Web Security report ---- assignment 1

57118423 宋昌霖

1.Environment

配置hosts文件

```
sudo gedit /etc/hosts
```

Host Name	IP Address	Domain Name
host1	10.0.0.2	http://web.cybersecurity.seu.edu
host2	10.0.0.3	http://time.cybersecurity.seu.edu
host3	10.0.0.4	http://jsonp.cybersecurity.seu.edu

2.在http://time.cybersecurity.seu.edu上实现三个接口

功能如下：

Path	Utility
/api/date	返回形式{date: Date.now()}的JSON数据
/api/datecors	返回形式{date: Date.now()}的JSON数据，并设置CORS头部字段
/api/jsonpdate	返回形式JSONP数据

```
const express = require('express')
const { createReadStream } = require('fs')
const bodyParser = require('body-parser')
const app = express()

app.use(bodyParser.urlencoded({ extended: false }))
app.listen(80)
app.get('/', (req, res) => {
    createReadStream('index.html').pipe(res)
    })

app.get('/api/date', (req, res) => {
 res.send({ date: Date.now() })
})

app.get('/api/datecors', (req, res) => {
 res.set('Access-Control-Allow-Origin', '*')
 res.send({ date: Date.now() })
})

app.get('/api/jsonpdate', (req, res) => {
 res.jsonp({ date: Date.now() })
```

```
})
```

3.web.cybersecurity.seu.edu

在 web.cybersecuiry.seu.edu 下实现一个页面，在页面中通过 js 代码读取 time.cybersecurity.seu.edu 的接口数据，分别测试在 time.cybersecurity.seu.edu 中设置和未设置 CORS 头的情况下，web.cybersecuiry.seu.edu 读取接口数据的情况，提供读取成功和未读取成功模式下的截图

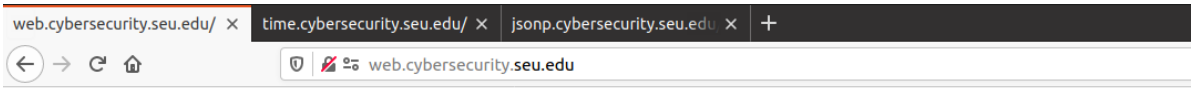
html文件如下：

```
<html>
<body>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<h4>web.cybersecurity.seu.edu</h4>
<div id="date">/api/date : </div>
<div id="datecors">/api/datecors : </div>
<script type="text/javascript">
    const divdatecors = document.querySelector('#datecors')
    const rescors =
fetch('http://time.cybersecurity.seu.edu/api/datecors').then(res =>
res.json()).then(data => {
            divdatecors.textContent = '/api/datecors : ' + data.date
        }
    )
    const divdate = document.querySelector('#date')
    const resdate = fetch('http://time.cybersecurity.seu.edu/api/date').then(res
=> res.json()).then(data => {
            divdate.textContent = '/api/date : ' + data.date
        }
    )
</script>
</body>
```

js文件如下：

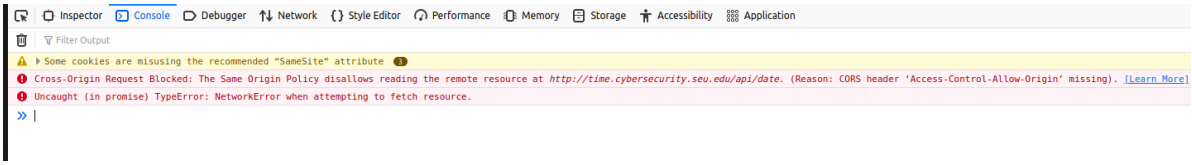
```
const express = require('express')
const { createReadStream } = require('fs')
const bodyParser = require('body-parser')
const app = express()

app.use(bodyParser.urlencoded({ extended: false }))
app.listen(80)
app.get('/', (req, res) => {
    createReadStream('index.html').pipe(res)
    })
```

访问web.cybersecurity.seu.edu



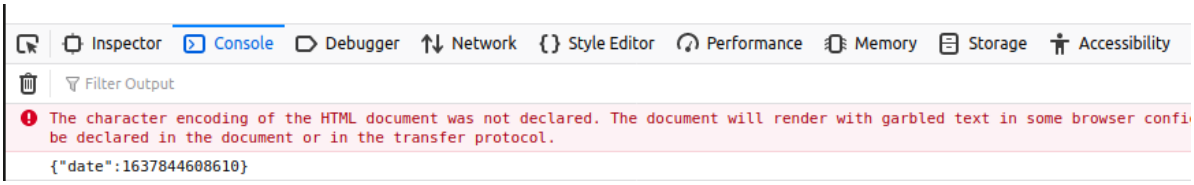
web.cybersecurity.seu.edu

/api/date :
/api/datecors : 1637843275964



未设置CORS头部的时候浏览器提示不符合同源策略

设置CORS头部后：获取到数据



4.jsonp实现页面

在未设置CORS头部，读取接口成功获得数据：