最好用的开源Web漏扫工具梳理 - FreeBuf互联网安全新媒体平台

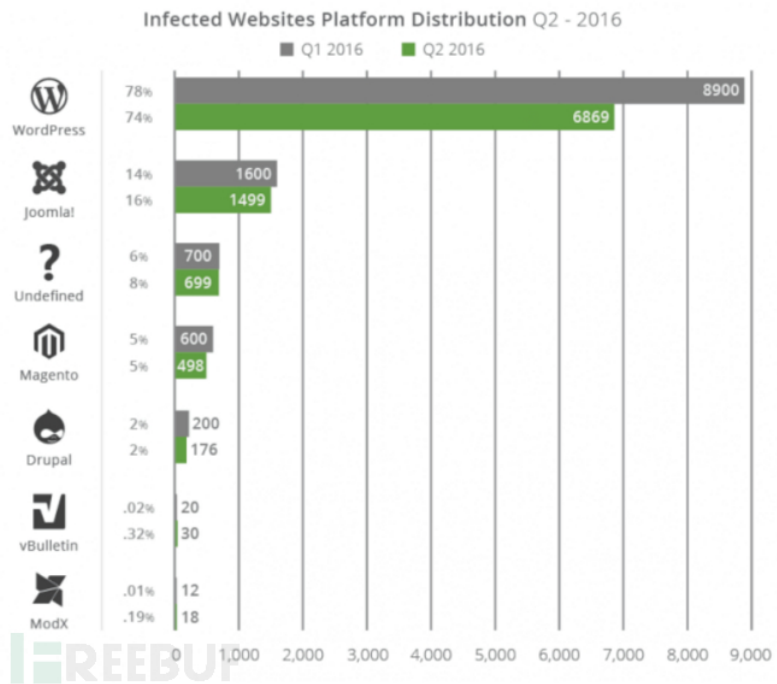
freebuf.com/articles/web/155209.html

最好用的开源Web漏扫工具梳理

柚子 2017-12-02 共**1130599**人围观 ， 发现 **9** 个不明物体 WEB安全

***本文中涉及到的相关漏洞已报送厂商并得到修复，本文仅限技术研究与讨论，严禁用于非法用途，否则产生的一切后果自行承担。**

赛门铁克2017年互联网安全威胁报告中提出在他们今年扫描的网站中，有76%都含有恶意软件。如果你在用WordPress，SUCURI的另一份报告也显示，超过70%的被扫描网站也都存在一个或多个漏洞。



如果你刚好是某个网络应用程序的所有者，怎样才能保证你的网站是安全的、不会泄露敏感信息?

如果是基于云的安全解决方案，那么可能只需要进行常规漏扫。但如果不是，我们就必须执行例行扫描，采取必要的行动降低安全风险。

当然很多付费扫描器功能会更加全面、严谨，包含报表输出、警报、详细的应急指南等等附加功能。

开源工具最大的缺点是漏洞库可能没有付费软件那么全面。

1. Arachni

Arachni是一款基于Ruby框架搭建的高性能安全扫描程序，适用于现代Web应用程序。可用于Mac、Windows及Linux系统的可移植二进制文件。

Arachni不仅能对基本的静态或CMS网站进行扫描，还能够做到对以下平台指纹信息（(硬盘序列号和网卡物理地址)）的识别。且同时支持主动检查和被动检查。

> Windows、Solaris、Linux、BSD、Unix
>
> Nginx、Apache、Tomcat、IIS、Jetty
>
> Java、Ruby、Python、ASP、PHP
>
> Django、Rails、CherryPy、CakePHP、ASP.NET MVC、Symfony

一般检测的漏洞类型包括：

> NoSQL/Blind/SQL/Code/LDAP/Command/XPath注入
>
> 跨站请求伪造
>
> 路径遍历
>
> 本地/远程文件包含
>
> Response splitting
>
> 跨站脚本
>
> 未验证的DOM重定向
>
> 源代码披露

另外，你可以选择输出HTML、XML、Text、JSON、YAML等格式的审计报告。

Arachni帮助我们以插件的形式将扫描范围扩展到更深层的级别。Arachni的详细介绍与下载地址：click here。

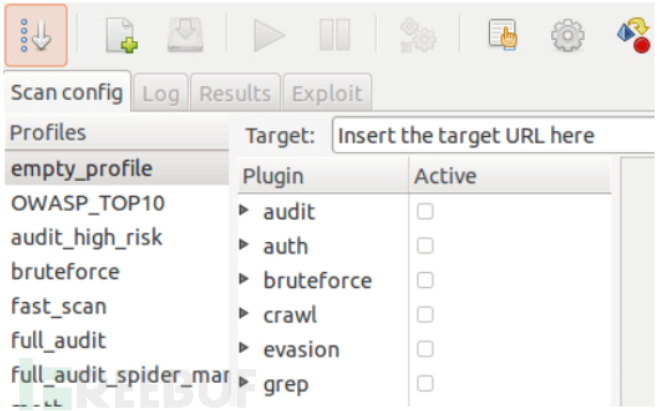
2. XssPy

一个有力的事实是，微软、斯坦福、摩托罗拉、Informatica等很多大型企业机构都在用这款基于python的XSS（跨站脚本）漏洞扫描器。它的编写者Faizan Ahmad才华出众，XssPy是一个非常智能的工具，不仅能检查主页或给定页面，还能够检查网站上的所有链接以及子域。因此，XssPy的扫描非常细致且范围广泛。

下载地址：click here。

3. w3af

w3af是一个从2006年年底开始的基于Python的开源项目，可用于Linux和Windows系统。w3af能够检测200多个漏洞，包括OWASP top 10中提到的。



w3af能够帮你将payload注入header、URL、cookies、字符串查询、post-data等，利用Web应用程序进行审计，且支持各种记录方法完成报告，例如：

> CSV
>
> HTML
>
> Console
>
> Text
>
> XML
>
> Email

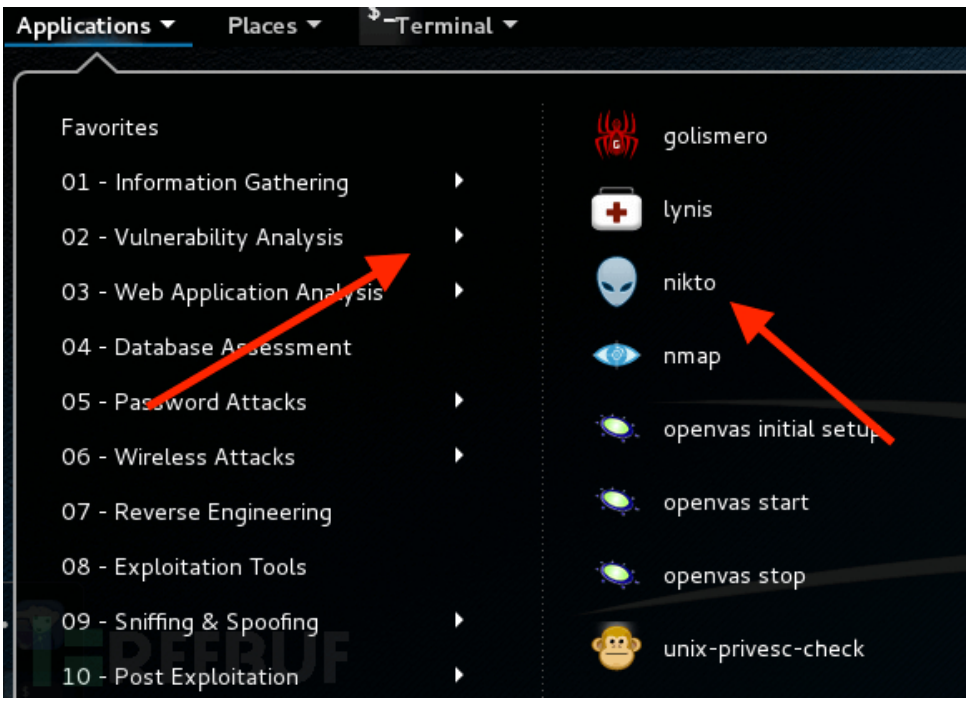
这个程序建立在一个插件架构上，所有可用插件地址：click here。

w3af下载地址：click here。

4. Nikto

相信很多人对Nikto并不陌生，这是由Netsparker（专做web安全扫描器企业，总部坐标英国）赞助的开源项目，旨在发现Web服务器配置错误、插件和Web漏洞。Nikto对6500多个风险项目进行过综合测试。支持HTTP代理、SSL或NTLM身份验证等，还能确定每个目标扫描的最大执行时间。

Nikto也适用于Kali Linux。



Nikto在企业内部网络解决方案中查找web服务器安全风险的应用前景非常广阔。

下载地址：click here。

5. Wfuzz

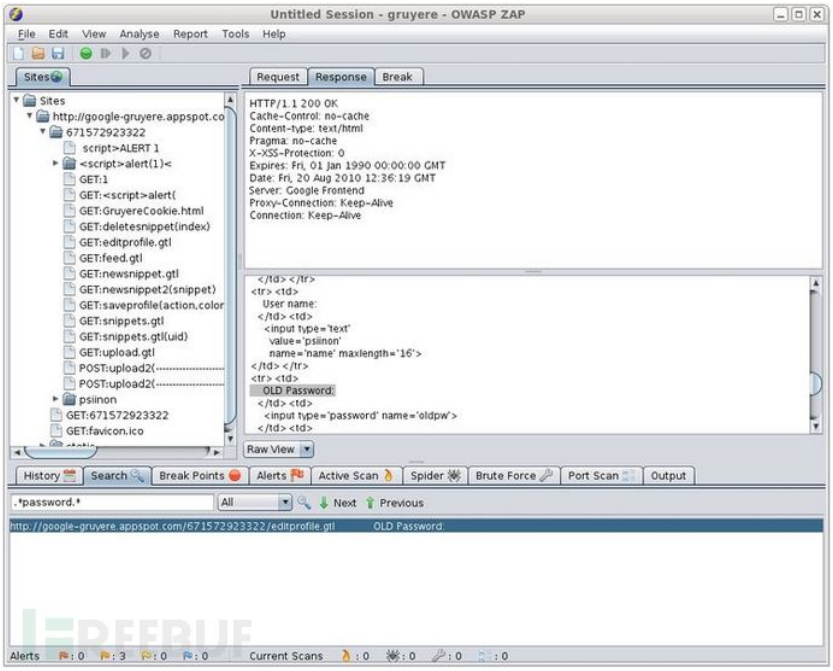
Wfuzz（Web Fuzzer）也是渗透中会用到的应用程序评估工具。它可以对任何字段的HTTP请求中的数据进行模糊处理，对Web应用程序进行审查。

Wfuzz需要在被扫描的计算机上安装Python。具体的使用指南可参见这个：链接。

Wfuzz下载地址：click here。

6. OWASP ZAP

ZAP（Zet Attack Proxy）是全球数百名志愿者程序员在积极更新维护的著名渗透测试工具之一。它是一款跨平台的Java工具，甚至都可以在Raspberry Pi上运行。ZAP在浏览器和Web应用程序之间拦截和检查消息。



ZAP值得一提的优良功能：

> Fuzzer
>
> 自动与被动扫描
>
> 支持多种脚本语言
>
> Forced browsing（强制浏览）

下载地址：click here。

7. Wapiti

Wapiti扫描特定的目标网页，寻找能够注入数据的脚本和表单，从而验证其中是否存在漏洞。它不是对源代码的安全检查，而是执行黑盒扫描。

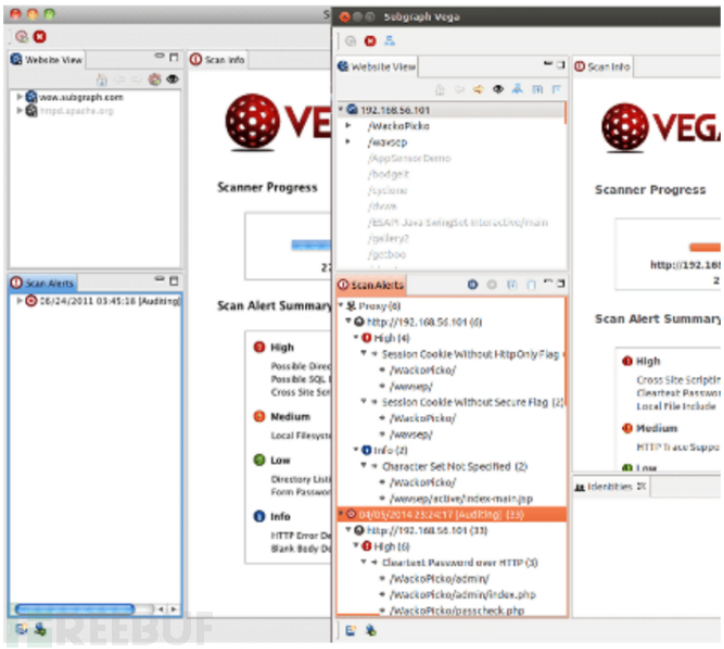
支持GET和POST HTTP请求方式、HTTP和HTTPS代理以及多个认证等。

下载地址：click here。

8. Vega

Vega由Subgraph开发，Subgraph是一个用Java编写的多平台支持工具，用于查找XSS，SQLi、RFI和很多其它的漏洞。

Vega的图形用户界面相对来说比较美观。它可以通过特定的凭证登录某个应用后执行自动扫描。



如果你懂开发，还可以利用vega API创建新的攻击模块。

下载地址：click here。

9. SQLmap

顾名思义，我们可以借助sqlmap对数据库进行渗透测试和漏洞查找。

支持所有操作系统上的Python 2.6或2.7。如果你正在查找SQL注入和数据库漏洞利用，sqlmap是一个好助手。

下载地址：click here。

10. Grabber

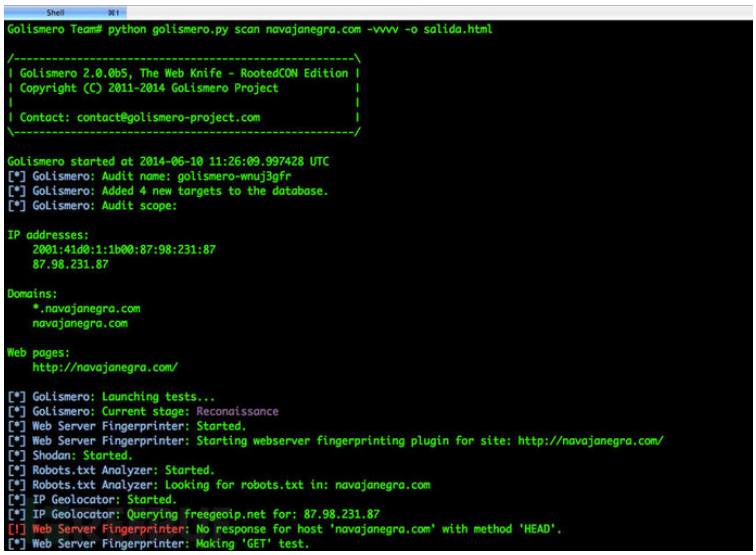
这也是一个做得不错的Python小工具。这里列举一些特色功能：

> JavaScript源代码分析器
>
> 跨站点脚本、SQL注入、SQL盲注
>
> 利用PHP-SAT的PHP应用程序测试

下载地址：click here。

11. Golismero

这是一个管理和运行Wfuzz、DNS recon、sqlmap、OpenVas、机器人分析器等一些流行安全工具的框架。

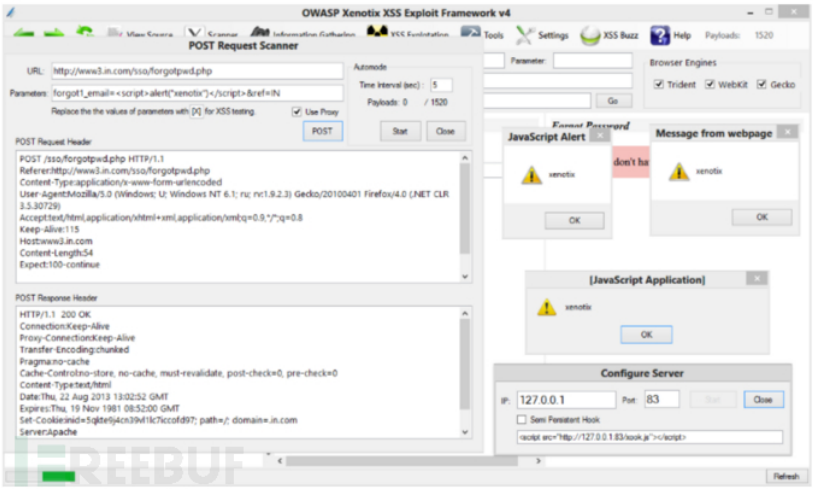


Golismero非常智能，能够整合其它工具的测试反馈，输出一个统一的结果。

下载地址：click here。

12. OWASP Xenotix XSS

OWASP的Xenotix XSS是一个用于查找和利用跨站点脚本的高级框架，内置了三个智能模糊器，用于快速扫描和结果优化。



这款工具有上百个功能，详细的功能列表与下载地址：click here。

网络安全对于在线业务至关重要，希望上面这些免费的漏扫程序能够帮助各位读者及时发现风险，在被恶意人员利用之前即完成漏洞修复。

***参考来源：geekflare，FB小编柚子编译，转载请注明来自FreeBuf.COM**

更多精彩 # 开源 # 漏洞
柚子 *21* 篇文章 等级： *5*级
|

|

- 上一篇：血淋林的例子告诉你，为什么防“上传漏洞”要用白名单
- 下一篇： 注意了，使用XSS平台的你可能被“偷窥”