



Audit intrusif externe

 Rapport d'audit

Vos interlocuteurs

Yves Duchesne	Gwenn Feunteun
Responsable d'audit	Expert en sécurité de l'information
yves@acceis.fr	gwenn@acceis.fr
06.16.46.26.36	07.80.53.12.49

Maîtrise du document

Réf. Document	DHMTS-001-RAP01
Version	1.0
Validé le	29/09/2017
Validé par	Gwenn Feunteun

Historique des modifications

Version	Date	Modifications apportées
1.0	29/09/2017	Rédaction initiale du document

Diffusion

Niveau de classification	Restreint
Liste de diffusion	DHIMYOTIS

DEFINITION DES NIVEAUX DE CLASSIFICATION UTILISÉS :

- **Public** : les informations contenues dans ce document peuvent être diffusées sans aucune restriction
- **Restreint** : les informations contenues dans ce document ne peuvent être communiquées qu'à des personnels d'**ACCEIS** ou de ses partenaires.
- **Confidentiel** : les informations contenues dans ce document ne peuvent être communiquées qu'à des personnels d'**ACCEIS** ou des tiers explicitement identifiés dans la liste de diffusion.
- **Secret** : les informations contenues dans ce document ne peuvent être communiquées qu'aux personnes physiques identifiées dans la liste de diffusion.

Sommaire

1. PRESENTATION DU DOCUMENT	4
1.1. OBJET DU DOCUMENT	4
1.2. PRESENTATION DU CONTEXTE ET DE LA CIBLE.....	4
2. RESULTATS DE L'AUDIT	5
2.1. SYNTHESE MANAGERIALE	5
2.1. VULNERABILITES IDENTIFIEES	6
2.2. RECOMMANDATIONS FORMULEES.....	7
3. DEMARCHE DETAILLEE	9
3.1. PHASE DE DECOUVERTE	9
3.1.1. IDENTIFICATION DES SERVICES EXPOSES.....	9
3.1.1. RECHERCHE DE VULNERABILITES APPLICATIVES	16
3.1.2. ANALYSE DU CHIFFREMENT DES COMMUNICATIONS	17
3.1.3. COLLECTE INDIRECTE D'INFORMATIONS.....	23
3.1. RECHERCHE DE VULNERABILITES.....	26
3.1.1. CROSS-SITE SCRIPTING (XSS).....	26
3.1.2. CONTOURNEMENT DU CODE DE VERIFICATION	28
3.2. TESTS NON CONCLUANTS	29

1. PRESENTATION DU DOCUMENT

1.1. Objet du document

Ce document constitue le rapport final d'analyse, présentant les résultats de l'audit intrusif externe effectué par ACCEIS, en mode boîte noire, à la demande DHIMYOTIS.

1.2. Présentation du contexte et de la cible

Dans le cadre de sa certification ISO/CEI 27001, ainsi que pour ses activités de prestataire de service de confiance à l'échelle nationale (notamment au travers de la production de certificats RGS *, ** et ***), mais également européenne grâce à la délivrance de certificats qualifiés eIDAS, DHIMYOTIS doit faire réaliser de manière régulière des audits de sécurité de son système d'information.

C'est à ce titre qu'elle a souhaité mener une campagne d'audits intrusifs externes sur ses points d'interconnexion avec Internet, en mode boîte noire ; c'est-à-dire sans connaissance préalable de la cible (autre que les adresses) et sans disposer d'accès spécifique aux applications présentes.

Le périmètre d'intervention portait sur les adresses IP suivantes :

- 109.197.245.10 ;
- 109.197.245.5 ;
- 109.197.245.9 ;
- 46.29.127.152 ;
- 46.29.127.177 ;
- 46.29.127.180 ;
- 46.29.127.181 ;
- 46.29.127.186 ;
- 46.29.127.179 ;
- 46.26.127.185.

Les tests ont été réalisés au travers d'Internet, depuis les locaux d'ACCEIS à Rennes, du 28 août au 5 septembre 2017. Une autorisation d'audit a été transmise à ACCEIS par M. Josselin ALLEMANDOU pour la période et les adresses IP correspondantes.

2. RESULTATS DE L'AUDIT

2.1. Synthèse managériale

Les tests d'intrusion réalisée pour le compte de la société DHIMYOTIS ont mis en évidence un assez bon niveau de sécurité sur le périmètre.

Plusieurs fuites d'information mineures ont pu être identifiées et celle-ci ont mis en évidence à l'utilisation d'un serveur Oracle GlassFish a priori obsolète et présentant de nombreuses vulnérabilités. Toutefois ces dernières concernent principalement l'interface d'administration, qui n'est pas joignable depuis Internet. Il est cependant recommandé de changer ce composant au plus vite.

D'autre part, assez peu d'applications sont présentes. La surface d'exposition reste donc plutôt limitée. Les auditeurs ont cependant mis en évidence la présence de deux vulnérabilités de type Cross Site Scripting (ou XSS), permettant un individu malintentionné (sous certaines conditions) de faire exécuter à un utilisateur du service <https://sae.certigna.fr/> du code JavaScript à son insu.

De même un des services identifiés requiert la saisie d'un code de validation lors de la demande de génération d'un nouveau certificat. Ce code à quatre chiffres, envoyés par e-mail, peut facilement être attaqué via des essais successifs. Il serait souhaitable, si l'usage d'un tel mécanisme est nécessaire, d'utiliser un code plus complexe.

La mise en œuvre des recommandations présentes au sein de ce rapport permettra à DHIMYOTIS d'atteindre un niveau de sécurité proche de l'état de l'art.











2.1. Vulnérabilités identifiées



Le tableau ci-dessous présente les vulnérabilités identifiées lors de l'audit, classées par ordre de gravité décroissante.

ID	Description	Gravité
<u>Utilisation de logiciels obsolètes</u>		
2	La présence d'un serveur Oracle GlassFish en version 3.1.2 a été mis en évidence. Ce serveur applicatif n'est plus supporté par son éditeur et présente de très nombreuses vulnérabilités. De plus, la version d'Apache utilisée pour certains services présente également des vulnérabilités.	7,5
<u>Présence de Cross-Site Scripting</u>		
4	Certains paramètres de l'application https://sae.certigna.fr ne sont pas correctement filtrés et permettent l'injection de code HTML ou JavaScript dans certaines pages. Un pirate pourrait faire exécuter du code malveillant à un utilisateur dans le contexte de l'application en l'incitant à cliquer sur un lien malformé (transmis dans un e-mail par exemple).	7,1
<u>Multiples fuites d'informations techniques</u>		
1	La configuration des services exposés sur Internet permet la diffusion de nombreuses informations techniques relatives aux applicatifs installés, ainsi qu'à leur version. De plus, des ont été découverts, fournissant un très grand nombre d'informations techniques sur les systèmes sous-jacents.	5,3
<u>Contournement du code de validation</u>		
5	Il est possible de contourner le mécanisme de validation des demandes de l'application i milo, car le code demandé n'a pas une complexité suffisante (quatre caractères numériques. Un attaquant peut énumérer rapidement toutes les combinaisons possibles afin de trouver la bonne.	5,3
<u>Configuration cryptographique perfectible</u>		
3	La configuration cryptographique de certains services SSL/TLS peut être améliorée. Elle présente actuellement des défauts de paramétrage, voire de mise à jour des applicatifs, pouvant permettre sous certaines conditions la réalisation d'attaques visant à diminuer la qualité de la protection des communications ou de provoquer un déni de service.	5,0

2.2. Recommandations formulées

Le tableau ci-dessous présente les recommandations formulées lors de l'audit, classées par ordre de priorité et de difficulté de mise en œuvre décroissante.

ID	Description	Priorité	Complexité
<u>Utilisation de logiciels obsolètes</u>			
RC-2.1	Mettre régulièrement à jour tous les composants logiciels de son infrastructure et désactiver des applicatifs obsolètes.		
<u>Présence de Cross-Site Scripting</u>			
RC-4.1	Il est recommandé de mettre en place (ou d'étendre) une solution de protection contre les attaques par XSS qui procédera à l'échappement ou l'encodage des caractères dangereux par l'intermédiaire d'une fonction dédiée à cet effet ou par l'intégration d'un framework d'interface incluant une couche de sécurité.		
<u>Multiples fuites d'informations techniques</u>			
RC-1.1	Supprimer les fichiers PHP info.		
<u>Multiples fuites d'informations techniques</u>			
RC-1.2	Modifier la configuration des services pour ne pas afficher les versions dans les bannières, les entêtes, ainsi que les pieds de page.		
<u>Contournement du code de validation</u>			
RC-5.1	Utiliser un code secret plus complexe pour la validation des demandes ou désactivées la demande après un trop grand nombre de tentatives infructueuses.		
<u>Configuration cryptographique perfectible</u>			
RC-3.1	Désactiver l'usage de TLS en version 1.0 et lui préférer les version 1.1 et 1.2.		

ID	Description	Priorité	Complexité
<u>Configuration cryptographique perfectible</u>			
RC-3.1	Utiliser des suites de chiffrements robustes (proscrire MD5, SHA-1, RC4 et dans la mesure du possible, les algorithmes utilisant un mode CBC).		

3. DEMARCHE DETAILLEE

3.1. Phase de découverte

3.1.1. Identification des services exposés

Plusieurs actions ont été réalisées pour identifier les services exposés sur les différents hôtes du périmètre. A ce titre, les auditeurs ont réalisé une série de scan de ports via l'outil *nmap*. Les informations suivantes ont été mises en évidence :

```
nmap -sV -n -A -T4 -PN -p- -vv -iL ../ips.txt -oA dhimytis
```

▪ 109.197.245.10

```
Host is up, received user-set (0.11s latency).
Scanned at 2017-08-28 11:49:15 CEST for 17274s
Not shown: 65534 filtered ports
Reason: 65534 no-responses
PORT      STATE SERVICE REASON      VERSION
```

▪ 109.197.245.5

```
Host is up, received user-set (0.053s latency).
Scanned at 2017-08-28 11:49:15 CEST for 17274s
Not shown: 65510 filtered ports
Reason: 65510 no-responses
PORT      STATE SERVICE REASON      VERSION
80/tcp    open  tcpwrapped syn-ack ttl 55
1000/tcp  open  ssl/cadlock? syn-ack ttl 54
1001/tcp  open  ssl/webpush? syn-ack ttl 54
1002/tcp  open  ssl/http syn-ack ttl 54 Oracle GlassFish 3.1.2
(Servlet 3.0; JSP 2.2; Java 1.8)
1003/tcp  open  ssl/http syn-ack ttl 54 Oracle GlassFish 3.1.2
(Servlet 3.0; JSP 2.2; Java 1.8)
1004/tcp  open  ssl/unknown syn-ack ttl 54
1005/tcp  open  ssl/http syn-ack ttl 54 Apache httpd 2.4.25
((Debian))
8008/tcp  open  http syn-ack ttl 55 Fortinet FortiGuard block
page
```

▪ 109.197.245.9

```
Host is up, received user-set (0.074s latency).
Scanned at 2017-08-28 11:49:15 CEST for 17274s
Not shown: 65534 filtered ports
Reason: 65534 no-responses
PORT      STATE SERVICE REASON      VERSION
```

▪ 46.29.127.152

```
Host is up, received user-set (0.029s latency).
Scanned at 2017-08-28 11:49:15 CEST for 17274s
Not shown: 65514 filtered ports
Reason: 65514 no-responses
```

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack ttl 53	Apache httpd
443/tcp	open	ssl/https	syn-ack ttl 52	
8008/tcp	open	http	syn-ack ttl 53	Fortinet FortiGuard block page

▪ 46.29.127.177

```
Host is up, received user-set (0.035s latency).
Scanned at 2017-08-28 11:49:15 CEST for 17274s
Not shown: 65510 filtered ports
Reason: 65510 no-responses
```

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	tcpwrapped	syn-ack ttl 54	
1000/tcp	open	ssl/cadlock?	syn-ack ttl 53	
1001/tcp	open	ssl/webpush?	syn-ack ttl 53	
1002/tcp	open	ssl/http	syn-ack ttl 53	Oracle GlassFish 3.1.2 (Servlet 3.0; JSP 2.2; Java 1.8)
1003/tcp	open	ssl/http	syn-ack ttl 53	Oracle GlassFish 3.1.2 (Servlet 3.0; JSP 2.2; Java 1.8)
1004/tcp	open	ssl/unknown	syn-ack ttl 53	
1005/tcp	open	ssl/http	syn-ack ttl 53	Apache httpd 2.4.25 ((Debian))
8008/tcp	open	http	syn-ack ttl 54	Fortinet FortiGuard block page

▪ 46.29.127.180

```
Host is up, received user-set (0.035s latency).
Scanned at 2017-08-28 11:49:15 CEST for 17274s
Not shown: 65519 filtered ports
Reason: 65519 no-responses
```

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	tcpwrapped	syn-ack ttl 53	
443/tcp	open	ssl/https	syn-ack ttl 52	CertignaTS/1.0
8008/tcp	open	http	syn-ack ttl 53	Fortinet FortiGuard block page

■ 46.29.127.181

```
Host is up, received user-set (0.041s latency).
Scanned at 2017-08-28 11:49:15 CEST for 17274s
Not shown: 65510 filtered ports
Reason: 65510 no-responses
```

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack ttl 54	Apache httpd
389/tcp	open	ldap	syn-ack ttl 53	(Anonymous bind OK)
8008/tcp	open	http	syn-ack ttl 54	Fortinet FortiGuard block page

■ 46.29.127.186

```
Host is up, received user-set (0.030s latency).
Scanned at 2017-08-28 11:49:15 CEST for 17274s
Not shown: 65517 filtered ports
Reason: 65517 no-responses
```

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	tcpwrapped	syn-ack ttl 53	
443/tcp	open	ssl/http	syn-ack ttl 52	Oracle GlassFish 3.1.2 (Servlet 3.0; JSP 2.2; Java 1.8)
8008/tcp	open	http	syn-ack ttl 53	Fortinet FortiGuard block page

■ 46.29.127.179

```
Host is up, received user-set (0.032s latency).
Scanned at 2017-08-28 11:49:15 CEST for 17274s
Not shown: 996 filtered ports
Reason: 996 no-responses
```

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack ttl 53	
113/tcp	closed	ident	reset ttl 53	
443/tcp	open	tcpwrapped	syn-ack ttl 52	
8008/tcp	open	tcpwrapped	syn-ack ttl 53	

Sur l'ensemble des hôtes scannés, il apparaît que deux d'entre-eux (109.197.245.9 et 109.197.245.10) ne semble pas exposer de service sur Internet (ou une restriction d'accès par adresse IP source est en place à minima).

Les services présentés semblent tous légitimes, mais l'analyse révèle que la plupart expose publiquement des bannières détaillées. Les technologies suivantes sont utilisées :

- 3 Oracle GlassFish 3.1.2 (Servlet 3.0; JSP 2.2; Java 1.8) ;
- 4 serveurs Apache (dont au moins 2 en version 2.4.25 sur un système Debian) ;
- 1 service LDAP ;
- 1 pare-feu de type Fortinet.

D'autre-part, au-delà de certains services présentant des bannières fournissant des informations sur la version des applications utilisées, certains d'entre, notamment dans leur page d'erreur, fournissent également ses données.

- 109.197.145.5, port 1005 (2D-Origin)

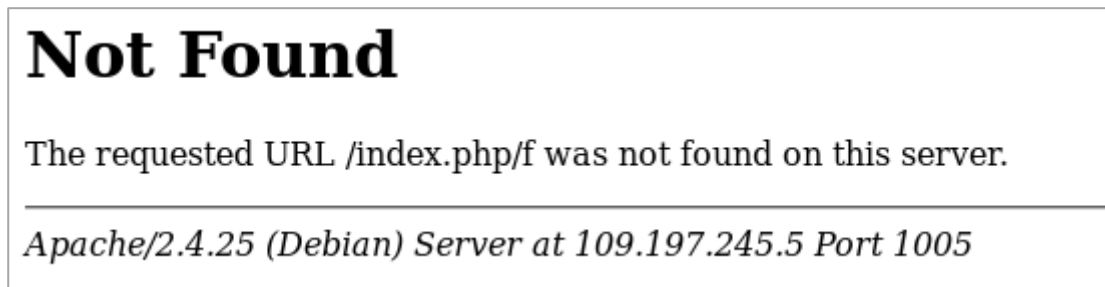


Figure 1 – Erreur HTTP 404 affichant la version du service.

De même, deux page *phpinfo* ont été identifiées. Elles fournissent une très grande quantité de données sur la configuration des systèmes utilisés.

- 109.197.145.5, port 1005 (2D-Origin)


PHP Version 7.0.19-1 	
System	Linux 2dorigin-vm-pp-dc1 4.9.0-3-amd64 #1 SMP Debian 4.9.30-2+deb9u3 (2017-08-06) x86_64
Build Date	May 11 2017 14:04:47
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-curl.ini, /etc/php/7.0/apache2/conf.d/20-dom.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-simplexml.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini, /etc/php/7.0/apache2/conf.d/20-wddx.ini, /etc/php/7.0/apache2/conf.d/20-xmlreader.ini, /etc/php/7.0/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.0/apache2/conf.d/20-xsl.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012.NTS
PHP Extension Build	API20151012.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2

Figure 2 - Extrait de page *phpinfo* de 109.197.145.5.

- 46.29.127.177, port 1005 (2D-Origin)


PHP Version 7.0.19-1	
	
System	Linux 2dorigin-vm-pp-dc2 4.9.0-3-amd64 #1 SMP Debian 4.9.30-2+deb9u3 (2017-08-06) x86_64
Build Date	May 11 2017 14:04:47
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-curl.ini, /etc/php/7.0/apache2/conf.d/20-dom.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-simplexml.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini, /etc/php/7.0/apache2/conf.d/20-wddx.ini, /etc/php/7.0/apache2/conf.d/20-xmlreader.ini, /etc/php/7.0/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.0/apache2/conf.d/20-xsl.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012.NTS
PHP Extension Build	API20151012.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*
This program makes use of the Zend Scripting Language Engine:	










Figure 3 - Extrait de page phpinfo de 46.29.127.177.

La connaissance de ces informations facilite le travail d'un attaquant. Il est recommandé de modifier la configuration des services exposés pour ne plus fournir de détails techniques sur les technologies utilisées.

5,3

VULN-1 – Multiples fuites d'informations techniques

La configuration des services exposés sur Internet permet la diffusion de nombreuses informations techniques relatives aux applicatifs installés, ainsi qu'à leur version. De plus, des ont été découverts, fournissant un très grand nombre d'informations techniques sur les systèmes sous-jacents.

Exploitation		Impact			CVSS v3
Facilité	Exposition	D	I	C	
					AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Mesure(s) corrective(s)					
Id.	1.1	Supprimer les fichiers <i>PHP info</i> .			
Priorité					
Complexité					
Id.	1.2	Modifier la configuration des services pour ne pas afficher les versions dans les bannières, les entêtes, ainsi que les pieds de page.			
Priorité					
Complexité					

La suppression des informations de version dans les bannières exposées, ainsi qu'en bas des pages par défaut des services peut être réalisée en changeant les éléments de configuration suivants :

- **Apache** (fichier */etc/apache2/conf.d/security* sous Debian)

```
#....
ServerTokens Prod
#....
ServerSignature Off
```

- **Oracle GalssFish**

Ajouter ou modifier l'option *-Dproduct.name=""* à la JVM.

La présence de services HTTPS a également permis de collecter des informations sur les domaines utilisés au travers des certificats fournis. La capture suivante illustre ce point pour le serveur 109.197.245.5, sur le port TCP 1002 :

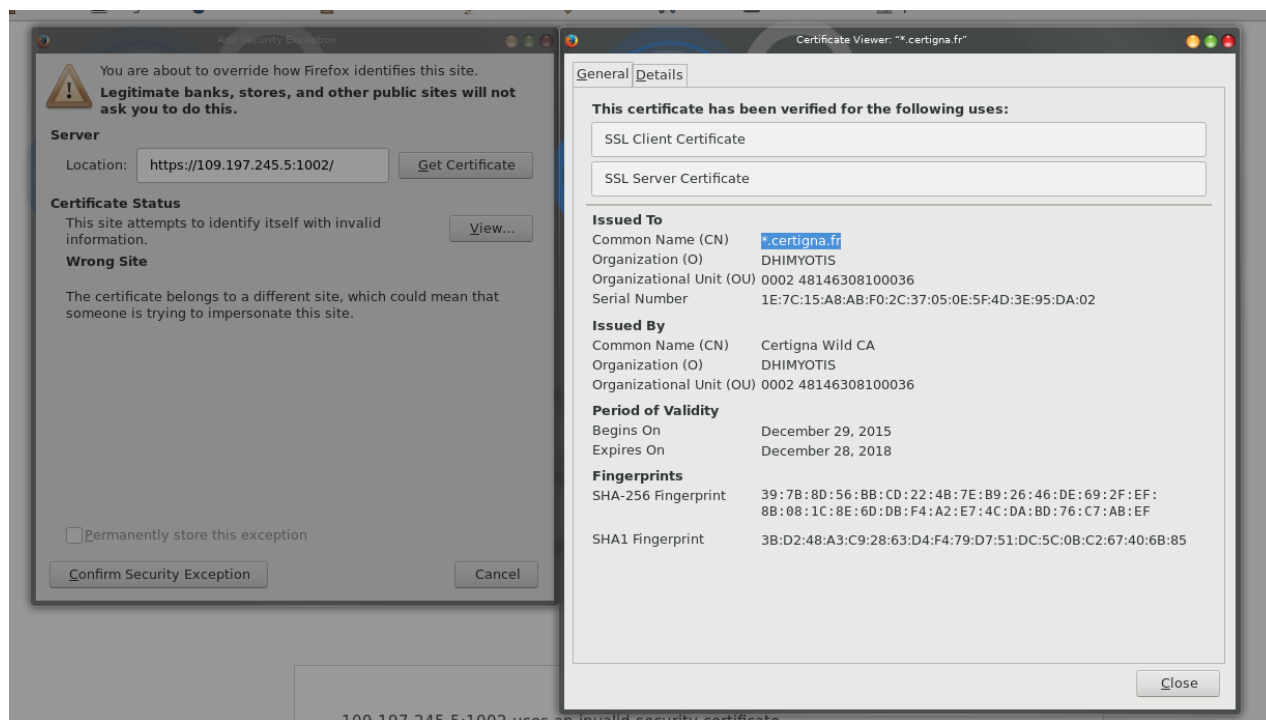


Figure 4 - Certificat *.certigna.fr.

Les CN suivant ont ainsi été identifiés :

CN	Hôte:port
api.mapreuve.com	109.197.245.5:1000 46.29.127.177:1000
gest.certigna.fr	109.197.245.5:1001 46.29.127.152:443
*.certigna.fr	109.197.245.5:1002 109.197.245.5:1003 46.29.127.177:1002 46.29.127.177:1003 46.29.127.180:443
*.dhimyotis.com	109.197.245.5:1004 46.29.127.177:1004
2dorigin.com	46.29.127.177:1005
ws.certigna.fr	46.29.127.186:443
www.certigna.com	46.29.127.179:443

D'autre part, le service LDAP exposé autorise les connexions en mode anonyme. D'après les éléments remontés, il semblerait que ce serveur soit utilisé pour la publication de listes de révocation de certificat.



attribute type	value
subschemaSubentry	cn=Subschema
structuralObjectClass	oLDistributionPoint
modifyTimestamp	20160909091701Z
modifiersName	cn=admin,dc=certigna,dc=fr
hasSubordinates	FALSE
entryUUID	f98f242f937-102f-93d0-8f2b14d62
entryDN	cn=Certigna Authentication PRIS***,ou=IGC,dc=certigna,dc=fr
entryCSN	20160909091701.997164Z#000000#000#000000
creatorName	cn=admin,dc=certigna,dc=fr
createTimestamp	20110412100418Z
authorityRevocationList	certigna Authentication PRIS*** (non string data)
certificateRevocationList	(non string data)
objectClass	oLDistributionPoint
objectClass	pkcA
crossCertificatePair	
deltaRevocationList	

Figure 5 - Accès au service LDAP.

Le scan de ports n'a pas remonté la présence de services LDAPS, prenant en charge le chiffrement des communications et assurant ainsi la sécurité d'une éventuelle authentification sur l'annuaire. Il semblerait que les informations de révocation soient mises à jour par l'administrateur disposant d'un compte spécifique. Dans ce contexte, il est légitime de supposer que ces tâches de mise à jour soient réalisées via le protocole LDAP et non pas sa version sécurisée (sauf si le service LDAPS n'est exposé qu'à une liste prédéfinie d'autres).

Cela peut donc présenter un risque pour la sécurité des éléments d'authentification de l'administrateur. En cas d'attaque de type *Man in the Middle*, une personne malveillante serait susceptible de voler le mot de passe utilisé.

En l'état, et sans informations complémentaires, il n'est pas possible de noter ce point comme une vulnérabilité, mais une attention particulière doit y être portée.

3.1.1. Recherche de vulnérabilités applicatives

La version 3.1.2 du serveur GlassFish a été publiée en février 2012. Il s'agit d'une version obsolète (la dernière version publiée est la 5.0) qui présente 11 vulnérabilités connues dont une avec score CVSS de 10 (https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-20700/version_id-136591/Oracle-Glassfish-Server-3.1.2.html) :

- CVE-2017-3626
- CVE-2017-3247
- CVE-2016-5519
- CVE-2013-1508
- CVE-2017-3250
- CVE-2017-3239
- CVE-2016-3607
- CVE-2012-3155
- CVE-2017-3249
- CVE-2016-5528
- CVE-2015-3237








Toutefois, les codes d'exploitation présents publiquement sur Internet nécessitent de pouvoir accéder à l'interface d'administration du service (même sans être authentifié). Or, elle n'est pas exposée sur les cibles auditées, ce qui permet de réduire le risque.

De même, la version 2.4.25 des services Apache présente également des vulnérabilités identifiées (https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-218176/Apache-Http-Server-2.4.25.html). Cependant, ils semblent être utilisés sur des plateformes de type Debian, connue pour « backporter » les correctifs de sécurité publiés sans faire évoluer les numéros de version de service. Il est donc difficile à ce stade de confirmer si ces services sont vulnérables ou non.

7,5

VULN-2 – Utilisation de logiciels obsolètes

La présence d'un serveur Oracle GlassFish en version 3.1.2 a été mis en évidence. Ce serveur applicatif n'est plus supporté par son éditeur et présente de très nombreuses vulnérabilités. De plus, la version d'Apache utilisée pour certains services présente également des vulnérabilités.

Exploitation		Impact			CVSS v3
Facilité	Exposition	D	I	C	
					AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
Mesure(s) corrective(s)					
Id.	1.1	Mettre régulièrement à jour tous les composants logiciels de son infrastructure et désactiver des applicatifs obsolètes.			
Priorité					
Complexité					

3.1.2. Analyse du chiffrement des communications

L'analyse a mis en évidence l'usage de mécanismes de chiffrement des communications afin d'assurer la confidentialité des échanges avec les clients applicatifs. Il s'agit de manière générale d'une bonne mesure de sécurité, mais la mise en œuvre de telles solutions doit respecter plusieurs exigences afin de garantir réellement la protection des données transférées. En effet, l'histoire du protocole SSL/TLS et parsemée de faiblesses et de vulnérabilités permettant sous certaines conditions de diminuer le niveau de sécurité des communications (voire de supprimer les fonctions de chiffrement), de manipuler le contenu des échanges ou même de récupérer des données sensibles au niveau du serveur.

Afin d'analyser la configuration des services, plusieurs outils ont été utilisés, notamment *testssl.sh*. Les points nécessitant une attention particulière sont synthétisés ci-après.

Versions de protocole supportées

Le tableau suivant reprend les versions du protocole SSL/TLS supportées par l'ensemble des services utilisant HTTPS :

Version	Supporté	Vulnérable
TLS v1.2	Oui	Non
TLS v1.1	Oui	Non
TLS v1.0	Oui	Oui
SSL v3.0	Non	Oui
SSL v2.0	Non	Oui

L'usage du protocole TLS en version 1.0 ne peut être jugé comme sûr à condition de prendre certaines précautions ; ce qui n'est pas le cas avec les versions 1.1 et 1.2 qui ne posent pas de problèmes de sécurité à leur actuelle. C'est pourquoi il n'est pas recommandé d'utiliser TLS 1.0. À ce titre, de nombreux éditeurs ont décidé d'arrêter son support. Le NIST a également décidé de le considérer comme obsolète et il ne peut plus être utilisé dans un environnement certifié PCI DSS.

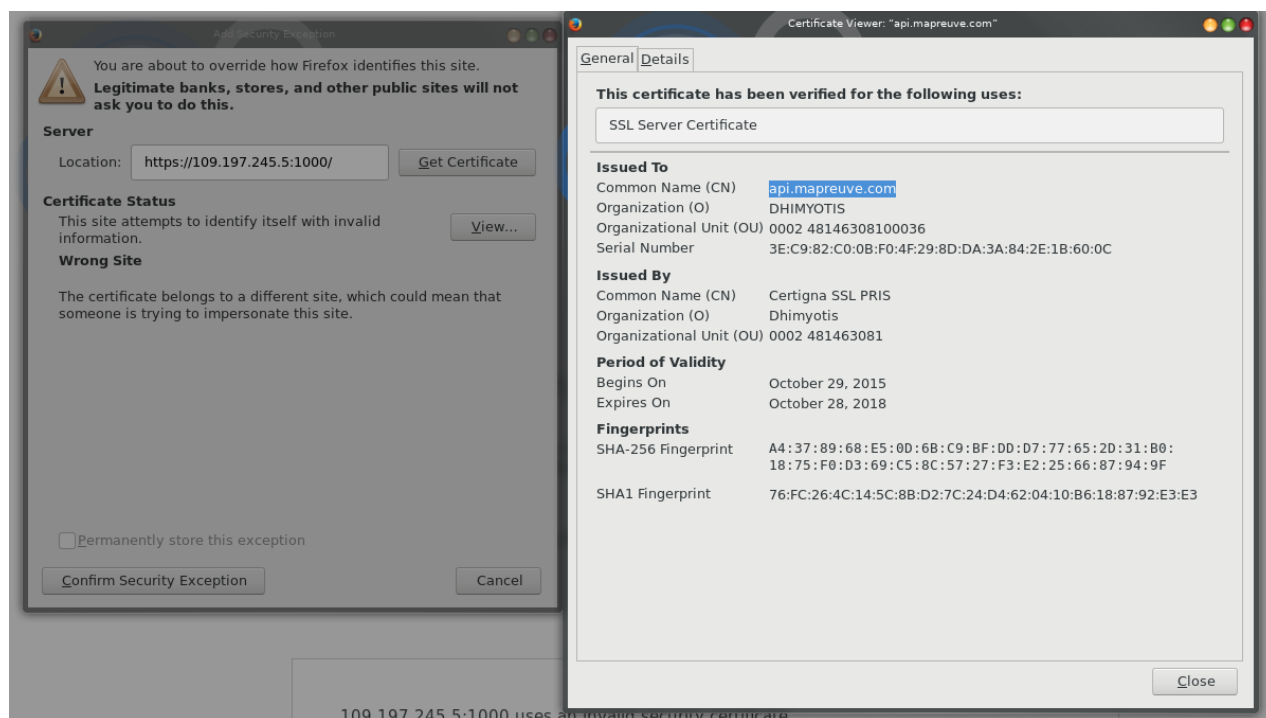
Suites de chiffrement supportées

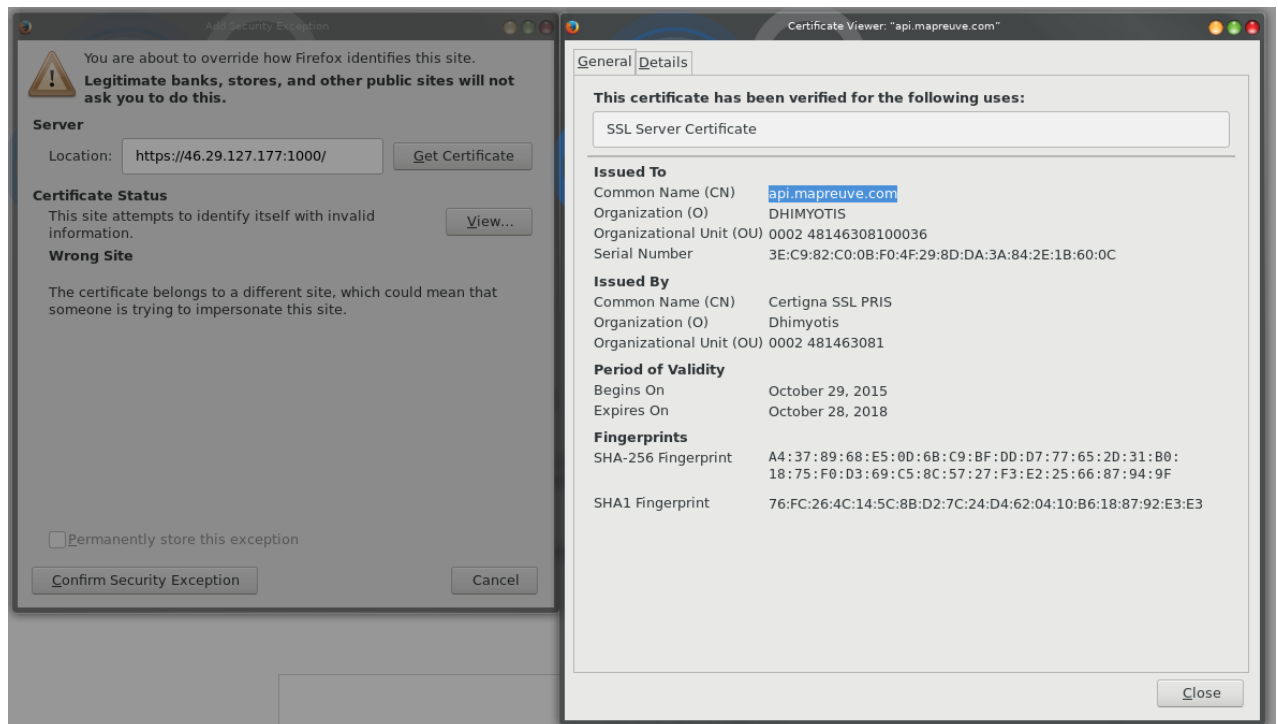
Les sites de chiffrement supporté par les services ont été analysés afin de déterminer si certaines présentent un risque de sécurité du fait de l'utilisation de taille de clés, d'algorithmes de chiffrement ou de mécanismes d'échange de clé présentant des faiblesses cryptographiques.

Le service localisé sur la machine 46.29.127.177, port 1000 autorise l'usage des suites RC4-SHA et RC4-MD5 qui ne sont plus considérées comme suffisamment robustes. Il est donc recommandé de les désactiver.

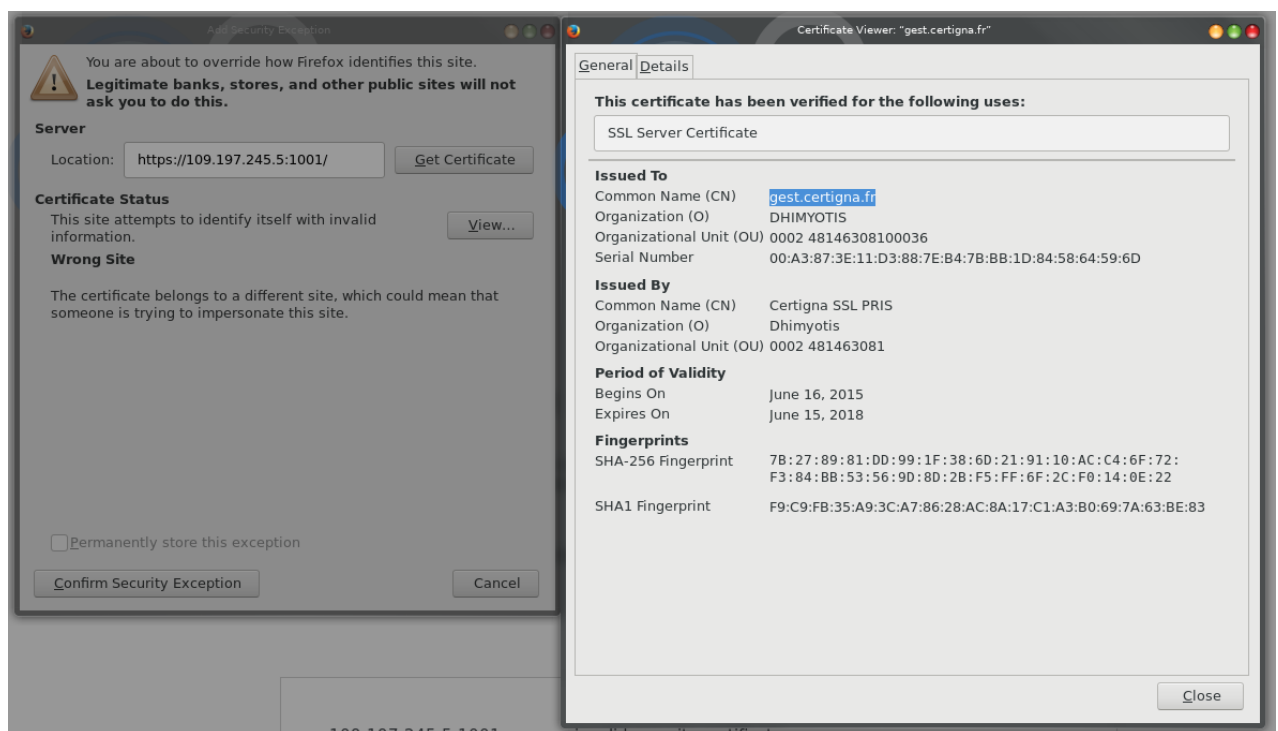
Sécurité du certificat

Le point d'entrée des différents services étend l'adresse IP des serveurs, il est difficile de déterminer l'adéquation entre le nom du dépositaire du certificat (CN ou SAN) et le FQDN de la machine. Les analyses montrent cependant qu'une grande part des certificats déployés sur les équipements ne semble pas correspondre au nom des hôtes (pour les certificats non wildcards) :

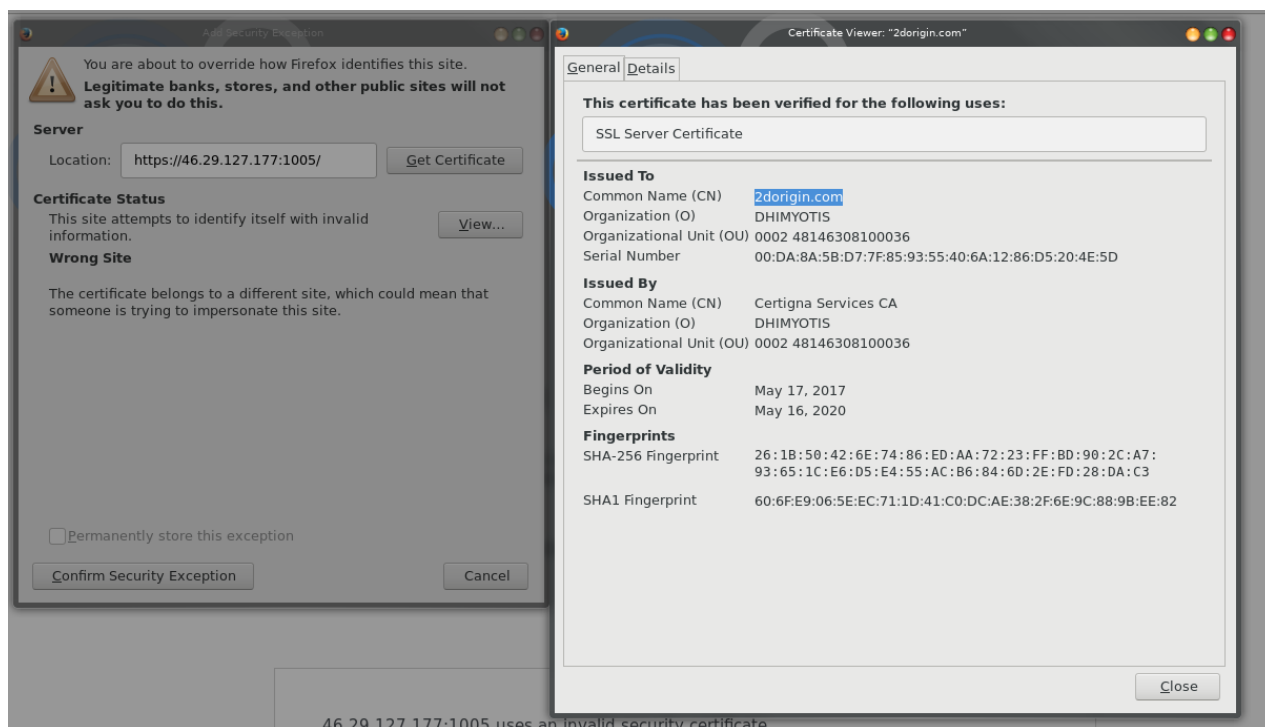




➔ Adresse IP de *api.mapreuve.com* : 46.29.127.184.



➔ Adresse IP de *gest.certigna.fr* : 46.29.127.152.



→ Adresse IP de 2dorigin.com : 109.197.245.8.

En dehors de situations très spécifiques liées à l'utilisation de translation d'adresse, il y a peu de raisons légitimes pour que les certificats portés ne correspondent pas au nom des hôtes. Bien que pouvant être légitime, car signée par une autorité reconnue, ces certificats n'en sont pas moins invalides en l'état il est nécessaire cependant de déterminer si les services exposés sont accessibles au grand public ou non. **Si c'est le cas, la mise en place de certificats valides est indispensable.**

Exposition aux attaques spécifiques

Il existe plusieurs attaques ciblant le protocole SSL/TLS dépendantes des versions utilisées, de l'implémentation des algorithmes, etc. La plupart vise à réduire le niveau de sécurité du chiffrement des communications afin d'en manipuler le contenu ou d'en extraire les données en clair. Il existe également certaines vulnérabilités affectant le serveur permettant de récupérer des données sensibles (comme des portions de mémoire pouvant contenir des mots de passe ou des clés par exemple).































Attaque	Vulnérable	Risque
Renégociation TLS non sûre	Non	Injection de données, déni de service
Renégociation initiée par le client	109.197.245.5:1000	Déni de service
	109.197.245.5:1002	
	109.197.245.5:1003	
	109.197.245.5:1004	
	109.197.245.5:1005	
	46.29.127.177:1000	
	46.29.127.177:1002	
	46.29.127.177:1003	
	46.29.127.177:1004	
	46.29.127.177:1005	
Attaque BEAST	46.29.127.180:443	Déchiffrement partiel des échanges
	46.29.127.186:443	
	109.197.245.5:1000	
	109.197.245.5:1001	
	109.197.245.5:1002	
	109.197.245.5:1003	
	109.197.245.5:1004	
	109.197.245.5:1005	
	46.29.127.152:443	
	46.29.127.177:1000	
Attaque POODLE sur SSL v3.0	46.29.127.177:1001	Déchiffrement des échanges
	46.29.127.177:1002	
	46.29.127.177:1003	
	46.29.127.177:1004	
	46.29.127.180:443	
	46.29.127.186:443	
	Attaque POODLE sur TLS	
	Attaque Heartbleed	
Attaque par injection CCS	Non	Déchiffrement des échanges
Attaque Ticketbleed	Non	Lecture partielle de la mémoire d'équipement <i>F5 Big IP</i> .
Attaque CRIME	Non	Déchiffrement partiel des échanges
Attaque BREACH (potentiellement)	46.29.127.177:1005	Déchiffrement partiel des échanges
Attaque TLS fallback SCSV	109.197.245.5:1000	Dégradation du niveau de chiffrement
	109.197.245.5:1002	
	109.197.245.5:1003	
	109.197.245.5:1004	
	109.197.245.5:1005	
	46.29.127.177:1000	
	46.29.127.177:1002	
Attaque TLS fallback SCSV	46.29.127.177:1003	

Attaque	Vulnérable	Risque
Attaque SWEET32	46.29.127.177:1004	Déchiffrement des échanges
	46.29.127.177:1005	
	46.29.127.180:443	
	46.29.127.186:443	
	109.197.245.5:1000	
	109.197.245.5:1002	
	109.197.245.5:1003	
	109.197.245.5:1004	
	109.197.245.5:1005	
	46.29.127.177:1002	
	46.29.127.177:1003	
	46.29.127.177:1004	
	46.29.127.177:1005	
	46.29.127.180:443	
	46.29.127.186:443	
Attaque FREAK	Non	Déchiffrement des échanges
Attaque DROWN	Non	Déchiffrement des échanges
Attaque LUCKY13 (potentiellement)	109.197.245.5:1000	Déchiffrement partiel des échanges
	109.197.245.5:1001	
	109.197.245.5:1002	
	109.197.245.5:1003	
	109.197.245.5:1004	
	109.197.245.5:1005	
	46.29.127.152:443	
	46.29.127.177:1000	
	46.29.127.177:1001	
	46.29.127.177:1002	
	46.29.127.177:1003	
	46.29.127.177:1004	
	46.29.127.177:1005	
	46.29.127.180:443	
	46.29.127.186:443	



VULN-3 – Configuration cryptographique perfectible

La configuration cryptographique de certains services SSL/TLS peut être améliorée. Elle présente actuellement des défauts de paramétrage, voire de mise à jour des applicatifs, pouvant permettre sous certaines conditions la réalisation d'attaques visant à diminuer la qualité de la protection des communications ou de provoquer un déni de service.

Exploitation		Impact			CVSS v3
Facilité	Exposition	D	I	C	
   	   	 	 	 	AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
Mesure(s) corrective(s)					
Id.	3.1	Désactiver l'usage de TLS en version 1.0 et lui préférer les version 1.1 et 1.2.			
Priorité	   				
Complexité	   				
Id.	3.2	Utiliser des suites de chiffrements robustes (proscrire MD5, SHA-1, RC4 et dans la mesure du possible, les algorithmes utilisant un mode CBC).			
Priorité	   				
Complexité	   				

3.1.3. Collecte indirecte d'informations

En parallèle, ne disposant que d'une liste d'adresse IP, une des premières phases a été de collecter en sources ouverte et de manière indirecte un maximum d'information pouvant être pertinentes pour identifier de manière plus précises les contours techniques de la cible (domaines, noms d'hôtes, etc.), mais également organisationnels (noms de contact, adresses emails, etc.).

Ces éléments peuvent par la suite faciliter l'identification des technologies mises en œuvre, d'accéder à des espaces non visibles au premier abord, voire d'inférer des mots de passe pour des accès en mode privilégié.

3.1.3.1. Identification des noms d'hôtes

Afin d'identifier de manière plus précise les noms d'hôtes susceptibles d'être utilisés par chaque serveur (correspondant aux éventuels *vhosts* des services), une énumération des candidats en s'appuyant sur un dictionnaire de noms courants a été réalisée pour chaque domaine identifié, via l'outil *fierce.pl*, dont voici un exemple :

```
Now logging to fierce_certigna.fr
DNS Servers for certigna.fr:
    ns.ovh.net
    dns.ovh.net

Trying zone transfer first...
Testing ns.ovh.net
Request timed out or transfer not allowed.
```

```

Testing dns.ovh.net
    Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 1904 test(s)...
46.29.127.181    beta.certigna.fr
109.197.245.16  certificates.certigna.fr
109.197.245.7   crm.certigna.fr
46.29.127.181   file.certigna.fr
46.29.127.179   ftp.certigna.fr
213.186.33.14   ftp2.certigna.fr
109.197.245.14  helpdesk.certigna.fr
46.29.127.178   hermes.certigna.fr
46.29.127.181   ldap.certigna.fr
213.186.33.155  mail.certigna.fr
109.197.245.3   mars.certigna.fr
213.186.33.155  pop.certigna.fr
213.186.33.155  pop3.certigna.fr
213.186.33.155  smtp.certigna.fr
46.29.127.187   ssl.certigna.fr
91.121.124.37   wordpress.certigna.fr
46.29.127.186   ws.certigna.fr
46.29.127.179   www.certigna.fr

Subnets found (may want to probe here using nmap or unicornscan):
    109.197.245.0-255 : 4 hostnames found.
    213.186.33.0-255  : 5 hostnames found.
    46.29.127.0-255   : 8 hostnames found.
    91.121.124.0-255  : 1 hostnames found.

Done with Fierce scan: http://ha.ckers.org/fierce/
Found 25 entries.

Have a nice day.

```

Les adresses IP situées en dehors du périmètre de l'audit ont été expurgées pour ne garder que les informations suivantes :

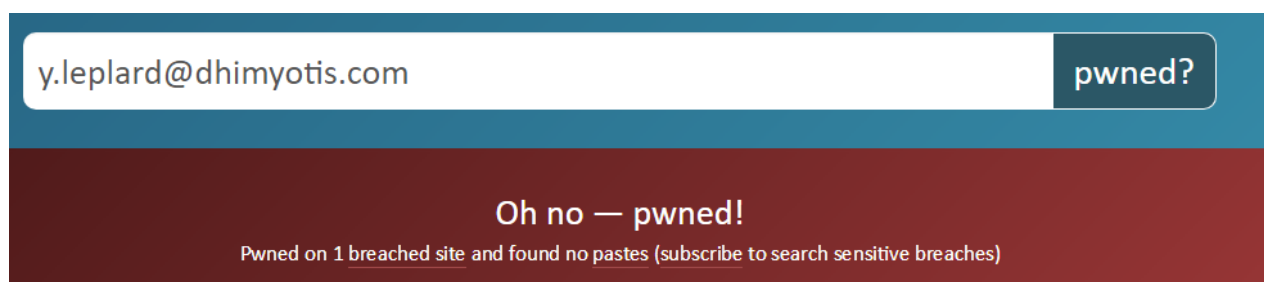
Adresse IP	Nom d'hôte associé
46.29.127.152	gest.certigna.fr ocsp.certigna.fr publication.certigna.fr:servicesca.ocsp.certigna.fr sslpris.ocsp.certigna.fr wildca.ocsp.certigna.fr
46.29.127.177	gestb.certigna.fr test.api.mapreuve.com

Adresse IP	Nom d'hôte associé
	wsb.certigna.fr api.mapreuve.com
46.29.127.181	autorite.certigna.fr cgu.certigna.fr crl.certigna.fr debian.certigna.fr formulaire.certigna.fr ldap.certigna.fr politique.certigna.fr
46.29.127.186	ws.certigna.fr
46.29.127.179	ftp.certigna.fr

3.1.3.2. Recherche de compromissions antérieures

A l'aide d'outils spécialisés dans la recherche d'information en sources ouvertes (*Maltego*), les auditeurs ont pu identifier collecter un grand nombre d'informations sur les hôtes, noms de domaine, adresse email, etc. En particulier, l'adresse y.leplard@dhimyotis.com a été identifiée au cours de ces recherches.

Il apparaît que cette adresse email a été utilisée comme adresse de contact auprès de la société *Adobe* et que l'ensemble des informations qui y sont associées (tels que des informations de contact), mais plus particulièrement le condensat du mot de passe, fait parti de la liste des informations qui ont été dérobées à cette entreprise en octobre 2013 lors d'un gigantesque piratage qui a permis l'exfiltration d'environ 153 millions de comptes.



Si cette adresse e-mail est toujours valide, est en cours d'utilisation et que des informations telles que le mot de passe ont pu être réutilisées entre le compte Adobe et d'autres sites (ou en interne de l'entreprise), il est impératif de les modifier au plus vite.

3.1. Recherche de vulnérabilités

3.1.1. Cross-Site Scripting (XSS)

Les attaques par Cross-Site Scripting (XSS) consistent à injecter des portions de langage HTML dans les paramètres d'une application vulnérable, afin de modifier l'interface qu'elle présente aux utilisateurs. En procédant ainsi, un attaquant est capable de piéger une victime en ajoutant des portions de pages malveillantes à une interface existante. L'exploitation la plus directe consiste à ajouter un script local qui sera exécuté par le client et qui compromettra la valeur du jeton de session de la victime. Il existe plusieurs types d'attaques XSS :

- Attaques réfléchies, lorsque le vecteur d'attaque est transmis dans un lien fourni à la victime ;
- Attaques stockées, lorsque le vecteur est d'abord stocké au sein des données de l'application, et affiché aux utilisateurs qui consultent les pages vulnérables ;
- Attaques « DOM Based », qui utilisent un mécanisme complexe de parcours du document HTML affiché à l'utilisateur.

Des attaques XSS ont été menées sur les applications identifiées, en insérant des portions de langage HTML au sein de paramètres fournis. Il est apparu que certaines pages présentent des paramètres vulnérables sur le site <https://sae.certigna.fr/>.

- **En mode *POST*, via les informations sur la demande.**

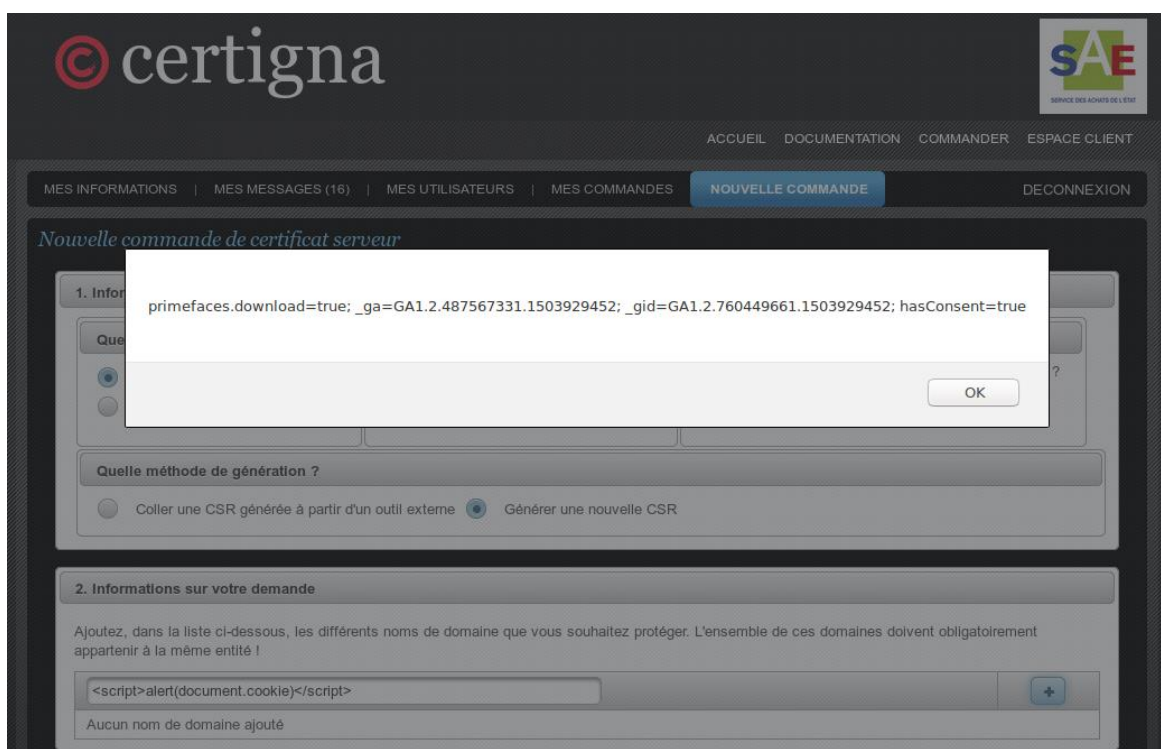


Figure 6 - Attaque XSS POST sur <https://sae.certigna.fr/>.

- En mode **GET**, via l'URL suivante :

[https://sae.certigna.fr/Partners/newserverorder.xhtml?authsae=CERTIGNA_SS%3Cscript%3Ealert\(1\)%3C/script%3EL_RGS](https://sae.certigna.fr/Partners/newserverorder.xhtml?authsae=CERTIGNA_SS%3Cscript%3Ealert(1)%3C/script%3EL_RGS)

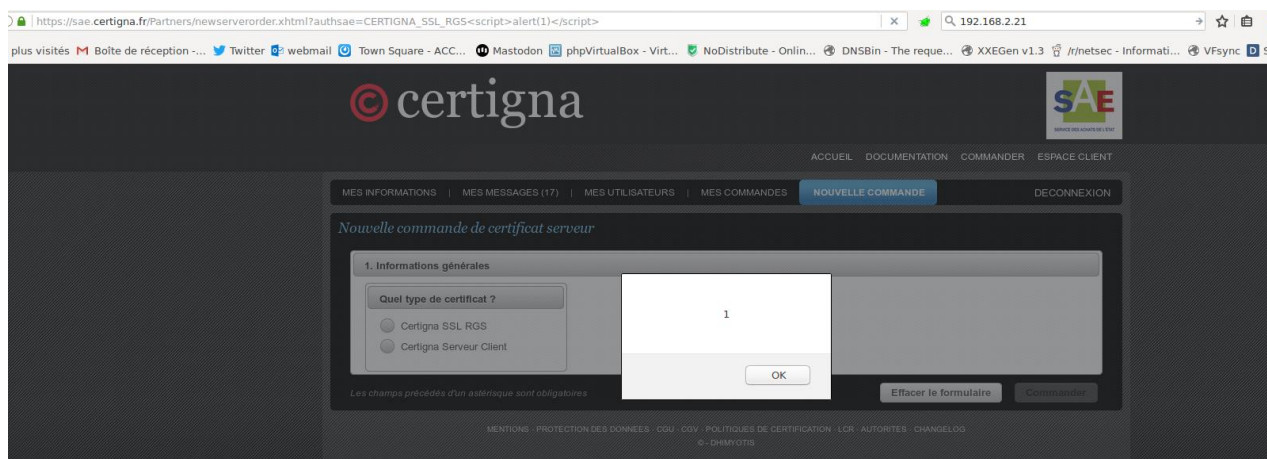


Figure 7 - Attaque XSS GET sur <https://sae.certigna.fr/>.



VULN-4 – Présence de Cross-Site Scripting

Certains paramètres de l'application <https://sae.certigna.fr> ne sont pas correctement filtrés et permettent l'injection de code HTML ou JavaScript dans certaines pages. Un pirate pourrait faire exécuter du code malveillant à un utilisateur dans le contexte de l'application en l'incitant à cliquer sur un lien malformé (transmis dans un e-mail par exemple).

Exploitation		Impact			CVSS v3
Facilité	Exposition	D	I	C	
●●○○	●●●○	●○	●●	●●	AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N
Mesure(s) corrective(s)					
Id.	4.1	Il est recommandé de mettre en place (ou d'étendre) une solution de protection contre les attaques par XSS qui procédera à l'échappement ou l'encodage des caractères dangereux par l'intermédiaire d'une fonction dédiée à cet effet ou par l'intégration d'un framework d'interface incluant une couche de sécurité.			
Priorité	●●●○				
Complexité	●●○○				

3.1.2. Contournement du code de vérification

La cinématique de demande de certificat pour *i-milo* (109.197.245.5 et 46.29.127.177, port 1002) prévoit, pour confirmer la demande, l'envoi d'un e-mail à l'adresse déclarée. Ce dernier contient un code qu'il faut saisir afin de pouvoir finaliser la demande.

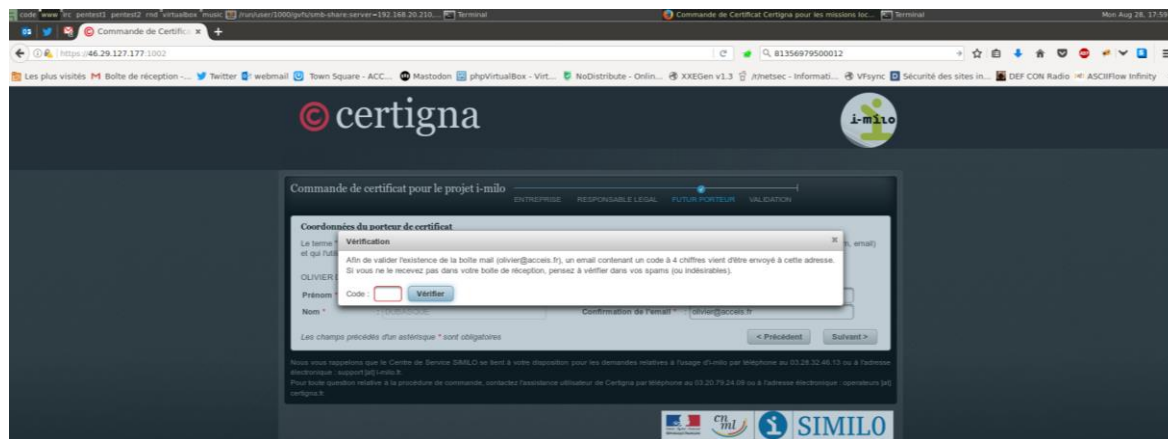


Figure 8 - Demande de code de validation.

Il s'agit d'un code numérique à quatre caractères. Or, durant l'audit, il est apparu qu'aucun mécanisme de restriction n'était en place pour saisir le code en question (pas de limitation du nombre d'essais par exemple). La complexité du code étant relativement faible, un attaquant peut rapidement tester toutes les combinaisons possibles et ainsi valider la demande même s'il n'est pas détenteur de l'adresse à qui a été envoyé l'e-mail de confirmation.

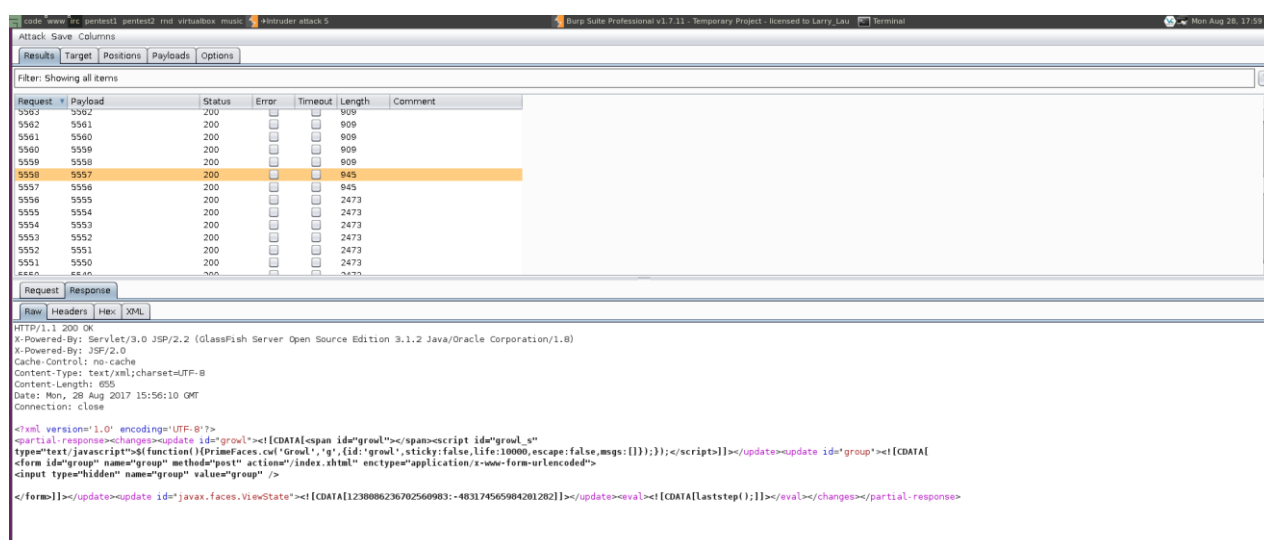









Figure 9 - Contournement du code de validation.

Cette vulnérabilité reste cependant limitée car l'obtention du certificat nécessite en aval d'imprimer, de compléter et de transmettre le dossier établi, ainsi qu'une liste de pièces justificatives.



VULN-5 – Contournement du code de validation

Il est possible de contourner le mécanisme de validation des demandes de l'application *i-milo*, car le code demandé n'a pas une complexité suffisante (quatre caractères numériques). Un attaquant peut énumérer rapidement toutes les combinaisons possibles afin de trouver la bonne.

Exploitation		Impact			CVSS v3
Facilité	Exposition	D	I	C	
					AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Mesure(s) corrective(s)					
Id.	5.1	Utiliser un code secret plus complexe pour la validation des demandes ou désactivées la demande après un trop grand nombre de tentatives infructueuses.			
Priorité					
Complexité					

3.2. Tests non concluants

De nombreuses actions ont été réalisées durant cette dite afin de mettre en évidence la présence de vulnérabilités. Déteste relatifs aux failles présentées ci-dessous ont été menés sans succès. Cela signifie qu'au moment et dans le contexte de cet audit, aucun élément tangible n'a pu être relevé permettant d'établir la présence de ces vulnérabilités.

- Injections SQL ;
- Cross-Site Request Forgery ;
- Inclusion de fichier ;
- Envoi ou téléchargement arbitraire de fichier ;
- Défaut de cloisonnement applicatif ;
- Contournement des mécanismes d'authentification ;
- Oracle utilisateur.