

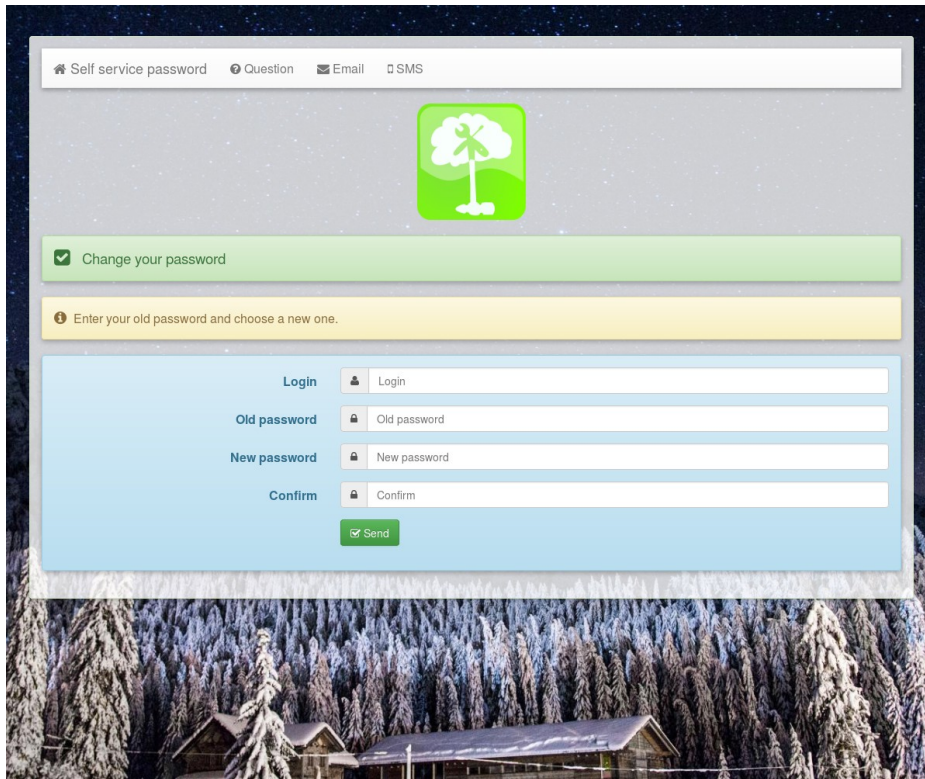
Pass the SALT 2018

**Warning: this can destroy my
reputation**

Clément OUDOT



Self Service Password



The screenshot shows a web interface for password management. At the top, there is a navigation bar with links for 'Self service password', 'Question', 'Email', and 'SMS'. Below this is a green tree icon. A green bar indicates 'Change your password' is selected. A yellow bar contains the instruction 'Enter your old password and choose a new one.' The main form area has a light blue background and contains the following fields: 'Login' (with a user icon), 'Old password', 'New password', and 'Confirm' (each with a lock icon). A green 'Send' button is located at the bottom of the form. The background of the page features a winter forest scene with snow-covered trees and a wooden cabin.

- Web interface to modify password
- LDAP directory (OpenLDAP, 389DS, Active Directory...)
- Reset by mail, SMS or questions
- Change SSH key

CVE-2018-12421

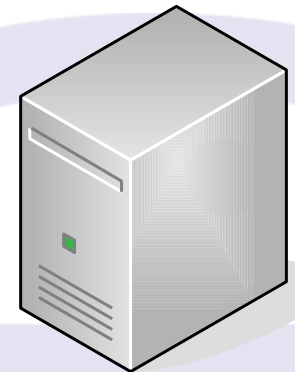
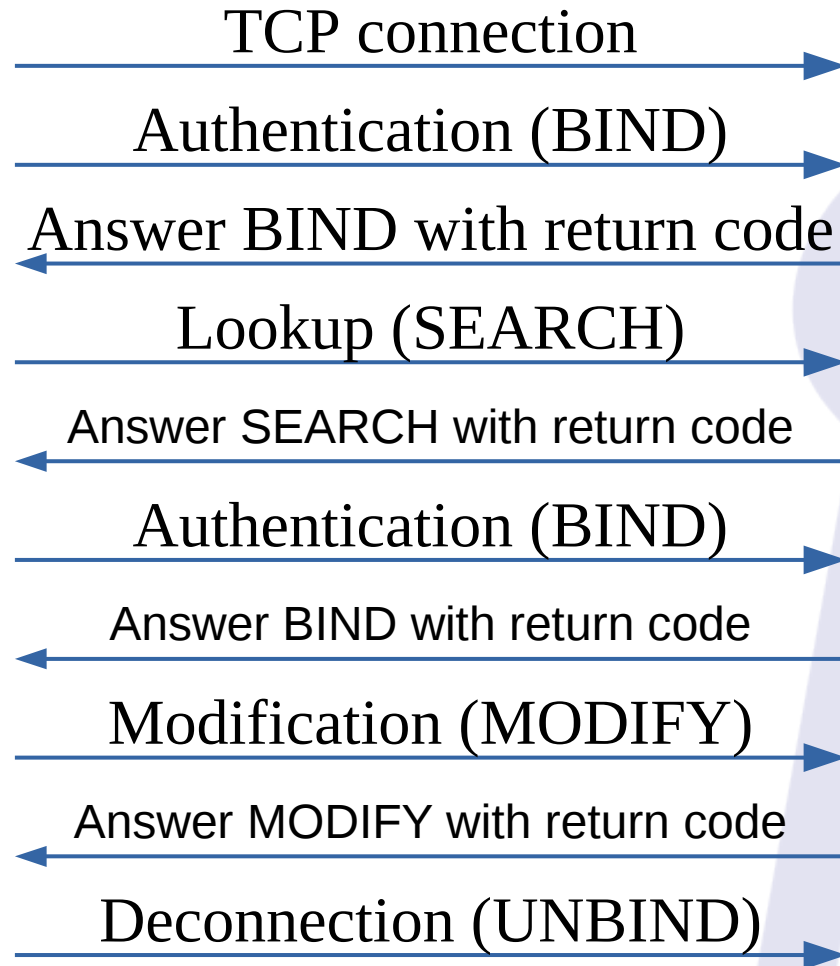
LTB (aka LDAP Tool Box) Self Service Password before 1.3 allows a change to a user password (without knowing the old password) via a crafted POST request, because the ldap_bind return value is mishandled and the PHP data type is not constrained to be a string.



LDAP connection



LDAP client



LDAP server

Faulty code

```
$bind = ldap_bind($ldap, $userdn, $oldpassword);  
$errno = ldap_errno($ldap);  
if ( $errno ) {  
    $result = "badcredentials";  
    error_log("LDAP - Bind user error $errno  
(".ldap_error($ldap).")");  
} else {  
    # Code for valid credentials  
}
```



Fixed code

```
$bind = ldap_bind($ldap, $userdn, $oldpassword);  
if ( !$bind ) {  
    $result = "badcredentials";  
    $errno = ldap_errno($ldap);  
    if ( $errno ) {  
        error_log("LDAP - Bind user error $errno  
        (".ldap_error($ldap).")");  
    }  
} else {  
    # Code for valid credentials  
}
```

