实验吧-让我进去 Writeup

原创

baynk 于 2019-08-17 13:05:31 发布 814 收藏

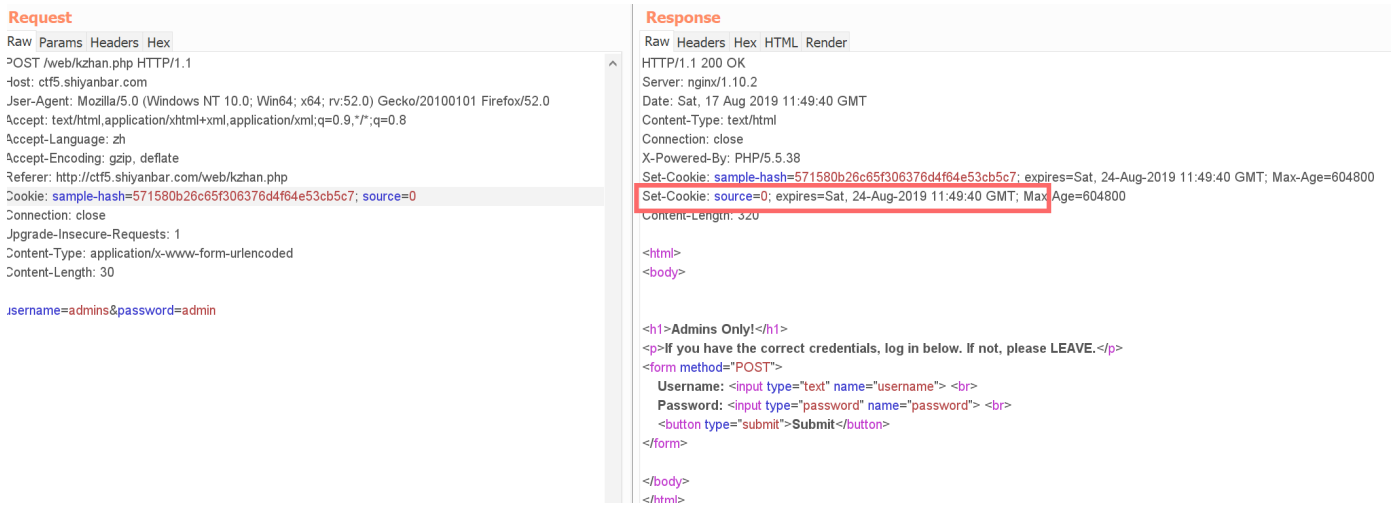
分类专栏： # 实验吧 Writeup 文章标签： CTF 实验吧

本文链接：https://blog.csdn.net/u014029795/article/details/99691215

难得中午有时间写，昨天夜里就搞完了。。。

过程

- 链接：http://ctf5.shiyanbar.com/web/kzhan.php
- 点进去后有个登陆窗口，随便填了下，用户名为admins，密码admin，burpsuite拦截看信息。

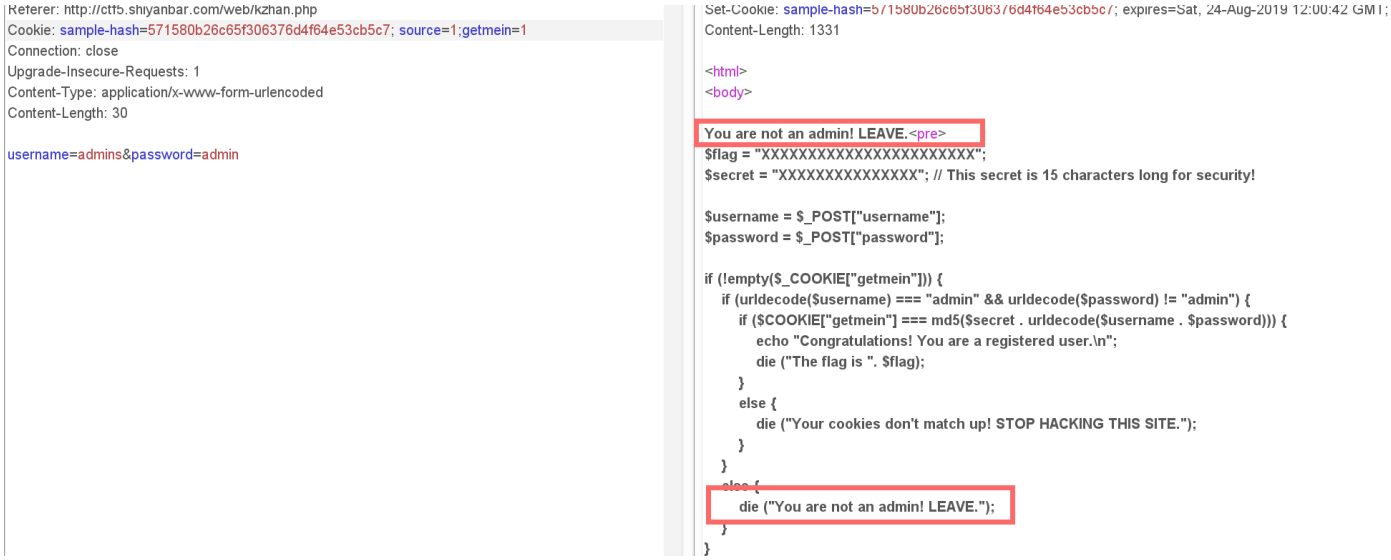


- 有个奇怪的source=0，改为1就能看到源码。

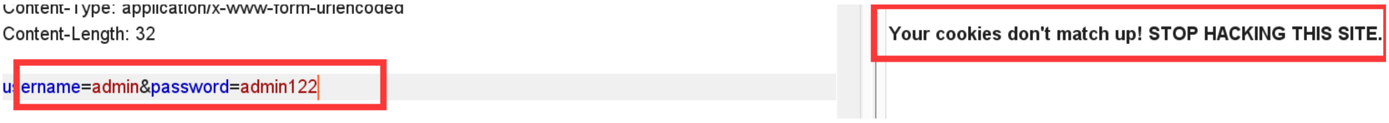
```
<pre>
$flag = "XXXXXXXXXXXXXXXXXXXXXXXX";
$secret = "XXXXXXXXXXXXXXX"; // This secret is 15 characters long for security!

$username = $_POST["username"];
$password = $_POST["password"];

if (!empty($_COOKIE["getmein"])) {
    if (urldecode($username) === "admin" && urldecode($password) != "admin") {
        if ($COOKIE["getmein"] === md5($secret . urldecode($username . $password))) {
            echo "Congratulations! You are a registered user.\n";
            die ("The flag is " . $flag);
```

```
        die ("The flag is " . $flag);
    }
    else {
        die ("Your cookies don't match up! STOP HACKING THIS SITE.");
    }
  }
  else {
    die ("You are not an admin! LEAVE.");
  }
}

setcookie("sample-hash", md5($secret . urldecode("admin" . "admin")), time() + (60 * 60 * 24 * 7));

if (empty($_COOKIE["source"])) {
  setcookie("source", 0, time() + (60 * 60 * 24 * 7));
}
else {
  if ($_COOKIE["source"] != 0) {
    echo ""; // This source code is outputted here
  }
}
  </pre>
```

- 分析下源码发现，首先是判断cooike是否有getmein，才会执行其余的，先加上。



- 然后再看第二个条件，username必须为admin，密码不可以为admin，再随便写。



- 最后一个条件了，如果getmein的值，等于md5($secret+admin+xxx)就可以打印出flag了。
- 这里着实把我难住了，因为$secret不知道是多少，所以根本没法算出来，又仔细看了下提示，看看到底有没有$secret的提示，在最后的源码中有这么一行，告诉我们cookie中的hash是md5($secret+admin+admin)算出来的，但是hash也不可逆，所以还是没有办法，但是这里明显是一个提示，所以就去找writeup了。

> setcookie("sample-hash", md5($secret . urldecode("admin" . "admin")),

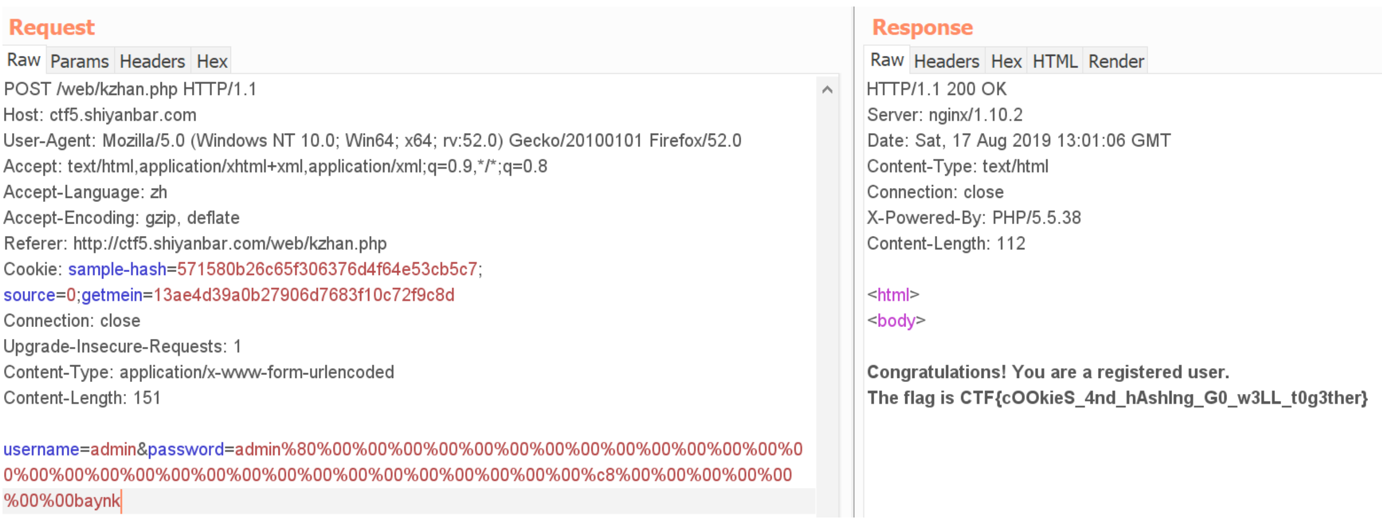
- 果然是有关于md5的，叫做md5长度扩展攻击，原理后面再补上。先干起来。可以用Python脚本的exp也可以直接用工具来完成，这里直接在kali里面安装hashpump使用。
- 安装方法

```
git clone https://github.com/bwall/HashPump
apt-get install g++ libssl-dev
cd HashPump/
make && make install
```

- 可以直接使用了。

```
root@kali191a:/usr/bin# hashpump
Input Signature: 571580b26c65f306376d4f64e53cb5c7   #secret+admin+admin的hash
Input Data: admin  #固定的参数，这里指的是最后的password对应的admin
Input Key Length: 20  #虽然secret只有15位，但是还有一个admin也占了5位，所以这里是20
Input Data to Add: baynk  #这里是自己要算的值所需要加的参数
13ae4d39a0b27906d7683f10c72f9c8d  #算出新的hash，填到getmein中。
admin\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xc8\x00\x00\x00\x00\x00\x00\x00baynk  #payload(baynk可以随便换)，这也是要填的password
```

- 将'\x'替换换成'%'以urlencode的方式提交，然后拿结果就好~



总结

- 这个md5扩展长度攻击看了快两个小时才明白，不过搞明白了后这个题是真的挺简单的，回头再写下这个攻击实现的具体原理吧。