



建造插件众筹的分布式  
社区化漏洞扫描平台

「01」契机

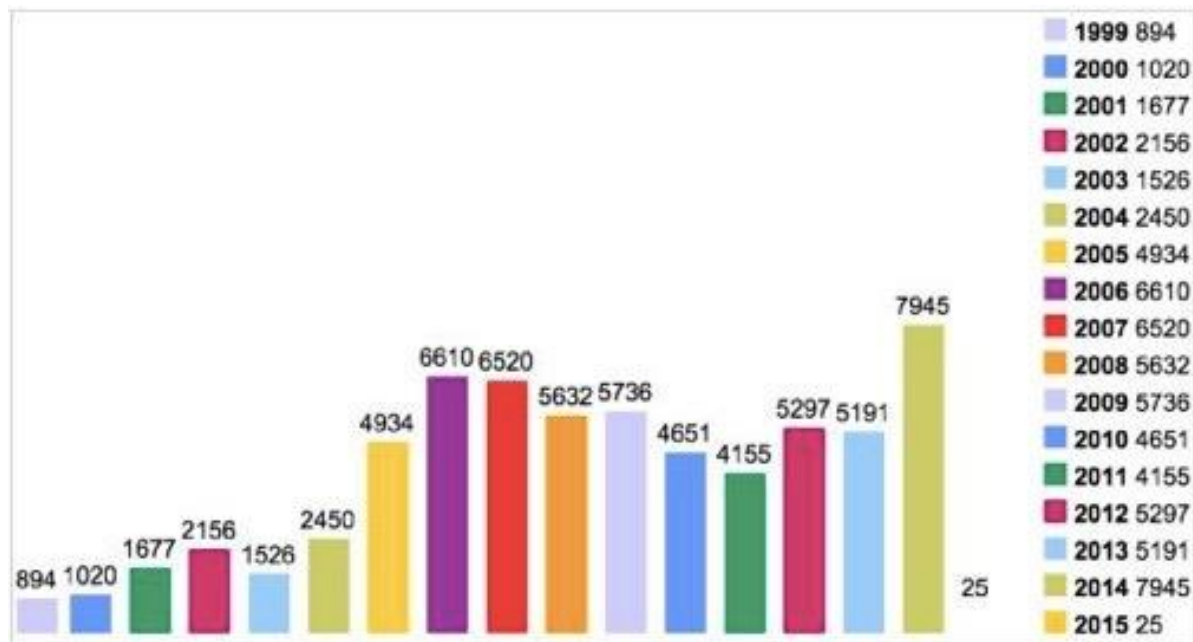
「02」团队

「03」功能

「04」特性

「05」优势

BugScan の 诞生五部曲



# The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular cryptographic software library. This weakness allows stealing of information protected, under normal conditions, by the SSL encryption used to secure the Internet. SSL/TLS provides security and privacy over the Internet for applications such as instant messaging (IM) and some virtual private networks.

The Heartbleed bug allows anyone on the Internet to reach the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify providers and to encrypt the traffic, the names and passwords of users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and impersonate services and users.

关于这个安全漏洞的细节可参看：CVE-2014-6271 和 CVE-2014-7169。

漏洞概况信息如下：

漏洞英文名称	Bash Shellshock
中文命名	破壳 (X-CERT)
威胁响应等级	A级
漏洞相关CVE编号	CVE-2014-6271
漏洞发现者	Stéphane Chazelas (法国)
漏洞发现事件	2014年9月中旬
漏洞公布时间	9月25日
漏洞影响对象	bash 1.14至bash 4.3的Linux/Unix系统

2014年9月，UNIX、Linux系统中广泛使用的Bash软件被曝出了一系列、已经存在数十年的漏洞（Bash或Shellshock），在业界引起了非常大的影响。

最初的bug已经修复了，但引发了人们对Bash的解析程序可能产生0day漏洞的关切，随后又挖掘出了第二个漏洞CVE-2014-7169，这个漏洞也在很快得到了修复。

不少Linux发行版本连夜发布了修复版本的Bash，在服务器领域占有不少份额的大多数FreeBSD和NetBSD已经默认关闭了自动导入函数的功能，以应对未来可能出现的漏洞。

在这个漏洞的风波逐渐平息之余，不少业内人士也在思考，它为何波及如此之广，影响如此之大。

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成员



四叶草安全  
CloverSec

cnfjhh

框架平台发起人

**13年**信息安全领域经验

专注于渗透测试方向

公司&团队负责人

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、Arpspoof  
等作品的作者

半块西瓜皮

BugScan扫描框架研发

7年以上二进制/逆向经验

4年以上python功底

熟悉各种漏洞原理  
插件圈子的作者

小武

BugScan延伸开发

**11年C++**开发经验

延伸新产品作者之一

不流畅

BugScan插件审核

5年以上固件研发经历

圈子插件审核员



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



# 功能

安全设备开始不安全



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®

# 特性

历时四年，五次重构

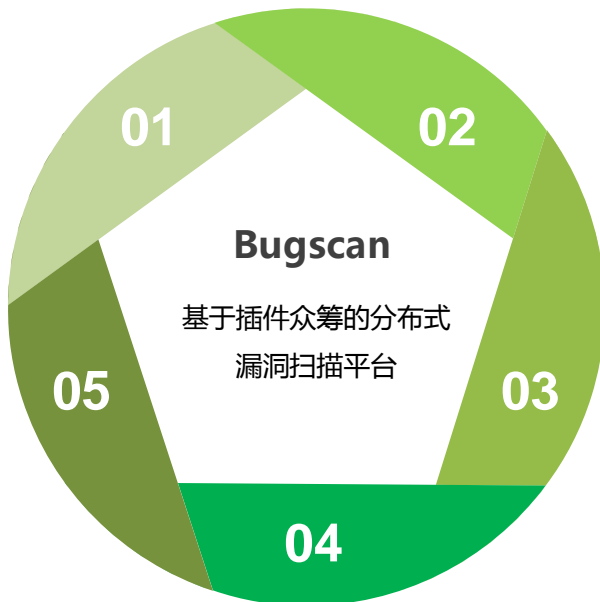


## 01.跨平台

核心扫描引擎使用python编写  
不受操作系统限制  
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  
由节点执行任务 无上限

## 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  
2005 - 2015

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

国外有Nessus、Metasploit 我们有BugScan

## 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



## ← 添加任务

任务名称扫描 (每行一个目标 比如: http://testphp.vulnweb.com/)

### 选项



爬虫

☐ 扫描子域名

☐ 深度端口扫描



全局

速度

超时时间

最大网页数



User Agent



用户名字典



密码字典



排除网页 ☐



Cookies

# 特性

## 云插件

### bash

```
def assign(service, arg):
    if service == "discuz":
        return True, arg

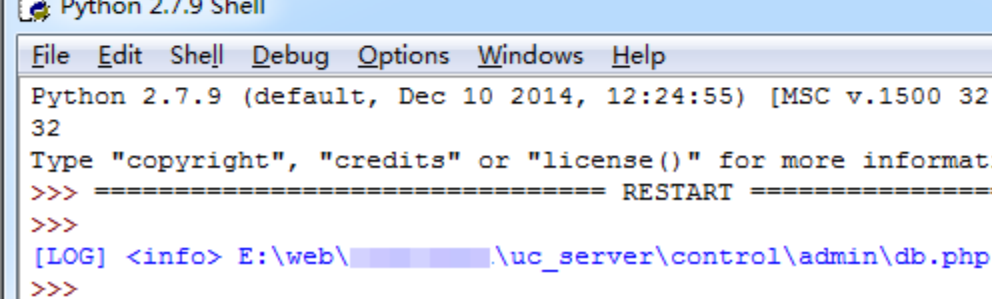
def audit(arg):
    url = arg
    code, head, res, errcode, _ = curl.curl2(url + 'uc_server/control/admin/db.php')
    if code == 200:
        m = re.search('not found in <b>([^\>]+)</b> on line <b>(\d+)</b>', res)
        if m:
            security_info(m.group(1))

if __name__ == '__main__':
    from dummy import *
    audit(assign('discuz', 'http://www.***.com.cn/')[1])
```

```
def audi
payl
code
if c

if __nam
from
audi

插件信息
```



# 特性

## 漏洞库

<https://www.bugscan.net/#!/x/19442>



### | OpenSSL TLS Heart

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

```
# Quick and dirty demonstra
# The author disclaims copy
```

```
import sys
import struct
import socket
import time
import select
import re
from optparse import Option
```

```
options = OptionParser(usag
options.add_option('-p', '-
```

```
def h2bin(x):
    return x.replace(' ', ' '
```

```
hello = h2bin(''
16 03 02 00 dc 01 00 00 d8
43 5b 90 9d 9b 72 0b bc 0c
bd 39 04 cc 16 0a 85 03 90
00 66 c0 14 c0 0a c0 22 c0
```

<https://www.bugscan.net/#!/x/20404>



### | BashedCgi Remote Command Execution

```
require 'msf/core'
```

```
class Metasploit3 < Msf::Auxiliary
```

```
    include Msf::Exploit::Remote::HttpClient
```

```
    def initialize(info = {})
```

```
        super(update_info(info,
```

```
            'Name' => 'bashedCgi',
```

```
            'Description' => %q{
```

```
                Quick & dirty module to send the BASH exploit payload (CVE-2014-6271) t
            },
```

```
            'Author' => [ 'Shaun Colley <scolley at ioactive.com>' ], # metasp
```

```
            'Author' => [ 'Stephane Chazelas' ], # vuln discovery
```

```
            'License' => MSF_LICENSE,
```

```
            'References' => [ 'CVE', '2014-6271' ],
```

```
            'Targets' =>
```

```
                [
                    [ 'cgi', {} ]
```

### 🏠🔍 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

#### 3 Sensitive File/Directory Discover

- [redacted]
- [redacted]
- [redacted]

#### 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

#### 1 .Net Sensitive Information Exposure

- [redacted]

#### 1 PPTP-Version

- [redacted]

LOW

#### 1 WebDAV Enabled

- [redacted]

#### 1 IIS Short File/Folder Name Disclosure

- [redacted]

HIGH

#### 1 ASP.NET Padding Oracle Vulnerability

- [redacted]

#### 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. [redacted] /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. [redacted]

INFO

### 🏠🔍 扫描记录

http://66.228. [redacted] / 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. [redacted]

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. [redacted]

# 优势

圈子是what?



bugscan > 插件编写教程

创建新主题



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



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

0



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

西瓜皮 [ADMIN](#) 管理

[/www.howmp.com](#)

5 0 98

收藏 rank

写互助 圈子bug反馈

上线的插件

插件编写教程

下线的插件



# 优势

## 对漏洞插件进行探讨和交流



BUGSCAN

大事记 贡献榜 扫描器

### ProFTPD 未授权文件复制 CVE-2015-3306

上线的插件 · ArchStacker · 发表于 1 周前 · 最后回复来自 半块西瓜皮 · 1 周前

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
#__Author__ = 'ArchStacker'
#_PlugName_ = ProFTPD_mod_copy
#_FileName_ = ProFTPD_mod_copy.py
"""
reference:
    bugs.proftpd.org/show_bug.cgi?id=4169
    http://www.beebeeto.com/pdb/poc-2015-0088/
"""
import socket

def assign(service, arg):
    if service == "ftp":
        return True, arg

def audit(arg):
    ip,port = arg
    try:
        s = socket.socket()
        s.connect((ip,port))
        s.recv(1024)
        s.send("SITE CPFR /etc/passwd\r\n")
        data = s.recv(1024)
        if '350' in data:
            security_hole("%s:%d" % (ip,port))
        s.close()
    except:
        pass
```

```
except:
    pass

if __name__ == '__main__':
    from dummy import *
    audit(assign('ftp', ('http://www.example.com/',21))[1])
```

加入收藏 新浪微博 顶0 踩0 rank 14

74 次点击 返回扫描器查看

共收到3条回复



ArchStacker ☆路人 1 周前

#1

之前有过这个漏洞的插件：ProFTPD 未授权文件复制CVE-2015-3306

但之前的代码是不可用的，不能检测出有问题的网站。代码中有几个问题：

- 1.第四次tel\_conn.write的时候应为tel\_conn.write(site cpto test@x5tTxil \n)，原插件中这里忘了加\n，因为这个问题导致后面的操作全部出错，得不到正确的结果
- 2.上面的'test@x5tTxil'应该换为一个肯定可写的地址，如/tmp/a.txt，否则的话有可能本来有漏洞但这里提示没有权限
- 3.其实压根就不用这么麻烦，直接判断能不能打开/etc/passwd就好了

因为有这么多问题，所以我又写了一遍这个插件

写的时候代码参考的这个：mongodb 未授权访问



ArchStacker ☆路人 1 周前

#2

@半块西瓜皮 之前不能用的插件都能加精，我这同一个漏洞的插件难道不应该加精鼓励一下吗？之前那个插件到现在Hits还是1，我这个上线1天Hits就是9了



半块西瓜皮 (ADMIN) 管理 1 周前

#3

@ArchStacker 是的，感谢细心发现问题

创建新的回复

A

B

I

≡

💬

🌐

✉

📷

👁

回复内容

# 圈子模式开启了

圈子（社区）核心成员

## L1nE

编程功底扎实，熟悉各种漏洞原理

## 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

## 星光点亮天

实时跟踪各种主流社区漏洞，能第一时间写成漏洞插件

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  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 xxxxxxx	79
10		不流畅  审核 暂无签名	78

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

---

WHAT ARE YOU 弄啥嘞?