

## ISR TP CAPTURE DE DRAPEAU

### Exercices Client 3 flags :

#### *Flag 1 :*

Il faut examiner l'élément avec la touche F12 ou bien clic droit « Inspecter l'élément ». On découvre alors du code HTML. Dans la partie « body » il y a un commentaire concernant le flag numero 1. Le flag 1 **CLIENT1{69C298598C}**

```
<!DOCTYPE html>
<html>
  <head>...</head>
  <body bgcolor="#000000">
    <!-- flag1: CLIENT1{69C298598C} --> == $0
    <script>...</script>
    <!-- flag3 : http://isr.istic.univ-rennes1.fr/client/redirect.html -->
    <script src="flag4.js"></script>
  </body>
</html>
```

#### *Flag 2 :*

En déroulant la première balise appelée script on peut apercevoir le flag2.

```
<body bgcolor="#000000">
  <!-- flag1: CLIENT1{69C298598C} -->
  <script>
    var
    flag2_urlencoded="%43%4c%49%45%4e%54%32%7b%32%43%46%34%34%44%35%35%46%32%7d";
    == $0
  </script>
  <!-- flag3 : http://isr.istic.univ-rennes1.fr/client/redirect.html -->
  <script src="flag4.js"></script>
</body>
</html>
```

Celui-ci n'étant pas lisible nous avons cherché à le décrypter. Il faut utiliser un convertisseur HTML en texte unicode car les entités HTML sont codées en nombre décimaux.

## ISR TP CAPTURE DE DRAPEAU

Nous avons utilisé le site : <http://www.online-toolz.com/tools/unicode-html-entities-converter.php>

### Unicode Entities to Text Converter

Converts from HTML Entities to Unicode Text

Example: &#1593;&#1585;&#1576;&#1609; to عربي

**Note:** HTML Entities are in decimal numbers

#### HTML Entities

%43%4c%49%45%4e%54%32%7b%32%43%46%34%34%44%35%35%46%32%7d

Convert

#### Unicode Text

CLIENT2{2CF44D55F2}

Le flag 2 est alors révélé : **CLIENT2{2CF44D55F2}**

### Flag 3 :

Pour le flag 3 nous remarquons également un commentaire le concernant.

```
<!-- flag3 : http://isr.istic.univ-rennes1.fr/client/redirect.html --> == $0
```

Nous complétons l'URL actuelle avec « redirect.html ». La page de redirection s'ouvre et à la fin du timer nous sommes redirigés à nouveau. Pour arriver à la dernière page afin de trouver le flag nous

## ISR TP CAPTURE DE DRAPEAU

décidons d'inspecter une requête GET dans l'onglet « Network ». On peut observer dans ce nouveau code HTML, dans l'en-tête plus précisément, dans la balise « meta » le contenu de la prochaine redirection.

```
<head>
  <title>Redirection</title>
  <meta http-equiv="refresh" content="256;URL='redirect_d3d94468.html'">
</head>

<body>
  Redirection 9/13 avant le flag.<br>
  Vous allez &ecirc;tre redirig&eacute;(e) vers la page suivante dans 256 secondes.
</body>
html>
```

Ici nous sommes à la page 9 qui a un timer de 256 secondes et qui nous redirige à la fin de ce timer vers « redirect\_d3d94468.html ».

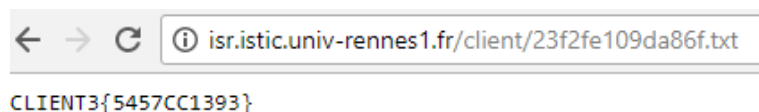
Pour ne pas attendre il nous suffit de copier cette partie et de la coller dans notre URL comme tel « http://isr.istic.univ-rennes1.fr/client/redirect\_d3d94468.html ».

Arrivé sur la page suivante nous répétons le processus jusqu'à arriver à la dernière page.

```
<html>
  <head>
    <title>Redirection</title>
    <meta http-equiv="refresh" content="4096;URL='23f2fe109da86f.txt'">
  </head>

  <body>
    Redirection 13/13 avant le flag.<br>
    Vous allez &ecirc;tre redirig&eacute;(e) vers le flag dans 4096 secondes.
  </body>
</html>
```

Une fois sur cette dernière page, le contenu de la page suivante est un fichier texte. Que nous coller comme précédemment dans l'URL. Le troisième flag apparaît **CLIENT3{5457CC1393}**.



← → ↻ ⓘ isr.istic.univ-rennes1.fr/client/23f2fe109da86f.txt

CLIENT3{5457CC1393}

## ISR TP CAPTURE DE DRAPEAU

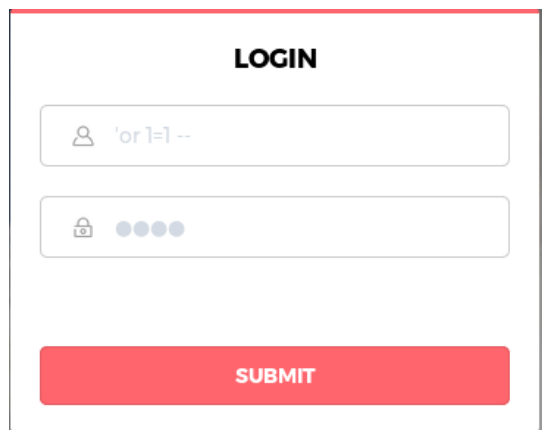
### Exercices SQL 2 flags :

#### *Flag 1 :*

Permet d'injecter une commande qui sera toujours vrai dans le champs login et on met en commentaire le champs password. Par défaut il prend la première ligne de la base de données soit l'user 1.

On injecte cette commande dans le login : ' or 1=1 --

Et on met un mot de passe, n'importe lequel, **mdp =1234**. Puis on obtiens le flag suivant.  
**SQL1{4D220DFA0C}**



#### Member zone

Welcome, **arya** !

#### Status

admin: no

FLAG USER

FLAG-ADMIN

#### Users

id	username
1	arya
2	sansa
3	admin
4	jon

## ISR TP CAPTURE DE DRAPEAU

### *Flag 2 :*

Permet de se connecter en mode admin. Dans le champs login. On ferme la requete SQL et le reste est en commentaire donc, le mot de passe.

**Login= admin'--**

**mdp =1234**

SQL2{7A50BE1791}

#### LOGIN

### Member zone

Welcome, **admin** !

#### Status

admin: yes

FLAG-USER

FLAG ADMIN

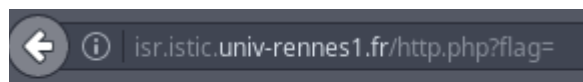
## ISR TP CAPTURE DE DRAPEAU

### Exercices HTTP 3 flags :

#### **Flag 1 :**

Dans l'adresse URL on tape **?flag=** qui nous permet d'obtenir le premier flags.

**HTTP1{594ECC9EDF}**

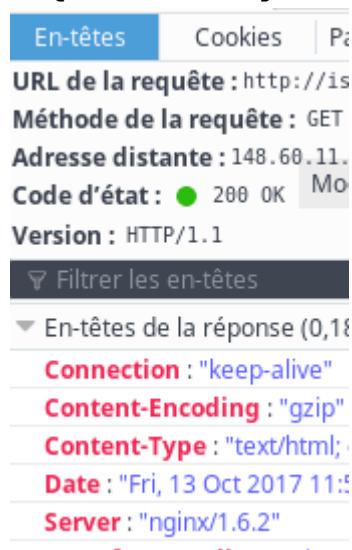


**HTTP1{594ECC9EDF}**

#### **Flag 2 :**

Dans l'onglet « réseaux » on clique sur une requête puis dans en-tête on a le champs server : « nginx/1.6.2 ». On entre donc nginx comme étant le serveur et 1.6.2 comme étant la version de celui-ci.

**HTTP2{F18385EC0D}**



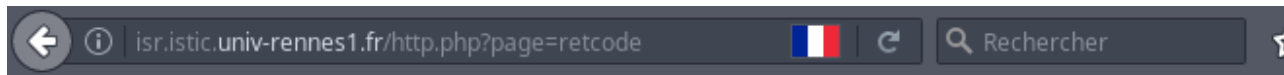
**HTTP2{F18385EC0D}**

## ISR TP CAPTURE DE DRAPEAU

### Flag 3 :

On change la requête GET en requête PUT après avoir inspecter l'élément et être allé dans l'onglet réseaux.

**HTTP3{68BCC7D77C}**



To get the flag, follow the HTTP return codes.

- 1. Put the HTTP return code in an additional *code* parameter on this page
- 2. Get the new return code of the obtained page
- 3. Repeat

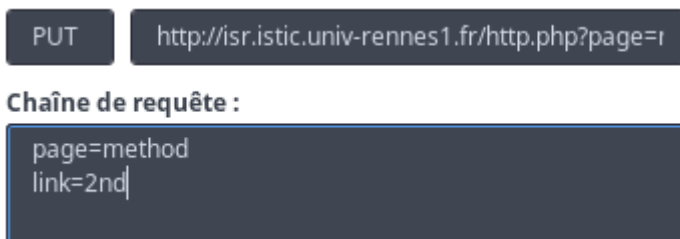


**HTTP3{68BCC7D77C}**

### Flag 4 :

On remplace dans notre URL retcode par method. On nous demande de changer la requête GET en requête PUT puis on renvoie la requête. Il nous suffit de regarder la réponse et de compléter notre URL. On répète le processus plusieurs fois et nous obtenons le flag.

**HTTP4{F18385EC0D}**



## ISR TP CAPTURE DE DRAPEAU

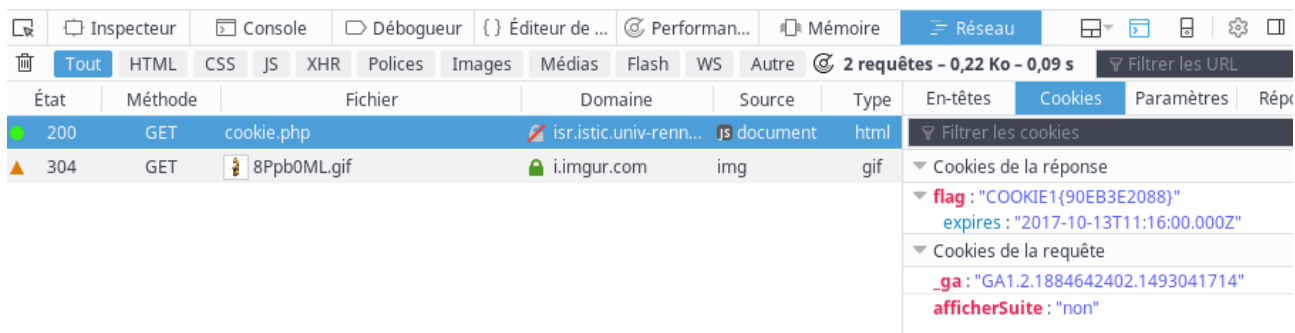
### Exercices Cookie 2 flags :

#### *Flag 1 :*

On inspecte l'élément. Dans l'onglet réseaux on clique sur une requête et on regarde l'onglet cookie pour obtenir le premier flag. On peut également trouver le flag dans l'en tête avec les accolades au format %7.

**COOKIE1%7B90EB3E2088%7D** : Ici dans l'entête avec les accolades en Unicode.

**COOKIE1{90EB3E2088}** : Dans l'onglet cookie.



#### *Flag 2 :*

Toujours dans l'onglet réseaux. On clique sur une requête. Dans l'en-tête de la requête on cherche l'User-Agent. On clique sur « Modifier et Renvoyer ». Puis on modifie l'User Agent de Mozilla en admin avant de renvoyer.





## ISR TP CAPTURE DE DRAPEAU

### Exercices SSH 2flags :

#### **Flag 1 :**

Pour se connecter à SSH c'est à dire à un serveur distant il faut taper dans un shell

« ssh [tpcft@url](#) »

tpcft étant le login et également le mot de passe. L'URL est celle où l'on veut se connecter.

Nous obtenons alors ce flag. Après avoir fait un « cat flag »

UNIX1{3D8A39946F}

```
urlshell-4.3$ ssh tpcft@isr.istic.univ-rennes1.fr
tpcft@isr.istic.univ-rennes1.fr's password:
tpcft@isr:~$
```

#### **Flag 2 :**

Le deuxième flag étant caché. On utilise la commande « ls-a » qui fait apparaître un répertoire « hidden ». On se déplace dedans avec cd hidden. Et nous trouvons le deuxième flag avec la commande cat.

UNIX2{ED79EDF145}

```
tpcft@isr:~$ ls -a
.  ..  flag  -flag 3  .hidden  infos.txt  labyrinth
tpcft@isr:~$ cd .hidden
tpcft@isr:~/.hidden$ ls
tpcft@isr:~/.hidden$ ls -a
.  ..  .flag2
tpcft@isr:~/.hidden$ cat .glag2
cat: .glag2: Aucun fichier ou dossier de ce type
tpcft@isr:~/.hidden$ cat .flag2
UNIX2{ED79EDF145}
```