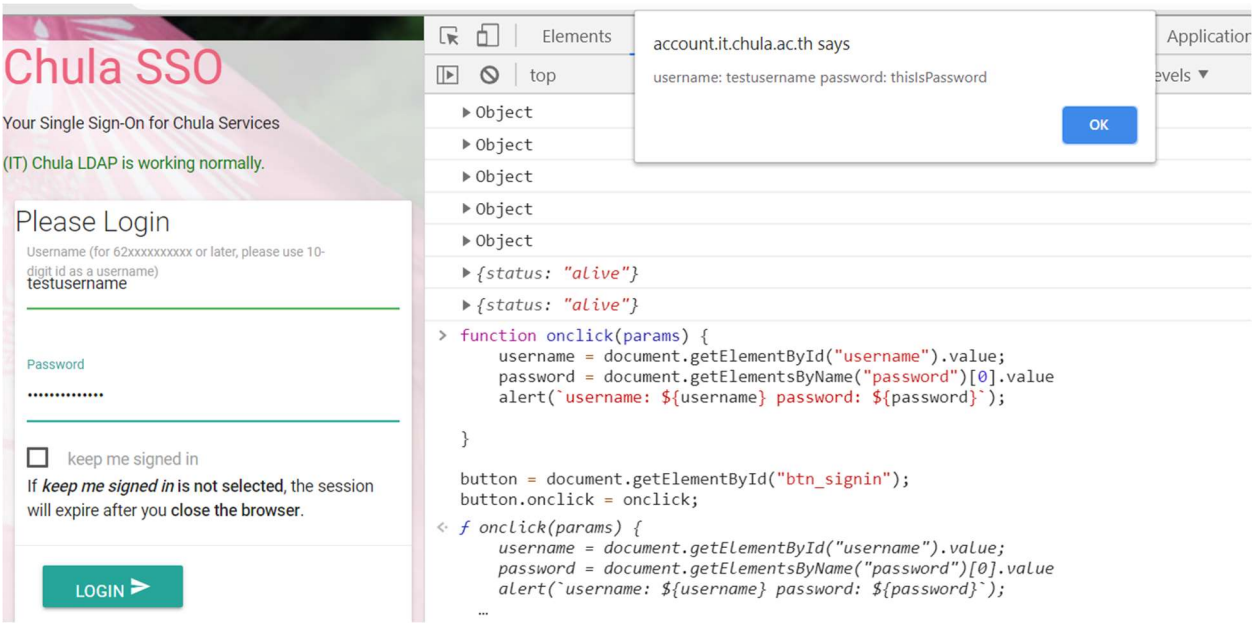
1. Inject to browser console
   With following code

```
function onclick(params) {
    username = document.getElementById("username").value;
    password = document.getElementsByName("password")[0].value
    alert(`username: ${username} password: ${password}`);

}

button = document.getElementById("btn_signin");
button.onclick = onclick;
```

   The result

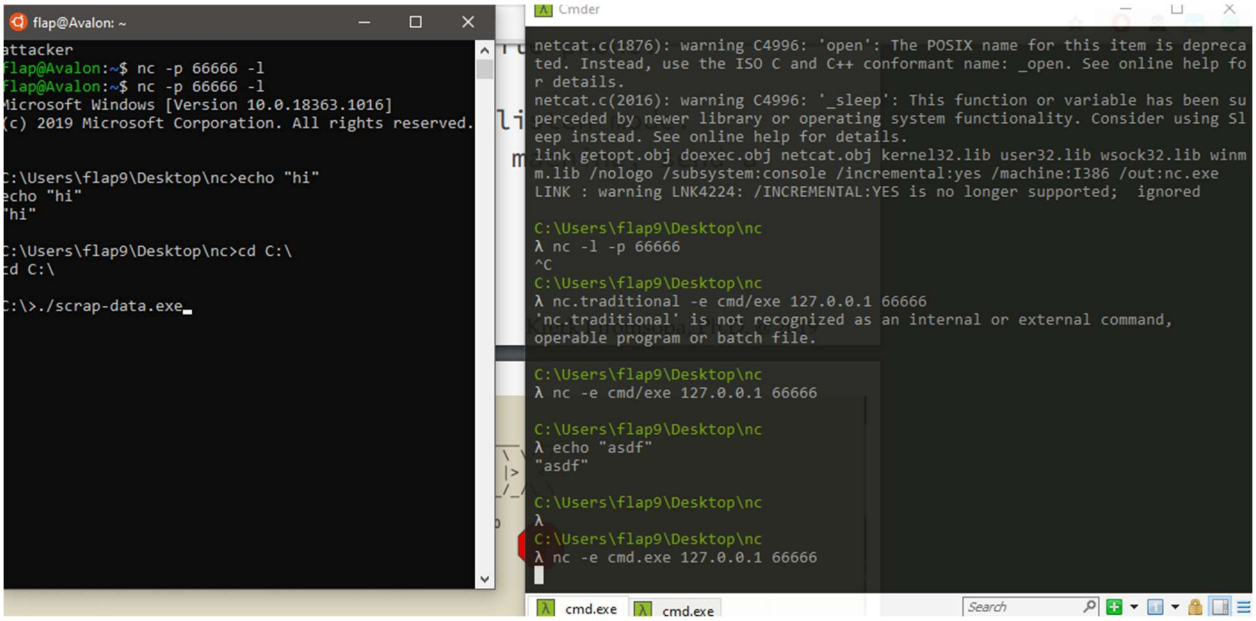


2. I'm using wsl attack to window cmd due to physical limitation

   - fix makefile on netcat which is broken (tab/space problem)

   - run visual studio developer env to build nc

   - on wsl apt-get netcat-traditional



3.

Worse case

- ในกรณีร้าน Internet café คือโดน js injection เก็บบัญชี social media ที่ไม่มี 2 factor authentication
- ในกรณีเครื่องส่วนตัวของผมคือ Attacker run script เก็บ personal data ไปทั้งหมด + เปิดโพรงให้มา monitor ระบบ เก็บ data เพิ่ม, run-script เก็บข้อมูล browser เพิ่มได้อีก, เปิดกล้องโดยที่เรามีรู้ตัว

วิธีป้องกัน

- อย่าใช้ internet café
- ใช้ account proxy ส่งไฟล์ (account ปลอมที่คอบเปลี่ยนพาสเวิดตลอด ให้ account หลักส่งไฟล์ที่จำทำงานมาให้อีกทีหนึ่ง), refresh browser
- อย่าให้ใครใช้คอมเรานาน คอยดูตลอด
- Check startup process, schedule task ใน window ที่แปลกๆ, service ที่แปลกๆ