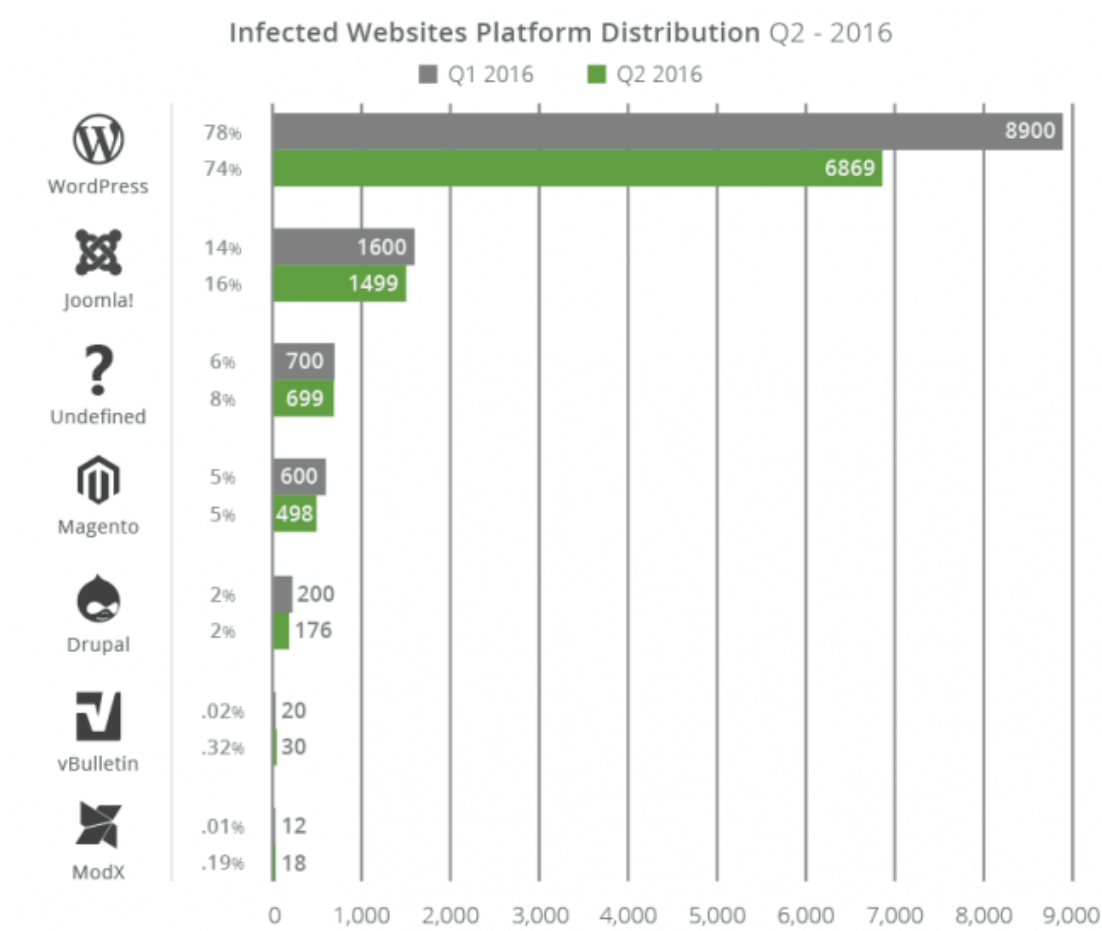


开源 Web 安全扫描程序来查找漏洞

赛门铁克的一个有趣的报告显示，76%的被扫描网站有恶意软件



如果您使用的是 WordPress，那么 SUCURI 的另一份报告显示，超过 70% 的被扫描网站被感染了一个或多个漏洞。



作为网络应用程序所有者，您如何确保您的网站免受在线威胁的侵害？不泄

露敏感信息？

如果您正在使用基于云的安全解决方案，则最有可能定期进行漏洞扫描是该计划的一部分。但是，如果没有，那么你必须执行例行扫描，并采取必要的行动来降低风险。

有两种类型的扫描软件

商业(收费) - 给你一个选项来自动扫描持续的安全，报告，警报，详细的缓解说明等，行业中的一些已知的厂商是：

Acunetix

Detectify

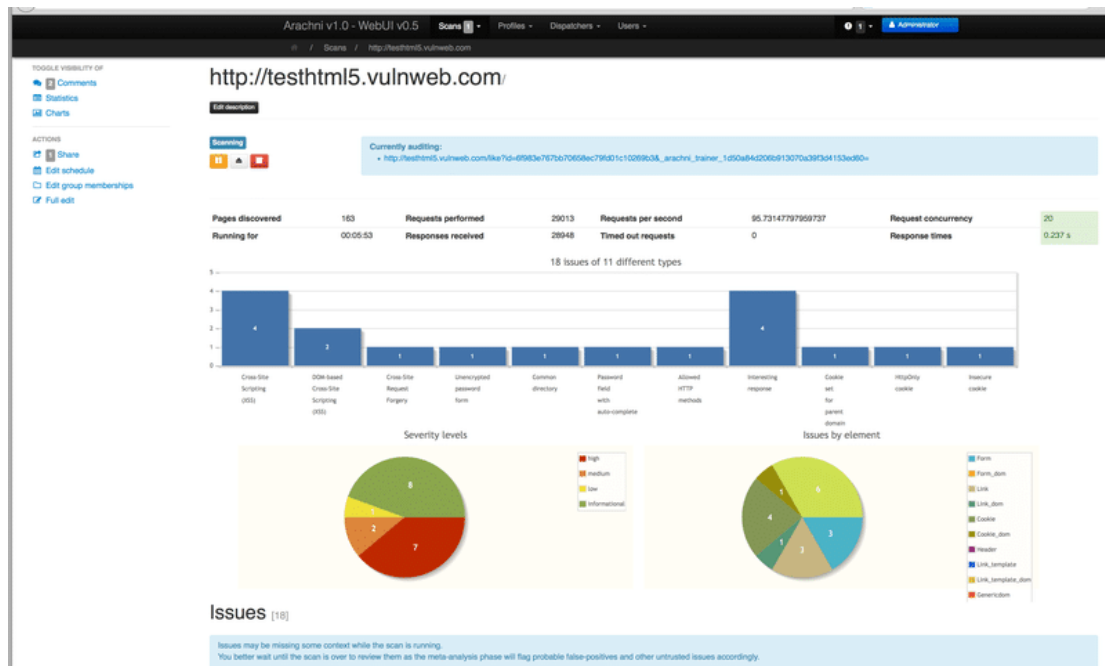
Qualys

开源/免费 - 您可以下载并按需执行安全扫描。但不能够覆盖所有漏洞，如商业漏洞。

看看下面的开源 Web 漏洞扫描器

1. Arachni

Arachni 是一款基于 Ruby 框架构建的高性能安全扫描程序，适用于现代 Web 应用程序。它可用于 Mac，Windows 和 Linux 的便携式二进制文件



Arachnin 能适用于下面的平台和语言

Windows, Solaris, Linux, BSD, Unix

Nginx, Apache, Tomcat, IIS, Jetty

Java, Ruby, Python, ASP, PHP

Django, Rails, CherryPy, CakePHP, ASP.NET MVC, Symfony

漏洞检测有下面这些:

NoSQL/Blind/SQL/Code/LDAP/Command/XPath injection

Cross-site request forgery

Path traversal

Local/Remote File inclusions

Response splitting

Cross-site scripting

Unvalidated DOM redirects

Source code disclosure

可以选择使用 HTML, XML, 文本, JSON, YAML 等格式的审计报告,Arachni 可以利用插件将扫描范围扩展到下一个级别

2. XssPy

一个基于 Python 的 XSS (跨站脚本) 漏洞扫描器

3. w3af

w3af,从 2006 年开始使用 python 开发的开源项目, 可以用在 window 和 linux 环境下,

w3af 可以将有效载荷注入到标题, URL, cookie, 查询字符串, 后期数据等, 以利用 Web 应用程序进行审计。它支持各种记录方法进行报告。例如:

CSV

HTML

Console

Text

XML

Email

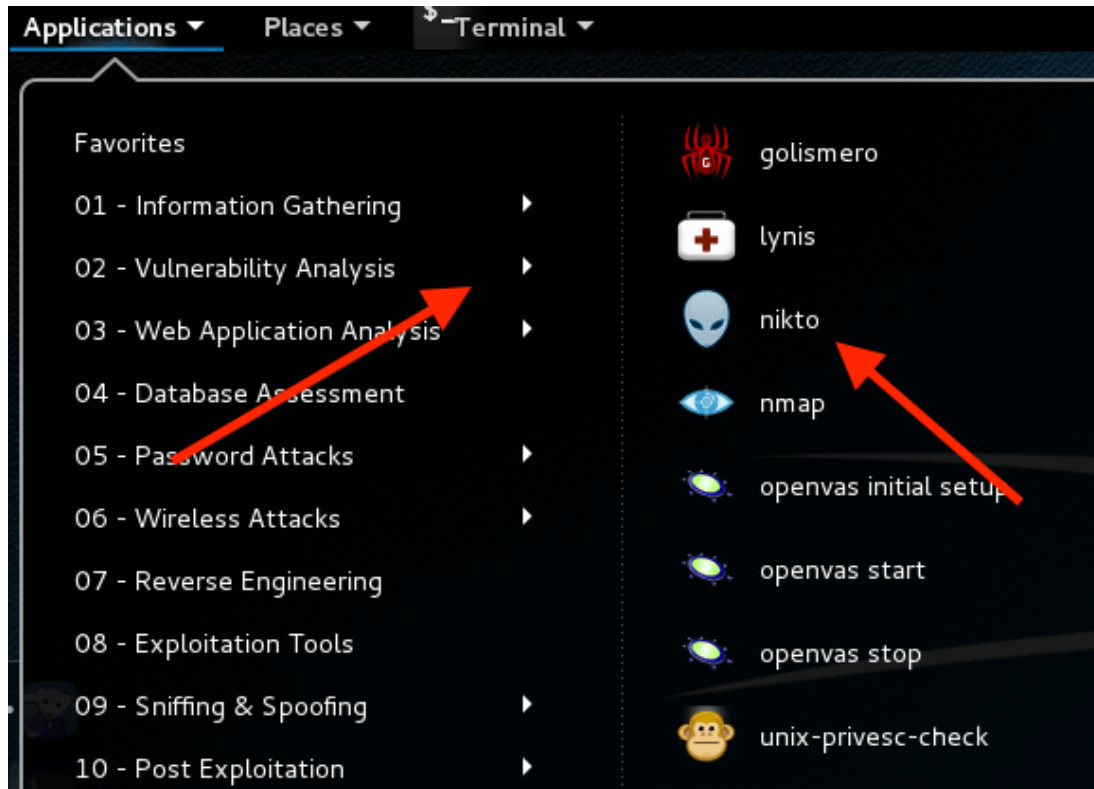
更多的功能可利用插件库

4. Nikto

Netsparker 赞助的开源项目旨在发现 Web 服务器的配置错误, 插件和网页漏洞。 Nikto 对 6500 多个风险项目进行综合测试。

它支持 HTTP 代理, SSL, 或 NTLM 身份验证等, 并可以定义每个目标扫描的最大执行时间。

Nikola 也可以在 Kali Linux 中使用



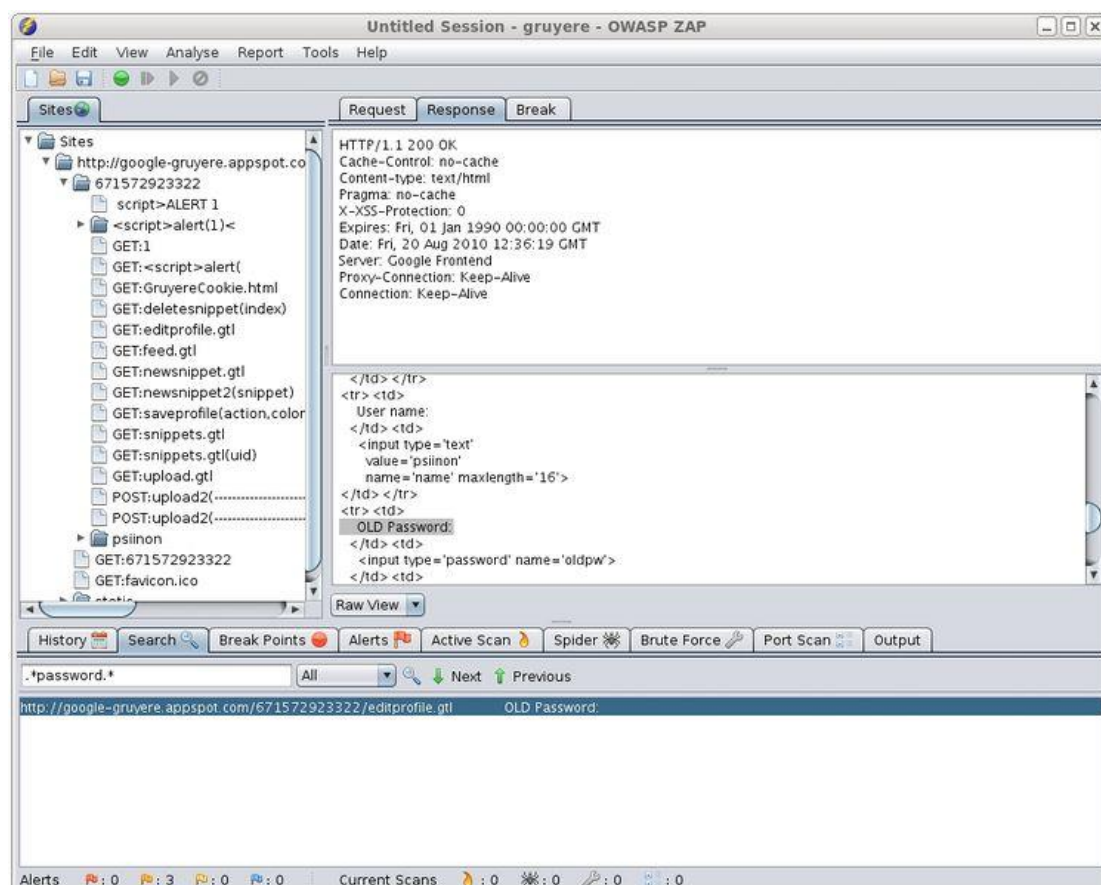
它看起来很有希望用于 Intranet 解决方案来查找 Web 服务器的安全风险

5. Wfuzz

Wfuzz (Web Fuzzer) 是针对渗透测试的应用程序评估工具。您可以对任何字段的 HTTP 请求中的数据进行模糊处理，以利用该 Web 应用程序并审核 Web 应用程序。 Wfuzz 需要在要运行扫描的计算机上安装 Python。

6. OWASP ZAP

ZAP (Zet Attack Proxy) 是全球数百名志愿者积极更新的著名渗透测试工具之一。它是跨平台的基于 Java 的工具，可以在 Raspberry Pi 上运行。ZIP 位于浏览器和 Web 应用程序之间，用于拦截和检查消息



下面的一些值得一提的是 ZAP 的功能。

Fuzzer

Automated & passive scanner

Supports multiple scripting languages

Forced browsing

强烈建议查看 OWASP ZAP 教程视频来学习

7. Wapiti

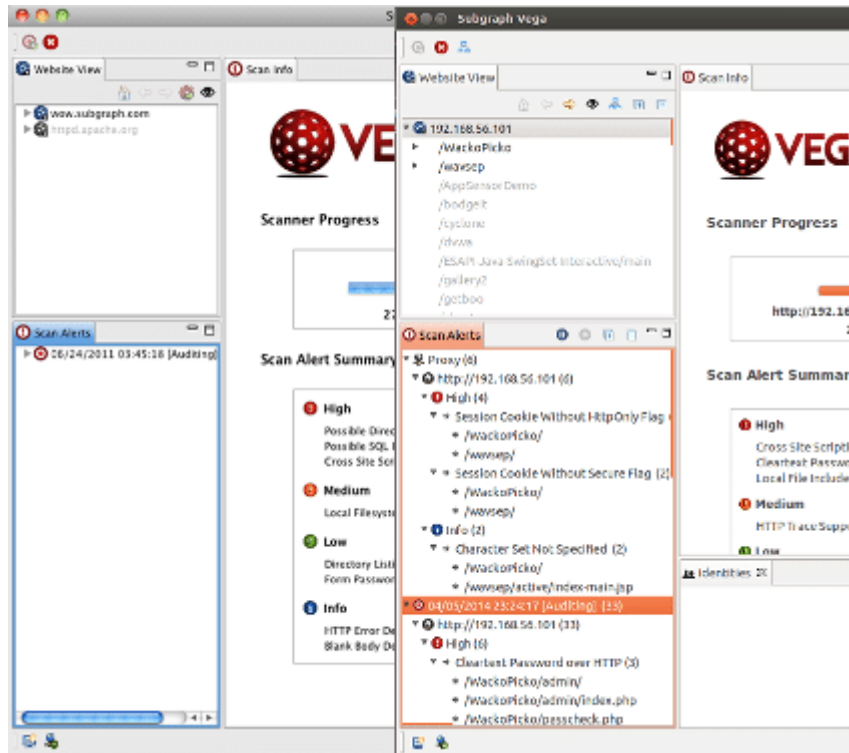
Wapiti 扫描给定目标的网页，并寻找脚本和表单来注入数据，看看是否有漏洞。它不是一个源代码安全检查，而是执行黑盒扫描。



它支持 GET 和 POST HTTP 方法，HTTP 和 HTTPS 代理，多个认证等。

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 和许多其他漏洞。维加有良好的图形用户界面，并能够通过登录到具有给定凭据的应用程序来执行自动扫描。



如果您是开发人员，则可以利用 vega API 创建新的攻击模块

9. SQLmap

利用 SQLmap 可以对数据库执行渗透测试来发现缺陷。

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
{1.0.5.63#dev}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is
illegal. It is the end user's responsibility to obey all applicable local, state and fed
eral laws. Developers assume no liability and are not responsible for any misuse or damage
caused by this program

[*] starting at 17:43:06

[17:43:06] [INFO] testing connection to the target URL
[17:43:06] [INFO] heuristics detected web page charset 'ascii'
[17:43:06] [INFO] testing if the target URL is stable
[17:43:07] [INFO] target URL is stable
[17:43:07] [INFO] testing if GET parameter 'id' is dynamic
[17:43:07] [INFO] confirming that GET parameter 'id' is dynamic
[17:43:07] [INFO] GET parameter 'id' is dynamic
[17:43:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
(possible DBMS: 'MySQL')
```

它适用于任何操作系统上的 Python 2.6 或 2.7。如果你正在寻找 SQL 注入和利用数据库，那么 sqlmap 会有帮助。

10. Grabber

它是基于 Python 的小工具，并且做得很不错。一些 Grabber 的功能是：

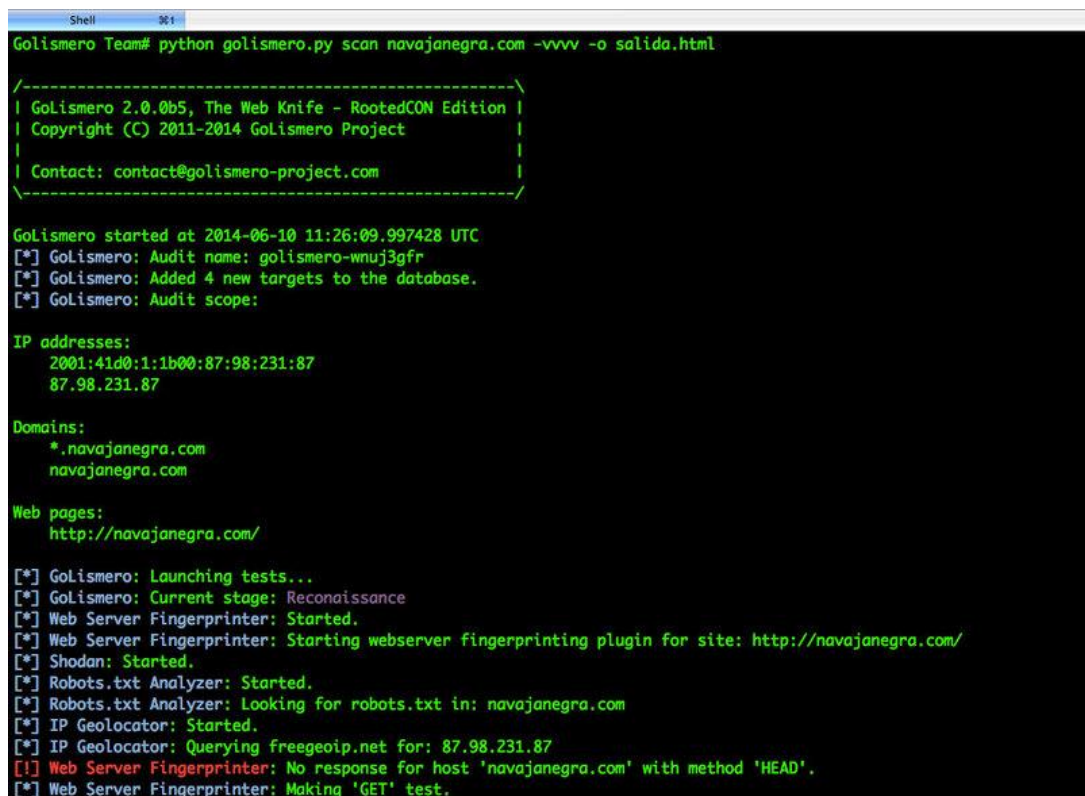
JavaScript 源代码分析器 跨站点脚本，

SQL 注入，

盲注 SQL PHP 应用程序测试使用 PHP-SAT

11. Golismero

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。



```
Shell 001
Golismo Team# python golismero.py scan navajanegra.com -vvvv -o solida.html

/-----\
| Golismero 2.0.0b5, The Web Knife - RootedCON Edition |
| Copyright (C) 2011-2014 Golismero Project           |
|                                                     |
| Contact: contact@golismero-project.com             |
\-----/

Golismero started at 2014-06-10 11:26:09.997428 UTC
[*] Golismero: Audit name: golismero-wnuj3gfr
[*] Golismero: Added 4 new targets to the database.
[*] Golismero: Audit scope:

IP addresses:
    2001:41d0:1:1b00:87:98:231:87
    87.98.231.87

Domains:
    *.navajanegra.com
    navajanegra.com

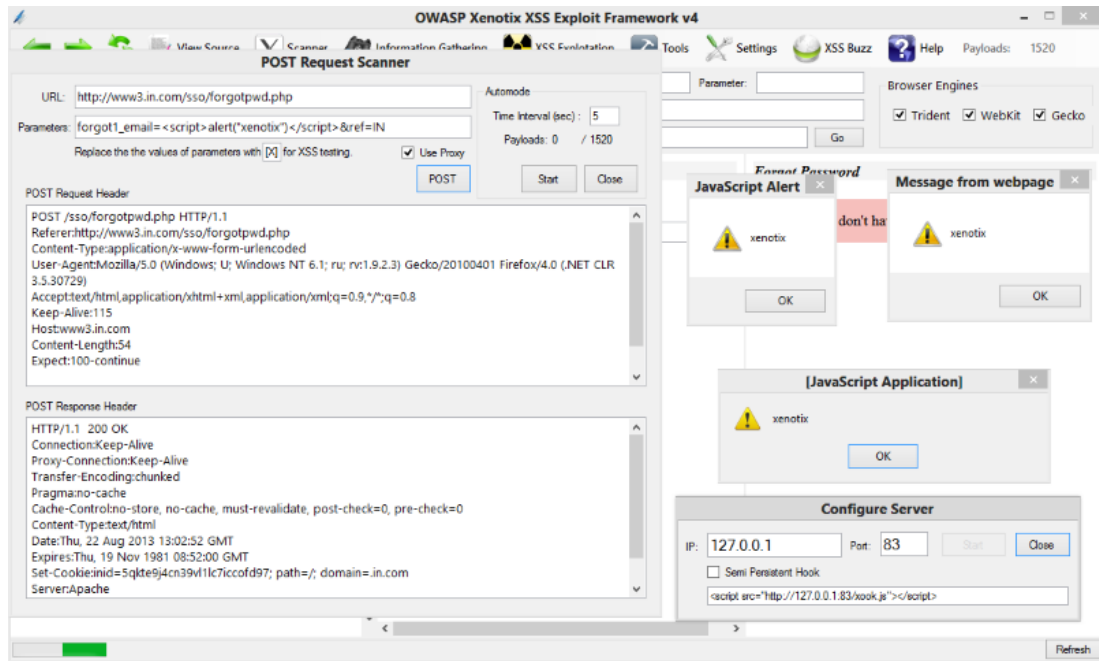
Web pages:
    http://navajanegra.com/

[*] Golismero: Launching tests...
[*] Golismero: Current stage: Reconnaissance
[*] Web Server Fingerprinter: Started.
[*] Web Server Fingerprinter: Starting webserver fingerprinting plugin for site: http://navajanegra.com/
[*] Shodan: Started.
[*] Robots.txt Analyzer: Started.
[*] Robots.txt Analyzer: Looking for robots.txt in: navajanegra.com
[*] IP Geolocator: Started.
[*] IP Geolocator: Querying freegeoip.net for: 87.98.231.87
[!] Web Server Fingerprinter: No response for host 'navajanegra.com' with method 'HEAD'.
[*] Web Server Fingerprinter: Making 'GET' test.
```

Golismero 非常棒，它可以巩固来自其他工具的测试反馈，并合并显示一个单一的结果。

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。它内置了三个智能模糊器，用于快速扫描和改进结果。



它有数百个功能，我们可以看看这里列出的所有。

网络安全对于在线业务至关重要，我希望上面列出的免费/开源漏洞扫描程序可以帮助您找到风险，以便在有人利用此漏洞之前减轻风险