DarkEye开源 免费的cloudeye.me

索马里的海贼 / 2016-11-29 15:31:10 / 浏览数 17947 安全工具 工具 顶(0) 踩(0)

概述

cloudeye.me是个好东西啊，碰上盲注 盲xxe 无回显命令执行再也不用怕了。穷屌当年买不起邀请码 现在也够不上活跃份子 只好自己写一个
只实现了简单的dns三级域名请求记录，weblog懒得写，不过支持自定义dns解析，可以解析到你自己的webserver来获取weblog.
dns response参考了网上python版的cloudeye

功能

1.多用户
2.dns请求记录
3.自定义dns解析ip和ttl
4.hex解码

存在的问题

config.php做了一个简单的针对$_GET的全局防注入。好不好使我可不保证。
用户名处存在 selfxss 不过有32个字符的限制
操作没有做csrf防御 修改配置啦 清空数据啦 都是 可以被csrf的（被M哥分分钟教做人）
很多操作的提示都没处理 用起来不明不白的 包括登录注册等等等等……

使用说明

测试环境

- win(php 5.5.4+apache2.4.10+mysql 5.0.11)
- linux(php 5.3.10-1ubuntu3.24 + apache2.2.22+ mysql 5.5.50)
- 新建数据库 导入dkeye.sql
- 修改config.php中的数据库连接信息和$domain
- 运行php DNSfakeServer.php 看看是不是报错（以后可以后台运行，是screen还是nohup随便）
- 这个应该是1。。先买个域名 修改域名dns为你的服务器地址

ps 为了测试买了好多域名- - 说一下各家的情况
阿里云 先知修改的DNS需要是在ICANN或者CNNIC注册过的有效DNS
花生壳 虽然不限制修改DNS 但特么改了3天了还没生效- - 醉了
西部数码 也限制修改的DNS需要是在ICANN或者CNNIC注册过的有效DNS 不过 发个工单让人工修改就行了 秒改的噢~

开源协议

MIT 随意修改 改了卖钱都行 只要保留许可协议

dkeye.zip (0.0 MB) 下载附件

上一篇：我的WafBypass之道（Upl... 下一篇：【来点鸡汤】你必须非常努力，才能看...

1. 10 条回复


小小子 2016-11-29 15:40:51

海贼牛逼了，强烈支持

0 回复Ta


sofia 2016-11-29 15:57:17

快看，海贼今天又赚3万多

0 回复Ta


prolog 2016-11-30 01:15:02

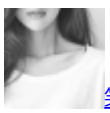
快看，海贼今天又赚3万多

0 回复Ta


hades 2016-11-30 01:19:51

快看，海贼今天又赚3万多

0 回复Ta


笑然 2016-11-30 04:51:32

海贼厉害了

阿里云 先知修改的DNS需要是在ICANN或者CNNIC注册过的有效DNS

这个明明是“限制”...我猜海贼是先知的真爱粉

0 回复Ta


blueboy 2016-12-05 09:25:29

bugscan dnslog

0 回复Ta


shin 2016-12-11 17:39:28

一直在用这个 ceye.io

0 回复Ta


0wen 2016-12-13 03:47:40

0 回复Ta


null 2017-06-29 09:05:47

0 回复Ta


VS0X 2017-12-15 12:37:26

牛逼

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板