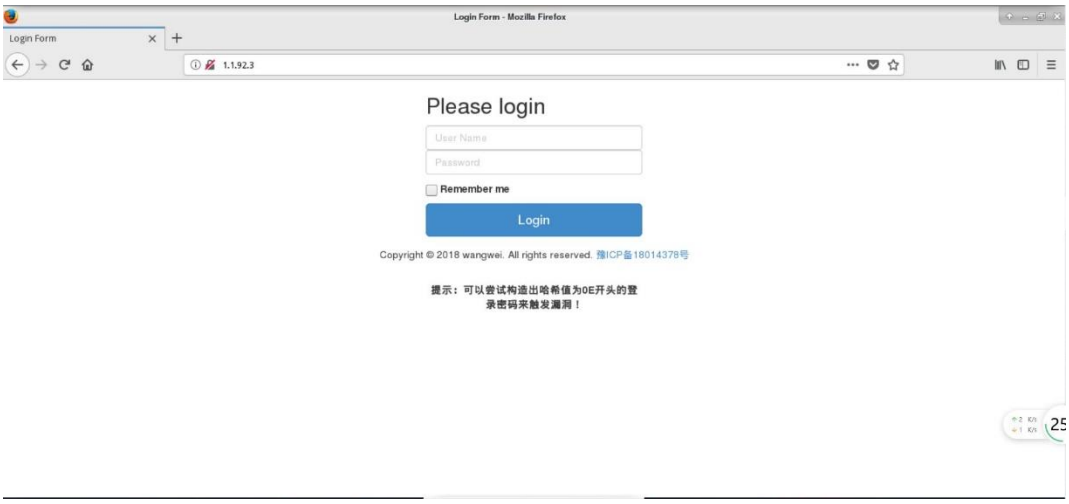
系统安全平台第五次作业

第一题

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{
    positon: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="" 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0E开头的登录密码来触发漏洞！
    </p>
    </div>

</body>
</html>
```

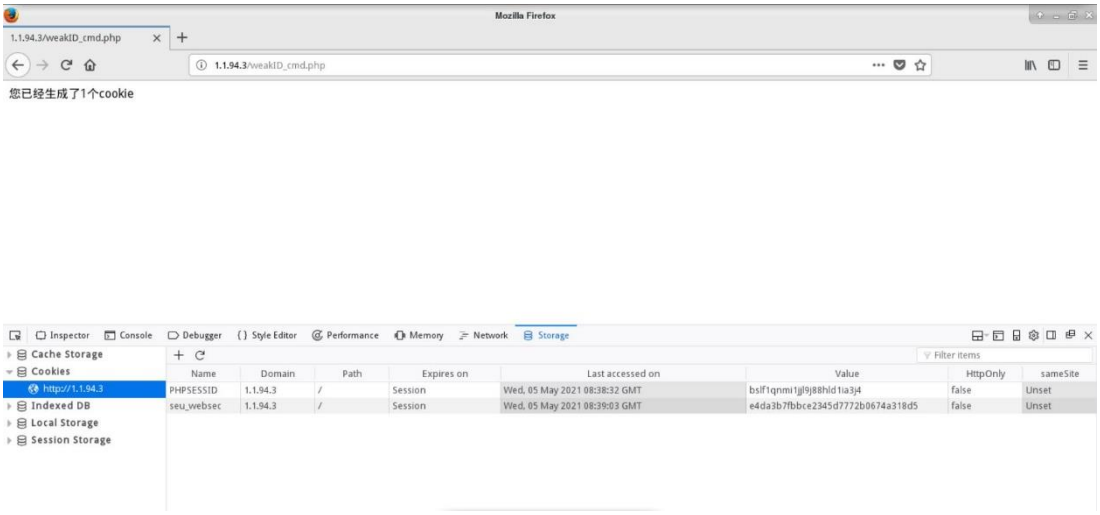
在百度搜索一下 md5 漏洞，会有一些经过 md5 加密后开头为 0e 的字符串，复制一个当作密码。

登录后就可得到 flag。

第二题

利用浏览器登录网页。

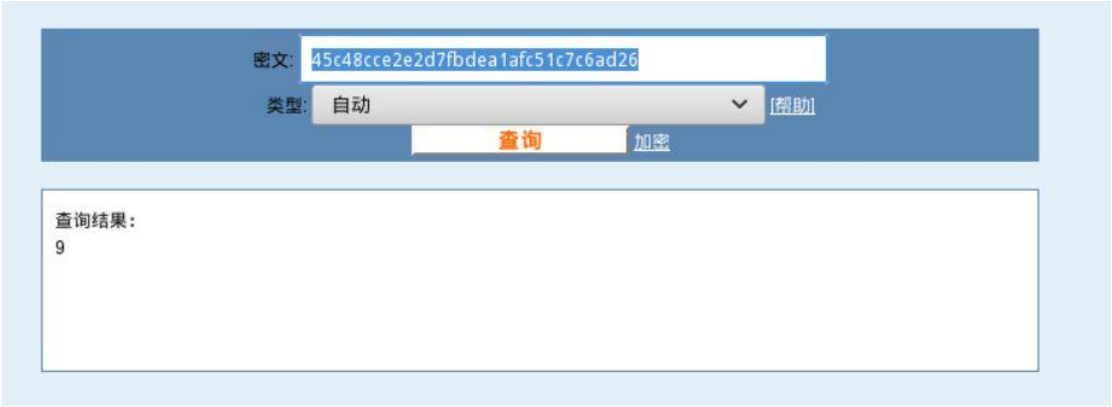
按 F12 打开控制台，在 storage 下面可以看到 cookie。



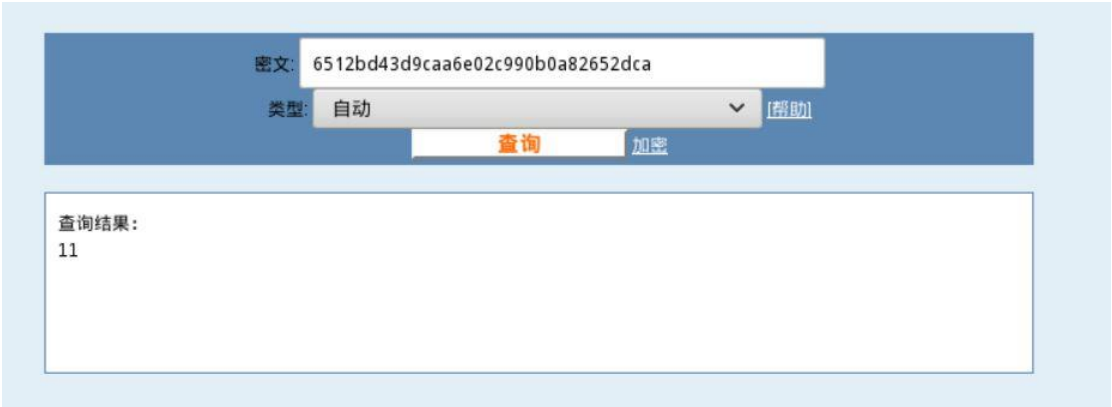
点击一次，查看 cookie 解密后的值为 5。

第二次是 7。

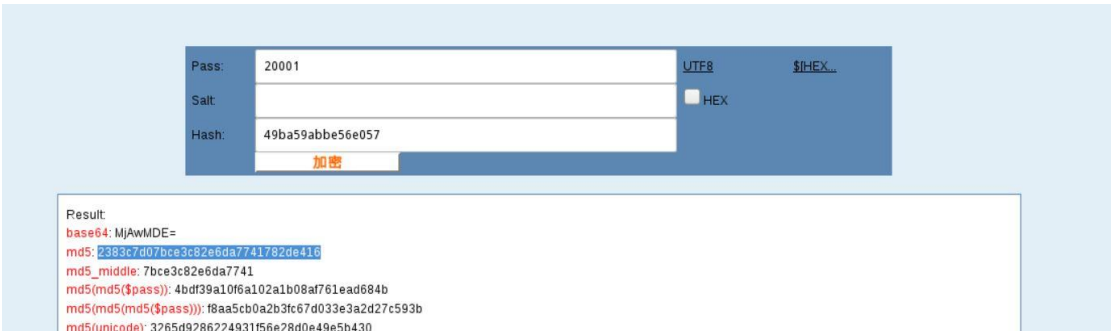
第三次是 9。



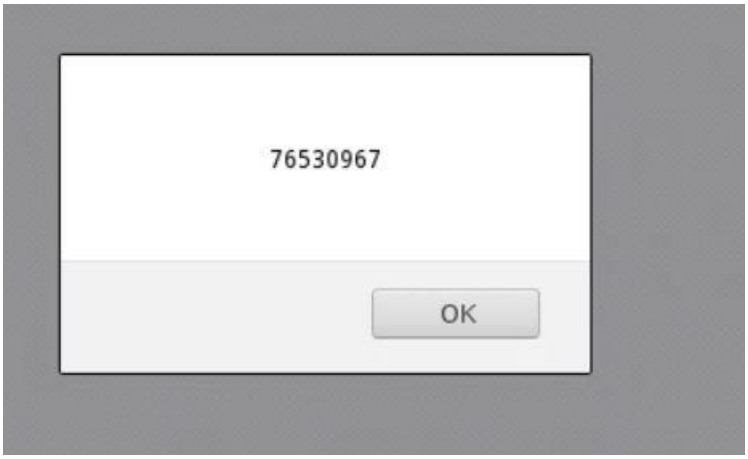
第四次是 11。



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:
20001
UTF8
$HEX...
Salt:
HEX
Hash:
49ba59abbe56e057
加密
Result:
base64: MjAwMDE=
md5: 2383c7d07bce3c82e6da7741782de416
md5_middle: 7bce3c82e6da7741
md5(md5($pass)): 4bdf39a10f6a102a1b08af761ead684b
md5(md5(md5($pass))): f8aa5cb0a2b3fc67d033e3a2d27c593b

最后得到 flag。


76530967
OK