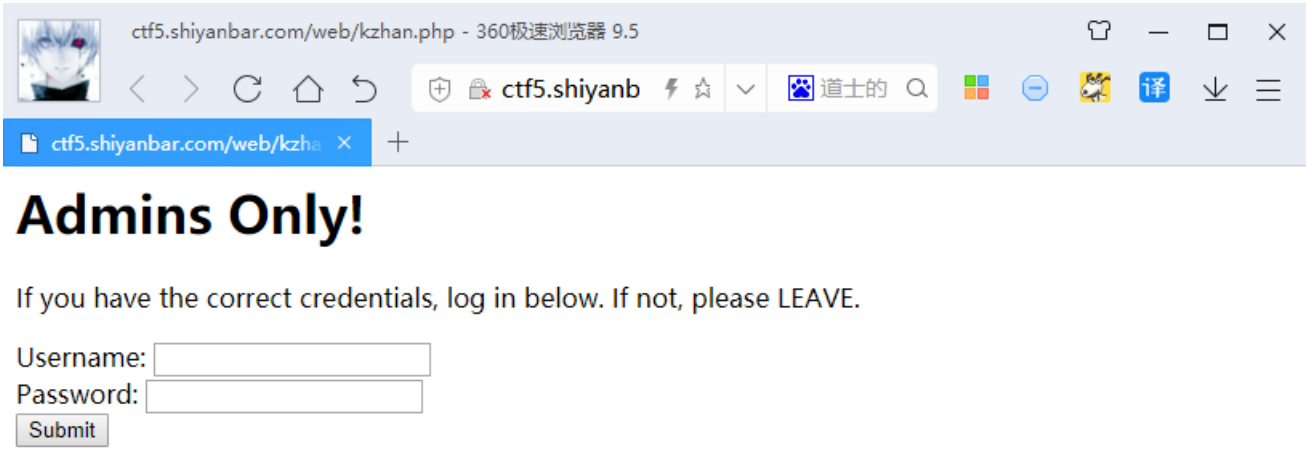
CTF实验吧让我进去writeup

转载

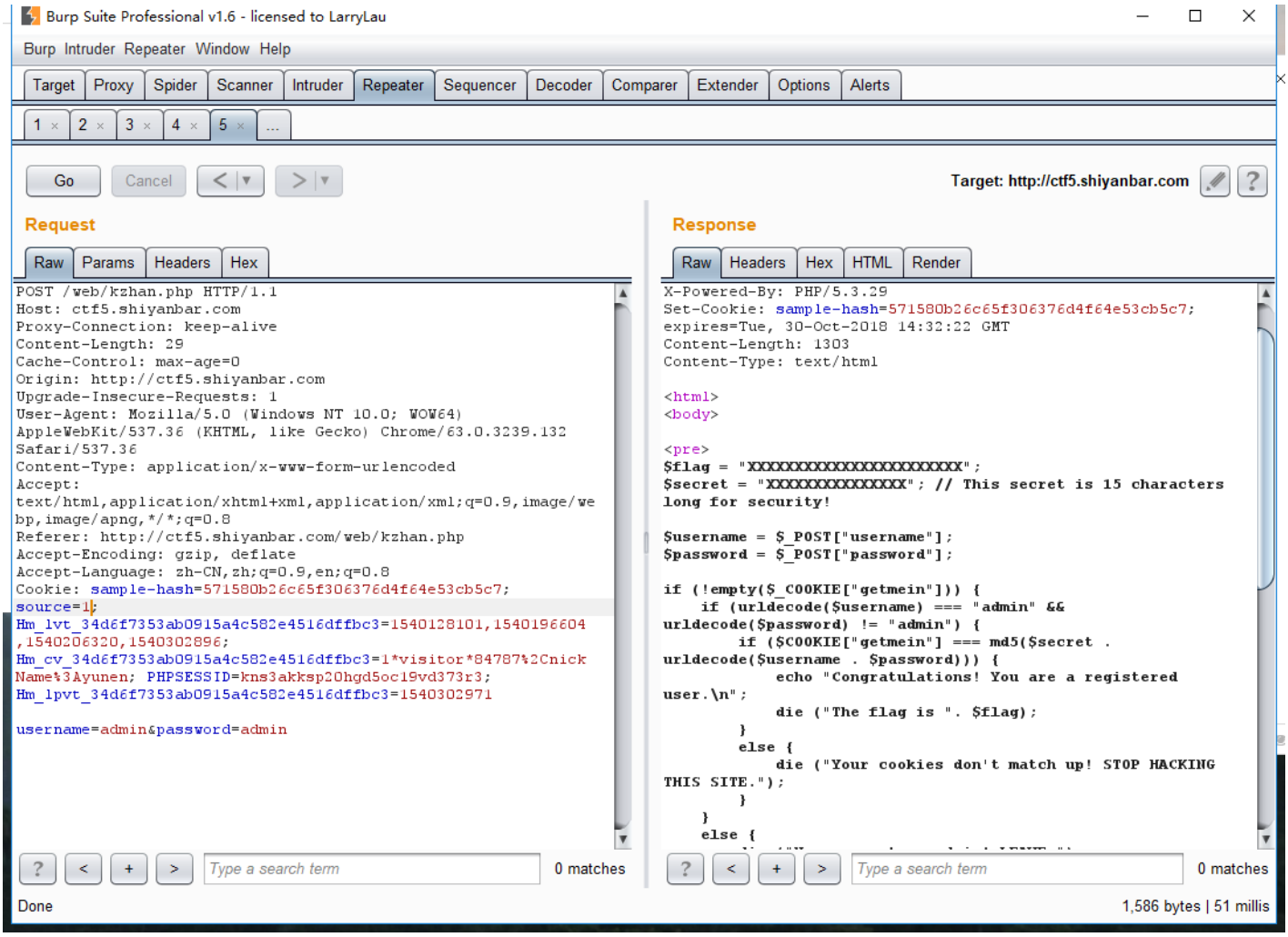
weixin_30496751 于 2019-03-26 23:28:00 发布 208 收藏
原文链接：http://www.cnblogs.com/yunen/p/10604681.html
版权

初探题目



两个表单，我们用burp抓包试试

这时候我们发现Cookie值里有个很奇怪的值是source，这个单词有起源的意思，我们就可以猜测这个是判断权限的依据，让我们来修改其值为1，发送得到如下显示：



代码审计

发现爆出了源代码，让我们来审计一下

```
$flag = "XXXXXXXXXXXXXXXXXXXXXXX";
$secret = "XXXXXXXXXXXXXX"; // 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
    }
}
```

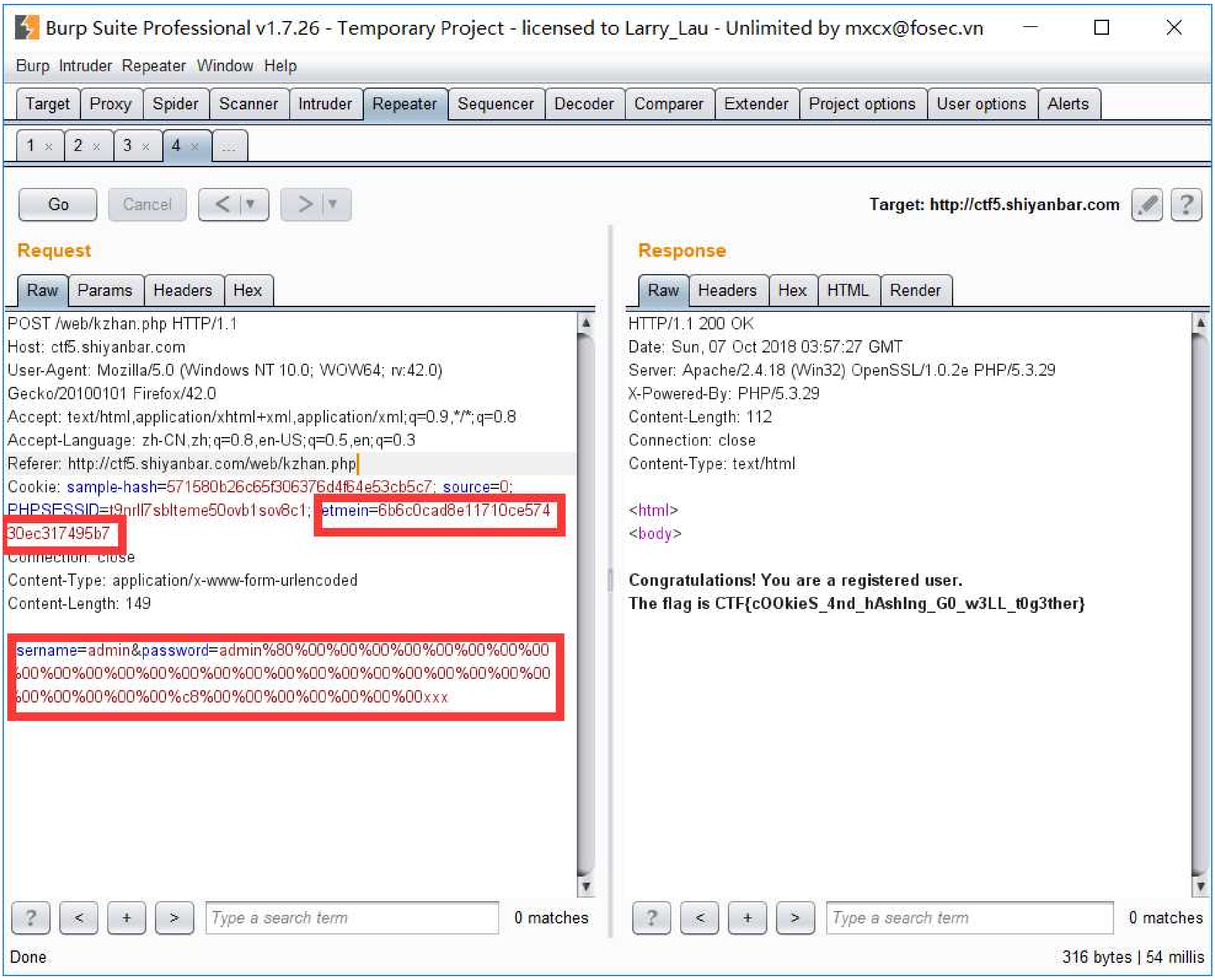
我们如果需要获得flag，需要满足一下条件：
1.Cookie中getmein的值不能为空
2.username必须为admin和password不能为admin
3.Cookie中的getmein必须等于`md5($secret.urldecode($username.$password))`
满足这三个条件才可获得flag，可是我们无法得知$secret的值为多少
`setcookie("sample-hash", md5($secret . urldecode("admin" . "admin")), time() + (60 * 60 * 24 * 7));`
发现下面有行代码是这样写的，将输出的`md5($secret . urldecode("admin" . "admin"))`作为cookie输出，结合前面的数据包我们可以知道输出的值为`571580b26c65f306376d4f64e53cb5c7` 可是这串md5是由$secret+'adminadmin'转md5而得到的，如果我们在password输入admin将不满足前面所需的三个条件

死局转生

我们知道常见的md5是16位的，而这里的md5正是16位，我们的$secret是十五位的,加上'adminadmin'就变成25位了，很明显这里的md5肯定会出现重复，所以我们可以哈希长度拓展攻击绕过这个死局
这里附两个讲述具体原理的链接:
http://www.freebuf.com/articles/web/69264.html https://www.cnblogs.com/p00mj/p/6288337.html

在Kali下用hashpump操作

最好我们构造数据包，把生成的数据发送即可获得flag



转载于:https://www.cnblogs.com/yunen/p/10604681.html