Web 安全作业一

Git 账号:zzr2867　学号：57118435　姓名：　赵泽瑞

1.实现 3 个主机配置，在/etc/hosts 文件中配置如下：

Open　*hosts　/etc

```
10.0.0.2 web.cybersecurity.seu.edu
10.0.0.3 grade.cybersecurity.seu.edu
10.0.0.4 attacker.cybersecurity.seu.edu

10.0.0.2 web.cybersecurity.seu.edu
10.0.0.3 time.cybersecurity.seu.edu
10.0.0.4 jsonp.cybersecurity.seu.edu
```

2.在 time.cybersecurity.seu.edu （10.0.0.3）上实现三个接口：/api/data，/api/datecors，/api/jsondate，host2 文件夹中 server.js 的代码：

Open　server.js　~/Desktop/homework1/host2

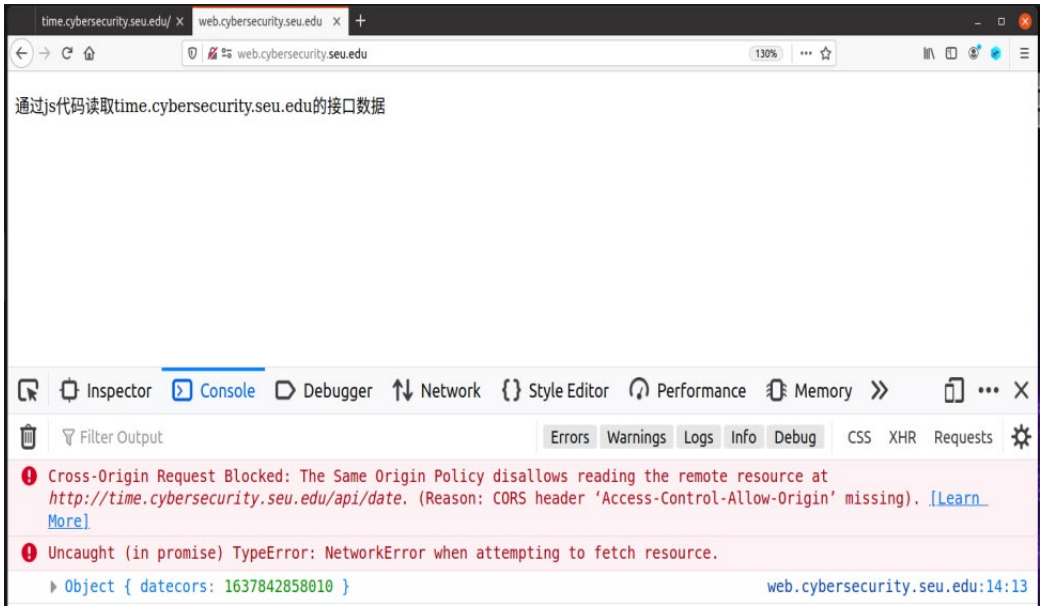
```
1 const express = require('express')
2 const { createReadStream } = require('fs')
3 const bodyParser = require('body-parser')
4 const app = express()
5 app.use(bodyParser.urlencoded({ extended: false }))
6 app.listen(80)
7 app.get('/', (req, res) => {
8 createReadStream('index.html').pipe(res)
9 })
10 app.get('/api/date', (req, res) => {
11 res.send({ date: Date.now() })
12 })
13 app.get('/api/datecors', (req, res) => {
14 res.set('Access-Control-Allow-Origin', 'http://web.cybersecurity.seu.edu')
15 res.send({ datecors: Date.now() })
16 })
17 app.get('/api/jsondate', (req, res) => {
18 let callback = req.query.callback;
19 let Str = `${callback}(${JSON.stringify({ datejson: Date.now() })
20 })`;
21 res.send(Str);
22 })
23
```

3.在web.cybersecurity.seu.edu（10.0.0.2）实现页面，页面通过js代码读取time.cybersecurity.seu.edu（10.0.0.3）的接口的数据，host1文件的index.html代码：

Open server.js ~/Desktop/homework1/host2

```
1 const express = require('express')
2 const { createReadStream } = require('fs')
3 const bodyParser = require('body-parser')
4 const app = express()
5 app.use(bodyParser.urlencoded({ extended: false }))
6 app.listen(80)
7 app.get('/', (req, res) => {
8 createReadStream('index.html').pipe(res)
9 })
10 app.get('/api/date', (req, res) => {
11   res.send({ date: Date.now() })
12 })
13 app.get('/api/datecors', (req, res) => {
14   res.set('Access-Control-Allow-Origin', 'http://web.cybersecurity.seu.edu')
15   res.send({ datecors: Date.now() })
16 })
17 app.get('/api/jsondate', (req, res) => {
18   let callback = req.query.callback;
19   let Str = `${callback}(${JSON.stringify({ datejson: Date.now() })})`;
20   res.send(Str);
21 })
22
```

4. 在web.cybersecurity.seu.edu页面读取time.cybersecurity.seu.edu的接口，可以看到：



因为在host2：server.js设置了CORS头，可以读取到/api/datecors的接口数据，而无法读取到/api/date的数据，并且在控制台看到“同源请求被阻止：同源策略不允许读取http://time.cybersecurity.seu.edu/api/date的远程资源，原因：cors头缺失”。

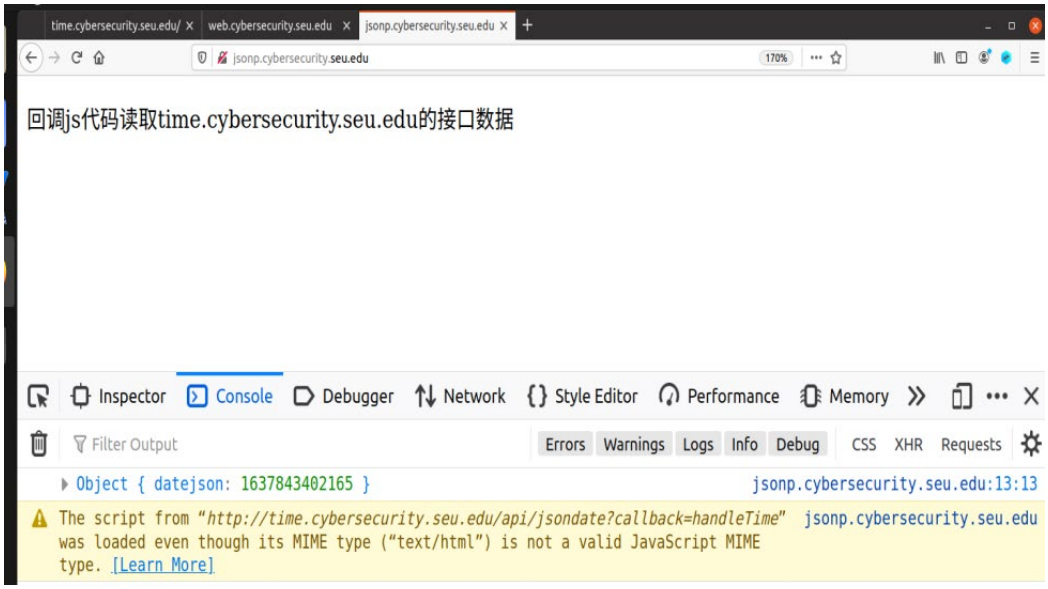
5.在jsonp.cybersecurity.seu.edu（10.0.0.4）下实现页面，通过回调js代码读取time.cybersecurity.seu.edu网页接口的数据，host3文件夹index.html代码：

```
<<!DOCTYPE html>
<html>

<head>
<meta charset="utf-8">
<title>jsonp.cybersecurity.seu.edu</title>
</head>

<body>
<p>回调js代码读取time.cybersecurity.seu.edu的接口数据</p>
<script>
function handleTime(data) {
    console.log(data)
}
</script>
<script src='http://time.cybersecurity.seu.edu/api/jsondate?callback=handleTime'></script>
</body>
</html>
```

6. .在jsonp.cybersecurity.seu.edu下回调js代码成功读取time.cybersecurity.seu.edu接口数据:



成功读取到/api/jsonpdate的数据。