Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 14 septembre 2010
N° CERTA-2002-INF-001-001

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Vulnérabilité de type « Cross Site Scripting »

Gestion du document

Référence	CERTA-2002-INF-001-001
Titre	Vulnérabilité de type Cross Site Scripting (XSS)
Date de la première version	22 mars 2002
Date de la dernière version	14 septembre 2010
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Introduction

Une vulnérabilité de type *Cross Site Scripting*, injection de code indirecte en français, est exploitable sur les serveurs web ou sur les applications web qui publient du texte fourni par le visiteur sans l'avoir filtré. Un utilisateur malintentionné peut, en utilisant cette vulnérabilité, insérer du code dans une page HTML renvoyée dynamiquement par le serveur. Ce code est généralement écrit dans un langage de script (par exemple JavaScript ou VBscript) qui est interprété par le navigateur de la victime.

Le terme anglais *Cross Site Scripting* est abrégé en XSS car l'acronyme CSS est déjà utilisé dans le monde du web pour *Cascading Style Sheet*.

2 Historique et évolution du Cross Site Scripting

Les vulnérabilités de type *Cross Site Scripting* sont apparues lors de la généralisation de l'usage des langages de script dans les pages web. Ces vulnérabilités ont fait l'objet d'un premier communiqué officiel en février 2000 par le CERT/CC (voir section documentation).

Depuis, leur exploitation s'est diversifiée et concerne toutes sortes de services (webmails, enchères en ligne, forums...).

Beaucoup de logiciels ont été touchées par cette vulnérabilité dont les plus connus sont les serveurs web IIS et Apache, les serveurs d'applications IBM Websphere et Tomcat mais aussi les nombreux gestionnaires de contenus (CMS), de forum, les outils de statistiques (phpMyVisites, AwStats), le relais mandataire Squid...

3 Exemples de Cross Site Scripting

3.1 Moteur de recherche d'un serveur web

Cet exemple est extrêmement fréquent.

Dans ce cas, un serveur web propose un formulaire de recherche à ses visiteurs. Les mots-clefs entrés pour la recherche sont souvent renvoyés à l'internaute dans des messages de la forme (pour une recherche avec le mot CERTA) :

```
14 documents trouvés pour la recherche de CERTA.
```

Un site vulnérable à l'injection de code indirecte ne filtre pas les données entrées par le visiteur avant de les lui retourner. Donc l'insertion dans le formulaire de la chaîne de caractères :

```
<script>alert('Ce serveur est vulnérable !')</script>
```

retournera cette séquence JavaScript au navigateur de l'internaute qui l'interprètera en ouvrant une fenêtre avec le message : `Ce serveur est vulnérable !`

L'exploitation malveillante ne se contente évidemment pas de cet affichage bénin.

Plus généralement, toute entrée par formulaire et toute variable présente dans une adresse réticulaire (URL) peuvent servir à une attaque par injection de code indirecte.

3.2 Génération automatique du message d'erreur d'un serveur web

Lorsqu'un serveur web génère un message d'erreur à partir de l'adresse réticulaire qu'il a reçue, sans avoir au préalable pris la précaution de l'analyser, il est également vulnérable à cette faille.

Prenons le cas d'un serveur ayant pour nom d'hôte `www.exemple.tld`, sur lequel l'internaute cherche la page `xxx`. Si ce serveur ne trouve pas la page demandée, il retourne une réponse du type :

```
Erreur 404 : Page xxx non trouvée.
```

Imaginons qu'un utilisateur malintentionné crée sur un site web (ou dans un courriel) une page HTML contenant le lien hypertexte suivant :

```
<a href="http://www.exemple.tld/<script>alert('Ce serveur est vulnérable !')
</script>''> Texte incitant le visiteur (ou le destinataire) à cliquer</a>}.
```

Le visiteur répondant à l'incitation envoye l'URL du champ `href` au serveur `www.exemple.tld`. Ce dernier cherchera alors le fichier `<script>alert('Ce serveur est vulnérable !')</script>` qu'il ne trouvera pas. Il renverra donc une réponse d'erreur 404 contenant le script (inoffensif dans ce cas) qui aura pour effet d'afficher une fenetre avec le texte : `Ce serveur est vulnérable !`

Cette vulnérabilité était présente sur le serveur web Microsoft IIS version 4.0 et version 5.0 (voir avis de sécurité CERTA-2000-AVI-035 du CERTA).

3.3 Vol d'un cookie par envoi d'un courriel

Un serveur web est chargé d'afficher les courriels au format HTML contenus dans la boîte aux lettres d'un utilisateur (webmail). L'authentification de l'utilisateur est réalisée au moyen de *cookies* d'identification envoyés par le serveur web. Si le serveur est vulnérable, un utilisateur malintentionné peut, par le biais d'un courriel astucieusement écrit, récupérer le cookie d'identification envoyé par le serveur web.

Le courriel envoyé par l'utilisateur malintentionné est de la forme :

sujet : `du texte anodin`

corps : `du texte anodin`

```
<\textarea>
<script>un script qui récupère le cookie d'identification</script>
```

En lisant ce courriel à travers les pages créées par le serveur, la victime n'a pas connaissance du texte se trouvant après la balise `<\textarea>` qui est alors considéré comme du code HTML. L'emploi de la balise `<script>` permet l'exécution d'un code qui sera interprété par le navigateur.

3.4 Situations voisines du Cross Site Scripting, forums et blocs-notes (blogs)

Les forums qui permettent la publication de messages contenant du HTML facilitent l'injection de code dans ce qui sera retourné à l'internaute visiteur.

De même les commentaires ajoutés à des billets dans des blogs sont propices à ce type d'injection.

L'interdiction du HTML ou le contrôle strict de celui-ci dans ces messages et ces commentaires réduisent les possibilités d'attaques.

4 Impacts du Cross Site Scripting

Les impacts de cette vulnérabilité sont liés au langage de script utilisé pour réaliser l'attaque par *Cross Site Scripting*, en particulier aux opérations qu'il permet et aux droits accordés à l'interpréteur de script.

Si le langage JavaScript est utilisé, il est alors possible :

- de modifier ou d'ajouter des clefs à la base de registre de la machine victime ;
- d'afficher une fenêtre demandant à l'utilisateur de rentrer son login et son mot de passe puis de valider, après quoi le résultat sera envoyé par courriel à l'attaquant ;
- de récupérer les *cookies* présent sur la machine victime ;
- d'exécuter des commandes systèmes ;
- de construire un lien vers un site malveillant et de diriger l'internaute vers celui-ci...

Les risques liés à cette vulnérabilité sont donc nombreux : déni de service de la machine victime, utilisation de la machine victime à des fins malveillantes, récupération de données personnelles.

5 Recommandations pour limiter le Cross Site Scripting

5.1 Recommandation sur les serveurs

La vulnérabilité est fondamentalement l'acceptation sans vérification de données fournies par l'internaute et leur renvoi tel quels.

Pour contrer les attaques basées sur l'injection de code indirecte, il convient donc de filtrer ces données :

- vérification syntaxique des entrées, avec suppression des caractères ne pouvant intervenir dans des entrées légitimes. Une attention particulière sera portée sur les caractères qui ont un rôle spécifique dans la grammaire HTML ou dans les langage interprétés, comme les caractères inférieur (<), supérieur (>), barre oblique (/), etc. ;
- vérification sémantique le cas échéant ;
- transcodage des caractères (signe inférieur transformé en `<`, par exemple) pour un renvoi sans interprétation à l'internaute ;
- suivi des logiciels utilisés et mise à jour de ceux-ci, en particulier quand une vulnérabilité XSS vient d'être corrigée.

La surveillance des journaux de connexion et des journaux d'interrogation des bases de données (sites dynamiques) peut indiquer des tentatives et des réussites d'exploitation de ces vulnérabilités.

5.2 Recommandation sur les navigateurs

L'utilisateur ne peut corriger cette vulnérabilité du serveur, mais en restreindre la possibilité d'exploitation.

Il est recommandé à l'internaute :

- de désactiver l'exécution des langages de script intéprétables par le navigateur ;
- d'être prudent lors de la navigation sur des sites inconnus et de se méfier des liens cachés, c'est-à-dire dont un texte masque l'URL ;
- d'utiliser son ordinateur (navigation, messagerie, etc.) avec des droits limités ;
- de visualiser ses courriels en texte brut, de manière à voir les liens réels cachés derrière des textes ou des liens apparents.

6 Documentation

- Note d'information CERTA-2004-INF-001 du CERTA
  http://www.certa.ssi.gouv.fr/site/CERTA-2004-INF-001
- Avis de sécurité CERTA-2000-AVI-035 du CERTA
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-AVI-035
- Recommandation CERTA-2000-REC-001 du CERTA
  http://www.certa.ssi.gouv.fr/site/CERTA-2000-REC-001
- Avis de sécurité CA-2000-02 du CERT/CC
  http://www.cert.org/advisories/CA-2000-02.html

Gestion détaillée du document

22 mars 2002 version initiale.
14 septembre 2010 actualisation.