

Forum:[Hack Forums](#)

Thread: [Hacking into wifi router](#)

Dusk42 - October 6, 2019, 8:27 am

Hey everyone!

Recently I moved into a new apartment and one night my neighbour knocked on my door asking for my wifi password. Being the idiot that I am I gave it to him, but now I regret it and want to change it. However I can't access my router because the default password has been changed and possibly the username as well. I'm renting the place and the router was already setup when I got here. I need to change this password. It's been driving me insane and I've tried lots of things to make it work.

So I decided to pull the http request and got some code from the router with which it checks if the password is correct. I can't find a way to use this to my advantage however.

The router doesn't use the usual browser login request but has it's own fields setup for input so I don't know if I could make a brute force attack. My knowledge of hacking is minimal. Could someone please help me out?

Here's the function with which the router checks for the password validity I managed to find

```
function LoginClick(loginUsername, loginPassword, hiddenUsername, hiddenPassword)
{
    var usernameStr;
    var passwordStr;
    if (null == loginUsername || 0 == loginUsername.value.length)
    {
        alert ("Please input a username");
        key_flag = 0;
        return false;
    }
    if (null == loginPassword || 0 == loginPassword.value.length)
    {
        alert ("Please input a password");
        key_flag = 0;
        return false;
    }
    usernameStr = passwordMD5(loginUsername.value);
    passwordStr = passwordMD5(loginPassword.value);
    hiddenUsername.value = usernameStr;
    hiddenPassword.value = passwordStr;
    loginPassword.value = "Ha2S+eOKqmzA6nrlmTeh7w==";
    return true;
}
```

This second to last line seems interesting as it has a proper value but it seems to be encrypted. The passwordMD5 function connects to a function called "calcMD5" which I guess encrypts the entered

username and password before checking them?

If there is a way for me to get into this router that would be great. I'm worried that I'm at risk of being hacked myself because I gave away the wifi password. Please help!

EDIT : The router is a ZTE ZXV10 W300

EDIT 2 : I just tried factory resetting it.... The router doesn't want to factory reset. It resets but all settings seemingly stay the same. I really need to hack into it. Apparently this router has something called a rom-0 vulnerability? How can I make use of that?

KidFlippaCudi - October 7, 2019, 5:54 am

(Oct 6, 2019 08:27 AM)Dusk42 Wrote: [\[CITE\]](#) Hey everyone!

Recently I moved into a new apartment and one night my neighbour knocked on my door asking for my wifi password. Being the idiot that I am I gave it to him, but now I regret it and want to change it. However I can't access my router because the default password has been changed and possibly the username as well. I'm renting the place and the router was already setup when I got here. I need to change this password. It's been driving me insane and I've tried lots of things to make it work.

So I decided to pull the http request and got some code from the router with which it checks if the password is correct. I can't find a way to use this to my advantage however.

The router doesn't use the usual browser login request but has it's own fields setup for input so I don't know if I could make a brute force attack. My knowledge of hacking is minimal. Could someone please help me out?

Here's the function with which the router checks for the password validity I managed to find

```
function LoginClick(loginUsername, loginPassword, hiddenUsername, hiddenPassword)
{
var usernameStr;
var passwordStr;
if (null == loginUsername || 0 == loginUsername.value.length)
{
alert ("Please input a username");
key_flag = 0;
return false;
}
if (null == loginPassword || 0 == loginPassword.value.length)
{
alert ("Please input a password");
key_flag = 0;
return false;
}
usernameStr = passwordMD5(loginUsername.value);
passwordStr = passwordMD5(loginPassword.value);
hiddenUsername.value = usernameStr;
hiddenPassword.value = passwordStr;
loginPassword.value = "Ha2S+eOKqmzA6nrlmTeh7w==";
return true;
}
```

This second to last line seems interesting as it has a proper value but it seems to be encrypted. The passwordMD5 function connects to a function called "calcMD5" which I guess encrypts the entered username and password before checking them?

If there is a way for me to get into this router that would be great. I'm worried that I'm at risk of being hacked myself because I gave away the wifi password. Please help!

EDIT : The router is a ZTE ZXV10 W300

EDIT 2 : I just tried factory resetting it.... The router doesn't want to factory reset. It resets but all settings seemingly stay the same. I really need to hack into it. Apparently this router has something called a rom-0 vulnerability? How can I make use of that?Go beat his ass lmao

Justforyou™ - October 7, 2019, 8:18 am

It al depends on which firmware it is running.

But the rom-0 backup file contains sensitive information such as the router password.
There is a disclosure in which anyone can download that file without any authentication by a simple GET request.

POC:

Code <http://192.168.1.1/rom-0>
<https://www.exploit-db.com/exploits/33803>

is_nimda - October 7, 2019, 1:20 pm

if you factory reset, it will restore default password... 100%, you didnt factory reset if password isnt the one on the label..

u can say ur trying to hack a router ;]