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

546325574@qq.com 作者:

web 2

```
右键查看源码
```

```
发现一个奇怪的is
                                                                                                                      <script src="http://libs.baidu.com/jquery/1.9.1/jquery.min.js"></script>
                                                                                                                      (script)
                                                                                                              $.ajax({
                                                                                                                                                                         ijax({
  type: 'GET',
  url: "index.php/flag",
                                                                                                 9 });
0 </script>
1
2 </html>
3
HTTF/1.1.200 CB
Date: Pai, 28 Mey 2016 13:31:42 CBT
Date: Pai, 28 Mey 2016 13:31:42 CBT
Date: Pai, 28 Mey 2016 13:31:42 CBT
Access-Control-Lallow-Pathods: *
Control-Langth: 68
Control-
                SET (Index Papel Heigransey/IIIII HTTP/A.)

Best: Junya-hosf.de

New Junya-hosf.de

Oser-Appent: Mosiliaria (Windows HT E.2; WUW4) ApplaWebEir/577,36 (IDII

Jabe Gecho) Chenca/Web.2004 95 Safatz/A57,36

Accept.—Boodling: gaip, deflate, width

Accept.—Boodling: gaip, deflate, width

Camment-John C. John C. Windows HT E.2 (WIM4) ApplaWebEir/577,36 (IDII

Camment-John C. John C. Windows HT E.2; WIM4) ApplaWebEir/577,36 (IDII

Camment-John C. John C. Windows HT E.2; WIM4) ApplaWebEir/577,36 (IDII

Camment-John C. John C. Windows HT E.2; WIM4) ApplaWebEir/577,36 (IDII

Camment-John C. John C. Windows HT E.2; WIM4) ApplaWebEir/577,36 (IDII

Camment-John C. John C. Windows HT E.2; WIM4) ApplaWebEir/577,36 (IDII

Camment-John C. John C. Windows HT E.2; WIM4) ApplaWebEir/577,36 (IDII

Camment-John C. John C. Windows HT E.2; WIM4) ApplaWebEir/577,36 (IDII

Camment-John C. Windows HT E.2; WIM4, W
            TIT (Mades php/Engymnory/11111 HTT7/1.1
Hoss: 13ng-lock t.s
Hoss: 13ng-lock t.s
Hoss: 13ng-lock t.s
Hoss: 12ng-lock t.s
Hoss: 
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       HTTP/1.1 COO CH

HTTP/1.1 COO CH

Date F1., I How TOLE 12:31 be GHT

between the Common 
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            ("weerage":"; "what is flag! give we money! DO you know RESTfull":")
                PUT_/index_pip/mnney/pill1 HTTI/L.1

Stort: jinja_hrkt.10

Accept; //

Accept; //

Stort: jinja_hrkt.10

Accept; //

Stort: jinja_hrkt.10

Accept; //

Stort: jinja_hrkt.10

Accept.-lampses; jinja_hrkt.10

Accept.-lampses; jhrdj, jotlars, ideh

Accept.-lampses; jhrdj, jotlars, ideh

Content-lampsh, il
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    MITS/1.1 TOU OF
Date: Fil. 25 New TOLE 13:32:04 GRT
Server: Apacher? 4.10 (behiam)
Access-Cantrol-Allow-Deshoot: *
Content-Langth: 64
Connection: close
Content-Type: application/jeon
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             ("message": "\"Your flag is hctf(Do_you_know_124987) web dog(\"")
                                              cney*L7450
```

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

```
在这里上传题的图片,我们将为题保存
选择文件 未选择任何文件
```

上传统功点此查看

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。

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

 ${\red{\$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?

(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)。



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



得到flag