【非原创】渗透测试标准

monika / 2017-06-06 03:02:48 / 浏览数 6157 安全技术 技术讨论 顶(0) 踩(0)

渗透测试标准

Web漏洞检测表

1 收集web相关信息，开放端口信息，服务信息等。

2 严禁增/删/改防火墙iptables，私自开通高危端口。

3 检查Flash跨域策略文件crossdomain.xml是否合法。

4 检查是否有CSRF漏洞,(根据系统条件进行检测)。

5
信息泄露漏洞安全性检查（例如test.cgi、phpinfo.php、info.php、.svn/entries、HTTP认证泄漏漏洞、管理后台泄漏漏洞、内网信息泄漏漏洞、错误详情信息泄漏等）。

6 检查是否有XSS漏洞（不合法的参数不能在页面原样返回，特别是openid/openkey）。

7 检查是否泄漏后台默认文件漏洞。

8 检查Flash跨域策略文件的安全性。避免Flash注入javascript或者actionscript脚本在浏览器或者flash中执行跨站攻击。

9 Cookie安全性检查。

10 检查是否有跳转漏洞。

11 检查是否有Header注入漏洞。

12 检查是否有源代码泄漏漏洞或者备份文件。

13 检查是否有Frame-proxy攻击漏洞。

14 检查是否有SQL注入攻击漏洞。

15 检查是否有并发漏洞。

16 敏感信息检查。应用需要对可能造成客户的敏感内容，以及用户生成内容（UGC，由用户发表的言论）进行检查和过滤。

17 检查通过WEB页面发起的临时会话窗口的所有显示内容。

18 目录浏览漏洞安全性检查。

19 检查是否泄漏员工电子邮箱漏洞以及分机号码。

20 查看是否有验证码机制，以及验证码机制是否完善。

21 检查用户名是否可进行枚举。

22 检测网站路径中是否存在robots.txt。

23 检查是否部署了Web服务器的控制台，控制台是否存在默认帐号、口令，是否存在弱口令。

24 检查网站目录是否可列。

25 检测目标认证系统是否存在绕过的可能，未授权访问等。

26 检测网站登录后修改密码是否存在缺陷。

27 检测Web程序在处理登录过程中用户名和口令的传输是否采用了加密传输的机制。

28 检测弱口令，web控制台，数据库，ftp，ssh，telnet，操作系统等。

29 检测是否提供注销登陆功能，或者退出后session自动失效。

30 检测是否存在浏览器窗口闲置超时后需重新登录的机制。

31 检测页面中是否存在的横向越权（水平越权）操作。

32 检测应用中存在的URL是否存在纵向越权（垂直越权）操作。

33 检测是否存在任意文件上传漏洞，并且是否可以解析相关木马文件。

34 检测是否存在任意下载，遍历下载系统或者web内的文件。

35 检测Web网站在处理用户提交的不存在的URL时会返回错误信息，是否可通过返回的错误信息来确认有敏感信息的泄漏问题。

36 检测是否存在遗留的测试页面。

37 检测是否会在本地存储不安全的敏感文件。

38 检测是否存在命令执行漏洞。

39 检测逻辑上的安全问题，是否存在篡改。

40 检测是否可通过搜索引擎进行信息收集。

认证和授权类

1 密码明文传输。

2 用户名枚举。

3 暴力攻击。

4 会话标示未更新。

5 未授权访问。

6 文件上传漏洞。

7 任意文件下载。

8 脆弱的SSL算法。

9 越权访问。

命令执行类

1 Struts2 远程命令执行。

2 Jboss远程命令执行。

3 HTTP.sys远程代码执行漏洞。

4 文件包含。

逻辑攻击类

1 验证码功能缺陷。

2 并发漏洞。

3 Slow Http attack、慢速攻击。

4 短信攻击。

注入攻击类

1 SQL注入。

2 XML注入。

3 CRLF注入。

4 XFF注入。

5 XPATH注入。

6 命令注入。

7 连接或框架注入。

8 Json劫持漏洞。

9 宽字节注入。

客户端攻击类

1 XSS跨站脚本漏洞。

2 跨站伪造请求（CSRF）。

3 不安全的HTTP方法。

信息泄露类

1 目录遍历。

2 Web容器控制台地址泄漏。

3 PHPInfo()信息泄漏。

4 POODLE信息泄露漏洞。

5 SVN信息泄露。

6 备份文件泄露。

7 内网IP地址泄露。

8 Cookie信息泄露。

9 异常信息泄露。

10 敏感信息泄露。

11 IIS断文件名泄露。

12 Robots文件信息泄露。

其他类型

1 跨域访问漏洞。

2 URL重定向。

3 DNS域传送漏洞。

4 开放多余端口。

5 PHP multipart/form-data。

6 . ASP.NET Padding Oracle攻击。

7 HTTP Host头攻击。

8 SSRF攻击。

9 TLS1/SSLv3 重协商漏洞。

10 Web服务器解析漏洞。

附录

Web安全常见检测工具

1 APPScan：IBM Rational AppScan，在Web安全测试中所使用的自动化扫描工具。

2 WVS：Acunetix WVS Reporter 自动化的Web应用程序安全测试工具。

3 Netsparker：一款综合型的web应用安全漏洞扫描工具。

4 Httprint：Web服务器类型和版本的探测工具。

5 Sqlmap：SQL注入测试工具。

6 WireShark：网络协议抓包与分析工具。

7 Burp suite：神器，可以对浏览器与Web服务器之间的通信数据进行编辑修改。

8 Nmap：端口扫描，服务识别，操作系统指纹识别。

9 NetCat：端口连接，数据提交。

10 Tamper IE：HTTP数据包修改、转发工具（Firefox插件）。

11 Fiddler：Http协议调试代理工具。

12 Firefox/Chrome渗透测试插件推荐

firefox一直是各位渗透测试必备的利器，这里整理了34款Firefox插件和几款Chrome的插件，其中包含渗透测试、信息收集、代理、加密解密等功能。

Firefox插件

1 Firebug

Firebug

addon-1843-latest.xpi

Firefox的 五星级强力推荐插件之一

2 User Agent Switcher

User Agent Switcher

addon-59-latest.xpi

改变客户端的User Agent的一款插件

3 Hackbar

https://addons.mozilla.org/en-US/firefox/addon/hackbar/

https://addons.cdn.mozilla.net/user-media/addons/3899/hackbar-1.6.3-fx.xpi?filehash=sha256%3Ad339ec8e4c0862d932ee85f556bfd60d53dc10360d4fad769

攻城师们的必备工具，提供了SQL注入和XSS攻击，能够快速对字符串进行各种编码。

4 HttpFox

https://addons.mozilla.org/en-US/firefox/addon/httpfox/

https://addons.cdn.mozilla.net/user-media/addons/6647/httpfox-0.8.14-fx+sm.xpi?filehash=sha256%3Aa6699e588581cc5707c34278cbee32af249435ccb0303

监测和分析浏览器与web服务器之间的HTTP流量

5 Live HTTP Headers

https://addons.mozilla.org/en-US/firefox/addon/live-http-headers/

https://addons.cdn.mozilla.net/user-media/addons/3829/live_http_headers-0.17-fx+sm.xpi?filehash=sha256%3A335d8fed0d09475413e9148b6f9b95683959ff

即时查看一个网站的HTTP头

6 Tamper Data

https://addons.mozilla.org/en-US/firefox/addon/tamper-data/

https://addons.cdn.mozilla.net/user-media/addons/966/tamper_data-11.0.1-fx.xpi?filehash=sha256%3A4f0303b8685b2b190d011ed1329cdf7f351b0b3bc9c43

查看和修改HTTP/HTTPS头和POST参数

7 ShowIP

https://addons.mozilla.org/en-US/firefox/addon/showip/

https://addons.cdn.mozilla.net/user-media/addons/590/showip-2.7.7-sm+tb+fx.xpi?filehash=sha256%3Ae93e1f90f06b61d53bb8dd70cc9dcfae7eb76aa1133a

在状态栏显示当前页的IP地址、主机名、ISP、国家和城市等信息。

8 OSVDB

https://addons.mozilla.org/en-us/firefox/addon/osvdb/

https://addons.cdn.mozilla.net/user-media/addons/45607/osvdb-20091025.xml?filehash=sha256%3A9e63e42275a425433fdea755c93fa7d3dd2ca2c9bb22104

开放源码的漏洞数据库检索

9 Packet Storm search plugin

https://addons.mozilla.org/en-us/firefox/addon/packet-storm-search-plugin/

https://addons.cdn.mozilla.net/user-media/addons/46818/packetstorm_search_suggest-20091102.xml?filehash=sha256%3A8a5a93e46423c9d478822e601c74

Packet Storm提供的插件，可以搜索漏洞、工具和exploits等。

10 Offsec Exploit-db Search

https://addons.mozilla.org/en-us/firefox/addon/offsec-exploit-db-search/

https://addons.cdn.mozilla.net/user-media/addons/50241/offsec_exploit_archive_search-20100614.xml?filehash=sha256%3A70c9a23cb7395d3e1bdafd4223eb

搜索Exploit-db信息

11 Security Focus Vulnerabilities Search Plugin

https://addons.mozilla.org/en-us/firefox/addon/securityfocus-vulnerabilities-/

https://addons.cdn.mozilla.net/user-media/addons/14633/securityfocus_vulns_search_-20091001.xml?filehash=sha256%3A02f7afa02f1493d60eed33686745a7

在Security Focus上搜索漏洞

12 Cookie Watcher

Cookie Watcher

在状态栏显示cookie

13 Header Spy

https://addons.mozilla.org/en-us/firefox/addon/header-spy/

https://addons.cdn.mozilla.net/user-media/addons/4276/header_spy-1.3.4.3-fx.xpi?filehash=sha256%3A88a29a7fb2595bd99115abda82d93f18bc2aece251eb9

在状态栏显示HTTP头

14 Groundspeed

https://addons.mozilla.org/en-us/firefox/addon/groundspeed/

https://addons.cdn.mozilla.net/user-media/addons/46698/groundspeed-1.2-fx.xpi?filehash=sha256%3A1a742ad15c26d5d993f388a41f008422d0cc1729aa005

Manipulate the application user interface.

15 CipherFox

https://addons.mozilla.org/en-us/firefox/addon/cipherfox/

https://addons.cdn.mozilla.net/user-media/addons/8919/cipherfox-4.1.1-fx+sm.xpi?filehash=sha256%3A2b0e4a62e5a949f56deccbd5cc89d1c15fdf803b78f53

在状态栏显示当前SSL/TLS的加密算法和证书

16 XSS Me

https://addons.mozilla.org/en-us/firefox/addon/xss-me/

https://addons.cdn.mozilla.net/user-media/addons/7598/xss_me-0.4.6-fx.xpi?filehash=sha256%3Ab9a9b65339481e3706925537f68ecbacaecae81211458a6fe7

XSS测试扩展

17 SQL Inject Me

https://addons.mozilla.org/en-us/firefox/addon/sql-inject-me/

https://addons.cdn.mozilla.net/user-media/addons/7597/sql_inject_me-0.4.7-fx.xpi?filehash=sha256%3Ad476622cc47a69e904b37e27c374ed307e16fc17ad15

SQL注入测试扩展

18 Wappalyzer

https://addons.mozilla.org/en-us/firefox/addon/wappalyzer/

https://addons.cdn.mozilla.net/user-media/addons/10229/wappalyzer-3.2.11-fx.xpi?filehash=sha256%3Aab961c199f0b3749685fab2701f9fa91e7e15baebeb88

查看网站使用的应用程序

19 Poster

https://addons.mozilla.org/en-us/firefox/addon/poster/

https://addons.cdn.mozilla.net/user-media/addons/2691/poster-3.1.0-fx.xpi?filehash=sha256%3Ace27e3743f7641b6cd18eae0410ae134426f58bf48445bc5c4e

发送与Web服务器交互的HTTP请求，并查看输出结果

20 Javascript Deobfuscator

Javascript Deobfuscator

21 Modify Headers

https://addons.mozilla.org/en-us/firefox/addon/modify-headers/

https://addons.cdn.mozilla.net/user-media/addons/967/modify_headers-0.7.1.1-fx.xpi?filehash=sha256%3Ab0e269324a42c2b0f63346d8e8db837ec20abd287

修改HTTP请求头

22 FoxyProxy

https://addons.mozilla.org/en-us/firefox/addon/foxyproxy-standard/

https://addons.cdn.mozilla.net/user-media/addons/2464/foxyproxy_standard-4.6.5-fx+sm+tb.xpi?filehash=sha256%3Ab8109fc59ba13a58e9a7adb5263cacc92

代理工具

23 FlagFox

FlagFox

可以在地址栏或状态栏上显示出当前网站所在国家的国旗，也有更多的其他功能，如：双击国旗可以实现WOT功能；鼠标中键点击是whois功能。当然用户可以在选项里设

24 Greasemonkey

https://addons.mozilla.org/en-us/firefox/addon/greasemonkey/

https://addons.cdn.mozilla.net/user-media/addons/748/greasemonkey-3.11-fx.xpi?filehash=sha256%3A028aae4a9db333bca9958324b92ce2020159a1339852

greasemonkey 使你可以向任何网页添加DHTML语句(用户脚本)来改变它们的显示方式。就像CSS可以让你接管网页的样式，而用户脚本(User Script)则可以让你轻易地控制网页设计与交互的任何方面。例如:

- 使页面上显示的 URL 都成为可以直接点击进入的链接。 增强网页实用性，使你经常访问的网站更符合你的习惯。 绕过网站上经常出现的那些烦人的 Bug。

25 Domain Details

https://addons.mozilla.org/en-us/firefox/addon/domain-details/

https://addons.cdn.mozilla.net/user-media/addons/2166/domain_details-2.7-fx.xpi?filehash=sha256%3A8e066a1fff23ada8076b6f4d338a1a92792a294eab580

显示服务器类型、IP地址、域名注册信息等

26 Websecurify

https://addons.mozilla.org/en-us/firefox/addon/websecurify/

https://addons.cdn.mozilla.net/user-media/addons/337391/websecurify-5.5.0-fx.xpi?filehash=sha256%3Afd2cd352319d5b16338f6f6cf40d4ba27156e54765f7

Websecurify是WEB安全检测软件的Firefox的扩展，可以针对Web应用进行安全评估

27 XSSed Search

XSSed Search

搜索XSSed.Com跨站脚本数据库

28 ViewStatePeeker

https://addons.mozilla.org/en-us/firefox/addon/viewstatepeeker/

https://addons.cdn.mozilla.net/user-media/addons/7167/viewstatepeeker-2.5-fx.xpi?filehash=sha256%3Ac1acffce9595a9f4a74041d125d5c36f0ed46e3dae0e0

查看asp.net的iewState

29 CryptoFox

https://addons.mozilla.org/en-US/firefox/addon/cryptofox/

https://addons.cdn.mozilla.net/user-media/addons/12065/cryptofox-2.2-fx.xpi?filehash=sha256%3A1a67808328ed28c07511c25767d3a786b371bc3068cb39b

30 WorldIP

WorldIP

显示服务器的IP、地址、PING、Traceroute、RDNS等信息

31 Server Spy

Server Spy

识别访问的web服务器类型，版本以及IP地址的插件

32 Default Passwords

https://addons.mozilla.org/en-US/firefox/addon/default-passwords-cirtne-58786/

https://addons.cdn.mozilla.net/user-media/addons/58786/default_passwords_-_cirt.net-20100110.xml?filehash=sha256%3A3da5ea0dc15be1286a846e147938

搜索CIRT.net默认密码数据库。

33 Snort IDS Rule Search

https://addons.mozilla.org/en-US/firefox/addon/snort-ids-rule-search/

https://addons.cdn.mozilla.net/user-media/addons/58787/snort_ids_rule_search-20100110.xml?filehash=sha256%3Af6a3aab54f708bed418f47aec3d30f0aeef4

搜索Snort的IDS规则，做签名开发的应该很有用。

34 FireCAT

FireCAT

FireCAT (Firefox Catalog of Auditing exTensions)
是一个收集最有效最有用的应用程序安全审计和风险评估工具的列表(这些工具以Firefox插件形式发布的),FireCAT中没有收集的安全工具类型包括:fuzzer,代理和应用程序扫描器.

上一篇：【原创】秒抢红包锁屏样本手动查杀操作 下一篇：【译】一套可用于强化红队基础设施的...
1. 8 条回复


simeon 2017-06-06 03:06:29

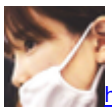
牛掰，学习收藏了！

0 回复Ta


hades 2017-06-06 03:16:18

感谢~~~~
渗透测试标准，总结的还不错 链接：https://www.processon.com/view/583e8834e4b08e31357bb727

0 回复Ta


hades 2017-06-06 03:20:48
0 回复Ta


静默 2017-06-06 07:55:59

为什么不能收藏

0 回复Ta


超级菜 2017-07-18 15:53:21

不赞，自己的良心过不去，继续努力！

0 回复Ta


c0de 2017-07-19 02:13:59

不错

0 回复Ta


飞鸟 2017-07-19 05:33:47

特别详细，谢谢分享

0 回复Ta


comeonbaby 2017-08-15 15:37:19

学习

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