实验吧 web渗透至后台登陆

原创

Chen_陈某人 于 2018-03-24 21:52:44 发布 3121 收藏

点开链接的源码可以发现密码是经过md5哈希加密的，所以先不考虑去破解密码，先看看有没有其他的提示可以看到php文件的名称并没有实际意义，于是就试了一下发现flag就是ffifdyop，所以说这道题完全是靠脑洞的。。。

http://ctf5.shiyanbar.com/web/houtai/ffifdyop.php

```
    <meta charset="UTF-8">
    <title>Document</title>
</head>
<body style="background-color: #999">
    <div style="position:relative;margin:0 auto;width:300px;height:200px;padding-top:100px;font-size:20px;">
    <form action="" method="post">
        <table>
            <tr>
                请用管理员密码进行登录~~
            </tr>
            <tr>
                <td>密码: </td><td><input type="text" name='password'></td>
            </tr>
            <tr>
                <td><input type="submit" name='submit' style="margin-left:30px;"></td>
            </tr>
        </table>
    </form>
    锟斤拷    </div>
    <!-- $password=$_POST['password'];
    $sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5($password,true)."'";
    $result=mysqli_query($link,$sql);
        if(mysqli_num_rows($result)>0){
            echo 'flag is :'.$flag;
        }
        else{
            echo '密码错误!';
        } -->
</body>
</html>

```