HackGame2 writeup

转载

网址：http://hackgame.blackbap.org/

第一关 突破客户端：无论输入什么密码都会提示“密码不能为空”，使用浏览器检查网页元素会发现提交时会触发 javascript 函数 chk_submit()，查看该函数的代码发现始终返回 `false`，于是我们在浏览器的 Console 中将函数的返回值改为 `true`，即输入 `chk_submit=true`，再在输入框中输入密码 `password` 就行了。

第二关 逆向解密：
根据提示得到一串 PHP 代码（路径为/tip/nozend.php），有加密的函数但是没有解密的函数，根据加密的过程逆向推出解密的过程并写出代码就可以了

```php
<?php

highlight_file( __FILE__ );

function notrealmd5code($string,$operation='ENCODE') {
    if ($operation=='ENCODE'){
        $OutTxt = "";
        for ($x=0;$x<strlen($string);$x++) {
            $nr = ord($string[$x]);
            if ($nr < 128) {
                $nr += 128;
            }
            elseif ($nr > 127) {
                $nr -= 128;
            }
            $nr = 255 - $nr;
            $OutTxt .= sprintf("%02x", $nr);
        }
        return $OutTxt;
    } else {
        /* DECODE MISS
        * ord Return ASCII value of character
        */
        $OutTxt = "";
        $str = str_split($string, 2);
        foreach ($str as $key => $value) {
            $dec = hexdec($value);
            $nr = 255 - $dec;
            if ($nr > 128) {
                $nr -= 128;
            }
            elseif ($nr < 127) {
                $nr += 128;
            }
            $OutTxt .= chr($nr);
        }
        return $OutTxt;
    }
}
echo notrealmd5code('1c10121a181e121a0f1016110b4d4d4d','DECODE');

?>
```

运行解密函数后得到答案为 `comegamepoint222`

第三关 寻找Password：

Windows 的密码存放路径和 Linux 的用户配置文件存放路径可以通过 Google 得到，分别是 `c:\windows\system32\config\SAM` 和 `/etc/passwd`，这样可以得到两个口令，分别是

```
d18e760f2b15a239328274a447cd67f7
- > NTLM?
```

和

```
$1$1zUVF6AN$uHBYbOv4WW1Z9kkKFnJ2v.
- > MD5(UNIX)?
```

使用提供的工具（注意更改暴力攻击的选项）破解其中一个，便得到答案 `*#!*`

第四关 挖掘规则里面的漏洞：下载所给的 PDF 文件，用编辑器（VIM，Sublime Text 等）打开，根据所给的提示（做该题的时候发现链接失效了，于是根据论坛的提示做的）,搜索“Action”字符串，发现后面的尖括号内有一串16进制代码 `70617373776F72642069733A706466697357696465 6C7921`，根据提示，这是一个字符串的16进制 ASCII 码，因此我们将其转换为字符串，代码如下

```
#!/usr/bin/env python3
# Author: renzongxian

s = '70617373776F72642069733A706466697357696465 6C7921'
for i in range(0, len(s), 2):
    print(chr(int(s[i:i+2], 16)), end = '')
```

运行得到“password is:pdfisWidely!”，答案是 `pdfisWidely!`

第五关 页面自身的缺陷：有一个输入框可以执行 JavaScript 语句，使用浏览器的检查元素功能发现，提交 JavaScript 语句时会触发一个 Javascript 函数 `do_try()`，找到该函数的源码发现还有一个 `do_other()` 函数，而且注释为 `getpwd`，显然这个函数跟获得密码有关，因此将提交时触发的函数更改为 `onclick="do_other('getpwd');"` 即可得到密码，答案是 `URsoGreat`

转载于:https://www.cnblogs.com/renzongxian/p/5619868.html