

## WRITE UPS CTF #2

CTF.INFOSECINSTITUTE.COM

Nama : -McMillan

Team : iL7Team, Sulawesi I.T Security, & Medan Cyber Security

### 1.1 LEVEL 07

### 1.2 Vulnerability: A2 Broken Authentication and Session Management

### 1.3 Screenshot soal :


Hello, John Doe.

| Name     | Age | Nationality |
|----------|-----|-------------|
| John Doe | 84  | Indian      |

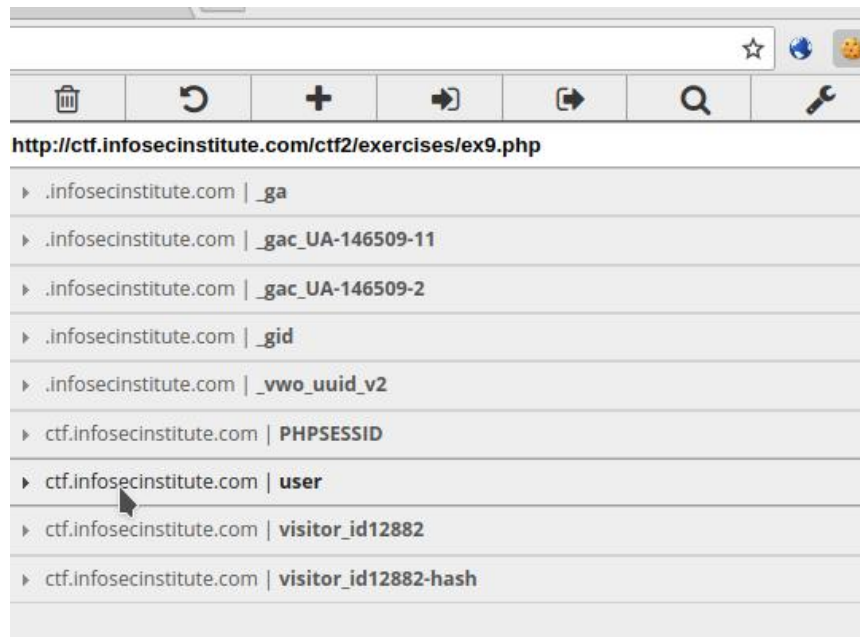
It seems you were automatically logged in as John Doe. Try to find a way to be logged in as the user Mary Jane in order to see her profile.

**Deskripsi soal :** Sepertinya Anda secara otomatis masuk sebagai John Doe. Coba cari cara untuk masuk sebagai pengguna Mary Jane agar dapat melihat profilnya.

**Write-up :**

 Get a Hint

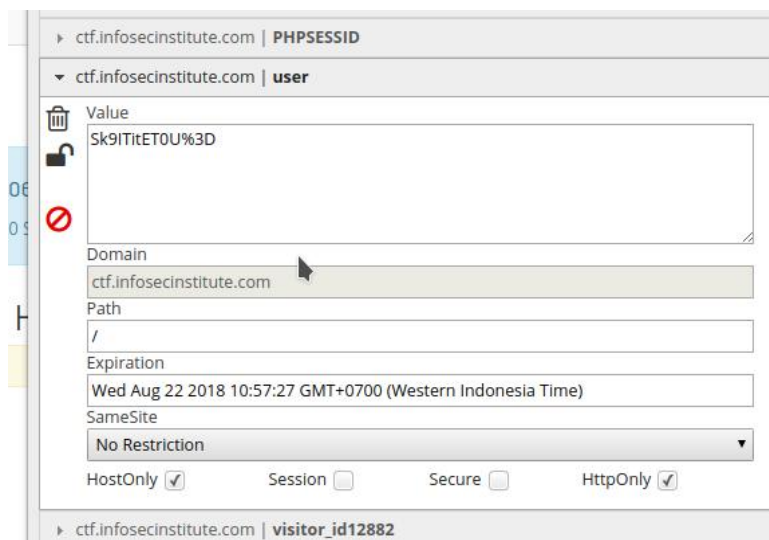
You must do something with a cookie.  
You need to modify the user cookie  
No more hints available!  
No more hints available!



Jika kita lihat ada cookie dengan nama *user* dengan *value* dengan akhiran

unicode %3D adalah =

*Ref : <http://www.greentea.markschwing1.com/unico.html>*



Jika kita ketahui jenis encode dengan akhiran = adalah *base32*, *base64*. dan saya rasa ini adalah jenis encode *base64*.

```
In [1]: import base64

In [2]: base64.b64decode('Sk9ITitET0U=')
Out[2]: 'JOHN+DOE'

In [3]: _
```

JOHN+DOE ... ?

Berarti kita hanya memasang cookie dengan nama kita yang di encode dengan base64

lalu kita set cookie.

```
In [2]: base64.b64decode('Sk9ITitET0U=')
Out[2]: 'JOHN+DOE'

In [3]: base64.b64encode('Adeputra')
Out[3]: 'QWRlcHV0cmE='

In [4]: _
```

The screenshot shows a web browser's cookie editor interface. The domain is set to 'ctf.infosecinstitute.com' and the path is '/'. The cookie name is 'user' and its value is 'QWRlcHV0cmE=' (which is the base64 encoding of 'Adeputra'). The expiration date is 'Wed Aug 22 2018 10:57:27 GMT+0700 (Western Indonesia Time)'. The 'SameSite' attribute is set to 'No Restriction'. The 'HostOnly' checkbox is checked, and the 'HttpOnly' checkbox is also checked. A green checkmark is visible at the bottom of the interface, indicating that the cookie has been successfully set.

Jika sudah tekan tombol centang dibawah.

Hello, Adeputra.

| Name    | Age     | Nationality |
|---------|---------|-------------|
| Unknown | Unknown | Unknown     |

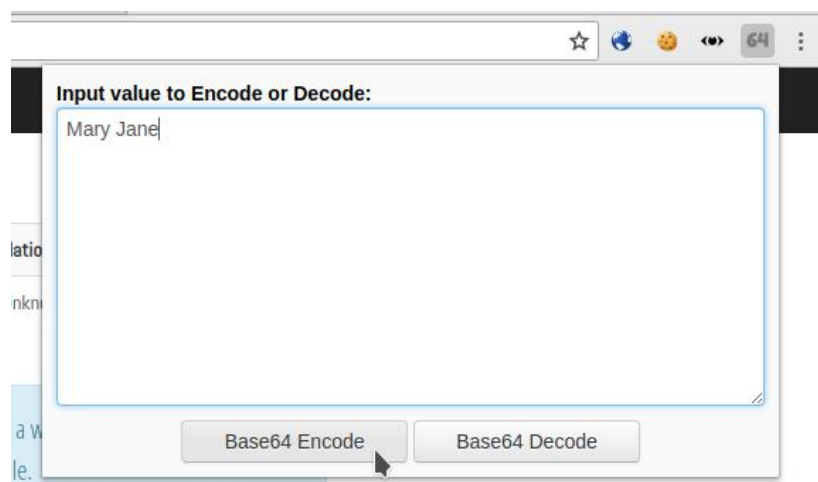
Dan kita sudah berhasil masuk sebagai adeputra. tapi kenapa level ini tidak sukses.

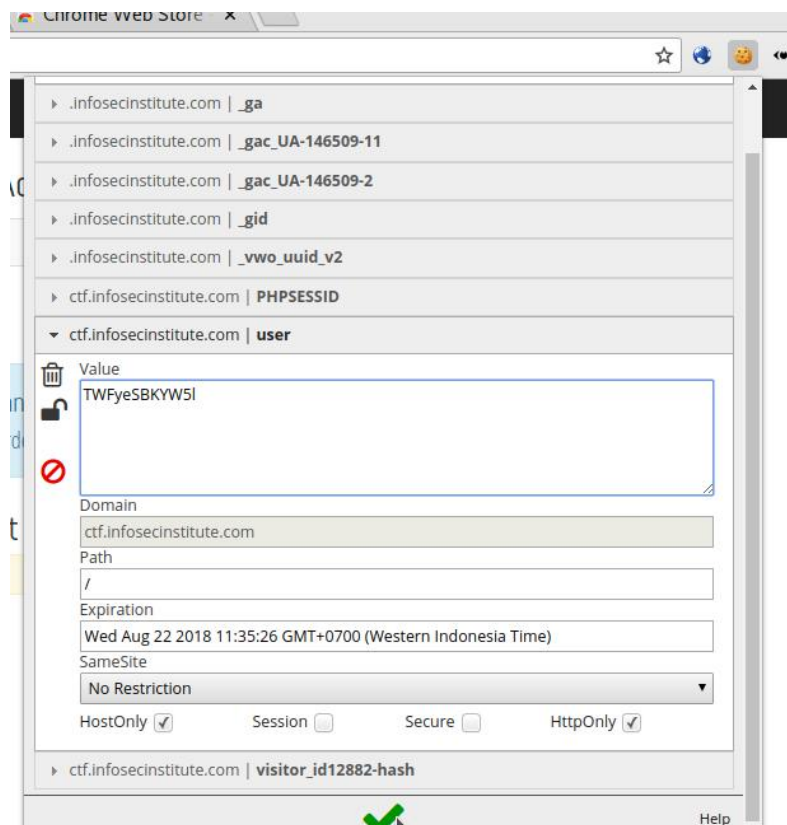
Tentu saja, mari kita lihat lagi soalnya

It seems you were automatically logged in as **John Doe**. Try to find a way to be logged in as the user **Mary Jane** in order to see her profile.

Kita diharuskan masuk sebagai Mary Jane bukan Adeputra.

Oke sekarang mari kita coba ulang.





Jika sudah di set, coba di refresh page nya.


---

Hello, Mary Jane.

| Name      | Age | Nationality |
|-----------|-----|-------------|
| Mary Jane | 18  | American    |

It seems you were automatically logged in as John Doe. Try to find a way to be logged in as the user Mary Jane in order to see her profile.

Oh yeah, you actually made it! You know the drill.

 Get a Hint