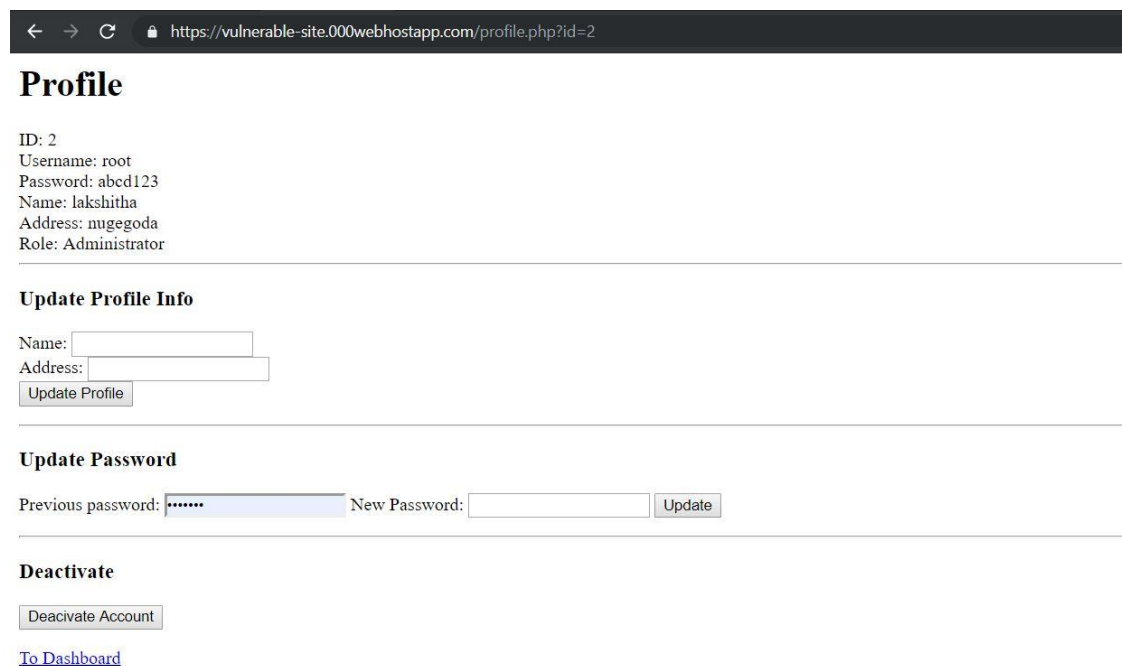


## 1. Session Hijacking

During a session hijacking, a malicious hacker places himself in between the computer and the website's server engaged in an active session. The malicious hacker actively monitors everything that happens on account, and can take control of it.

The biggest advantage of a session hijacking is that the malicious attacker can enter the server and access its information without having to hack a registered account. In addition, he can also make modifications on the server to help him hack it in the future or to simplify a data-stealing operation.



The screenshot shows a web browser window with the address bar displaying `https://vulnerable-site.000webhostapp.com/profile.php?id=2`. The page title is "Profile". The profile information is listed as follows:

- ID: 2
- Username: root
- Password: abed123
- Name: lakshitha
- Address: nugegoda
- Role: Administrator

---

**Update Profile Info**

Name:

Address:

---

**Update Password**

Previous password:  New Password:

---

**Deactivate**

[To Dashboard](#)

## 2. DOM XSS

This happens when the DOM environment was changed, but the client-side code does not change. The client-side code executes differently when the DOM environment is being modified in the victim's browser.

← → ↻ https://vulnerable-site.000webhostapp.com/profile.php?default=<script>alert(document.cookie)</script>

## Profile

Notice: Undefined index: id in /storage/ssd5/016/9878016/public\_html/profile.php on line 30

### Update Profile Info

Name:   
Address:

### Update Password

Previous password:  New Password:

### Deactivate

## 3. SQL injection

SQL injection is a type of web application security vulnerability in which an attacker attempts to use application code to access or corrupt database content. If successful, this allows the attacker to create, read, update, alter, or delete data stored in the back-end database.

← → ↻ https://vulnerable-site.000webhostapp.com

### Log-in

Username:   
Password:

[Contact Us](#)