实验吧 让我进去 writeup

原创

zero-L 于 2019-07-09 16:24:32 发布 231 收藏

分类专栏： ctf 实验吧 文章标签： ctf 实验吧 md5扩展攻击

本文链接：https://blog.csdn.net/weixin_39938635/article/details/95204367

题目传送门

看提示和注入应该没什么关系，随便输没有回显，用sqlmap扫一下没东西

查看session，有个变量值为0的变量，改成1试试

出来源码

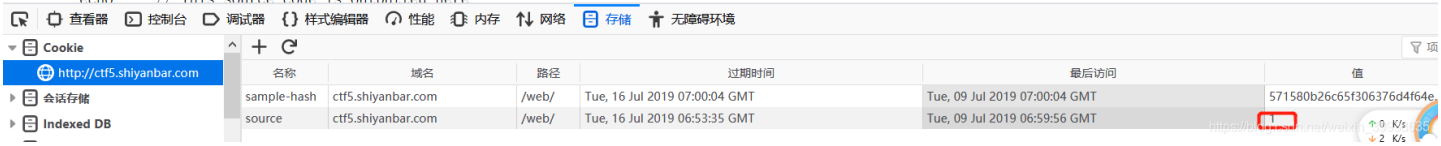
```
$flag = "XXXXXXXXXXXXXXXXXXXXXXX";
$secret = "XXXXXXXXXXXXXXX"; // This secret is 15 characters long for security!

$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);
        }
        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
```



username一定要是admin，password不能是admin，cookie要传一个getmein过去，然后这个getmein是由md5(secret,username,password)构造出来的，secret长度为15，sample-hash是secret+adminadmin得到的，所以不能直接得到hash值，需要自己构造

百度ing。。。是哈希长度扩展攻击

根据参考链接

https://github.com/iagox86/hash_extender

https://blog.csdn.net/qq_35078631/article/details/70941204

假如我们知道了，md5(“secret”)，我们不需要知道secret是什么，只要知道长度，人为将secret填充完，在新加一块假设为add，之前得到的MD5值作为最后一块加密的初始向量IV，最后加密得到的结果和MD5(secret+add)结果是一样的

使用burp修改下包的内容，得到flag