Computer Security Homework 0x03

Real name: 涂世昱

Nick name: R07922115

Student ID: R07922115

Unexploitable

打開連結(https://unexploitable.kaibro.tw/), 是一個奇怪的頁面, 觀察了一下頁面的html source code, 也只是跟動畫有關的東西。之後嘗試用用看dirsearch, 搜出一些檔案, 大多內容都只顯示`nice try`的字樣, 沒什麼內容, 除了changelog之外, 其內容為

```
Bucharesti.github.io

Nice try!
```

其中`Bucharesti.github.io`為一連結, 但也只是連到原本題目的link, 上網搜尋`Bucharesti`也找不到什麼線索, 最後經過同學的指導, 發現原來`Bucharesti`是一個Github的user, 進入`https://github.com/Bucharesti`, 發現它只有開一個repository, 正是`Bucharesti.github.io`, 在裡面看看commit history, 發現flag就藏在`Oct 17, 2019`的`added some files`當中。

Safe R/W

Introduction

觀察了一下source code, 大致上其內容為,

1. 將存取的目錄存為`$f`
2. 將寫入內容存為`$c`
3. 將include的檔案名稱存為`$i`
4. waf:
    - `$f`不能包含`. / -`
    - `$c`不能超過20個字
    - `$i`不能包含`ph`
5. 建資料夾(`system("mkdir " . escapeshellarg($sandbox . "/" . $f));`)
6. 把`$c`內容寫入`meow`當中 (`file_put_contents("meow", $c);`)
7. 將`$i`內容讀出來(`file_get_contents($i)`), 若其中有包含`<`, 就不會往下執行
8. include(`$i`)
9. 將檔案刪除

Ideas

從source code當中大概猜測這題解法應該是想辦法把`ls`指令塞進去並且讓結果能夠顯示出來, 之後再把flag用`cat`再把它印出來, 而能夠下手的點不外乎就是`system`, 及`include`。

system("mkdir " . escapeshellarg($sandbox . "/" . $f));

這邊可以改變的變量為`$f`, 原本是想說能不能夠塞一些像是引號, 雙引號之類的東西讓它能夠在`mkdir`之後執行`ls`, 但`escapeshellarg`無論如何就是會把我所輸入的東西全部包在一起變成`mkdir`的一個argument, 也就是資料夾的名稱, 所以這方法就不可行。

include(`$i`)

將php code放到檔案裡面, 照理來說include可以把它解析並且執行其中得php code, 但問題是在include之前有一個`file_get_contents`去把檔案內容讀出來並且比對是否其中有包含`<`符號, 那麼一般的php code在這邊就不會過, 上網找也找不到可以bypass`<`的方式。

經過同學的指導, 它發現網路上有一題ctf與這題設計方式類似 (https://ctftime.org/writeup/12921), 雖然writeup不是英文, 但是發現題目的程式碼也有相似的東西

```
if(!stripos(file_get_contents($_GET['page']),'<?') &&
!stripos(file_get_contents($_GET['page']),'php')) {
    include($_GET['page']);
}
```

其解法為,

```
file_get_contents('data:,xx/profile'); --> string 'xx/profile'
include('data:,xx/profile');           --> 'data:,xx/profile' adına sahip
dosyasının içeriği
```

大概理解就是`file_get_contents('data:mydir/meow')`的結果會是`mydir/meow`, 但`include('data:mydir/meow')`卻會把`mydir/meow`的內容解析出來, 這就是`php`的問題吧, 又之前有提到說將變數用array傳進去(`c[]=...`)就可以bypass字數的限制, 於是解題方式為`url: https://edu-ctf.csie.org:10155/?f=data:mydir&i=data:mydir/meow&c[]=<?php system('ls /'); ?>`, 之後再用相同的方式把flag印出來即可。