Product Description:

The DedeBIZ system is based on PHP7, which is highly extensible and completely open source. DedeBIZ supports the design and development of the popular Go language, which is more secure and efficient in addition to being easy to use and flexible expandable. The simple design and production of templates has always been a major feature of the system, continuing the previous labels, and using the responsive template engine Bootstrap as the system template rendering engine, making it easier to build cross-terminal and mobile all-media sites

Affected versions:

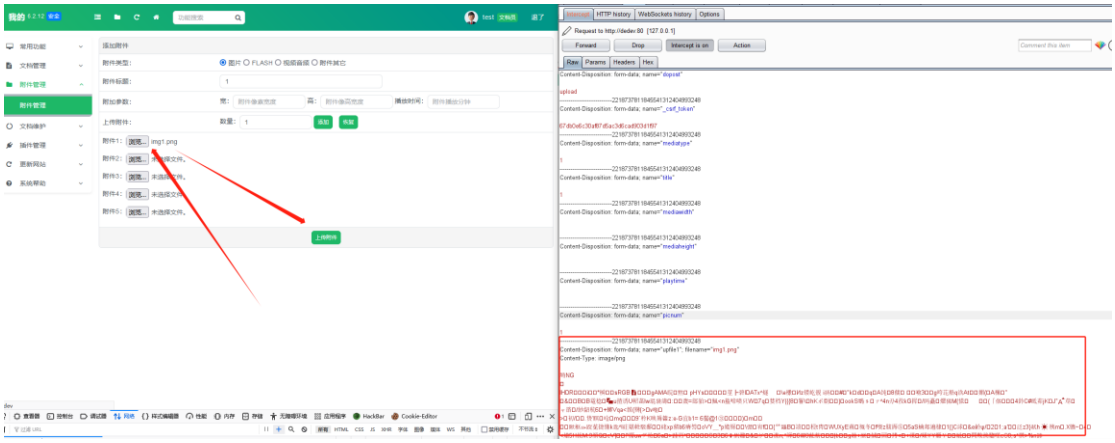
V6.2

Summary of vulnerabilities:

Due to the developer's negligence, there is a file upload vulnerability in DedeV6, which can upload webshell in the /admin/media_add.php interface, resulting in the system being taken over.

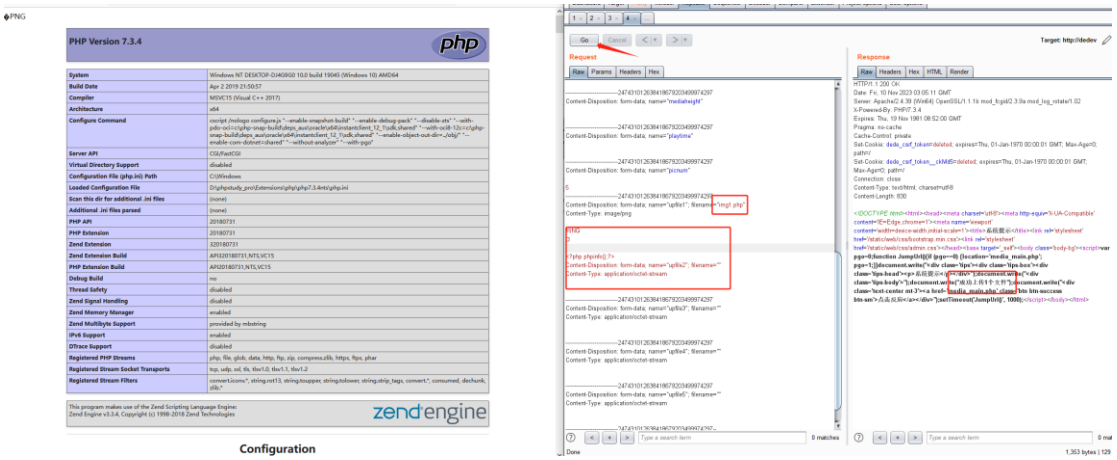
vulnerability Details:

a. Access the file upload interface /admin/media_add.php.



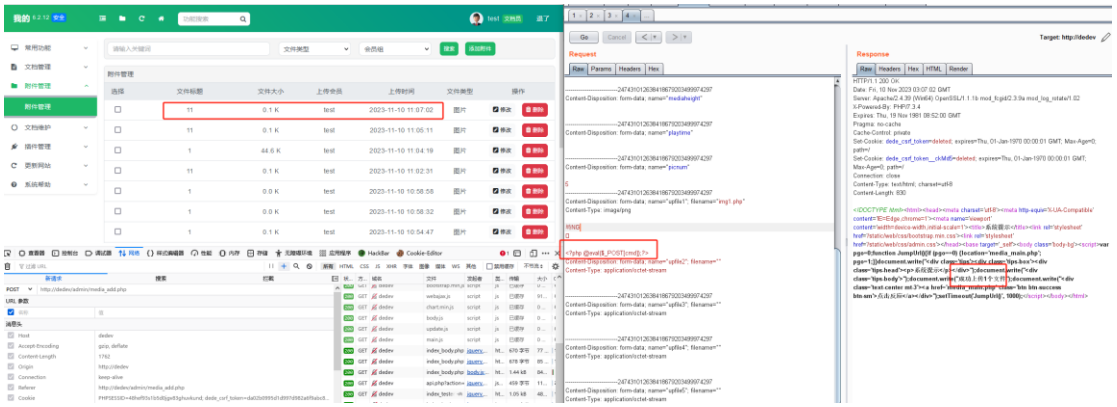
b. Poc:

Modify the file name and content:

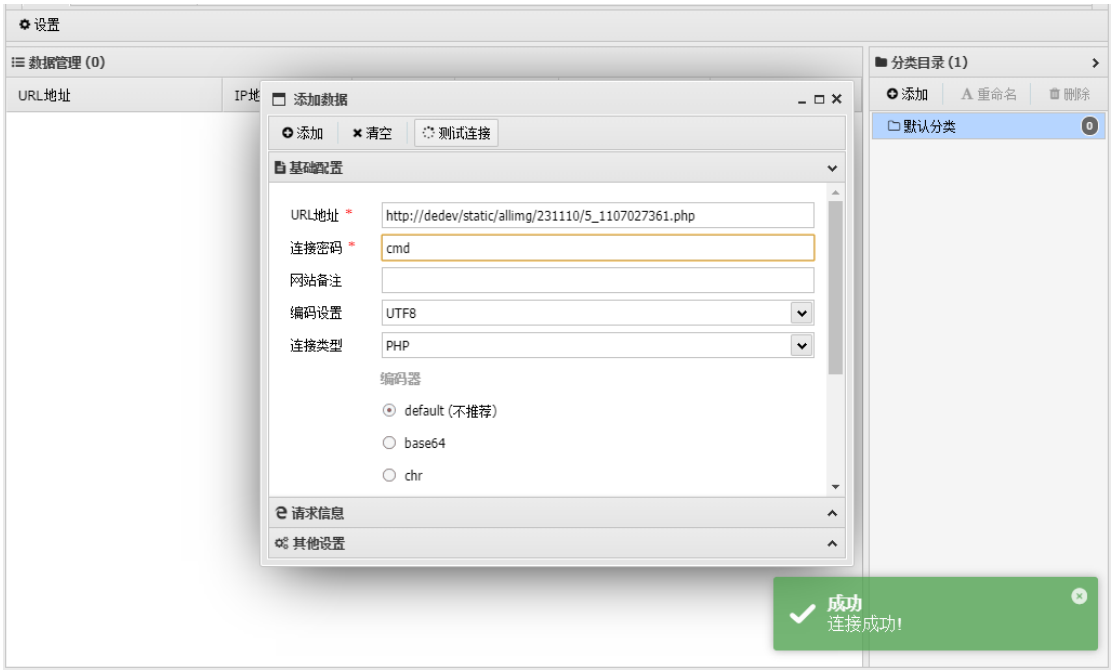


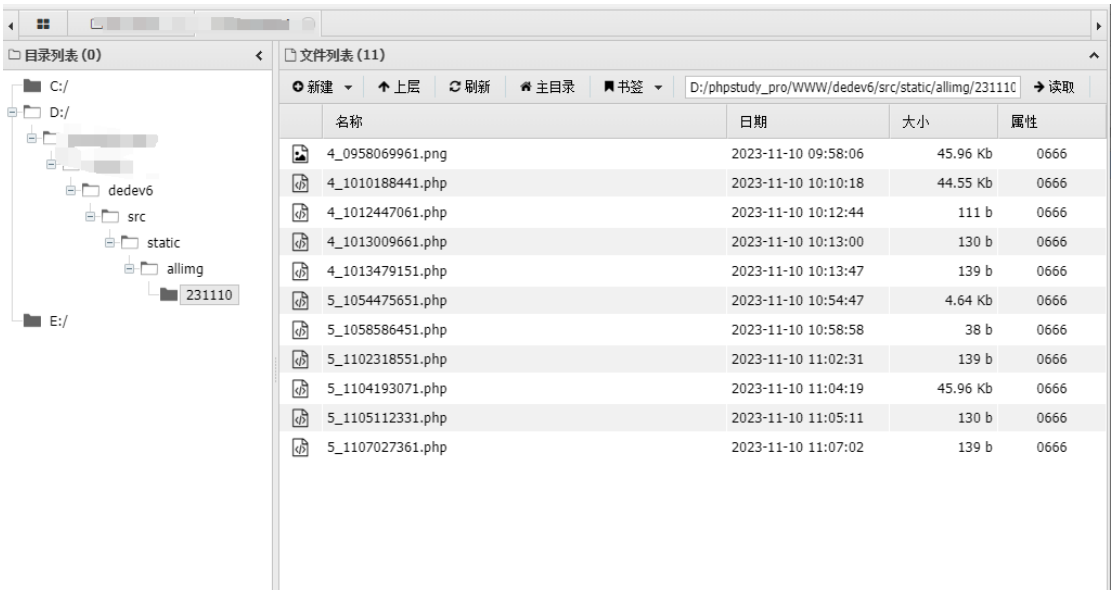
Successed

Upload a webshell:



Use Antsword connect:





Successed!

If the picture is not clear, click the link:

https://github.com/CP1379767017/cms/blob/dreamcms_vul/dedevCMS/File upload vulnerability exists at the location where add a file.md