Open in app ↗ Sign up Sign In
Search Medium

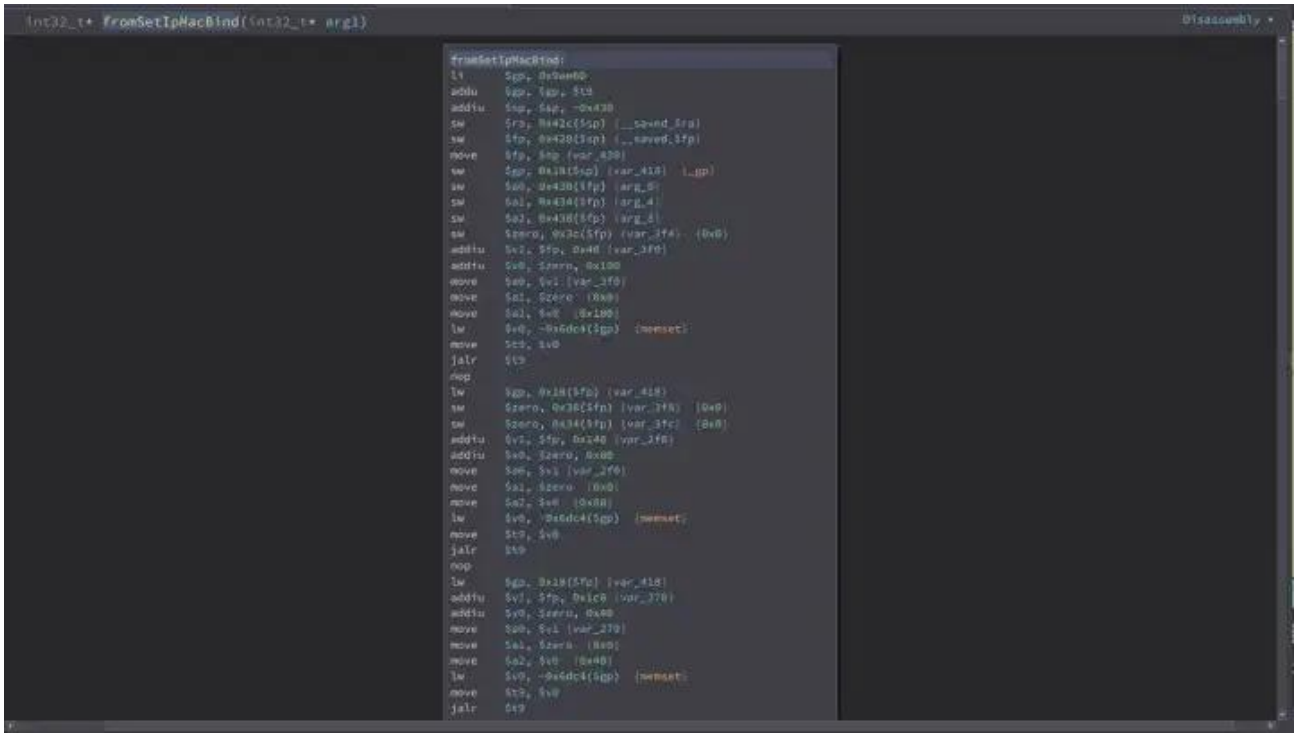
Brandon Roldan Follow
Aug 10, 2021 · 4 min read · Listen

Save

# Hacking the Tenda AC10–1200 Router Part 3: Yet Another Buffer Overflow

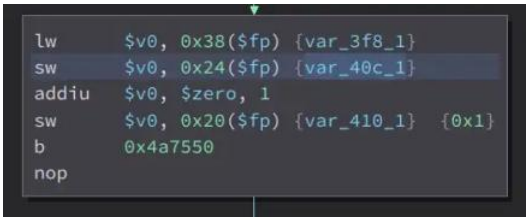
Hi. This is my third writeup in my hacking the tenda ac10 series where i try to get a cve. Lets get started.

So while looking through the functions that accept user inputs, i found this one function called `fromSetIpMacBind`



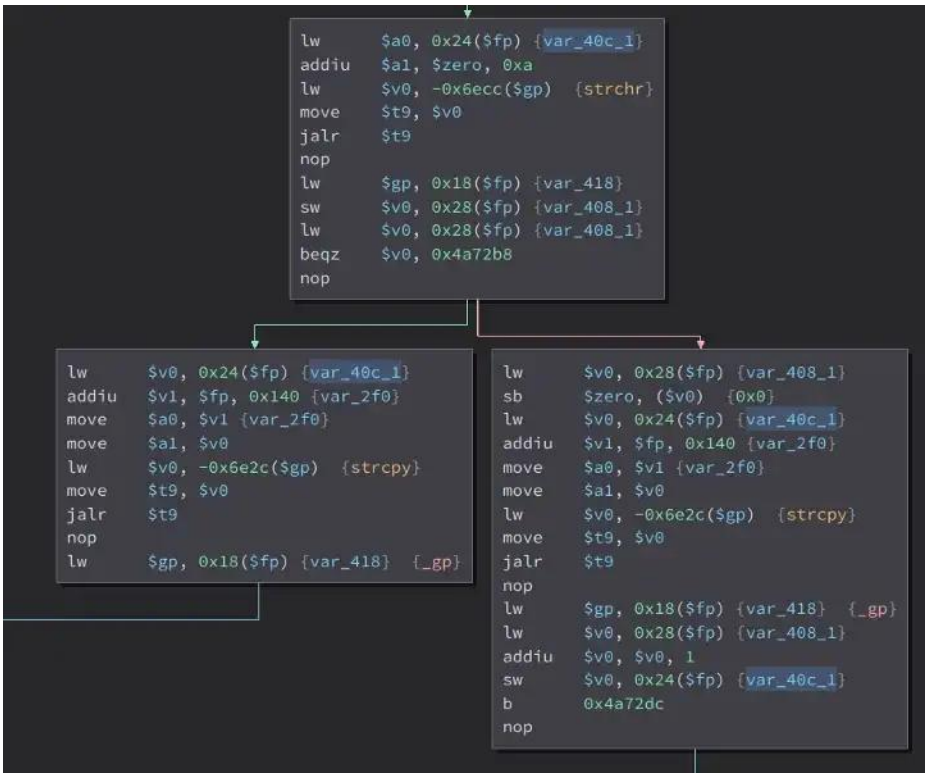
Here's what it do, first it get the value of the parameter list then store its value to the variable called `var_3f8_1`


Then, it move this `var_3f8_1` variable to another variable `var_40c_1`



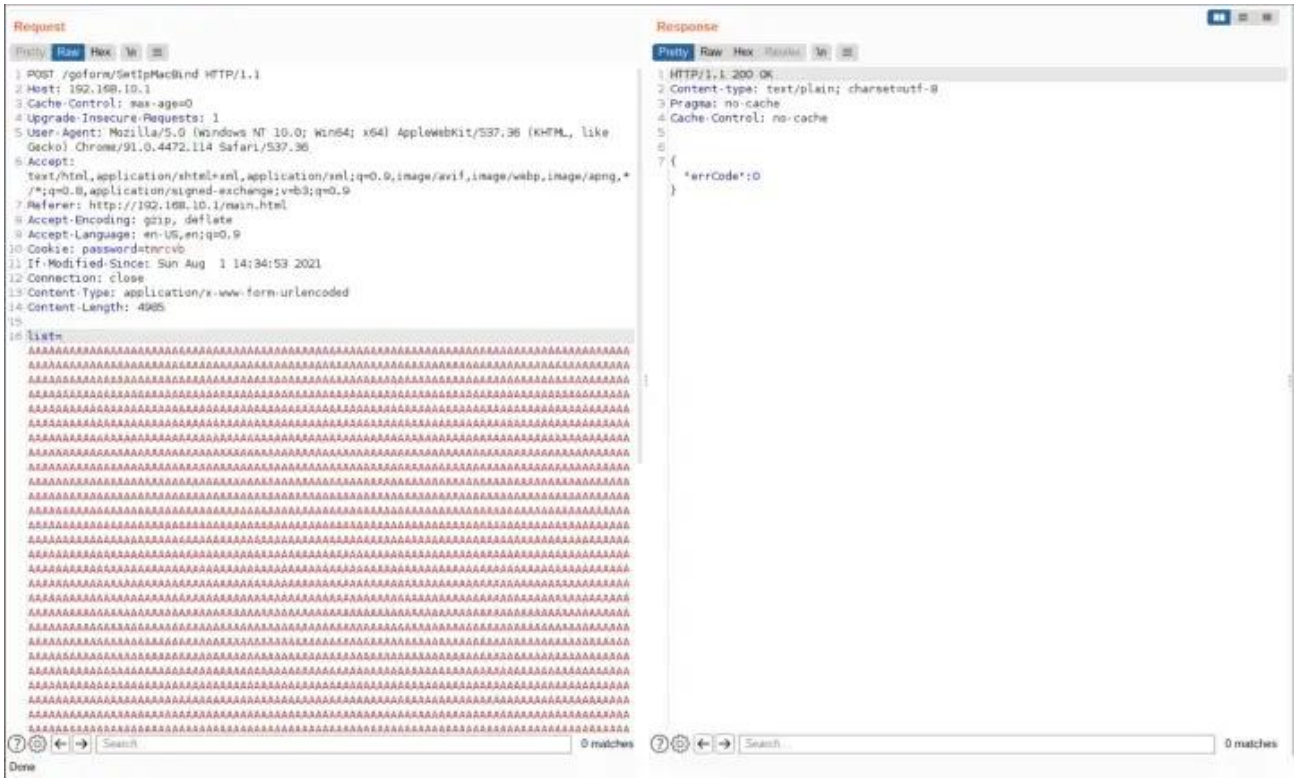

Then check if `0xa` is in `var_40c_1` using `strchr` which doesnt matter since either way, there will be a `strcpy` which will cause the buffer overflow.

101

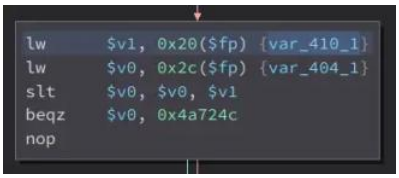



Now lets try it out. `fromSetIpMacBind` is referenced in `formDefineTenda`

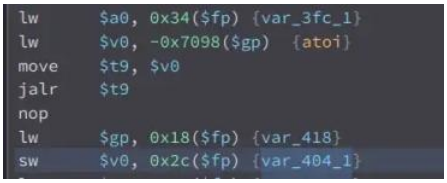

This means our vulnerable endpoint is `SetIpMacBind` . Now lets try it out



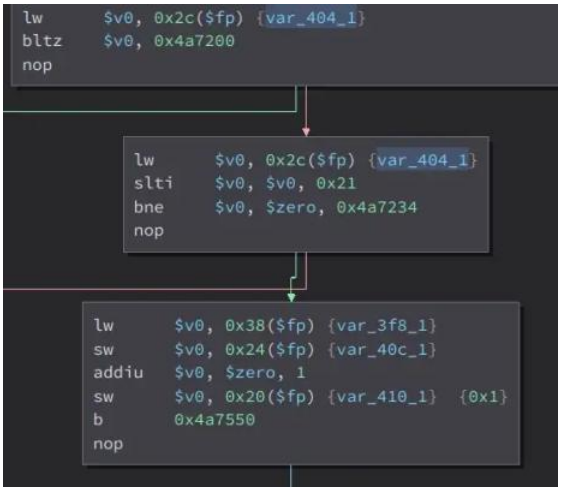

It doesnt work. For some reason, it didnt reach our `strcpy` . Lets track out why.



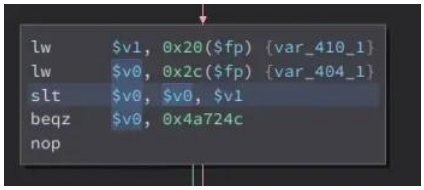

This is the code before the strchr that we expected. Here, we can see that it checks if `var_404_1` is less than `var_410_1`. If it is, it will jump somewhere else and will not execute the `strchr` and `strcpy` that we expected. Now lets see what is the value of these two. Starting with `var_404_1`


We can see that its value is the `atoi` of the bindnum parameter. What atoi does is it convert our string input to integer. Now lets find out what is the value of `var_410_1`. This one is a little complicated

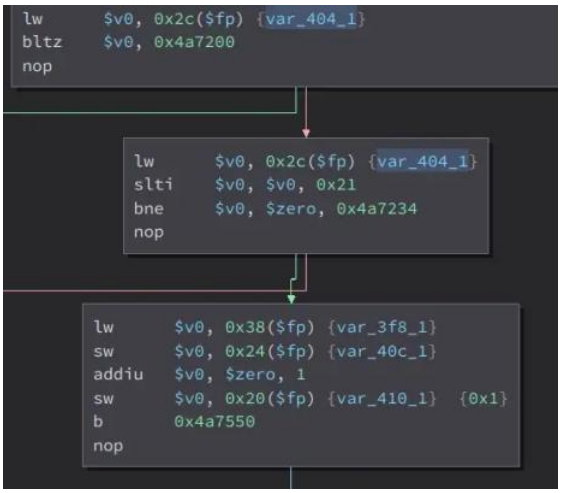



Here, it checks if `var_404_1` is not less than zero and less than `0x21`. (var_404_1 is the atoi of the bindnum parameter). If yes, it will set the value of `var_410_1` to 1 or 0x1. The other variables are not that important. Then, the check happens



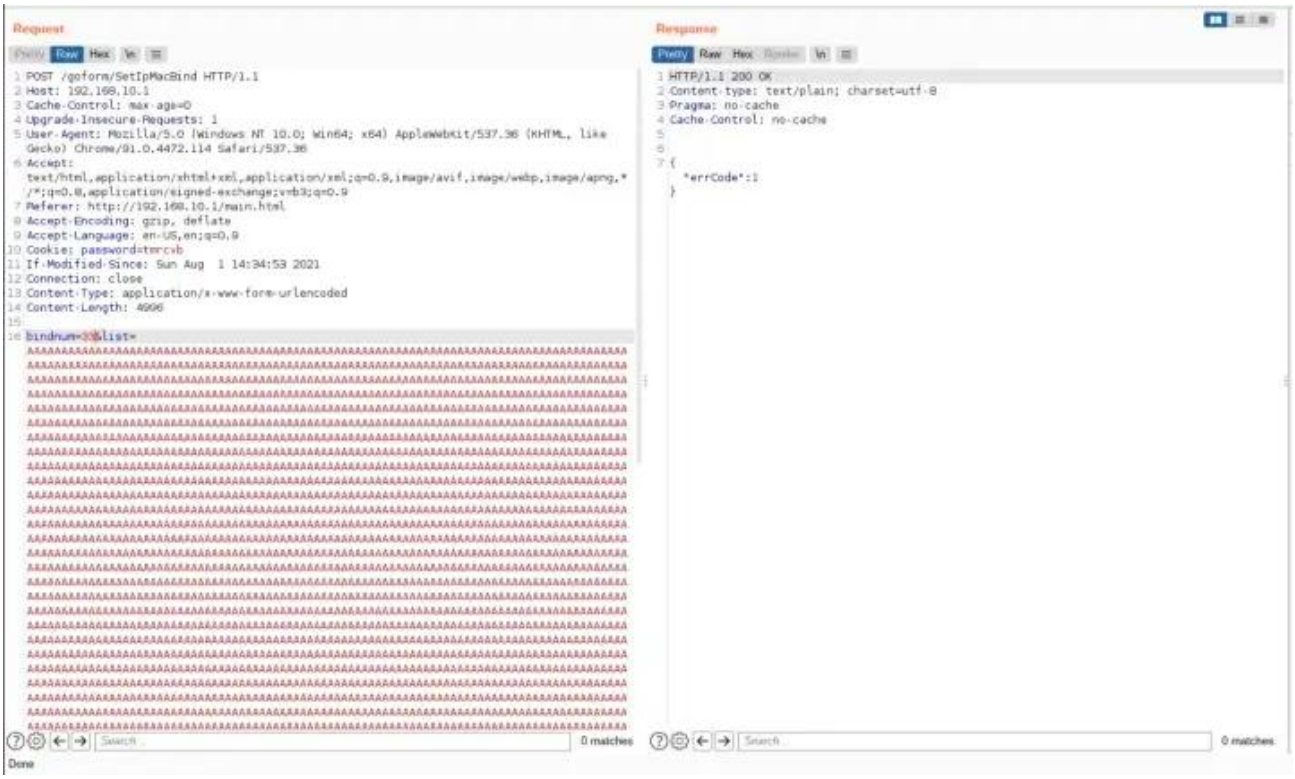

If `var_404_1` is less than `var_410_1`, it will not execute our strcpy and the exploit will fail. So what we have to do is make `var_401_1` to 1, because then, `var_404_1` will be greater than `var_410_1` which then will execute our strcpy.

Now to set `var_410_1` to 1, the value of the parameter `bindnum` should be greater than 0 and less than 0x21 as stated here

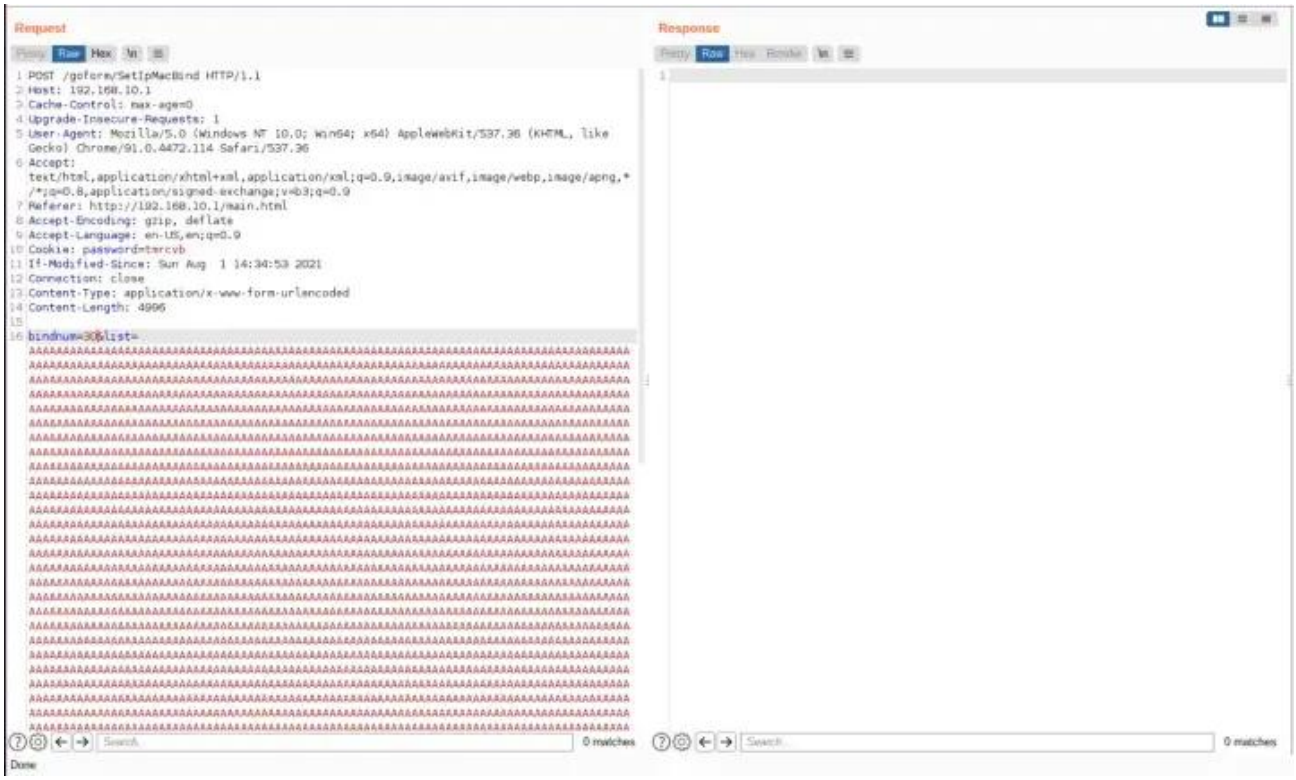



Now lets try it again but this time lets provide the bindnum parameter.

If we set `bindnum` parameter to 33(0x21) or higher, we can see that it will fail




But if we set it between 1 and 32, it will succeed




No response. That means we crashed the server and our exploit is successful.

We can further confirm it by looking at the emulation

This is the end of the writeup. I tried contacting tenda but they havent responded so i decided to disclose it now.

Thanks for reading

Join the discord server: https://discord.gg/bugbounty

Hacking Infosec Io T Hack Security

About Help Terms Privacy

Get the Medium app