qSEAp

pioneering innovation...

Hacking JSON Web Token

None Algorithm Attack

The Structure of JSON Web Token

- Header
- Payload
- Signature

```
{
"alg": "HS256",
"typ": "JWT"
}
```

JSON is Base64Url encoded to form the first part of the JWT

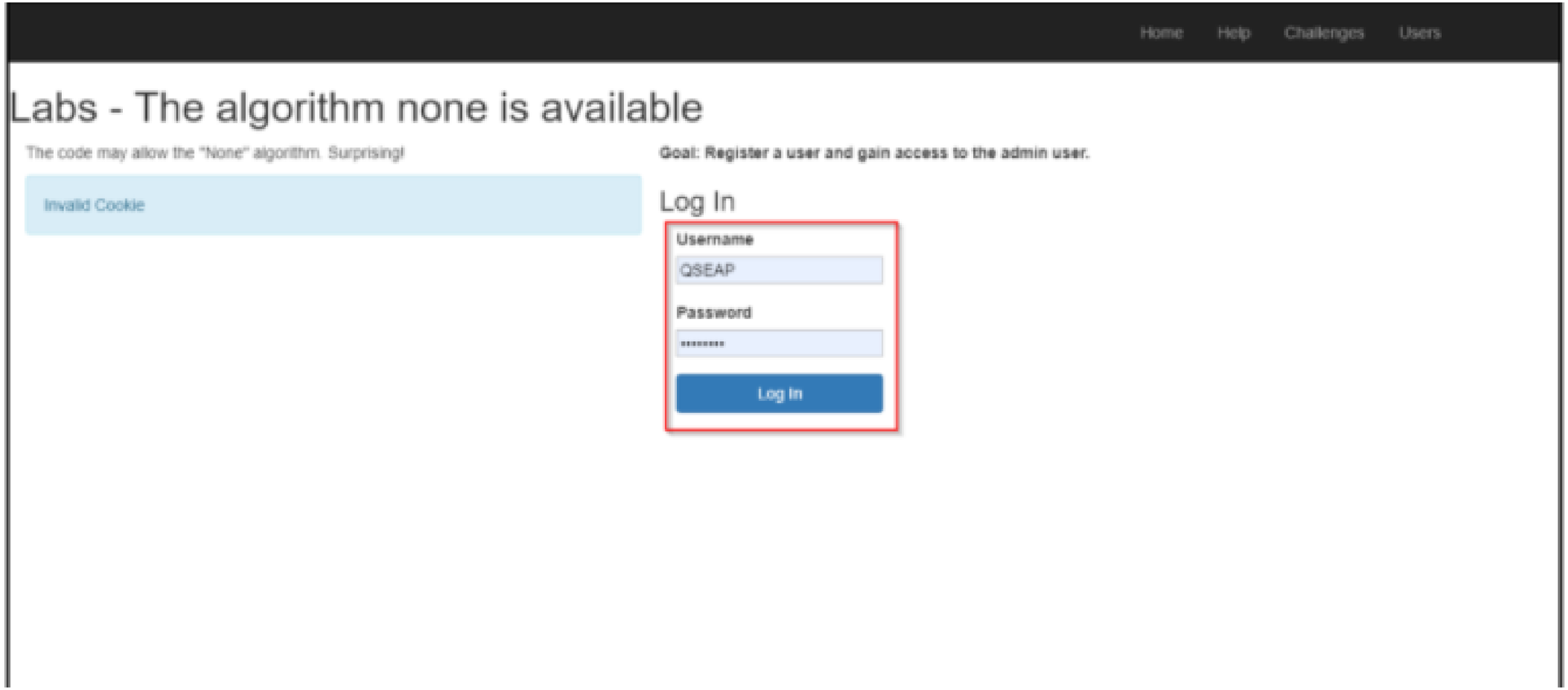
```
{
 "name": "Saajan D",

 "admin": true
}
```

Payload is Base64Url encoded to form the second part of JWT

```
HMACSHA256(
 base64UrlEncode(header) + "." +
 base64UrlEncode(payload),
 secret)
```

The signature is used to verify the message wasn't tampered, that the integrity is maintained and it also verifies the sender of JWT token in case if it is signed with the private key.

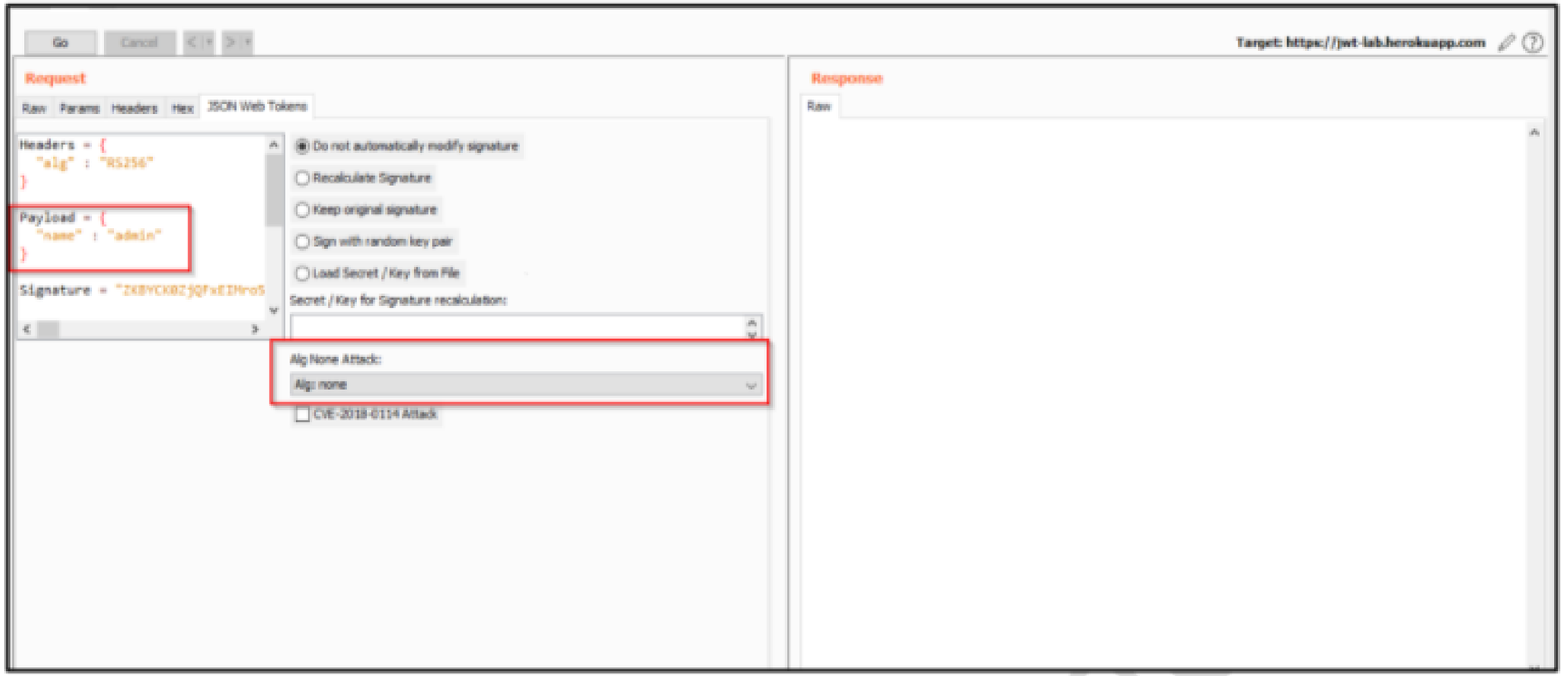


Step 1: Log in with the credentials and capture the request in proxy tool.

Step 2: Observe the highlighted JWT. Take the below request in the repeater

Step 3: manually decode the JWT header and payload with the help of the decoder.

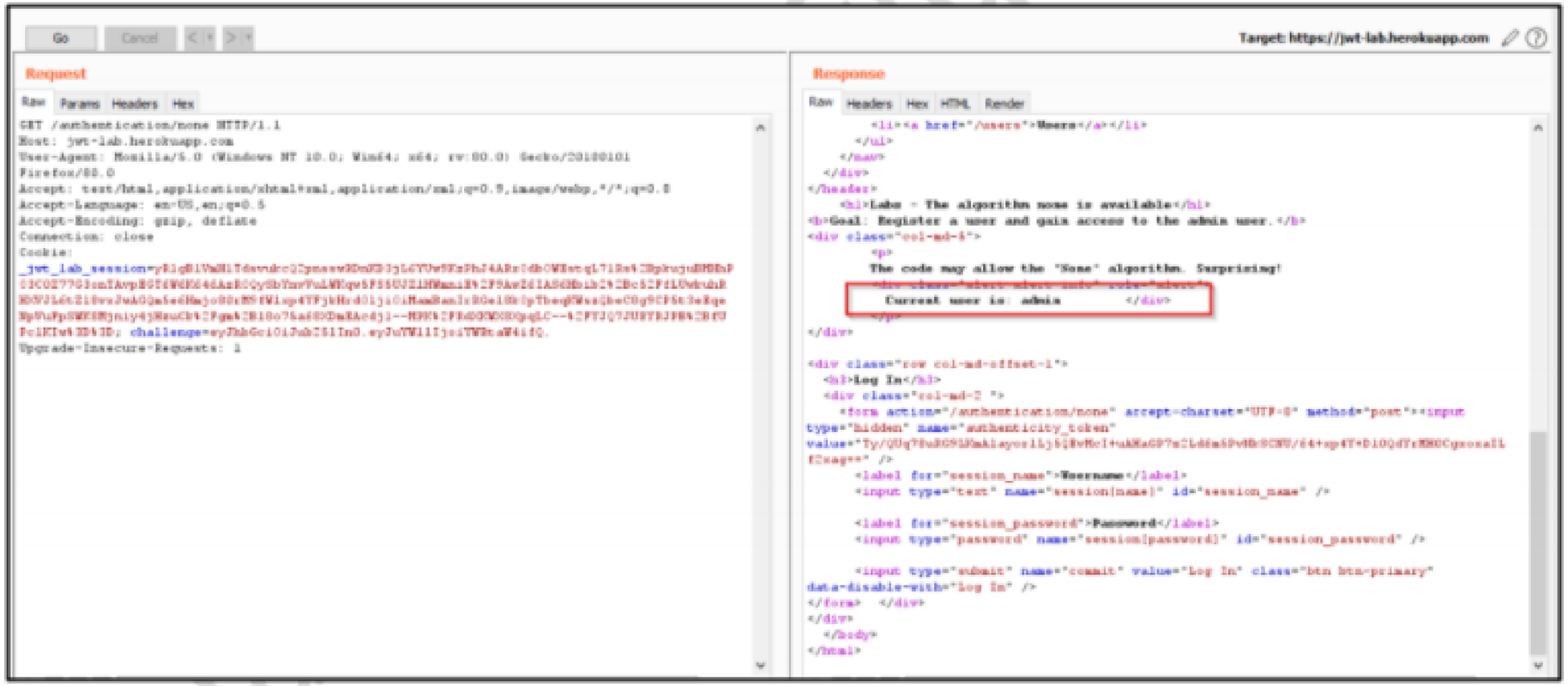
Else, you can also use JWT Burp extension



Step 4: Change the name from user “qseap” to “admin” and set the algorithm as “None” in JWT Burp extension. Forward the request in the repeater

qSEAp

pioneering innovation...



Step 5: BOOOOM!! We are now logged in as “admin”. Account takeover successful.

qSEAp
pioneering innovation...

Originally used for debugging purposes, if not turned off in a production environment, it would allow attackers to forge any token they want by setting the alg field to “none”.

They can then impersonate anyone on the site by using the forged tokens!

To have a thorough check on such vulnerabilities in your system, reach out to us.

Request Demo