File Inclusion	http://172.22.3.226	closed	Voir (3 clés)
6	Bullwark Momentum Series JAWS 1.0 - Local File Inclusion	http://172.22.3.226	closed	Voir (3 clés)
7	gSOAP 2.8 - Local File Inclusion	http://172.22.3.226	closed	Voir (3 clés)
8	Nextjs <2.4.1 - Local File Inclusion	http://172.22.3.226	closed	Voir (3 clés)
9	uWSGI PHP Plugin Local File Inclusion	http://172.22.3.226	closed	Voir (3 clés)





```
root@rtnnnpxx:~# dpkg -  
dpkg: avertissement: «  
dpkg: avertissement: «  
dpkg: erreur: 2 program  
Note : la variable PATH
```

```
$ export PATH=$PATH:/usr/local/bin  
$ env | grep PATH
```

Problèmes dpkg, path et root (voir email Masson)
+ le forwarding et le réseau de la VM nous sont inconnus donc Tunnel SSH ☺



FastApi : Complicé à comprendre pour le M2M Android/web



Flask
web development,
one drop at a time

Faire cohabiter différents frameworks

PProjet						
1,0Application Java Scanner CVE			R	A	C	I
T	1.1	Application CLI	Julien	Titouan	Groupe	Groupe
T	1.2	Gestion BdD		Yoann	Groupe	Groupe
T	1.3	Design UML		Adrien	Groupe	Groupe
T	1.4	Documentation / Guide		Julien	Groupe	Groupe
2,0Application Android						
T	2.1	[GUI] Activité n °1	Adrien	Titouan	Groupe	Groupe
T	2.2	[GUI] Activité n °2	Titouan	Adrien	Groupe	Groupe
T	2.3	[JAVA] Activité n °1	Adrien	Titouan	Groupe	Groupe
T	2.4	[JAVA] Activité n °2	Titouan	Adrien	Groupe	Groupe
T	2.5	Communication API	Titouan	Yoann	Groupe	Groupe
T	1.4	Documentation / Guide	Adrien, Titouan	Julien	Groupe	Groupe
3,0Communication FastAPI						
T	3.1	Intégration API	Yoann	Titouan	Groupe	Groupe
	3.21	Gestion BdD	Yoann	Julien	Groupe	Groupe
	3.22	Serveur Python	Yoann	Yoann	Groupe	Groupe
T	1.4	Documentation / Guide	Yoann	Julien	Groupe	Groupe
4.0Base de donnée						
T	4.1	Installation / Configs SQLite	Julien	Yoann	Groupe	Groupe
T	4.3	Intégration dans SQLite	Yoann , Julien	Julien	Groupe	Groupe
5.0Documents IA						
T	4.1	Julien	Julien	Julien	Groupe	Groupe
T	4.2	Adrien	Adrien	Julien	Groupe	Groupe
T	4.3	Titouan	Titouan	Julien	Groupe	Groupe
T	4.3	Yoann	Yoann	Julien	Groupe	Groupe

Bowser Shell

Ressenti :

C'était un peu serré avec l'alternance mais sinon ça va bien.

Test / QA :

On a eu le temps de test sur la VM linux, l'app Java et Web à chaque release.





Fork de metasploit :
Devenir une alternative à metasploit

Outils :
Rajoutez d'autres outils
comme NMAP



UX (Expérience utilisateur) :
Refaire le design.

Merci

