

Re: Web Application Testers.

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/vuln-dev/2001-09/0304.html>

From: Dennis Groves (dwg@uswest.net)

Date: 09/24/01

Date: Mon, 24 Sep 2001 13:34:53 -0700

Subject: Re: Web Application Testers.

From: Dennis Groves <dwg@uswest.net>

To: Dom De Vitto <Dom@devitto.com>, <pen-test@securityfocus.com>, <vuln-dev@securityfocus.com>

Message-ID: <B7D4E6FC.768B%dwg@uswest.net>

> *I've just been reading about Sanctum's AppScan, which appears to be on the
> right track, but I've nothing to compare it to...*

>

> *Any advice/experience.*

>

> *FYI, AppScan breaks/subverts web applications – there are plenty of tools
> to break web servers (apache/IIS), but it looks like appscan is on it's own
> on the test-the-bespoke-web-app front.*

>

> *Thanks all, in advance,*

> *Dom*

>

>

>

>

> *This list is provided by the SecurityFocus Security Intelligence Alert (SIA)*

> *Service. For more information on SecurityFocus' SIA service which*

> *automatically alerts you to the latest security vulnerabilities please see:*

> *<https://alerts.securityfocus.com/>*

>

Look else where. It is very interesting, however programs at this early stage of the game simply can not replace the human brain.

To Quote Minga "earlier on this list"

>>> *In short there is a real lack of expertise in the field and a huge demand.*

>>> *Some idiot running Nessus across your application is going to do nothing.*

>>

>> *Yes I agree with this. Most security audits are only automated scanners and
>> are rarely detailed application audits.*

>

> *Be sure to highlight the word MOST there. I've been doing Web Application*

SecurityFocus Vuln-Dev: Re: Web Application Testers.

- > *penetration test/vulnerability assessments/ and generic best-practices checks*
- > *by hand for a security firm for over 2 years now. It is automatically included*
- > *in the general security methodology that we use for all clients. Along with*
- > *non-tool based penetration tests/vulnerability assessments.*
- >
- > --
- >
- > *As for the TOOLS discussion there are 4 three tools I am absolutely*
- > *dependant on for my web applications tests.*
- >
- > *1) stunnel*
- > *2) A Sniffer*
- > *3) Perl*
- > *4) A Brain*
- >
- > *MAYBE some sort of proxy to catch requests. But pretty much all of them are*
- > *lame and overly complicated or broken in some matter. (Tis' why I use*
- > *stunnel and a sniffer instead).*
- >
- > *I have used Sanctum's tool for a few weeks. They are headed in the correct*
- > *direction. but have a loooooong way to go. On a test I performed, I ended up*
- > *with APPX 20 findings, 3 of which were High Risk. Sanctum's tool only found*
- > *about 4-5 of the findings. So if I (or anyone) was dependant on this type of*
- > *tool to be "secure", it would be a big waste of \$5000. The tools does not*
- > *check for most "Best Practices" types of risks (SSL Key Strength For Example)*
- > *It does check for comments inside of HTML (and will return you about 200*
- > *findings associated with them). It also floodes all variables with long*
- > *bits of data. But not the RIGHT type of data. It will try 1000 1's (for*
- > *example). But not 1000 !'s or 1000 ;'s . Or for that matter 10000 1's.*
- > *It doesnt try (as data for a variable) things like*
- > *!@#%&*()_+ = - { } \ | ; " , . / ? > < ` ~ . When those usually wreck havoc!*

I can not say it better myself...

Appscan in particular has little to set it apart from other products that do web audits (Unless you consider 80% false positives to be a selling point). The company "slant" is application testing, but it is pure spin, the product does no more and perhaps less than many of the following products:

(Gratuitously borrowed from various web databases, but compiled by me)

NetRecon
HackerShield
Retina
ISS
Nessus
CyberCop
SARA
SAINT
AppScan

Web application testing tools.

Re: Web Application Testers.

SecurityFocus Vuln-Dev: Re: Web Application Testers.

Achilles www.digizen-security.com/
Appscan www.sanctuminc.com
CIS www.cerberus-infosec.co.uk/cis.shtml
Curl curl.haxx.se
ELZA www.einet.bg/~philip
e-test tools www.rswsoftware.com
nessus www.nessus.org
PentaSafe tools www.pentasafe.com
WAST webtool.rte.microsoft.com
Whisker www.wiretrip.net/rfp/
"Write you own scripts"
"Contract out testing"

Other Web Scanners (35 Little Boys)

911 0.1

by Erik Tayler

<<http://63.248.48.143> >

<<http://www.securityfocus.com/tools/1751> >

Platforms: FreeBSD, Linux, NetBSD and OpenBSD

Size: 29.17Kb

Score: Not scored yet

Simple code which will eventually be a very useful tool for performing vulnerability assessments. Currently includes the ability to set certain nmap and whisker options [scan type & evasive mode, respectively]. Will eventually incorporate more tools, and have a nice, clean, centralized output.

Atlas 1.0

by Digital Monkey, dmonkey@arctik.com

<<http://www.securityfocus.com/tools/923> >

Platforms: Windows 95/98

Size: 23.79Kb

Score: Not scored yet

A Windows/MS-DOS CGI scanner (binary only) which scans for 65 remote vulnerabilities.

BASS – Bulk Auditing Security Scanner 1.0.7

by Liraz Siri <liraz@bigfoot.com>

<<http://www.securityfocus.com/tools/394> >

Platforms: Linux

Size: 61.50Kb

Score: 3.00 / 4 (1 vote)

BASS is a bulk auditing network scanner that features a highly-reliable, fail-safe architecture which efficiently utilizes the available bandwidth. It has a small memory and CPU footprint and can be easily extended.

Cerberus Internet Scanner 5.0

by David Litchfield

<<http://www.cerberus-infosec.co.uk/> >

<<http://www.securityfocus.com/tools/676> >

Re: Web Application Testers.

SecurityFocus Vuln-Dev: Re: Web Application Testers.

Platforms: Windows 2000 and Windows NT

Size: 298.77Kb

Score: 3.00 / 4 (1 vote)

CIS is a free security scanner written and maintained by Cerberus Information Security, Ltd and is designed to help administrators locate and fix security holes in their computer systems. This tool is a must! Runs on Windows NT and Windows 2000. Very comprehensive!

Cerberus WebScan

by Cerberus Information Security, services@cerberus-infosec.co.uk

< <http://www.cerberus-infosec.co.uk/> >

< <http://www.securityfocus.com/tools/695> >

Platforms: Windows 2000, Windows 95/98 and Windows NT

Size: 76.00Kb

Score: 3.00 / 4 (1 vote)

This is a web security scanner designed to find known web server security issues.

cgi scanner 3.6

by CKS

< <http://www.singnet.com.sg/~cksss/> >

< <http://www.securityfocus.com/tools/377> >

Platforms: AIX, BSDI, Digital UNIX/Alpha, FreeBSD, HP-UX, IRIX, Linux, NetBSD, OpenBSD, SCO, Solaris, SunOS, True64 UNIX, UNIX, Ultrix and Unixware

Size: 12.37Kb

Score: 2.00 / 4 (1 vote)

Cgi Scanner 3.6 is a simple program which facilitates the scanning of hosts on a network for known cgi vulnerabilities. Upon finding a given cgi program, the script will optionally download information from the author's web page, detailing the exploit. 3.6 includes a fix for a y2k problem in previous versions that would cause numerous false positives.

Cgi Sonar 1.0

by M.e.s.s.i.a.h

< <http://www.securityfocus.com/tools/1211> >

Platforms: Perl (any system supporting perl)

Size: 4.37Kb

Score: Not scored yet

A simple Cgi Scanner written in PERL ,scans for over 120 known vulnerabilities.

cgi-check99 0.3

by deepquest

< <http://www.deepquest.pf> >

< <http://www.securityfocus.com/tools/626> >

Platforms: BSDI, BeOS, DOS, FreeBSD, HP-UX, IRIX, Linux, MacOS, NetBSD, OS/2, OpenBSD, OpenVMS, PalmOS, Solaris, SunOS, UNIX, VMS, Windows 2000, Windows 3.x, Windows 95/98, Windows CE and Windows NT

Size: 10.64Kb

Score: 3.00 / 4 (1 vote)

This is one of the worlds most cross platform cgi scanners, running on 37

Re: Web Application Testers.

SecurityFocus Vuln-Dev: Re: Web Application Testers.

operating systems! Even PalmOS soon! Will check for hundreds of common cgi and other remote issues. Plus it will report you the Bugtraq ID of some vulnerabilities. Get the rebol interpreter at <http://www.rebol.com>.

CGI-Exploit Scanner (Japanese)

by Shadow Penguin Security Team

< <http://shadowpenguin.backsection.net/> >

< <http://www.securityfocus.com/tools/368> >

Platforms: UNIX

Size: 6.42Kb

Score: 3.00 / 4 (1 vote)

This utility lists the servers which have certain security vulnerabilities via CGI scripts. This utility currently checks for the phf, test-cgi, nph-test-cgi, campas, htmlscript, service & pwd vulnerabilities. The addition of new vulnerabilities is very easy.

cgichk 2.50

by Toby Deshane

< <http://sourceforge.net/projects/cgichk/> >

< <http://www.securityfocus.com/tools/1645> >

Platforms: FreeBSD and Linux

Size: 14.04Kb

Score: Not scored yet

cgichk is a Web vulnerability tool that automatically searches for a series of interesting directories and files on a given site. It also includes a whois lookup.

cgiscan

by Bronc Buster

< <http://www.securityfocus.com/tools/378> >

Platforms: AIX, BSDI, Digital UNIX/Alpha, FreeBSD, HP-UX, IRIX, Linux, NetBSD, OpenBSD, SCO, Solaris, SunOS, True64 UNIX and UNIX

Size: 4.43Kb

Score: 2.00 / 4 (1 vote)

cgiscan.c is another simple program which facilitates the scanning of hosts on a network for known cgi vulnerabilities. It lets the user know whether or not a given cgi was found on the host.

Cold Fusion Scan 1.0

by icos@arez.com

< <http://www.securityfocus.com/tools/1046> >

Platforms: Windows 95/98 and Windows NT

Size: 172.22Kb

Score: Not scored yet

Cold Fusion vulnerability scanner is a program that will run down a list of words/domain names, and scan each one for an Allaire Cold Fusion misconfiguration.

CUM Security Toolkit [CST]

by toxic ocean, cum@nirvanet.net

< <http://www.securax.org/cum/> >

Re: Web Application Testers.

SecurityFocus Vuln-Dev: Re: Web Application Testers.

<<http://www.securityfocus.com/tools/1799>>

Platforms: Java

Size: 12.70Kb

Score: 4.00 / 4 (1 vote)

This version contains a script scanner, that scans using a database of scripts (user editable). The sample databases included contains +350 possibly vulnerable scripts/dirs. You can scan with or without a proxyserver. The scanner has 5 different Anti-IDS tactics (hex-values, double slashes, self-reference dirs, parameter hiding and session splicing), and sends fake ³X-Forwarded-For:², ³Referer:² and ³User-Agent:² headers to hide your scan even more. You can also specify a waittime between 2 script fetches. The scanner uses HEAD requests instead of GET for faster scanning, and has support for scanning virtual hosts. You can also specify another port to scan instead of the standard port 80. The scanner outputs the scripts/dirs that return a 200, 403 or 401 HTTP code and outputs the webserver software.

I'm probably forgetting some options because there are alot in this new version - you have to try it to see...

Also included is a portscanner. It can perform TCP scans, and it outputs the open ports, and their reply.

A full and comprehensive manual is included, but if you have problems, you can always mail us.

ELZA 1.4.3

by philip_stoev@iname.com

<<http://phiphi.hypermart.net/elza-entry.html>>

<<http://www.securityfocus.com/tools/1127>>

Platforms: Linux and Solaris

Size: 40.36Kb

Score: Not scored yet

The ELZA is a scripting language aimed at automating requests on web pages. Scripts written in ELZA are capable of mimicing browser behavior almost perfectly, making it extremely difficult for remote servers to distinguish their activity from the activity generated by ordinary users and browsers. This gives those scripts the opportunity to act upon servers that will not respond to requests generated using netcat, rebot, telnet or similar tool.

Grinder

by Rhino9

<<http://207.98.195.250/software/grinder.htm>>

<<http://www.securityfocus.com/tools/108>>

Platforms: Windows 3.x, Windows 95/98 and Windows NT

Size: 1.13Mb

Score: 3.00 / 4 (1 vote)

Grinder is a scanning tool for the Windows operating systems that scans ranges of ip addresses for IIS web servers containing certain urls.

Guile CGI Scanner

by ImperialS

<<http://www.securityfocus.com/tools/555>>

Platforms: Linux

Re: Web Application Testers.

SecurityFocus Vuln-Dev: Re: Web Application Testers.

Size: 8.19Kb

Score: Not scored yet

A CGI Scanner written in C. Checks for 44 known CGI problems.

httptype 1.3.6

by Philip Tellis, philip.tellis@iname.com

<<http://members.nbc.com/philip3/downloads/httptype/INDEX.html> >

<<http://www.securityfocus.com/tools/1269> >

Platforms: Linux and Solaris

Size: 14.36Kb

Score: Not scored yet

httptype reads a list of http hosts and optionally the port number for each of these. It queries each host, displaying the type of HTTP server running on that host, if any. It reads the http_proxy and no_proxy environment variables to determine whether to use a proxy or not. These options may also be specified through the command line.

ISB

by UndeF

<<http://undef.vr9.com/> >

<<http://www.securityfocus.com/tools/1430> >

Platforms: Linux, Perl (any system supporting perl), Solaris and UNIX

Size: 11.83Kb

Score: Not scored yet

Security auditing tool for unix systems. Port scan, remote services version detect, log facility.

md-webscan 1.0.1

by Mordrian, mordrian@hotmail.com

<<http://www.internettrash.com/users/mordrian/> >

<<http://www.securityfocus.com/tools/1421> >

Platforms: Linux, Solaris and UNIX

Size: 7.69Kb

Score: Not scored yet

Allows system administrators to check for commonly known CGI vulnerabilities on machines they administrate. Scans for 180 vulnerabilities in total.

Nessus 1.0.6

by Renaud Deraison, deraison@cvs.nessus.org

<<http://www.nessus.org/> >

<<http://www.securityfocus.com/tools/201> >

Platforms: FreeBSD, IRIX, Linux, NetBSD, OpenBSD and Solaris

Score: 3.86 / 4 (7 votes)

Nessus is a remote security scanner for Linux, BSD, Solaris, and other Unices. It is multi-threaded and plug-in-based, has a GTK interface, and performs over 470 remote security checks. It allows for reports to be generated in HTML, LaTeX, and ASCII text, and suggests solutions for security problems.

Nsat 1.22

by Mixer, mixer@newyorkoffice.com

Re: Web Application Testers.

SecurityFocus Vuln-Dev: Re: Web Application Testers.

< <http://members.tripod.com/mixersecurity/> >

< <http://www.securityfocus.com/tools/810> >

Platforms: Linux and Solaris

Size: 799.86Kb

Score: 4.00 / 4 (1 vote)

Nsat (Network Security Analysis Tool) is a fast, stable bulk security scanner designed to audit remote network services and check for versions, security problems, gather information about the servers and the machine, and much more. Unlike many other auditing tools, it can collect information about services independently of vulnerabilities, which makes it less dependent on frequent updates as new vulnerabilities are found.

Perl CGI Checker

by Epicurus (epicurus@wilter.com)

< <http://www.securityfocus.com/tools/402> >

Platforms: Perl (any system supporting perl)

Size: 6.89Kb

Score: Not scored yet

A CGI vulnerability scanner written in PERL, checks for 62 CGI holes.

rvscan (remote vulnerability scanner)

by ben-z

< <ftp://portal.slacknet.org/pub/code/rvscan.v3-b1.tgz> >

< <http://www.securityfocus.com/tools/1625> >

Platforms: Linux

Size: 102.81Kb

Score: Not scored yet

scans a unix system for just about every remote vulnerability currently being used by hackers.

Shadow CGI check 1.00.007

by RedShadow

< <http://www.rsh.kiev.ua> >

< <http://www.securityfocus.com/tools/1229> >

Platforms: Windows 2000, Windows 95/98 and Windows NT

Size: 256.26Kb

Score: Not scored yet

CGI vulnerability scanner. Currently checks for over 129 vulnerabilities.

twwwscan 0.7

by pilot

< <http://search.iland.co.kr/twwwscan/> >

< <http://www.securityfocus.com/tools/1886> >

Platforms: Windows 2000, Windows 95/98 and Windows NT

Size: 127.32Kb

Score: 4.00 / 4 (1 vote)

Updated version of twwwscan with added -v option support html type report support CVE information included completed NT/2000 IIS detail patch information. Last(~2000/12/23) WWW Vulnerabilities 300 over bugs check

SecurityFocus Vuln-Dev: Re: Web Application Testers.

UCGI Vulnerability Scanner 1.56

by su1d sh3ll

<<http://infected.ilm.net/unlg/>>

<<http://www.securityfocus.com/tools/563>>

Platforms: FreeBSD, IRIX, Linux and Windows 95/98

Size: 147.18Kb

Score: Not scored yet

CGI vulnerability scanner version 1.56. Checks for over 90 CGI vulnerabilities. Tested on slackware linux with kernel 2.0.35-2.2.5, FreeBSD 2.2.1-3.2, IRIX 5.3, DOS, and windows.

VoidEye CGI scanner Build 461

by Duke

<<http://www.securityfocus.com/tools/556>>

Platforms: Windows 2000, Windows 95/98 and Windows NT

Size: 328.58Kb

Score: Not scored yet

VoidEye CGI scanner, build 461. Scans for 78 known vulnerabilities. Runs on: win9x, winNT, win2000. Features: user can add his own holes, editing ³exp.dat² in any text editor or via program interface, user can process a site list, editing it via the program interface or the file ³servers.dat², scanner can work via a proxy, for more security. Multi-threaded and fast. By Duke.

Weakness - Www Vulnerability Scanner

by John Bissell a.k.a. hight1mes

<<http://www.silcom.com/~royalblu/weakness.zip>>

<<http://www.securityfocus.com/tools/672>>

Platforms: DOS, Windows 95/98 and Windows NT

Size: 29.92Kb

Score: 4.00 / 4 (1 vote)

Weakness is basically a CGI vulnerability scanner coded for Windows/DOS. Weakness will scan up 94 vulnerabilities and output the results of the scan to a text file. Source is included.

Webcracker 4.0

by Daniel Flam, info@webcracker.net

<<http://www.webcracker.net>>

<<http://www.securityfocus.com/tools/706>>

Platforms: Windows 95/98 and Windows NT

Size: 1.24Mb

Score: Not scored yet

This software will allow you to test your restricted-access website to make sure that only authorized users are able to get in. Webcracker is a security tool that allows you to attempt to test id and password combinations on your web site. If you're able to guess a user's password with this program, chances are some hacker will be able to also. Webcracker helps you find these vulnerabilities and fix them before they're exploited by some unknown attacker.

SecurityFocus Vuln-Dev: Re: Web Application Testers.

WebDecoy

by Mixer, mixer@newyorkoffice.com

<<http://1337.tsx.org/>>

<<http://www.securityfocus.com/tools/832>>

Platforms: Linux and Solaris

Size: 2.22Kb

Score: Not scored yet

This is a simple script that examines your CGI folder, and can check for vulnerable scripts (-check), generate decoy scripts, which will log any access over the web as a possible exploit attempt (-create), or remove vulnerable scripts and previously installed decoy files (-clean).

Whisker 1.2.0

by Rain Forest Puppy

<<http://www.wiretrip.net/rfp>>

<<http://www.securityfocus.com/tools/585>>

Platforms: Perl (any system supporting perl)

Size: 166.38Kb

Score: 4.00 / 4 (2 votes)

Whisker is an advanced CGI vulnerability scanner. It is scriptable and has many good features, such as querying for system type and basing scans on the information gathered (ie, determining between IIS and Apache web servers)

Whisker 1.4

by rain forest puppy, rfp@wiretrip.net

<<http://www.wiretrip.net/rfp>>

<<http://www.securityfocus.com/tools/727>>

Platforms: Perl (any system supporting perl)

Size: 166.38Kb

Score: 4.00 / 4 (3 votes)

Whisker is an advanced CGI vulnerability scanner. It is scriptable and has many good features, such as querying for system type and basing scans on the information gathered (ie, determining between IIS and Apache web servers)

³Multi-threaded² front end (Unix only).

More updates to server.db and scan.db.

Changed the $\text{\textcircled{E}}$ set¹ command to take .= (append) as well.

Added multi-file scans

Changed options around.

whisker will internally $\text{\textcircled{E}}$ read¹ the output from a .cfm script and determine if it really exists, eliminating all false reports.

Added support for variables and tab¹s, cr¹s, and lf¹s in strings.

You can now use a variable for $\text{\textcircled{E}}$ server¹ and $\text{\textcircled{E}}$ scan¹ matching

Scan database files don't have to be in the current directory

Whisker defaults to scan.db, so it's not required to specify -s <file>

Whisker will automatically rescan servers with dumb.db if they need it

NMAP information is now available inside the scripts

Redid the bounce options

Support for distributed proxies

Ability to use other CGI scanners¹ databases

Better timeout control (Unix only).

Implemented ability to use $\text{\textcircled{E}}$ GET¹ method, but still close the connection

Re: Web Application Testers.

SecurityFocus Vuln-Dev: Re: Web Application Testers.

after all the headers have arrived.
EXPERIMENTAL SSL support.
SamSpade bounce by Styx was added
Other little tweaks to variable handling and new variables added
Netcraft changed their output, so I had to change to match it.

whisker 1.4+SSL
by H.D. Moore, hdm@digitaloffense.net
<<http://www.digitaloffense.net:8000/>>
<<http://www.securityfocus.com/tools/1798>>
Platforms: Perl (any system supporting perl)
Size: 169.34Kb
Score: Not scored yet
This is a modified version of the whisker web scanning tool written by RFP.
It adds native SSL support (the -x option) via the Net::SSL module and OpenSSL.

Windows Nessus Client
by Noam Rathaus, Aviram Jenik, Jordan Hrycaj, and Renaud Deraison
<<http://www.nessus.org/win32.html>>
<<http://www.securityfocus.com/tools/1295>>
Platforms: Windows 95/98 and Windows NT
Score: Not scored yet
Windows Nessus Client is an almost fully functional port of the UNIX Nessus Client and has the same look and feel.

WWWHack 1.946
by core
<<http://www.wwwhack.com>>
<<http://www.securityfocus.com/tools/1785>>
Platforms: Windows 2000, Windows 95/98 and Windows NT
Size: 430.61Kb
Score: Not scored yet
A simple 3brute force² password guessing program. Includes dictionary files, support for HTTP Basic, HTTP Form, FTP, POP, and News.

- **Previous message:** [Ron DuFresne: "RE: Bug in Apache 1.3.20 Server – Hackemate Research"](#)
- **Next in thread:** [Lists: "Re: Web Application Testers."](#)
- **Reply:** [Lists: "Re: Web Application Testers."](#)
- **Reply:** [Kevin Spett: "Re: Web Application Testers."](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)