CheckMK – CheckMk's Dokuwiki embedded

Author: Edgar Augusto Loyola Torres

Application: CheckMK Raw Edition 1.5.0 to 1.5.0p25

Attack type: Remote Code Execution

Solution: Update to Software Revision 1.6 or higher.

Summary: The web management console of CheckMk Raw Edition (versions 1.5.0 to 1.5.0p25) allows a misconfiguration of the web-app Dokuwiki (installed by default) which allows embedded php code. As a result, remote code execution is achieved. Successful exploitation requires access to the web management interface, either with valid credentials or with a hijacked session by a user with the role of administrator.

Technical Description:

[Described in the next sections]

- **RCE - CheckMK Raw Edition version < 1.6**

There is a way to execute remote code through a web-app that CheckMK has installed by default called "Dokuwiki", if we manipulate the configuration of this application from the web browser (no modification of the source code), so that it accepts embedded PHP, a possible attacker will have a command terminal. **Requirement**: Be authenticated with an administrator user (e.g. "cmkadmin") and have Dokuwiki installed within the CheckMK system.

1.1. Remote Code Execution

Obtaining a reverse shell through misconfiguration by the DokuWiki application installed by default in Checkmk.

1.1.1. Proof of concept

To get the reverse shell first we have to add the DokuWiki application to the sidebar, just add "Add snapin to the sidebar" shown in the first (Figure 1) on the left and do a search in the interface input shown in the (Figure 1) on the right, it will redirect us directly to the DokuWiki application.

Figure 1: Search Wiki in Dokuwiki

Once inside this application, click on the **“Admin”** button next to the “Export PDF” shown in the (Figure 2) and enter the area where the DokuWiki application is configured.

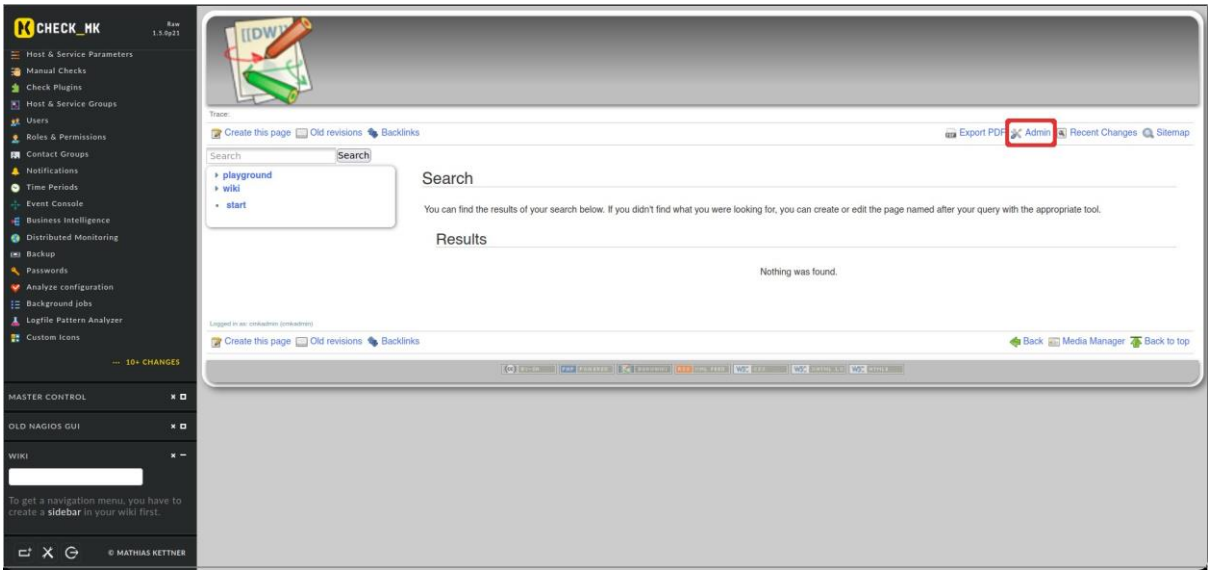

Figure 2: Dokuwiki

As you can see in the (Figure 3) we will go to the DokuWiki configuration to enable embedded php code.

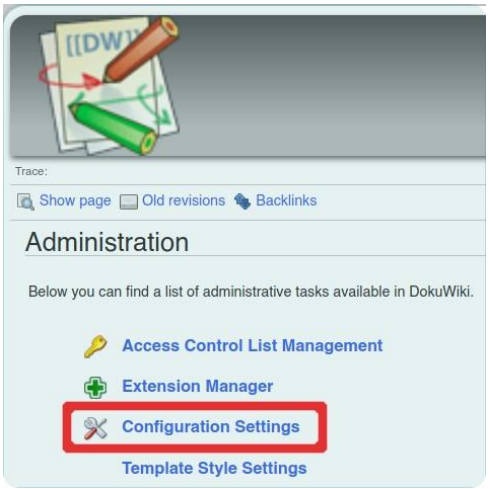

Figure 3: Configuration settings

If we go to the “Editing” area and look for the option **"Allow embedded PHP"** and check the checkbox, we will be able to embed php code in any Dokuwiki page.

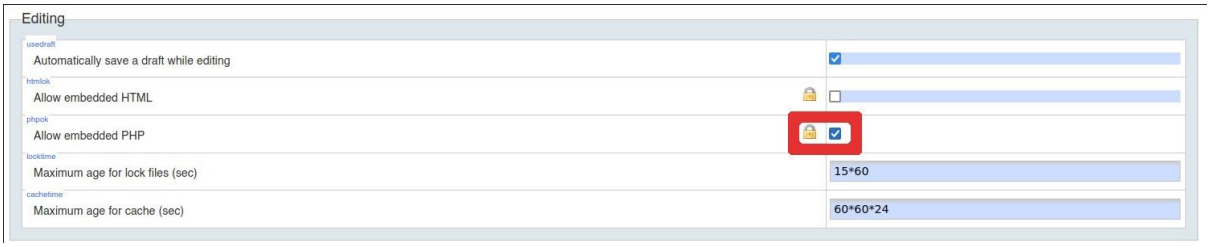

Figure 4: Editing configuration of Dokuwiki

But for this we need to edit any page, for example we will edit the main page called "start".

Figure 5: Edit this page

Once you are editing a page of the Dokuwiki application, you only need to insert php code between the "<>" symbols, i.e. **<php> Payload </php>,** as shown in the (Figure 6).

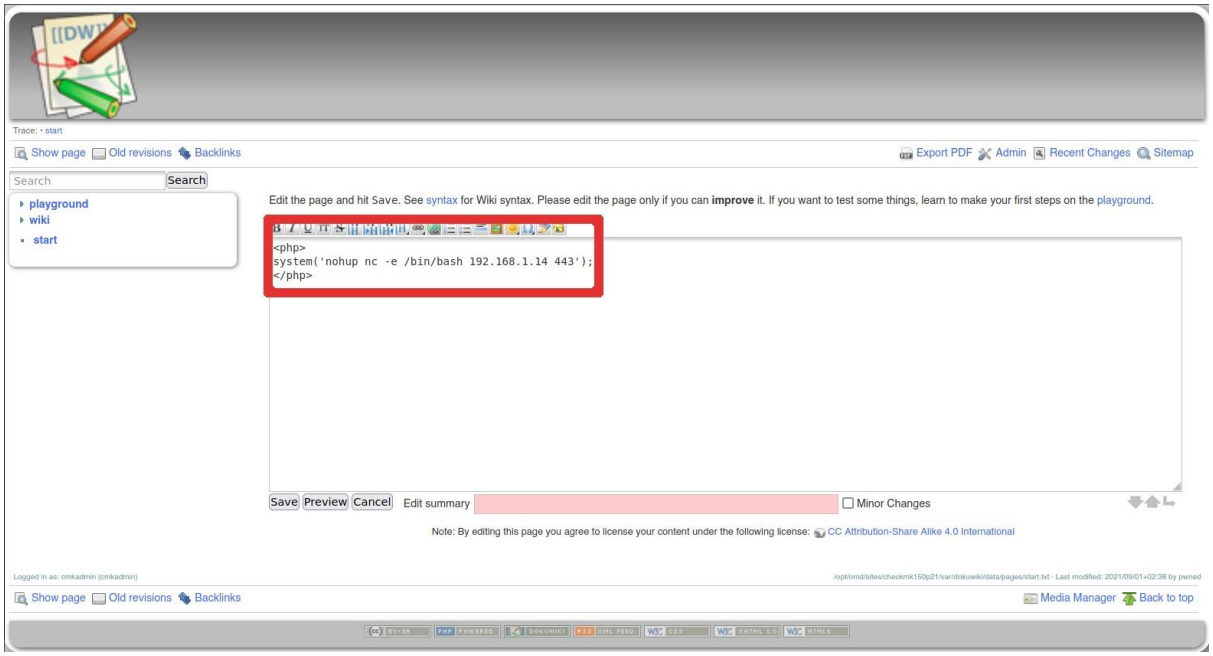

Figure 6: Write php embedded

Finally, to get a remote execution of commands, just by “**saving” or “previewing”** the php code embedded in the main page called "start” and listening with the netcat command on port 443 (this port was configured with the netcat payload) which in this

case serves as an example in the (Figure 7), we will have a reverse shell, i.e. control over the host that has installed the Checkmk.

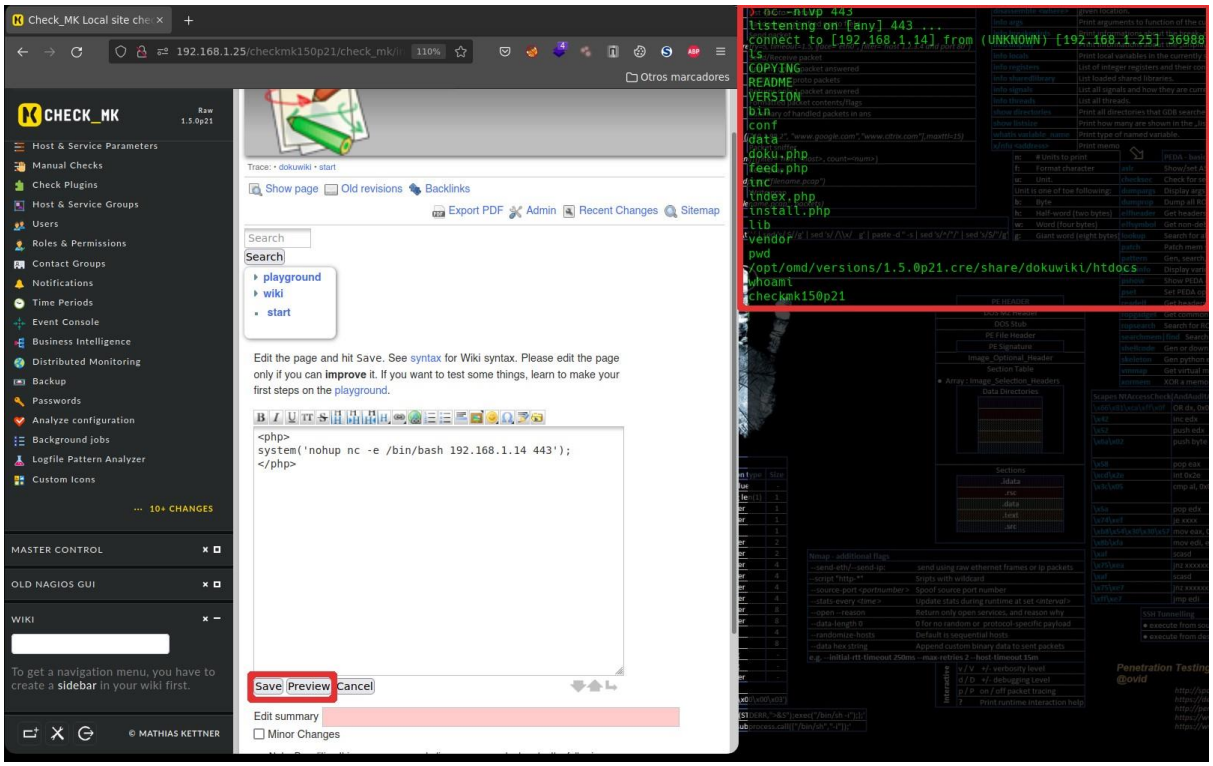

Figure 7: RCE - Reverse shell

1.1.2. Proposed solutions

Possible mitigations for this RCE vulnerability would be to either upgrade to versions higher than 1.6. or to disable the Dokuwiki configuration in the sense of prohibiting embedded php code on its pages. That not even an administrator user can put embedded php code, because you never know if that administrator has good intentions with the system that is monitoring.