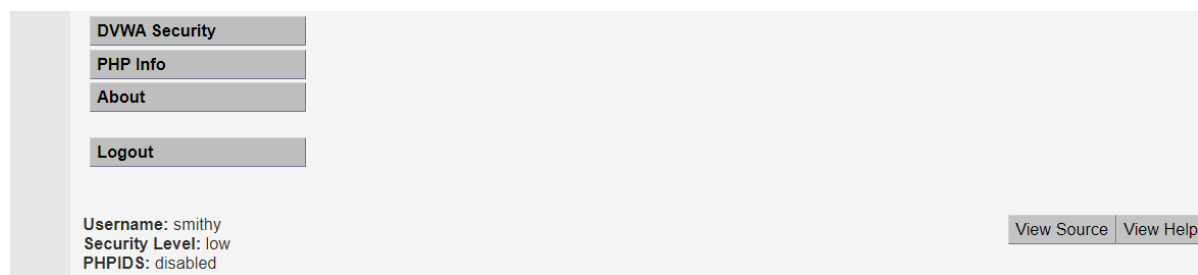


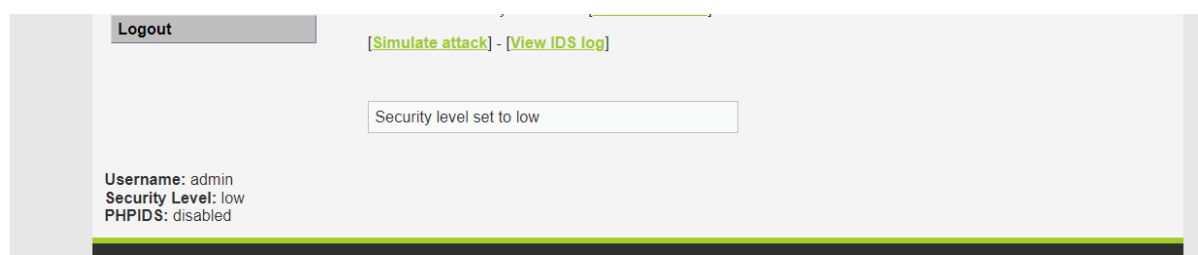
1.完成dvwa靶场中的csrf漏洞实验

登录smithy账号



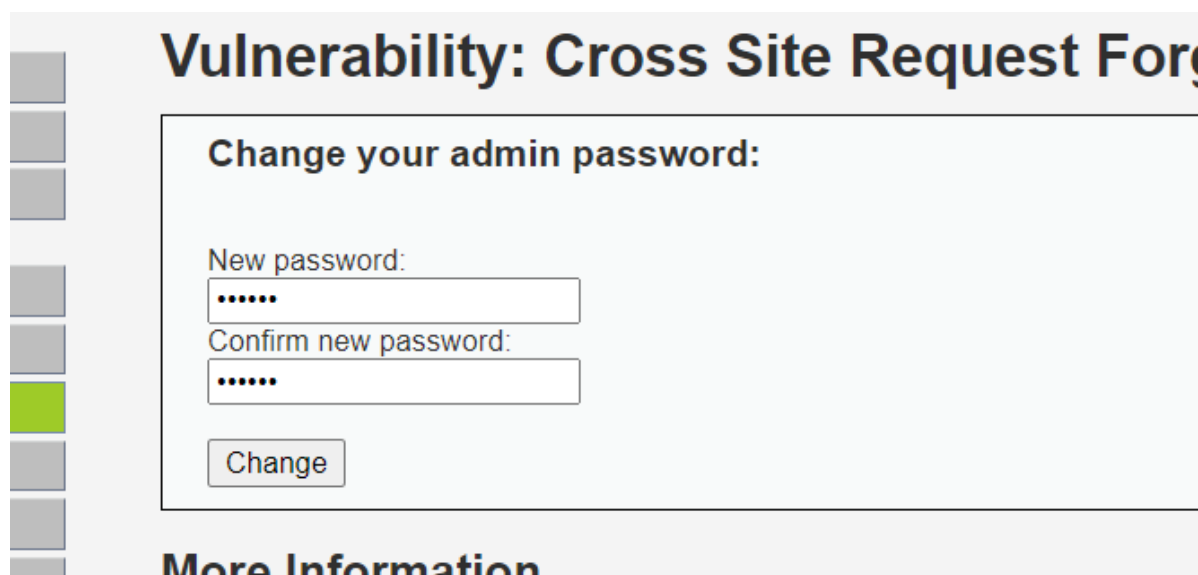
The image shows the 'DVWA Security' page. On the left, there are buttons for 'DVWA Security', 'PHP Info', 'About', and 'Logout'. Below these buttons, the user status is displayed: 'Username: smithy', 'Security Level: low', and 'PHPIDS: disabled'. On the right side, there are two buttons: 'View Source' and 'View Help'.

登录admin账户



The image shows the 'DVWA Security' page. At the top, there is a 'Logout' button. Below it, there are links for '[Simulate attack]' and '[View IDS log]'. A message box states 'Security level set to low'. At the bottom left, the user status is displayed: 'Username: admin', 'Security Level: low', and 'PHPIDS: disabled'.

修改smithy密码为123456



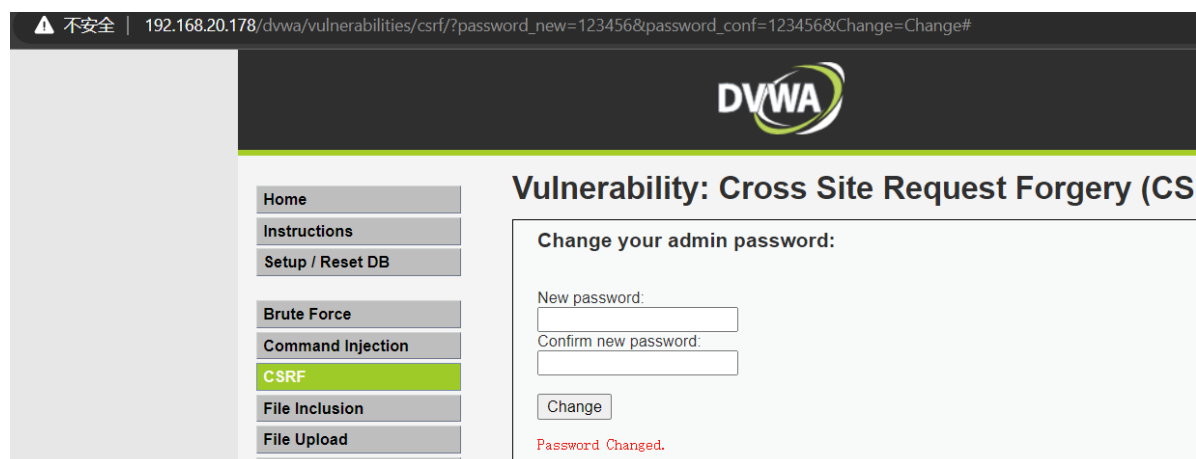
The image shows the 'Vulnerability: Cross Site Request Forgery' page. The main heading is 'Vulnerability: Cross Site Request Forgery'. Below it, there is a section titled 'Change your admin password:'. This section contains two input fields: 'New password:' and 'Confirm new password:'. Both fields are filled with six dots. Below these fields is a 'Change' button. At the bottom of the page, there is a section titled 'More Information'.

复制更改密码请求URL

```
1 http://192.168.20.178/dvwa/vulnerabilities/csrf/?  
password_new=123456&password_conf=123456&Change=Change#
```

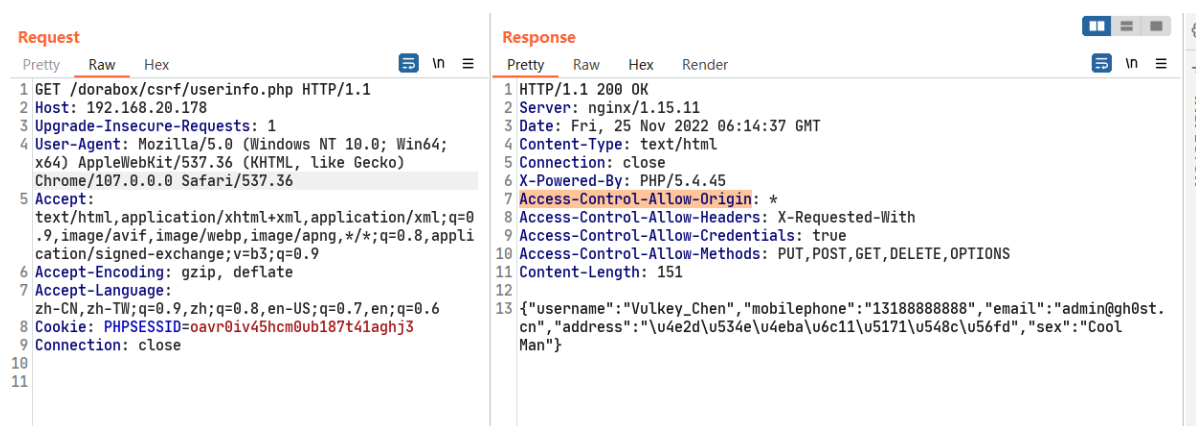
⚠ 不安全 | 192.168.20.178/dvwa/vulnerabilities/csrf/?password_new=123456&password_conf=123456&Change=Change#

在admin账户登录情况下请求该URL即可修改admin账户密码



2.完成dorabox靶场中的cors漏洞实验

用burp抓包请求CORS跨域资源读页面



可以看到

- Access-Control-Allow-Origin: *

Access-Control-Allow-Origin 响应标头指定了该响应的资源是否被允许与给定的源 ([origin](#)) 共享，* 表示允许任意来源的请求代码具有访问资源的权限，造成了一个跨域读取敏感信息的漏洞

- Access-Control-Allow-Credentials: true

Access-Control-Allow-Credentials 响应头用于在请求要求包含 credentials ([Request.credentials](#) 的值为) 时，告知浏览器是否可以将对请求的响应暴露给前端 JavaScript 代码，true 表示允许

编写利用代码并放入攻击者服务器

