

系统安全平台第五次作业

第一题

1.md5漏洞 (50分)

题目描述:

当前网站的后端登录处理中存在md5码漏洞。md5漏洞指的是php在处理哈希字符串时会利用“!”或“==”来对哈希值进行比较，它把每一个以“0E”开头的哈希值都解释为0，所以如果两个不同的密码经过哈希以后，其哈希值都是以“0E”开头的，那么PHP将会认为他们相同，都是0。
提示：可以尝试构造出哈希值为0E开头的登录密码来触发漏洞！

答案:

已生成虚拟环境

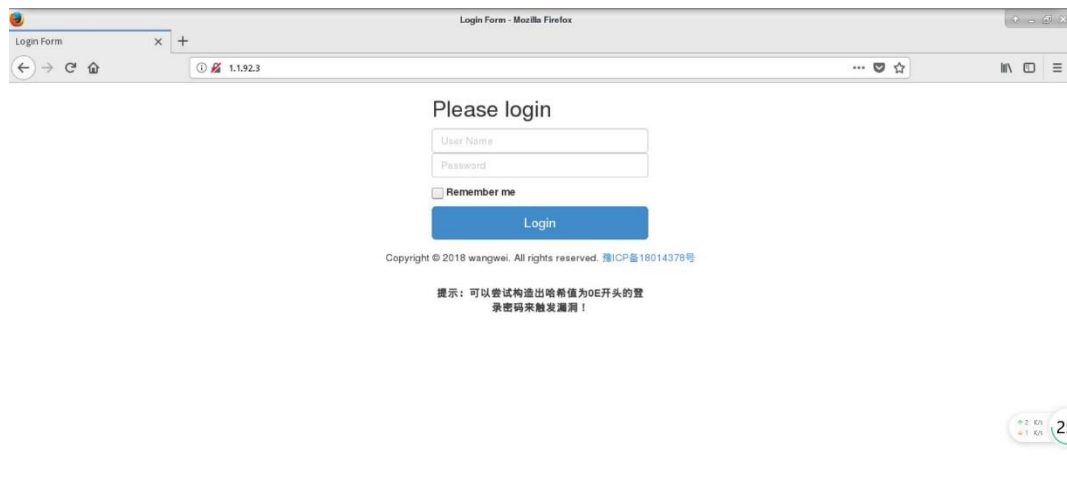
[前往远程桌面](#)

[删除虚拟环境](#)

① 倒计时: 0 小时, 59 分钟, 55 秒



利用浏览器登录网页 (靶机 IP)。



右键查看网页源代码，注意绿色的注释提示了用户名是“wangwei”。

```

color:black;
font-weight:bold;
text-align:center;
border-radius:6px;
padding:3px 0;

/* 定位 */
position:absolute;
z-index:1;
top:35px;
margin-left:100px;
}

.copyright{
position:absolute;
bottom:0;
}

</style>
</head>
<body>

<div class="wrapper" style="margin-bottom:15px">
<form class="form-signin" style="width:300px;margin:auto">
<h2 class="form-signin-heading">Please login</h2>
<input type="text" class="form-control" name="username" placeholder="User Name" required="" autofocus="true" value="" />
<input type="password" class="form-control" name="password" placeholder="Password" required="" value="" />
<label class="checkbox" >
<input type="checkbox" value="remember-me" id="rememberMe" name="rememberMe"> Remember me
</label>
<button class="btn btn-lg btn-primary btn-block" id="loginbtn" name="submit" type="button">Login</button>
</form>
</div>

<!-- <p>The login user name is wangwei</p> -->
<div style="text-align:center" class="copyright">Copyright &copy; 2018 wangwei. All rights reserved. <a href="http://www.miitbeian.gov.cn" target="_blank">豫ICP备18014378号</a>
<p style="margin:auto;margin-top:30px;width:300px;font-weight:bold;text-align:center">
提示： 可以尝试构造出哈希值为0x开头的登录密码来触发漏洞！
</p>
</div>

</body>
</html>

```

在百度搜索一下 md5 漏洞，会有一些经过 md5 加密后开头为 0e 的字符串，复制一个当作密码。

Please login

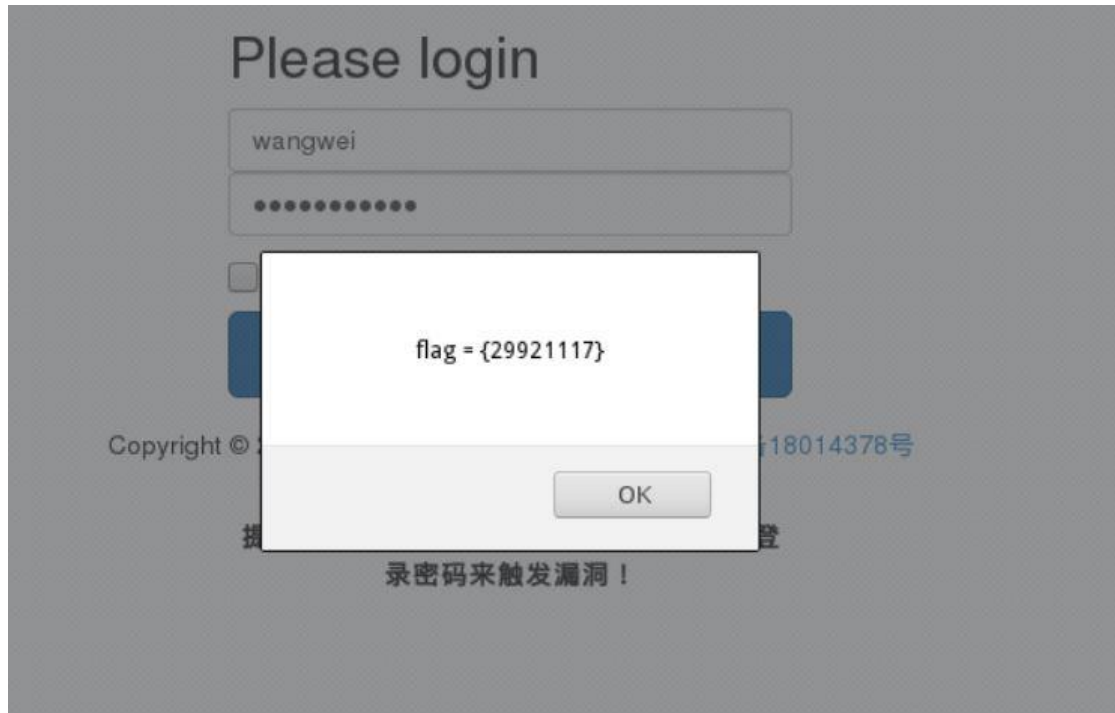
☐ Remember me

Login

Copyright © 2018 wangwei. All rights reserved. 豫ICP备18014378号

提示：可以尝试构造出哈希值为0E开头的登录密码来触发漏洞！

登录后就可得到 flag。



第二题

2.浏览器弱会话ID——简单难度 (50分)

题目描述:

浏览器进入靶机IP地址首页,根据网页提示查看对应cookie值,寻找每次cookie值的规律,flag隐藏其中!

提示: md5

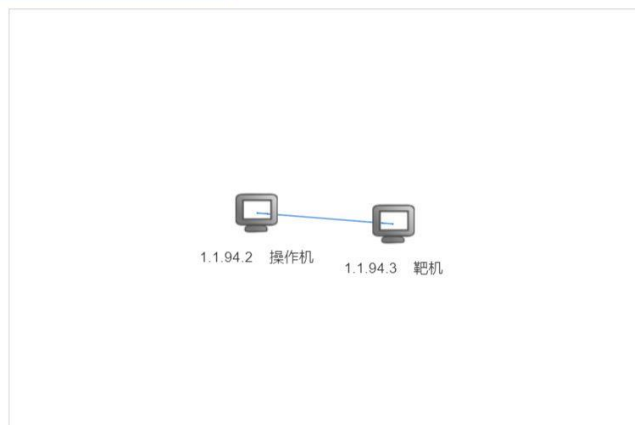
答案:

已生成虚拟环境

前往远程桌面

删除虚拟环境

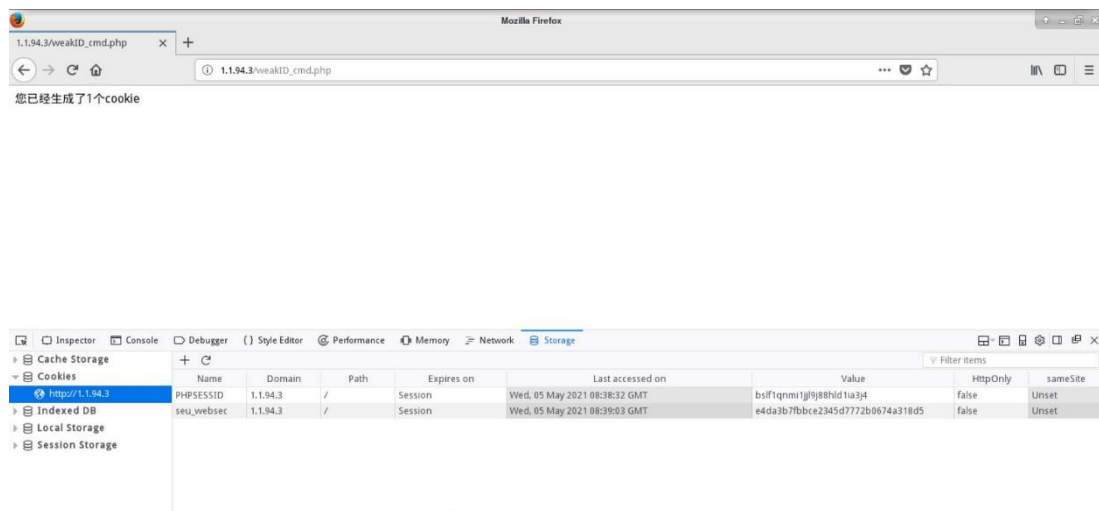
① 倒计时: 0 小时, 59 分钟, 56 秒



利用浏览器登录网页。



按 F12 打开控制台，在 storage 下面可以看到 cookie。



点击一次，查看 cookie 解密后的值为 5。



第二次是 7。

密文: 8f14e45fcea167a5a36dedd4bea2543

类型: 自动 [帮助]

查询 加密

查询结果:
7

第三次是 9。

密文: 45c48cce2e2d7fbdea1afc51c7c6ad26

类型: 自动 [帮助]

查询 加密

查询结果:
9

第四次是 11。

密文: 6512bd43d9caa6e02c990b0a82652dca

类型: 自动 [帮助]

查询 加密

查询结果:
11

由此我们猜测这是一个等差数列，因为每点击 19 次，就会重置，所以我们要求第 9999 项为 20001，经过 md5 加密后得到 cookie。

Pass:	<input type="text" value="20001"/>	<input checked="" type="radio"/> UTF8	<input type="radio"/> \$!-HEX...
Salt:	<input type="text"/>	<input type="checkbox"/> HEX	
Hash:	<input type="text" value="49ba59abbbe56e057"/>		
<input type="button" value="加密"/>			

Result:

base64: MJAwMDE=

md5: 2383c7d07bce3c82e6da7741782de416

md5_middle: 7bce3c82e6da7741

md5(md5(\$pass)): 4bdf39a10f6a102a1b08af761ead684b

md5(md5(md5(\$pass))): f8aa5cb0a2b3fc67d033e3a2d27c593b

md5(unicode): 3765d9286274931f56e28d0e49e5b430

最后得到 flag。

