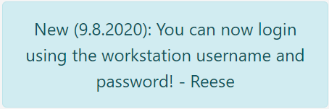
Phonebook – Challenge

As we start we see clue:

Reconciliation of the web page:

We can use get queries and the results will output in innerHTML of the return page.

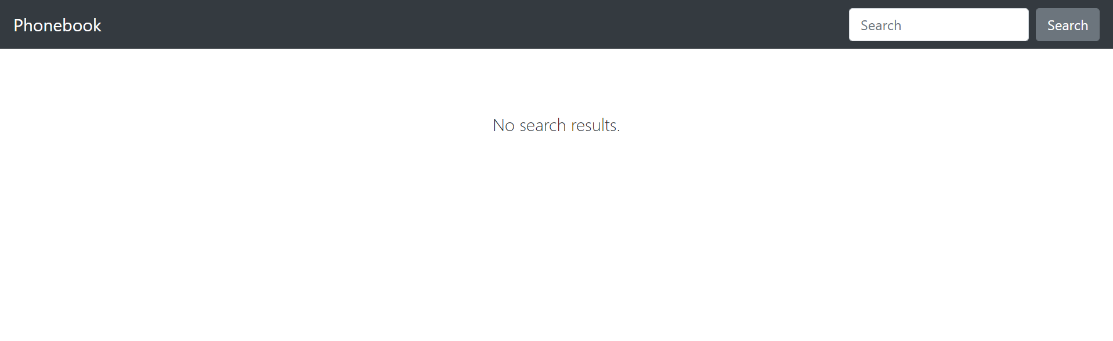
Lead us to HTML injection.

We tried successfully XSS from XSS dictionary payload: <https://github.com/payloadbox/xss-payload-list>

But unfortunately it's not lead us to nothing.

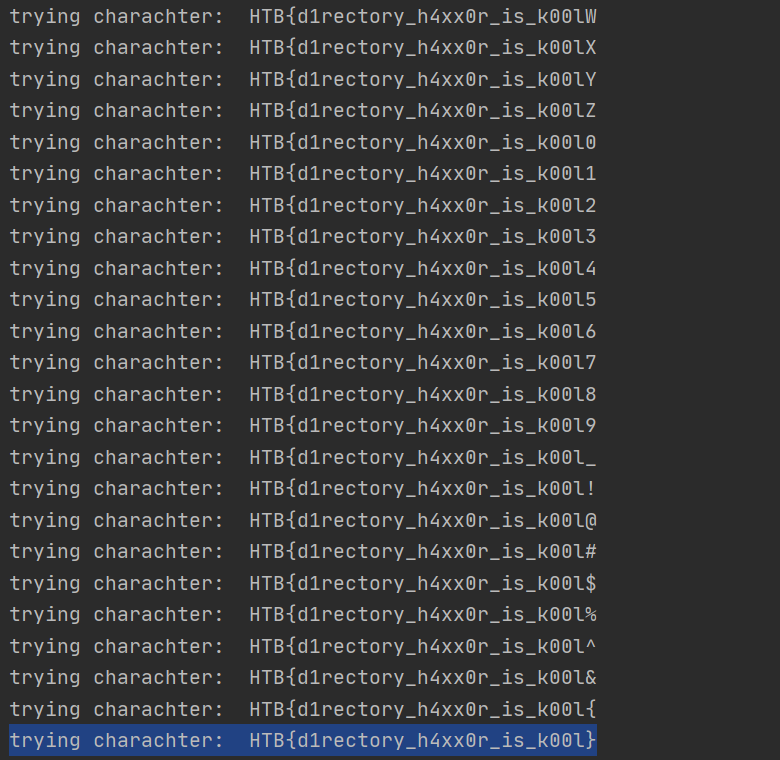
We consider again the first clue and it's lead us to think about LDAP injection.

We enter username:\* , password:\* and we passed to Phonebook:



There we can see actually the phone book se we first thought about Reese member or admin member but there is nothing there.

Eventually we got an idea to build the password of some member there, suppose that is "Reese" as username and build the password with the property of LDAP injection '\*'.

Flag: HTB{d1rectory\_h4xx0r\_is\_k00l}