



Stark0de Sanctuary

# Pwning rConfig part I

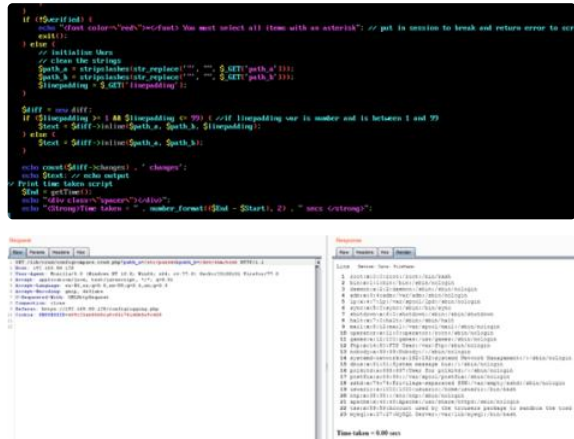
27 Aug 2020

## Pwning rConfig: part one

Hi everyone. I've been quite busy lately, but some weeks ago I decided to review the security of a software called rConfig version 3.9.5 ([www.rconfig.com](http://www.rconfig.com)) which is a Network Monitoring tool and I found several vulnerabilities. So let's take a look at them ;)

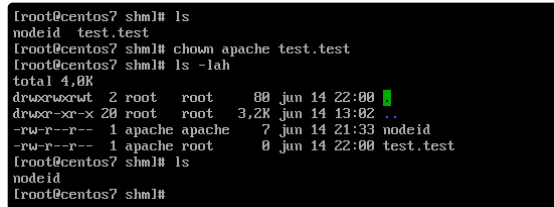
### LFI 1

Local file disclosure in `/lib/crud/configcompare.crud.php`, when comparing the parameter `path_a` to `path_b`, the file specified in `path_a` is disclosed if both files are completely different. Here we can see the contents of `/etc/passwd`



### Arbitrary file deletion

Arbitrary file deletion in `/lib/ajaxHandlers/ajaxDeleteAllLoggingFiles.php`. You can delete any file with an extension by specifying the file with the `path` parameter and the extension with the `ext` extension

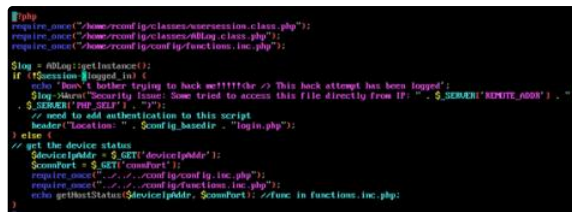


### Server-Side Request Forgery

Server-Side Request Forgery in `/lib/ajaxHandlers/ajaxDeviceStatus.php`, you can open a connection to the inside of the machine with the `deviceIpAddr` parameter and the `connPort` parameter.



### OPEN PORT:



Device Management

Add Device

Edit Device

Remove Device

Device Details

\* Device Name:

scriptalert@script

\* IP Address:

192.168.1.13

Enable Prompt:

router>

\* Main Prompt:

test

\* Vendor:

Cisco

\* Model:

<script>alert(2)</script>

Other Details

\* Category:

Switches

Custom Properties:

Location:

Credentials

Default username/password?

☐

Username:

username

Password:

password

Enable Password:

Enable Password

\* Template:

Cisco IOS - TELNET - No Er

Save

Close

## XSS 2

### XSS 3

Cross-Site Scripting in /snippets.php > Add snippet, introduce a payload such as <svg onload=alert(1)> in the Snippet field and click Save(fill the rest of fields first).

Configuration Tools > Config Snippets

Configuration Snippets

Edit Snippet 'TTF in Database'

Add Snippet Edit Snippet Remove Snippet

Snippet Name:

Snippet Description:

Snippet:

Save Close

Search

Snippet:  Contains:  Search text

Clear New Search

page 1 of 1000 and

1/1 Next Page Search your snippet

ManualPermissionEnvelope

## Privilege escalation 1

Using sudo zip:

[illegible]

## Privilege escalation 2

By doing `sudo crontab -e` and then `#!/bin/bash`

**Arbitrary file read:**

Following this we can read any privileged file: <https://gtfobins.github.io/gtfobins/tail/>

So those are some of the vulns I found during the research, hope you enjoyed the article. Back with the second part soon :)

### Comments

[Load Comments](#)

## Related Posts

Pwning rConfig part II 13 Oct 2020

## How I found a Remote Code Execution in OpenEDX 17 May 2020

Certified Red Team Professional Review 30 Apr 2020