



# Bugscan

基于插件众筹的分布式

漏洞扫描平台



契机

团队

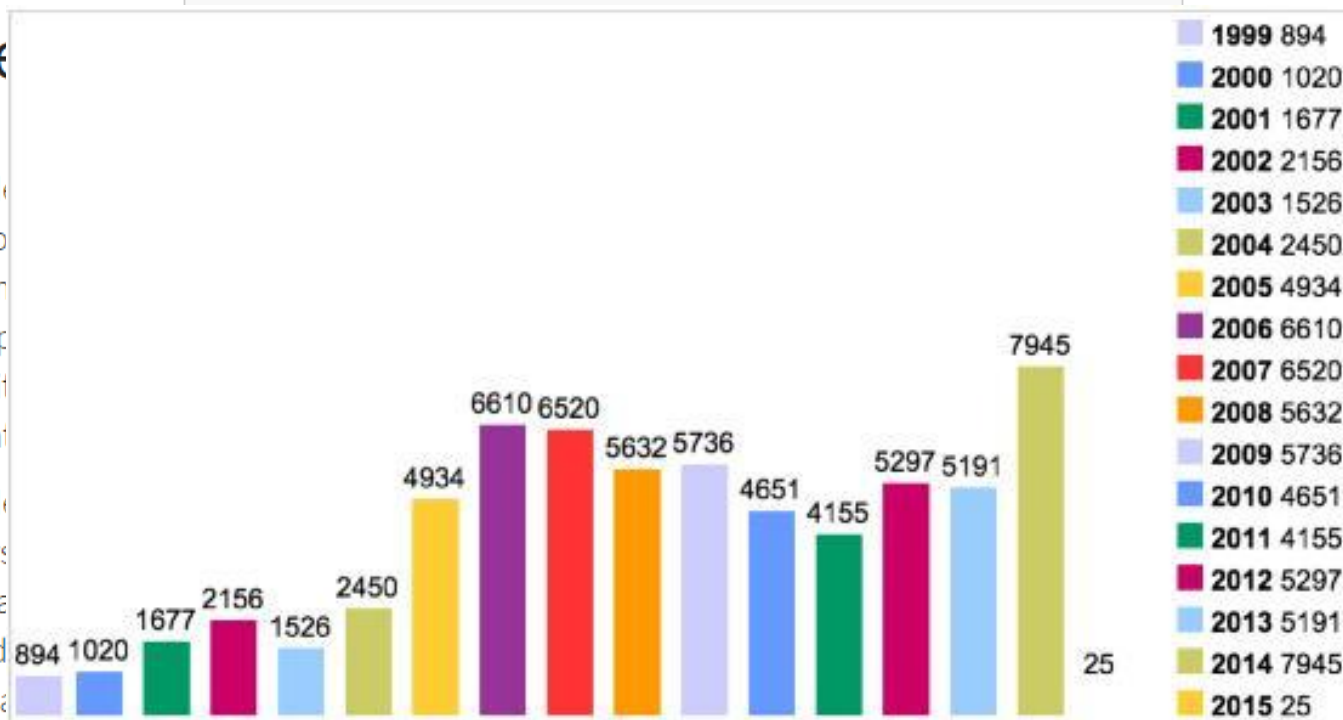
功能

特点

漏洞概况信息如下：

## The

The H  
crypto  
inform  
encrypt  
securi  
instanc  
  
The H  
the sys  
softwa  
provid  
users a



communications, impersonate serv

InfoWorld的专栏作者Andrew C. Oliver在一篇文章中表达了自己看法，他认为CGI技术的普及是个错误，正是因为CGI技术的不合理之处，Shellshock才有机可乘。

CGI技术是Web技术刚兴起的时候发明的，它是最早的可以创建动态网页内容的技术之一。它会把一个HTTP请求转化为一次shell调用。

# 团队成员

BugScan和圈子成员



四叶草安全  
CloverSec

## 马坤(cnfjhh)

---

公司&团队负责人

**12年**信息安全领域专家

专注于网络安全前沿研究

## 陈震国(Zero)

---

BugScan扫描引擎研发

10年全栈工程师经验

玩转各种编程语言

著名的Hijack、Gh0st、  
Arpspoof作品的作者

## 赵培源(半块西瓜皮)

---

BugScan扫描框架研发

7年以上python功底

熟悉各种漏洞原理

漏洞圈子的作者

## 贾林杰(不流畅)

---

BugScan插件审核

5年以上底层固件研发  
经历

圈子插件审核员

## 武成军

---

BugScan开发

**10年**以上C++开发经验

# 团队成员

圈子（社区）核心成员

## Medici.Yan

擅长各种系统服务的协议分析

## range

擅长各种web程序的漏洞

## Wyc0

能将各种热门漏洞收集分析，迅速写成漏洞插件

bugscan > 贡献者排行榜

1		Zero 🏆 核心 暂无签名	572
2		Medici_Yan 🏆 核心 西瓜皮把我名字里的点还给我... <a href="http://blog.evalbug.com">http://blog.evalbug.com</a>	137
3		range 🏆 核心 hello world <a href="http://range.pw">http://range.pw</a>	131
4		Wyc0 🏆 核心 俺就进城里看看	122
5		星光点亮天 🏆 核心 用代码点亮天	111
6		野地和尚 😊 普通 暂无签名	109
7		半块西瓜皮 ADMIN 管理 我是签名 <a href="http://www.howmp.com">http://www.howmp.com</a>	98
8		GreeM 😊 普通 暂无签名	98
9		b13 😊 普通 XXXXXXXX	79
10		不流畅 👤 审核 暂无签名	78

# 功能

服务的扫描



snmp rsync memcache smb socks5 nfs进行弱口令爆破和漏洞扫描

NGINX



elasticsearch.

struts2



ECShop



DEDECMS

文件上传 表单破解  
CMS识别 注入 跨站  
子域名 目录遍历 后台猜解  
服务识别  
任意url跳转 报错信息抓取  
端口扫描  
任意文件包含\下载



## 网络设备

D-Link  
友讯网络

网康科技  
NETENTSEC

天融信  
TOPSEC

海康威视  
HIKVISION

net·core 磊科®

# 特点

历时四年，五次重构



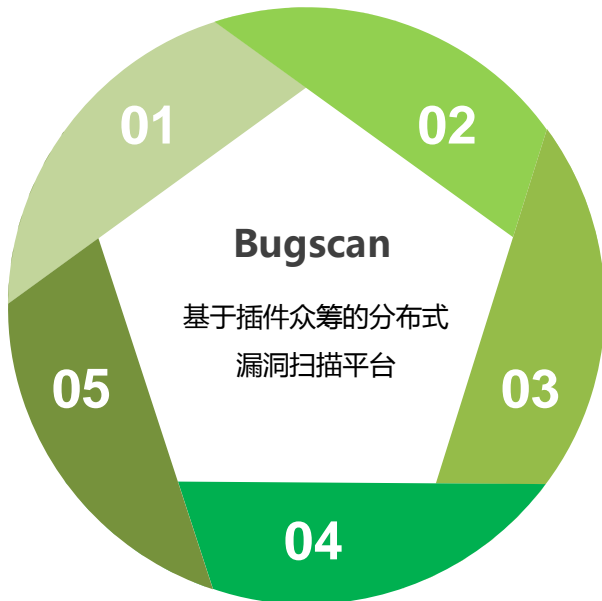
四叶草安全  
CloverSec

## 01.跨平台

核心扫描引擎使用python编写  
不受操作系统限制  
创建节点无需下载第三方安装包

## 05.高速、稳定

前端使用angularjs框架与rest技术  
后端采用go语言开发  
可承受更多的节点并发执行任务



## 02.分布式

一句命令即可创建节点  
多节点自动负载均衡

## 03.云插件

节点无需操作  
自动升级最新的插件

## 04.漏洞库

漏洞库实时更新  
现已有2万余条漏洞记录

[www.BugScan.net](http://www.BugScan.net)

# ← 添加任务



四叶草安全  
CloverSec

testphp.vulnweb.com

+ 多任务扫描 (每行一个目标 比如: http://testphp.vulnweb.com/ )

## 模块

☒ Common

☐ Weak Passv

## 节点 10

☒ 任何节点

☒ 101.2

python -c "

## 选项

爬虫

全局

User Agent

## 选项

爬虫

☐ 扫描子域名

☐ 深度端口扫描

全局

速度

6

超时时间

24

最大网页数

5000

User Agent

Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; .NET CLR 2.0.50727)

用户名字典

密码字典

排除网页 ☐

logout;log\_out;/admin;/manage;/phpmyadmin

Cookies

# 特点

## 云插件

名称

zoomla costme

Zoomla search

【已重复】Joo

Z-blog前台无需

socks5\_userpas

JCMS\_SQL que

大汉JCMS系统

Thinkox index

【等待提交特征

【等待添加特征

【等待提供验证

eyou邮件系统

【已重复】eyo

Wordpress Hist

佑友mailgard v

1 2 3

File Edit Format Run Options Windows Help

```
#!/usr/bin/env python
```

```
import re
```

```
def assign(service, arg):
```

```
    if service == "discuz":
```

```
        return True, arg
```

```
def audit(arg):
```

```
    url = arg
```

```
    code, head, res, errcode, _ = curl.curl2(url + 'uc_server/control/admin/db.php')
```

```
    if code == 200:
```

```
        m = re.search('not found in <b>([^\>]+)</b> on line <b>(\d+)</b>', res)
```

```
        if m:
```

```
            security_info(m.group(1))
```

```
if __name__ == '__main__':
```

```
    from dummy import *
```

```
    audit(assign('discuz', 'http://www. com.cn/')[1])
```

14:28

30:48

41:20

33:11

58:15

52:09

34:34

13:15

36:21

24:59

57:52

10:19

35:43

49:44

02:44

Python 2.7.9 Shell

File Edit Shell Debug Options Windows Help

Python 2.7.9 (default, Dec 10 2014, 12:24:55) [MSC v.1500 32 bit (Intel)] on win

32

Type "copyright", "credits" or "license()" for more information.

>>> ===== RESTART =====

>>>

[LOG] <info> E:\web\ \uc\_server\control\admin\db.php

>>>

# 特点

## 漏洞库

[WordPress](#)[Joomla](#)[Drupal](#)[phpBB](#)[Discuz](#)[Dede](#)[更多 ...](#)

名称	公开时间
<a href="#">Koha Open Source ILS - Multiple XSS and XSRF Vulnerabilities</a>	2015-06-27
<a href="#">Rubygems &lt;2.4.8 vulnerable to DNS request hijacking</a>	2015-06-27
<a href="#">Koha Open Source ILS Path Traversal in STAFF client</a>	2015-06-27
<a href="#">Koha Unauthenticated SQL injection</a>	2015-06-26
<a href="#">PCRE Library Heap Overflow Vulnerability in find_fixedlength</a>	2015-06-26
<a href="#">SAP NetWeaver Dispatcher Buffer Overflow RCE, DoS</a>	2015-06-26
<a href="#">SAP NetWeaver Portal XMLValidationComponent XXE</a>	2015-06-26
<a href="#">Thycotic Secret Server version 8.6.000000 to 8.8.000004 XSS</a>	2015-06-25
<a href="#">Apache Storm 0.10.0-beta Code Execution</a>	2015-06-25
<a href="#">Joomla Simple Image Upload Arbitrary File Upload</a>	2015-06-25
<a href="#">Wordpress huge-it-slider 2.7.5 &amp; Persistent JS-HTML Code injection</a>	2015-06-25
<a href="#">Agahi 1.6 Cross Site Scripting / SQL Injection</a>	2015-06-25
<a href="#">Thycotic Secret Server 8.8.000004 Cross Site Scripting</a>	2015-06-25
<a href="#">Kguard Digital Video Recorder Bypass Issues</a>	2015-06-25
<a href="#">IBall 150M Wireless-N ADSL2+ Router Authentication Bypass</a>	2015-06-25

[1](#)[2](#)[3](#)[4](#)[Next »](#)[Last](#)

# 特点

## 扫描报告



四叶草安全  
CloverSec

## 扫描记录

http://192.168.0.146/ 11 issues

状态: HIGH 插件: 301 子域名: false 端口: false 耗时: 53s, 日期: 2015-04-14 12:17:37

192.168.0.146

INFO

### 1 Sensitive File/Directory Discover

- ...
- ...
- ...

### 2 Port and Service Discover

- TCP: [80, 445]
- 80 => [www]; Ver => [('Server', 'Microsoft-IIS/6.0'), ('X-Powered-By', 'ASP.NET')]
- 445 => [smb]; Ver => Windows Server 2003 5.2

### 3 .Net Sensitive Information Exposure

- ...

### 1 PPTP-Version

- ...

LOW

### 1 WebDAV Enabled

- ...

### 1 IIS Short File/Folder Name Disclosure

- ...

HIGH

### 1 ASP.NET Padding Oracle Vulnerability

- ...

### 1 SMB缓冲区溢出漏洞(MS08-067)

- [ms08-067]Microsoft Windows Server服务RPC请求缓冲区溢出

## 扫描记录

http://61.153. /cgi-bin/test-cgi 3 issues

状态: HIGH 插件: 138 子域名: false 端口: false 耗时: 1m, 47s, 日期: 2015-03-02 11:05:43

61.153.

INFO

## 扫描记录

http://66.228. / 3 issues

状态: 51.16% 插件: 138 子域名: false 端口: false 耗时: 1m, 24s +, 日期: 2015-03-02 11:11:48

66.228.

INFO

### 2 Port and Service Discover

- TCP: [22, 80, 443, 3306]
- 80 => [www]; Ver => [('Server', 'nginx/1.0.15')]
- 443 => [ssl]; Ver => [('Server', 'nginx/1.0.15'), ('X-Powered-By', 'PHP/5.2.17p1')]
- 22 => [ssh]; Ver => SSH-2.0-OpenSSH\_6.0p1 Debian-3ubuntu1

HIGH

### 1 OpenSSL TLS Memory Disclosure

- 66.228.

bugscan &gt; 插件编写教程

创建新主题


常见节点导航

插件编写 插件编写教程

插件 审核中插件

圈子 公告

bugscan圈子诞生了

 圈子新人必  
公告 • 半块西瓜皮 markdown  
公告 • 半块西瓜皮 rank评定  
公告 • 半块西瓜皮 Zoomla sea  
审核中插件 Z-blog前台  
上线的插件

精 BugScan插件编写教程 Ver 1.0

插件编写教程 • LinE • 1 周前 • 最后回复来自 嗯嗯呢

3



关于postgresql 弱口令检测的过程简单分享

插件编写教程 • 不流畅 • 1 月前 • 最后回复来自 半块西瓜皮

1



精 Bugscan插件编写高级教程之 service 识别

插件编写教程 • Medici\_Yan • 2 月前 • 最后回复来自 8790

8



BugScan插件编写的一些小技巧

插件编写教程 • LinE • 2 月前 • 最后回复来自 Secer

1



BugScan弱口令相关

插件编写教程 • 半块西瓜皮 • 2 月前 • 最后回复来自 半块西瓜皮

3



BugScan插件状态说明

插件编写教程 • LinE • 2 月前



BugScan插件编写高(gǎo)级(jī)教程

插件编写教程 • Medici\_Yan • 2 月前 • 最后回复来自 sharecast

12

瓜皮 ADMIN 管理

www.howmp.com

0

收藏

98

rank

互助

圈子bug反馈

上线的插件

半编写教程

下线的插件

## 圈子（社区）上线 Q.BugScan.net

业界第一个基于扫描框架和插件研究的圈子

2月5

## Bugscan正式上线

仅开放注册**1周**，注册人数突破**2000**

（之后为邀请码注册阶段）

4月1

插件由发布时的90个增长到500多个，注册人数增加到**8000**个

6月1

目前已扫描超过**100万**的目标，**600万余**条漏洞记录



<https://www.bugscan.net/>

---

**THANKS FOR YOUR WATCHING**