

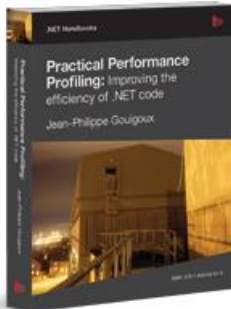
Sécurité des développements

IUT – JP Gouigoux – 09/2016

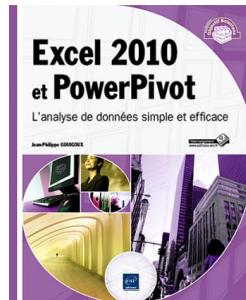
search://gouigoux.com



Mai 2011



Février 2012



Mars 2012



Février 2014



Août 2015



Octobre 2015



Mai 2016

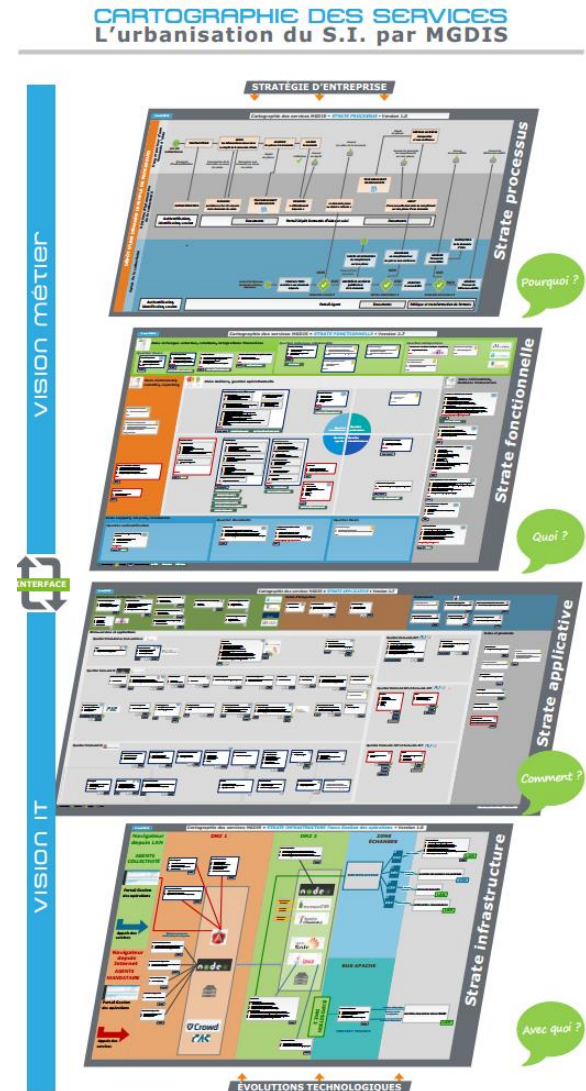


<http://www.mgdis.fr>



Notre architecture

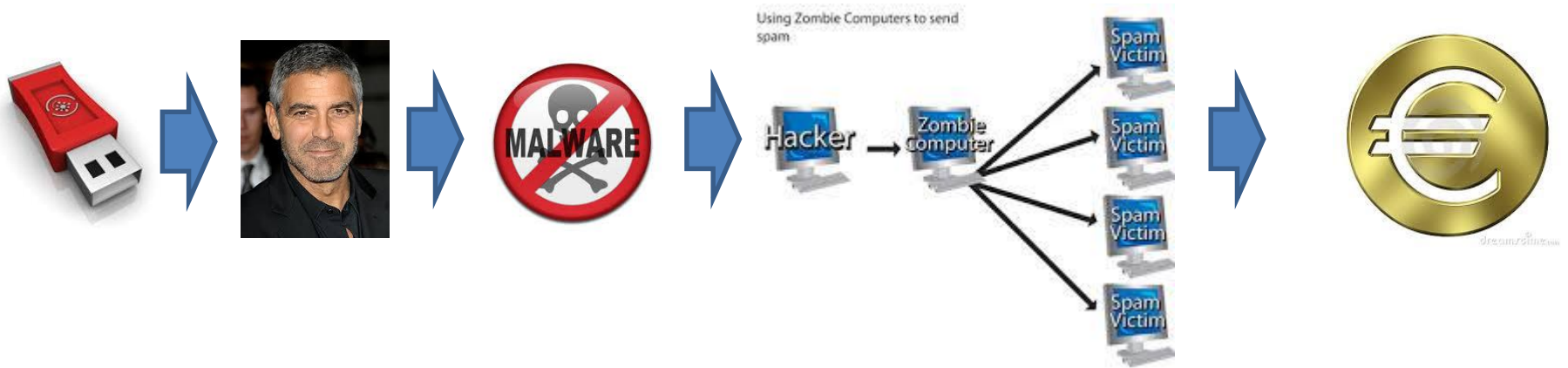
- Urbanisation
- Microservices
- Docker
- Node.JS
- AngularJS



Glossaire

- Virus / Backdoor / Troyen
- Vulnérabilité / Exploit / Faille / 0-day
- Injection / Déni de service / Canonicalisation
- Advanced Persistent Threat / Network scan
- Social Engineering / Malware / Scareware

Deux canaux principaux



Economie de la sécurité

- 66% des clés USB perdues sont piégées
- 17,7 M\$: CA produits sécurité 2011
- Incident sécurité pour 60% des entreprises en 2011 (39% en 2010)
- Twitter, LinkedIn, Facebook : tous avec une attaque critique en 2012
- NASA : hacké
- FBI, CIA, NSA : 1000+ attaques / jour !

Les dernières nouvelles

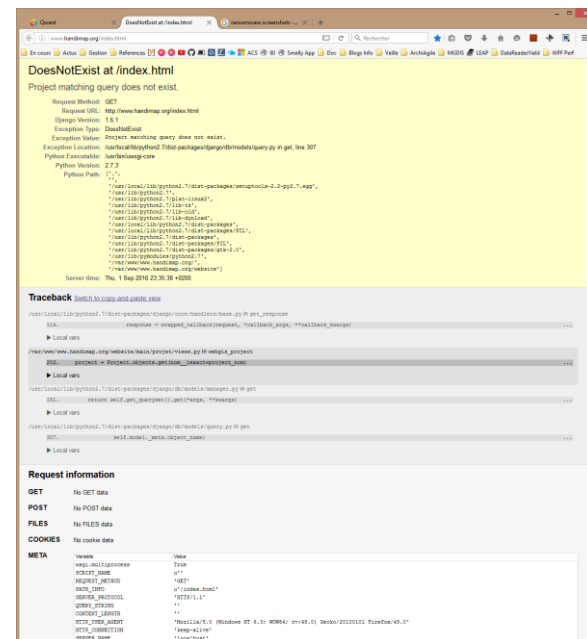
CADE METZ BUSINESS 04.05.16 11:00 AM

FORGET APPLE VS. THE FBI: WHATSAPP JUST SWITCHED ON ENCRYPTION FOR A BILLION PEOPLE

Un hôpital de Los Angeles paralysé par un rançongiciel

par Stéphane Larcher, le 16 février 2016 12:27 ★★★★★

Les hackers réclament 3,6 millions de dollars pour restituer les données et autoriser à nouveau le fonctionnement du système d'information. Dans l'intervalle, des patients sont déplacés dans d'autres centres hospitaliers de Los Angeles.



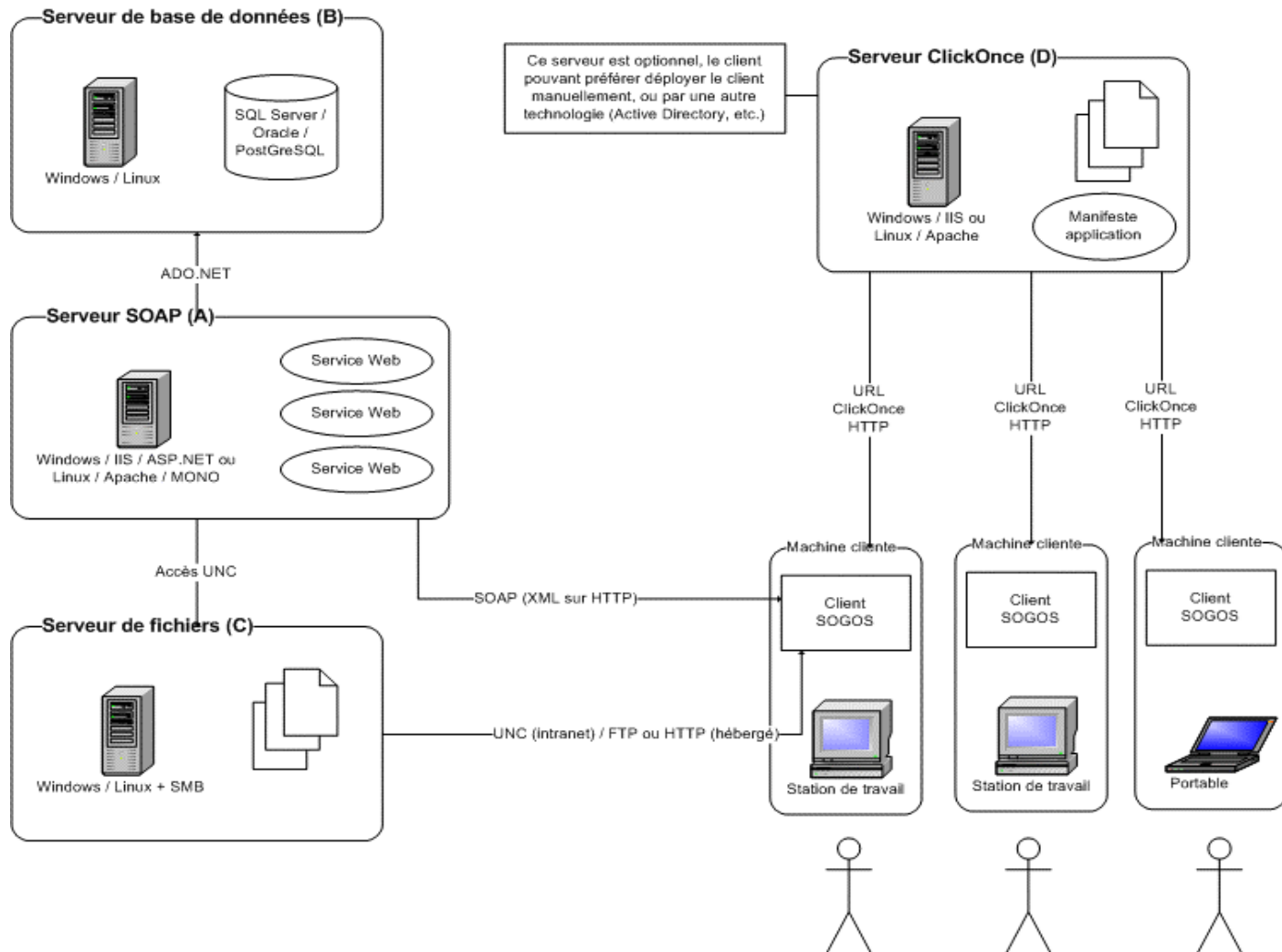
Sécurité & politique

- ANSSI
- RGS
 - FEROS
- Spécialité Cyberdéfense à l'ENSIBS

Les bases de la sécurité : pas une question technique, mais de méthode

- Modélisation des attaques
 - SD3 = Secure by Design / Default / Deployment
 - Analyse de risque : $\text{risque} = \text{occurrence} \times \text{sévérité}$
- Savoir sortir la tête de la technique
 - Veille technologique
 - Mise en place de bonnes pratiques de programmation
- Ne pas trop en faire
 - Le bon niveau, c'est état de l'art + 1
 - Le problème final est entre le clavier et la chaise

Architecture applicative standard



Attaques classiques

Client	Zone internet	DMZ	Zone intranet	Intranet enfoui
Affichage en clair du mot de passe Analyse des DLL Lancement usurpé	Attaque MITM Session hijacking	Injection SQL Déni de service Accès non identifié XML Bombing	Client non autorisé Déni de service Attaque brut MDP Escalade de privilèges	Injection SQL Déni de service Escalade de privilèges
Zone de mot de passe invisible à VUPassword MDP invisible en mémoire Certificat client Authentification sur proxy	HTTPS (100% flux + déploiement) Tunnel VPN Sessions sans cookie	Validation par Schema XML Cryptage MDP Annuaire LDAP	Blocage des UserAgent externes par défaut Timeout aléatoire sur validation MDP Code Access Security (XML)	Paramétrisation complète + validation préalable Comptes dédiés

Attaques sur le client

- Affichage en clair du mot de passe
 - Principe de VUPassword
 - Lock de session
 - SecureString
- Référence invisible en mémoire
 - Analyse DLL par ILDASM
 - Protection par hash
 - Ne pas oublier le sel... (voir plus loin)
- Authentification client
 - Authentification intégrée / LDAP / propriétaire
 - Problème d'accessibilité internet
 - Chiffage des crédentils

Attaques sur internet

- Par défaut, le flux HTTP est en clair
 - Man In The Middle
 - Capture TCP d'un GET avec Wireshark
- Mise en place de HTTPS
 - Principe de fonctionnement
 - Limitation de sécurité des certificats
- Session Hijacking
 - Déconnecter proprement
 - Attention aux cookies
 - Gérer les timeouts

Traffic Ethernet

Intel(R) 82567LM Gigabit Network Connection: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

Destination	Protocol	Info
172.16.10.123	TCP	pratt > http [FIN, ACK] Seq=1 Ack=1 win=64078 Len=0
172.16.1.7	TCP	http > pratt [ACK] Seq=1 Ack=2 win=65187 Len=0
172.16.1.7	TCP	http > pratt [FIN, ACK] Seq=1 Ack=2 win=65187 Len=0
172.16.10.123	TCP	cmmdriver > http [SYN] Seq=0 win=64512 Len=0 MSS=1460
172.16.1.7	TCP	http > cmmdriver [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=146
172.16.10.123	TCP	pratt > http [ACK] Seq=2 Ack=2 win=64078 Len=0
172.16.10.123	TCP	cmmdriver > http [ACK] Seq=1 Ack=1 win=64512 Len=0
172.16.10.123	HTTP	POST /TestMDP.html HTTP/1.1 (application/x-www-form-urlencoded)
172.16.1.7	HTTP	HTTP/1.1 100 Continue
172.16.10.123	TCP	[TCP segment of a reassembled PDU]
172.16.10.123	TCP	cmmdriver > http [ACK] Seq=576 Ack=1573 win=64512 Len=0
172.16.1.7	TCP	[TCP segment of a reassembled PDU]
172.16.1.7	HTTP	HTTP/1.1 405 Method not allowed (text/html)
172.16.10.123	TCP	cmmdriver > http [ACK] Seq=576 Ack=4381 win=64512 Len=0
172.16.10.123	TCP	cmmdriver > http [FIN, ACK] Seq=576 Ack=4381 win=64512 Len=0
172.16.1.7	TCP	http > cmmdriver [ACK] Seq=4381 Ack=577 win=64960 Len=0
172.16.10.141	TCP	http > 50675 [SYN, ACK] Seq=0 Ack=0 win=5840 Len=0 MSS=1460

Hypertext Transfer Protocol

POST /TestMDP.html HTTP/1.1\r\n

Request Method: POST

0160 00 01 72 0d 2d 73 72 0c 05 0e 05 01 04 05 04 0d form-urlencoded.
0170 0a 55 41 2d 43 50 55 3a 20 78 38 36 0d 0a 41 63 .UA-CPU: x86..AC
0180 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 cept-Encoding: g
0190 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 55 73 zip, deflate..us
01a0 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent : Mozill
01b0 61 2f 34 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c a/4.0 (compatibl
01c0 65 3b 20 4d 53 49 45 20 36 2e 30 3b 20 57 69 6e e; MSIE 6.0; win
01d0 64 6f 77 73 20 4e 54 20 35 2e 32 3b 20 53 56 31 dows NT 5.2; svl
01e0 3b 20 2e 4e 45 54 20 43 4c 52 20 31 2e 31 2e 34 ; .NET CLR 1.1.4
01f0 33 32 32 3b 20 2e 4e 45 54 20 43 4c 52 20 32 2e 322; .NET CLR 2.
0200 30 2e 35 30 37 32 37 29 0d 0a 48 6f 73 74 3a 20 0.50727) ..Host:
0210 67 6f 75 69 6f 6f 75 78 2d 6a 70 0d 0a 43 6f 6e gouigoux -jp..Con
0220 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 31 37 0d tent-Length: 17.
0230 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 .Connection: Kee
0240 70 2d 41 6c 69 76 65 0d 0a 43 61 63 68 65 2d 43 p-Alive. .Cache-C
0250 6f 6e 74 72 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 ontrol: no-cache
0260 0d 0a 0d 0a 6d 6f 74 64 65 70 61 73 73 65 3d 63motd epasse=c
0270 6f 75 63 6f 75

Text item (), 17 bytes

Packets: 44 Displayed: 44 Marked: 0

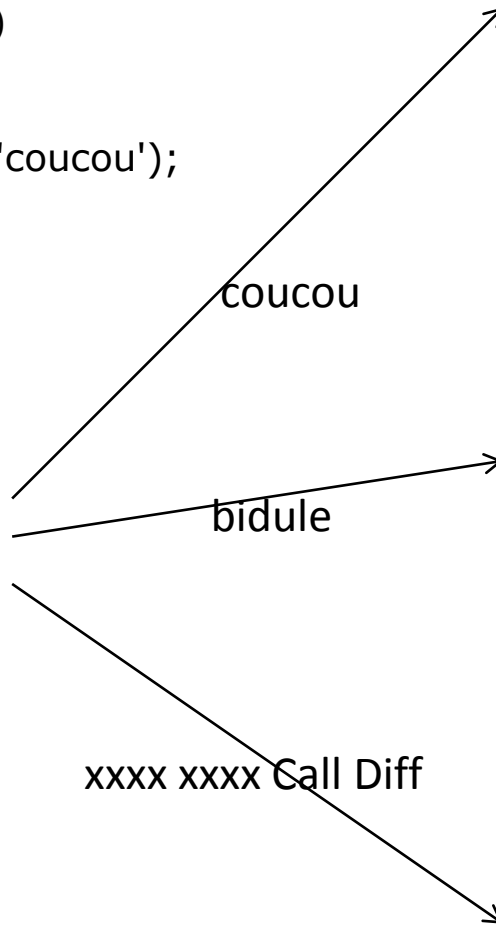
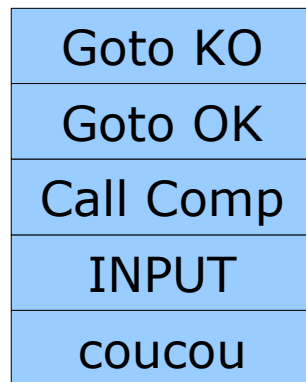
Profile: Default

Attaques sur le métier

- Injection SQL
 - Démonstration
 - Sécurisation : simplement coder proprement
- Débordement de tampons
 - Principe
 - Une des raisons pour les L4G
- Fonctionnalité non autorisée
 - Défaut de programmation
 - Backdoor intentionnelle
 - Abus de licence

```
if (VerifPassword())  
    // CodeConfidentiel  
else  
    // Rejeter
```

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



Faibles de cryptographie

- Cryptographie symétrique / asymétrique
- Algorithmes de hash / signature
 - MD5 : terminé
 - SHA1 : collisions possibles
 - SHA256 : pas sans sel
 - SHA256 + sel : pas nécessairement suffisant (LinkedIn)
- On commence par la base : démo

hash md5 - Recherche Google - Mozilla Firefox

Fichier Édition Affichage Historique Délicieux Marque-pages Outils ?

http://www.google.fr/search?q=hash+md5&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:fr:official&client=firefox 2628a3f83a77ab494817525ct

hash md5 - Recherche Google

Web Images Maps Actualités Vidéo Gmail plus Connexion

Google

hash md5 Rechercher Recherche avancée Préférences

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

Web Résultats 1 - 10 sur un total d'environ 546 000 pour hash md5 (0,54 secondes)

[Décryptez votre HASH MD5 instantanément.](#)
Voici un outil en ligne vous permettant de retrouver le mot de passe correspondant à votre HASH MD5.
[www.authsecu.com/decrypter-dechiffrer-cracker-hash-md5/decrypter-dechiffrer-cracker-hash-md5.php](#) - 49k - [En cache](#) - [Pages similaires](#)

[MD5 - Wikipédia](#)
13 nov 2008 ... L'algorithme MD5, pour Message Digest 5, est une fonction de hachage ...
Firefox comme MD Hash tool [1] afin d'automatiser ce contrôle. ...
[fr.wikipedia.org/wiki/MD5](#) - 47k - [En cache](#) - [Pages similaires](#)

[md5 Hash Generator](#) - [[Traduire cette page](#)]
About md5 Hash Generator... This is just a simple tool to compute the MD5 hash of a string.
String:. Copyright © 2004-2008, Sunny Walker, ...
[www.miraclesalad.com/webtools/md5.php](#) - 4k - [En cache](#) - [Pages similaires](#)

[AtoutFox \(Foxpro\) - hash md5](#)
Permet de calculer le hash md5 d'une chaîne de caractères, ou d'un fichier complet Version
Windows: Client: XP ou 2000 prof serveur: 2000 ou 2003 Utilise: ...
[www.atoutfox.org/articles.asp?ACTION=FCONSULTER&ID=0000000627](#) -
10k - [En cache](#) - [Pages similaires](#)

[HASH MD5 RESEARCH - PROGRAMME PERMETTANT DE RÉCUPÉRER LE MOT \(EN ...](#)
9 messages - 5 auteurs - Dernier message : 21 oct 2007
Exemple de programmation : HASH MD5 RESEARCH - PROGRAMME PERMETTANT DE
RÉCUPÉRER LE MOT (EN CLAIR) ASSOCIÉ À UN HASH MD5 VIA INTERNET, ...
[www.vbfrance.com/codes/HASH-MD5-RESEARCH-PROGRAMME-PERMETTANT-RECUPERER-MOT-CLAIR_40976.aspx](#) - [Pages similaires](#)

[Reverse MD5 hash lookup](#) - [[Traduire cette page](#)]
This form uses several MD5 databases to look up an MD5 hash and return its original
counterpart. You may use the second field to first generate an MD5 hash ...
[tools.benramsey.com/md5/](#) - 8k - [En cache](#) - [Pages similaires](#)

[hash md5 - Archives / Au secours, C / C++ / C++.NET](#)
6 messages - 2 auteurs - Dernier message : 23 déc 2004
Trouvez ici un message à propos de hash md5, C / C++ / C++.NET.
[www.enfance.com/forum/voir+HASH+MD5+267027.aspx](#) - [Pages similaires](#)

Terminé

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

Nexus Technology

Editeur solutions de sécurité
PKI, Chiffrement, SSO,
Messagerie.
www.nexusSAFE.com

Bracelets identification

Bracelets de sécurité Imprimés
à vos couleurs
www.a-gis.fr

Supervision en ligne

Supervisez vos parcs
informatiques sans faire
d'investissements mat.
www.netforge.fr

Routeurs VPN Multi WAN

Equilibrage de charge et
redondance VPN avec plusieurs
liens ADSL
www.netmetrics.net

Annonces Google

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` ...](#)

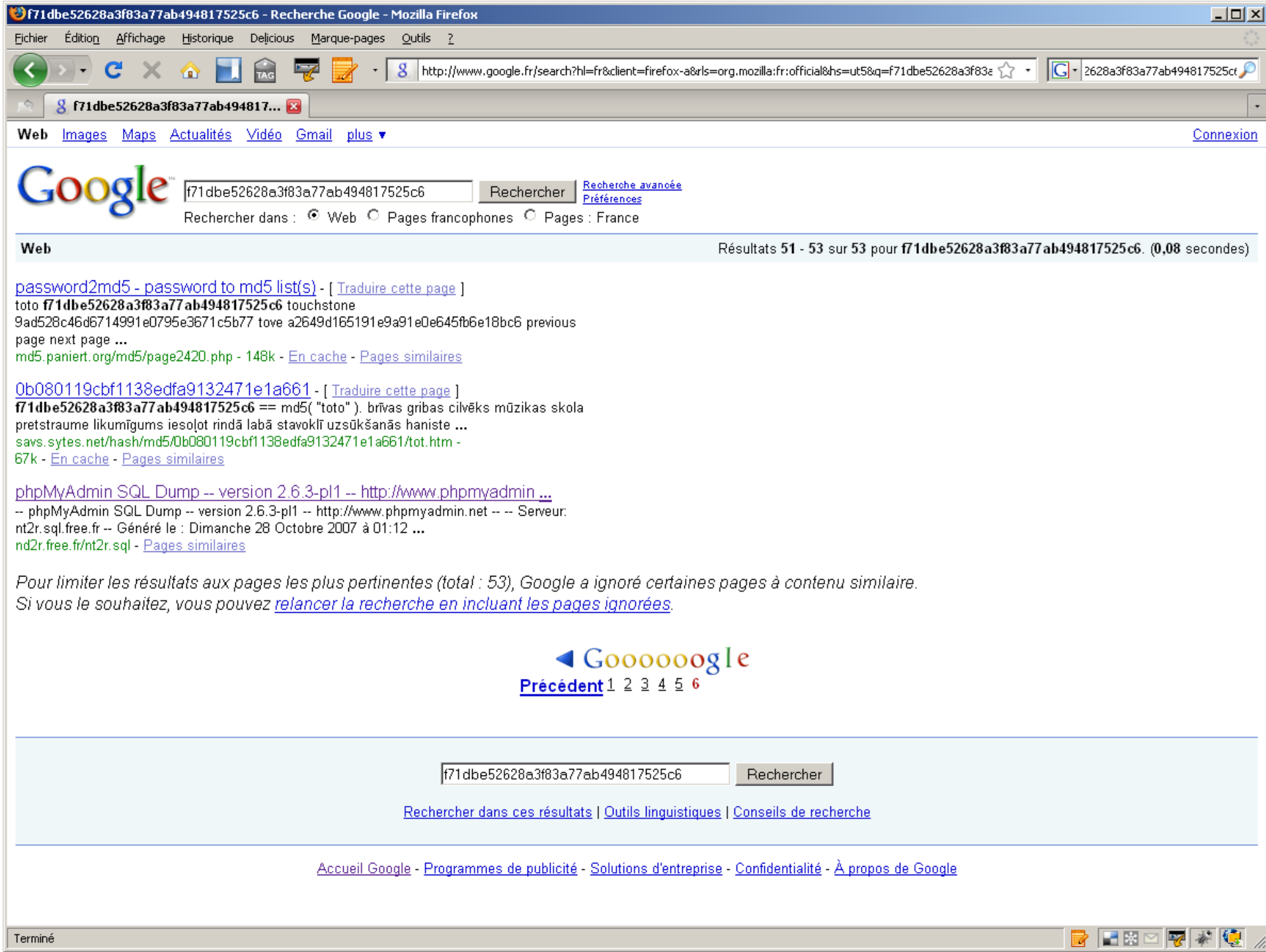
\n\n', 0, 1209824147, 1, NULL, NULL, NULL, '2.jpg', 0, '', NULL), (3, 'juju', 'juju', 'f71dbe52628a3f83a77ab494817525c6', 'h', '1986-10-19', ...
[forge.jelix.org/svn/wechange/app/install/wechange_install_data.mysql.sql](#) - 6k - [En cache](#) - [Pages similaires](#)

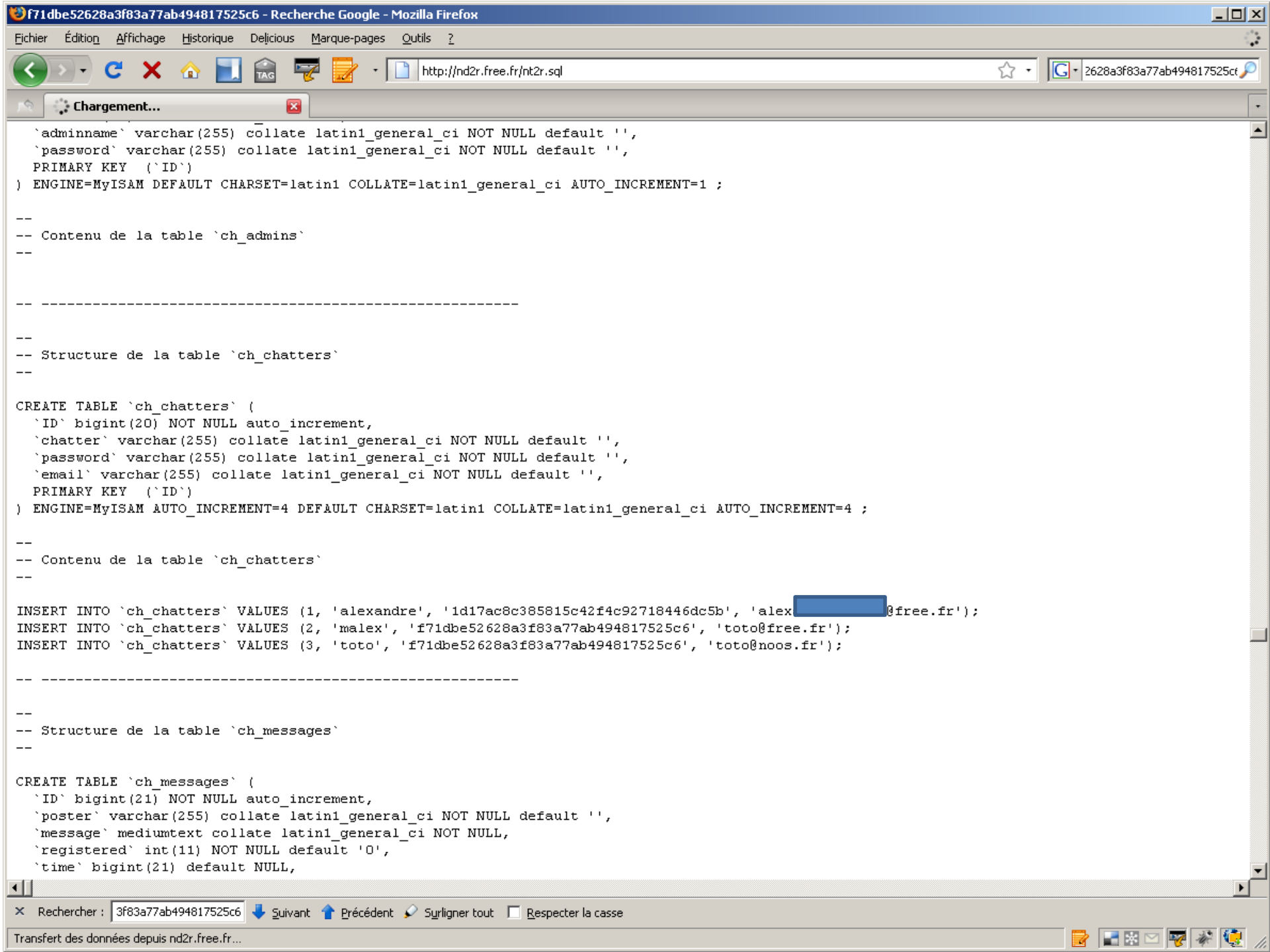
[wechange - Changeset 76 - Jelix Forge](#) - [[Traduire cette page](#)]

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 ...





Failles de cryptographie

- Force brute
 - Rarement utilisée seule
 - Exploit 0-day sur SSL = 16 000 \$
- Déchiffrement intelligent
 - Analyse de la durée de l'algorithme
 - Rainbow tables
- Faille dans les algorithmes de cryptographie
 - SSL 1024 inutile si génération de clé incorrecte
 - Difficile d'obtenir du hasard d'un ordinateur
 - Ne surtout jamais créer des algorithmes propriétaires

Principe du moindre privilège

- Si l'application est compromise
 - Ne pas être administrateur
- Principe de la défense en profondeur
 - Moindre privilège multi-niveaux

Etat de l'art

- Utilisation de normes (OAuth, SAML, etc.)
- Fédération d'identités
- Bien séparer authentication / identification / habilitation : approche microservices

Conclusion

- La sécurité est un vrai métier
 - Mythe du pirate informatique en berne
 - Aujourd'hui : une mafia organisée

