Web Vulnerability Scanners Evaluation - January 2009 (http://anantasec.blogspot.com/) anantasec@gmail.com

This evaluation was ordered by a penetration testing company that will remain anonymous.
The vendors were not contacted during or after the evaluation.

Applications (web scanners) included in this report

Web Scanner	Version
Acunetix WVS	6.0 (Build 20081217)
IBM Rational AppScan	7.7.620 Service Pack 2
HP WebInspect	7.7.869

Testing procedure

I've tested 13 web applications (some of them containing a lot of vulnerabilities), 3 demo applications provided by the vendors(testphp.acunetix.com, demo.testfire.net, zero.webappsecurity.com) and I've done some tests to verify Javascript execution capabilities. In total, 16 applications were tested.
I've tried to cover all the major platforms, therefore I have applications in PHP, ASP, ASP.NET and Java.

Note for Application Tests:
In this report I've only included "important" vulnerabilities like SQL injection, Local/Remote File Inclusion, XSS, ...
Vulnerabilities like "Unencrypted Login Form", "Directory listing found", "Email address found", ... were not included to avoid clutter.

SQL injection vulnerabilities can be discovered through error messages or blind SQL injection.
Some scanners are showing 2 alerts: one for the vulnerability found through error message and another for the blind technique.
In these cases only one vulnerability has been counted.

Legend

Icon	Explanation	Score
✓	A valid vulnerability was reported.	5 points
✗	A valid vulnerability was missed. (false negative)	-5 points
⊖	A false positive was reported.	-1 point

How score was calculated

- 5 points for each valid vulnerability
- -5 points for each false negative (valid vulnerability not found)
- -1 point for each false positive

Javascript tests

Javascript tests				
Test + description	**File**	**AppScan**	**WebInspect**	**Acunetix**
Test JS 1 - simple document.location	javascript-1.html	✓	✓	✓
Test JS 2 - simple javascript obfuscation	javascript-1.html	✓	✓	✓
Test JS 3 - script generated from document.write	javascript-1.html	✓	✓	✓
Test JS 4 - external script test 1	javascript-1.html	✓	✓	✓
Test JS 5 - external script test 2	javascript-1.html	✓	✓	✓
Test JS 6 - external script test 3	javascript-1.html	✓	✓	✓
Test JS 7 - simple variable concatenation	javascript-1.html	✓	✓	✓
Test JS 8 - javascript obfuscation + packing	javascript-1.html	✓	✓	✓
Test JS 9 - form generated from script	javascript-1.html	✗	✓	✓
Test JS 10 - <A href> generated from document.write (recursive)	javascript-1.html	✓	✓	✓
Test JS 11 - javascript encoding	javascript-1.html	✓	✓	✗
Test JS 12 - XMLHTTPRequest (XHR) open	javascript-2.html	✓	✓	✓
Test JS 13 - document.location + unescape on XHR callback	javascript-3.html	✓	✓	✓
Test JS 14 - javascript obfuscation + packing on XHR callback	javascript-4.html	✗	✓	✓
Test JS 15 - form created with createElement + appendChild	javascript-6.html	✗	✓	✓
Test JS 16 - usage of XHR.responseText on XHR callback	javascript-7.html	✓	✓	✓
Test JS 17 - document.write from frame1 to frame2	javascript-8.html	✗	✗	✗
Test JS 18 - XHR with POST and parameters	javascript-5.html	✓	✓	✓
Summary		4 missed 14 found	1 missed 17 found	2 missed 16 found
Score		**50**	**80**	**70**

Notes:

- A zip file containing all the javascript tests can be downloaded from http://drop.io/anantasecfiles/.

Application tests

1. Vanilla-1.1.4 / PHP / http://getvanilla.com/

Valid vulnerabilities

Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Cross Site Scripting (XSS)	people.php	NewPassword	✗	✓	✓	✓
Cross Site Scripting (XSS)	people.php	ConfirmPassword	✗	✓	✓	✓
Cross Site Scripting (XSS)	ajax/updatecheck.php	RequestName	✗	✗	✗	✓
Summary			3 missed 0 found	1 missed 2 found	1 missed 2 found	0 missed 3 found
Score			-15	5	5	15

False positives

Non-Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
MusicBox Multiple SQL Injection	index.php	page	⊖			
MxBB Portal index.php SQL Injection	index.php	page	⊖			
Summary			2 reported	0 reported	0 reported	0 reported
Score			-2	0	0	0
Total score			**-17**	**5**	**5**	**15**

Notes:

- The false positives reported by AppScan: MusicBox and MxBB were not installed on the web server.

2. VivvoCMS-3.4/ PHP / http://www.vivvo.net/

Valid vulnerabilities

Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Cross Site Scripting (XSS)	index.php	sort	✗	✓	✓	✓
Cross Site Scripting (XSS)	index.php	category	✗	✓	✗	✗
Cross Site Scripting (XSS)	/VivvoCMS-3.4/admin/tinymce/jscripts/tiny_mce/plugins/ibrowser/scripts/phpThumb/demo/phpThumb.demo.demo.php/>"><ScRiPt>alert(1272177526707)</ScRiPt>	N.A. The vulnerability is in the URI.	✗	✗	✗	✓
SQL Injection	sendemail.php	article_id	✗	✗	✓	✓
SQL Injection	index.php	category	✓	✓	✓	✓
SQL Injection	ajax.php	s	✗	✗	✗	✓
SQL Injection	search.php	category_id	✗	✗	✗	✓
File Inclusion (LFI)	admin/tinymce/jscripts/tiny_mce/plugins/ibrowser/ibrowser.php	lang (Cookie)	✗	✗	✗	✓
File Inclusion (LFI)	print_version.php	lang (Cookie)	✗	✗	✗	✓
Directory Traversal	index.php	author	✗	✗	✗	✓
Summary			9 missed 1 found	7 missed 3 found	7 missed 3 found	1 missed 9 found
Score			-40	-20	-20	40

False positives

Non-Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
MAXSITE index.php SQL Injection	index.php	category	⊖			
PHP Real Estate Classifieds header.php Remote File	index.php	loc	⊖			

Inclusion						
phpWordPress SQL Injection	index.php	ctg	⛔			
Summary			3 reported	0 reported	0 reported	0 reported
Score			-3	0	0	0
Total score			**-43**	**-20**	**-20**	**40**

Notes:

- For this application I didn't listed some XSS vulnerabilities found by Acunetix + AcuSensor in tinymce script included in this application. There were too many of those to be listed here.

3. fttss-2.0 / PHP / http://fttss.sourceforge.net/

Valid vulnerabilities						
Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
Cross Site Scripting (XSS)	index.php	texto_original	✓	✓	✓	✓
Remote Code Execution	index.php	voz	✗	✗	✗	✓
Summary			1 missed 1 found	1 missed 1 found	1 missed 1 found	0 missed 2 found
Score			0	0	0	10
False positives						
Non-Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
Summary			0 reported	0 reported	0 reported	0 reported
Score			0	0	0	0
Total score			**0**	**0**	**0**	**10**

Notes:
The advisory from milw0rm is http://www.milw0rm.com/exploits/7731.

4. Wordpress-2.6.5 / PHP / http://wordpress.org/

Valid vulnerabilities						
Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
Summary			0 missed 0 found	0 missed 0 found	0 missed 0 found	0 missed 0 found
Score			0	0	0	0
False positives						
Non-Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
WordPress Multiple Remote File Inclusion	wp-settings.php	require_once	⛔			
Summary			1 reported	0 reported	0 reported	0 reported
Score			-1	0	0	0
Total score			**-1**	**0**	**0**	**0**

5. vbulletin_v3.6.8 / PHP / http://www.vbulletin.com/

Valid vulnerabilities						
Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
Summary			0 missed 0 found	N/A N/A	0 missed 0 found	0 missed 0 found
Score			0	0	0	0
False positives						
Non-Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
SQL Injection	faq.php	faq	⛔	N/A		
Summary			1 reported	N/A	0 reported	0 reported
Score			-1	N/A	0	0
Total score			**-1**	0	**0**	**0**

Notes: In this case WebInspect didn't finished the scan. I stopped the application after two days of scanning. Unfortunately, this scan was scheduled so I didn't managed to investigate what happened. After that, I didn't started any schedulded scans with WebInspect because in WebInspect you don't have enough feedback (you have no idea what's going on with the scheduled scan).

6. riotpix v0.61 / PHP / http://www.riotpix.com/

Valid vulnerabilities

Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Cross Site Scripting (XSS)	message.php	reply	✓	✓	✓	✓
Cross Site Scripting (XSS)	message.php	message	✓	✓	✓	✓
Cross Site Scripting (XSS)	sessions_form.php	page	✗	✗	✗	✓
Cross Site Scripting (XSS)	sessions_form.php	forumid	✗	✗	✗	✓
Cross Site Scripting (XSS)	`/riotpix0_61/edit_posts.php/>"><ScRiPt>alert(547054737574)</ScRiPt>`	N.A. The vulnerability is in the URI.	✗	✗	✗	✓
Cross Site Scripting (XSS)	`/riotpix0_61/edit_posts_script.php/>"><ScRiPt>alert(547114737605)</ScRiPt>`	N.A. The vulnerability is in the URI.	✗	✗	✗	✓
Cross Site Scripting (XSS)	`/riotpix0_61/index.php/>"><ScRiPt>alert(546754737460)</ScRiPt>`	N.A. The vulnerability is in the URI.	✓	✗	✓	✓
Cross Site Scripting (XSS)	`/riotpix0_61/message.php/>"><ScRiPt>alert(546874737513)</ScRiPt>`	N.A. The vulnerability is in the URI.	✓	✗	✓	✓
Cross Site Scripting (XSS)	`/riotpix0_61/preview.php/>"><ScRiPt>alert(547414737684)</ScRiPt>`	N.A. The vulnerability is in the URI.	✗	✗	✗	✓
Cross Site Scripting (XSS)	`/riotpix0_61/read.php/>"><ScRiPt>alert(547474737703)</ScRiPt>`	N.A. The vulnerability is in the URI.	✗	✗	✗	✓

Cross Site Scripting (XSS)	/riotpix0_61/sessions_form.php/>"><ScRiPt>alert(547654737784)</ScRiPt>	N.A. The vulnerability is in the URI.	✗	✗	✗	✓
SQL Injection	edit_posts.php	username	✗	✗	✗	✓
SQL Injection	edit_posts_script.php	username	✗	✗	✗	✓
SQL Injection	index.php	username	✗	✗	✗	✓
SQL Injection	message.php	username	✗	✗	✗	✓
SQL Injection	read.php	username	✗	✗	✗	✓
Summary			12 missed 4 found	14 missed 2 found	12 missed 4 found	0 missed 16 found
Score			-40	-60	-40	80
False positives						
Non-Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
DVGuestbook Cross-Site Scripting	index.php	page	⊖			
WordPress Pool Theme Cross-Site Scripting in Path	index.php	<URI>	⊖			
Summary			2 reported	0 reported	0 reported	0 reported
Score			-2	0	0	0
Total score			**-42**	**-60**	**-40**	**80**

Notes:

- The advisory from milw0rm is located at http://www.milw0rm.com/exploits/7682.

7. pligg beta v9.9.0 / PHP / http://www.pligg.com/

Valid vulnerabilities

Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Cross Site Scripting (XSS)	index.php	category	✓	✓	✓	✓
Cross Site Scripting (XSS)	login.php	username	✓	✓	✓	✓
Cross Site Scripting (XSS)	login.php	category	✓	✓	✓	✓
Cross Site Scripting (XSS)	register.php	email	✓	✓	✓	✓
Cross Site Scripting (XSS)	register.php	username	✓	✓	✓	✓
Cross Site Scripting (XSS)	register.php	password	✓	✓	✓	✓
Cross Site Scripting (XSS)	register.php	password2	✓	✓	✓	✓
Cross Site Scripting (XSS)	register.php	reg_username	✓	✓	✓	✓
Cross Site Scripting (XSS)	register.php	reg_password	✓	✓	✓	✓
Cross Site Scripting (XSS)	register.php	reg_password2	✓	✓	✓	✓
Cross Site Scripting (XSS)	register.php	reg_email	✓	✓	✓	✓
SQL Injection	out.php	title	✓	✗	✓	✓
SQL Injection	story.php	title	✓	✓	✓	✓
SQL Injection	userrss.php	status	✓	✓	✓	✗
SQL Injection	cloud.php	categoryID	✗	✗	✗	✓
SQL Injection	login.php	username	✗	✓	✗	✗
SQL Injection	cvote.php	id	✗	✗	✗	✓
SQL Injection	editlink.php	id	✗	✗	✗	✓
SQL Injection	check_url.php	url	✗	✗	✗	✓
SQL Injection	out.php	url	✗	✗	✗	✓
SQL Injection	recommend.php	title	✗	✗	✗	✓
SQL Injection	rss.php	rows	✗	✗	✗	✓
SQL Injection	story.php	title	✗	✗	✗	✓

SQL Injection	story.php	id	✗	✗	✗	✓
SQL Injection	userrss.php	rows	✗	✗	✗	✓
SQL Injection	vote.php	id	✗	✗	✗	✓
Directory Traversal	live.php	template (Cookie)	✗	✗	✗	✓
Directory Traversal	sidebar_stories.php	template (Cookie)	✗	✗	✗	✓
Summary			14 missed 14 found	14 missed 14 found	14 missed 14 found	2 missed 26 found
Score			0	0	0	120
False positives						
Non-Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
eTicket Multiple SQL Injection	index.php	status	⊖			
Sphider Multiple Cross-Site Scripting	index.php	category	⊖			
SQL Injection	search.php	search		⊖		
Summary			2 reported	1 reported	0 reported	0 reported
Score			-2	-1	0	0
Total score			**-2**	**-1**	**0**	**120**

Notes:

- The advisory from milw0rm is located at http://www.milw0rm.com/exploits/6146.
- I didn't included some XSS vulnerabilities detected by Acunetix + AcuSensor. There are a lot of them.

8. javabb_v0.99 / Java & Tomcat / http://www.javabb.org/

Valid vulnerabilities

Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Cross Site Scripting (XSS)	save_new_member.jbb	(name, email, ...)	✓	✓	✓	N/A
Cross Site Scripting (XSS)	doSearch.jbb	query	✓	✓	✓	
Cross Site Scripting (XSS)	member_list.jbb	sortBy	✓	✓	✓	
Cross Site Scripting (XSS)	member_list.jbb	sortOrder	✓	✓	✓	
Cross Site Scripting (XSS)	quote.jbb	whoQuote	✗	✗	✓	
Cross Site Scripting (XSS)	quote.jbb	page	✗	✗	✓	
Cross Site Scripting (XSS)	viewtopic.jbb	page	✗	✓	✓	
Cross Site Scripting (XSS)	rss/pm.externalSend.jbb	userId	✗	✓	✓	
Cross Site Scripting (XSS)	rss/pm.externalSend.jbb	username	✗	✗	✓	
SQL Injection	member_list.jbb	sortBy	✓	✓	✓	
SQL Injection	member_list.jbb	sortOrder	✓	✓	✓	
Summary			5 missed 6 found	3 missed 8 found	0 missed 11 found	
Score			5	25	55	

False positives

Non-Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
SQL Injection	/rss/search_author.jbb	u		⊖		N/A
SQL Injection	unanswered_posts.jbb	page		⊖		
Summary			0 reported	2 reported	0 reported	
Score			0	-2	0	
Total score			**5**	**23**	**55**	

9. Yazd Discussion Forum_v3.0 / Java & Tomcat / http://www.forumsoftware.ca/

Valid vulnerabilities

Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Cross Site Scripting (XSS)	createAccount.jsp	(name, email, ...)	✓	✓	✓	N/A
Cross Site Scripting (XSS)	login.jsp	referer	✓	✓	✓	
Cross Site Scripting (XSS)	login.jsp	username	✓	✓	✓	
Cross Site Scripting (XSS)	login.jsp	password	✓	✓	✓	
Cross Site Scripting (XSS)	post.jsp	referer	✓	✓	✓	
Cross Site Scripting (XSS)	post.jsp	name	✓	✓	✓	
Cross Site Scripting (XSS)	post.jsp	email	✓	✓	✓	
Cross Site Scripting (XSS)	search.jsp	q	✓	✓	✓	
Cross Site Scripting (XSS)	error.jsp	msg	✓	✓	✗	
Summary			0 missed 9 found	0 missed 9 found	1 missed 8 found	
Score			45	45	35	

False positives

Non-Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Summary			0 reported	0 reported	0 reported	
Score			0	0	0	
Total score			**45**	**45**	**35**	

10. pebble_v2.3.1 / Java & Tomcat / http://pebble.sourceforge.net/

Valid vulnerabilities

Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Summary			0 missed 0 found	0 missed 0 found	0 missed 0 found	N/A
Score			0	0	0	0

False positives

Non-Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Cross Site Scripting (XSS)	faq.php	faq		⊖		N/A
SQL Injection	advancedSearch.action	tags		⊖		
Summary			0 reported	2 reported	0 reported	
Score			0	-2	0	
Total score			**0**	**-2**	**0**	

11. TriptychBlog_v.9.0 / ASP.NET / http://triptychstudios.net/triptychblog/

Valid vulnerabilities						
Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
Summary			0 missed 0 found	0 missed 0 found	0 missed 0 found	0 missed 0 found
Score			0	0	0	0
False positives						
Non-Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
SQL Injection	Default.aspx	Category	⛔	⛔		
SQL Injection	Default.aspx	Year	⛔			
SQL Injection	Comments.aspx	ArticleID	⛔			
SQL Injection	Comments.aspx	ArticleName	⛔			
SQL Injection	Comments.aspx	ctl00$Content$CommentContent	⛔			
SQL Injection	Comments.aspx	ctl00$Content$Submit_Content	⛔			
Summary			6 reported	1 reported	0 reported	0 reported
Score			-6	-1	0	0
Total score			**-6**	**-1**	**0**	**0**

Notes:

- Both WebInspect and AppScan are reporting false positives based on the following error message:
  - *"The changes you requested to the table were not successful because they would create duplicate values in the index, primary key, or relationship. Change the data in the field or fields that contain duplicate data, remove the index, or redefine the index to permit duplicate entries and try again."*
- That's not an SQL injection vulnerability. Anyway, I've checked the code just to be sure and I can confirm this is not a real vulnerability.
- Basically AppScan will report an SQL injection vulnerability everytime it finds "**OleDbException**" in the response. That's pretty lame.

12. DMG Forums_v3.1 / ASP.NET / http://www.dmgforums.com/

Valid vulnerabilities						
Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
Cross Site Scripting (XSS)	htmlform.aspx	TEXT	✗	✗	✗	✓
Summary			1 missed 0 found	1 missed 0 found	1 missed 0 found	0 missed 1 found
Score			-5	-5	-5	5
False positives						
Non-Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
Summary			0 reported	0 reported	0 reported	0 reported
Score			0	0	0	0
Total score			**-5**	**-5**	**-5**	**5**

13. Dave's CMS_v2.0.2 / ASP.NET / http://www.davidpirek.com/cms/

Valid vulnerabilities

Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
SQL Injection	blog.aspx	n	✓	✓	✓	✓
Summary			0 missed 1 found	0 missed 1 found	0 missed 1 found	0 missed 1 found
Score			5	5	5	5

False positives

Non-Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Summary			0 reported	0 reported	0 reported	0 reported
Score			0	0	0	0
Total score			**5**	**5**	**5**	**5**

Acunetix Test Application (Acunetix Acuart) / PHP / http://testphp.acunetix.com/

Valid vulnerabilities

Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Cross Site Scripting (XSS)	comment.php	name	✗	✓	✓	✓
Cross Site Scripting (XSS)	guestbook.php	name	✓	✓	✓	✓
Cross Site Scripting (XSS)	guestbook.php	text	✓	✓	✓	✓
Cross Site Scripting (XSS)	guestbook.php	login (Cookie)	✗	✗	✓	✓
Cross Site Scripting (XSS)	listproducts.php	cat	✓	✗	✓	✓
Cross Site Scripting (XSS)	listproducts.php	artist	✗	✓	✓	✓
Cross Site Scripting (XSS)	search.php	searchFor	✓	✓	✓	✓
Cross Site Scripting (XSS)	/secured/newuser.php	uuname	✗	✗	✓	✓
Cross Site Scripting (XSS)	/404.php/>"><ScRiPt>alert(443458495551)</ScRiPt>	N.A. The vulnerability is in the URI.	✗	✗	✗	✓
SQL Injection	/AJAX/infoartist.php	id	✗	✓	✓	✓
SQL Injection	/AJAX/infocateg.php	id	✗	✓	✓	✓
SQL Injection	/AJAX/infotitle.php	id	✗	✓	✓	✓
SQL Injection	artists.php	artist	✓	✓	✓	✓
SQL Injection	listproducts.php	cat	✓	✓	✓	✓
SQL Injection	listproducts.php	artist	✗	✓	✓	✓
SQL Injection	product.php	pic	✓	✓	✓	✓
Directory Traversal	showimage.php	file	✗	✗	✗	✓
Summary			10 missed 7 found	5 missed 12 found	2 missed 15 found	0 missed 17 found
Score			-15	35	65	85

False positives

Non-Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
SQL Injection	search.php	test	⛔			
File Inclusion	redir.php	r			⛔	
Summary			1 reported	0 reported	1reported	0 reported
Score			-1	0	-1	0
Total score			**-14**	**35**	**64**	**85**

Notes:
There is a PHP Code Execution vulnerability reported by Acunetix WVS. That vulnerability is only reported by Acunetix WVS and it seems to be a false positive. However, the attack vector from WVS works but any other PHP code doesn't work. Therefore, I suspect it's some kind of simulation for demonstration purposes.

AppScan Test Application (Altoro Mutual) / ASP.NET / http://demo.testfire.net/

Valid vulnerabilities

Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Cross Site Scripting (XSS)	bank/customize.aspx	lang	✓	✗	✗	N/A
Cross Site Scripting (XSS)	bank/login.aspx	uid	✓	✓	✓	
Cross Site Scripting (XSS)	bank/transfer.aspx	debitAccount	✓	✗	✗	
Cross Site Scripting (XSS)	bank/transfer.aspx	creditAccount	✓	✗	✗	
Cross Site Scripting (XSS)	comment.aspx	name	✓	✓	✓	
Cross Site Scripting (XSS)	search.aspx	txtSearch	✓	✓	✓	
Cross Site Scripting (XSS)	subscribe.aspx	txtEmail	✓	✓	✓	
Cross Site Scripting (DOM)	disclaimer.htm	<DOM based>	✓	✗	✗	
SQL Injection	bank/login.aspx	uid	✓	✓	✓	
SQL Injection	bank/login.aspx	passw	✓	✓	✓	
SQL Injection	bank/account.aspx	listAccounts	✓	✗	✗	
SQL Injection	/	amUserId (Cookie)	✓	✗	✗	
SQL Injection	bank/transaction.aspx	before	✓	✗	✗	
SQL Injection	bank/transaction.aspx	after	✓	✗	✗	
SQL Injection	bank/transfer.aspx	debitAccount	✓	✗	✗	
SQL Injection	bank/transfer.aspx	creditAccount	✓	✗	✗	
SQL Injection	subscribe.aspx	txtEmail	✓	✓	✓	
SQL Injection	bank/ws.asmx	__patternParameter__SOAP__creditAccount__2	✓	✗	✗	
SQL Injection	bank/ws.asmx	__patternParameter__SOAP__debitAccount__1	✓	✗	✗	
XPath Injection	bank/queryxpath.aspx	_ctl0:_ctl0:Content:Main:TextBox1	✓	✗	✗	
Local File Inclusion	default.aspx	content	✗	✓	✓	
Summary			1 missed 20 found	13 missed 8 found	13 missed 8 found	

Score			95	-25	-25	
False positives						
Non-Vulnerability	**File**	**Parameter**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
Summary			0 reported	0 reported	0 reported	N/A
Score			0	0	0	
Total score			**95**	**-25**	**-25**	

WebInspect Test Application (free Bank online) / ASP / http://zero.webappsecurity.com/

Valid vulnerabilities

Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
Cross Site Scripting (XSS)	rootlogin.asp	txtName	✓	✓	✓	N/A
Cross Site Scripting (XSS)	pformresults.asp	txtFirstName	✗	✓	✗	
Cross Site Scripting (XSS)	pformresults.asp	txtLastName	✗	✓	✗	
Cross Site Scripting (XSS)	pformresults.asp	dbConnectString	✗	✓	✗	
Cross Site Scripting (XSS)	join.asp	msg	✗	✓	✗	
Cross Site Scripting (XSS)	join.asp	mobilephone	✗	✓	✗	
Cross Site Scripting (XSS)	join.asp	country	✗	✓	✗	
Cross Site Scripting (XSS)	join.asp	postcode	✗	✓	✗	
Cross Site Scripting (XSS)	join.asp	homephone	✗	✓	✗	
Cross Site Scripting (XSS)	join.asp	town	✗	✓	✗	
Cross Site Scripting (XSS)	join.asp	address2	✗	✓	✗	
Cross Site Scripting (XSS)	join.asp	surname	✗	✓	✗	
Cross Site Scripting (XSS)	join.asp	email	✗	✓	✗	
Cross Site Scripting (XSS)	join.asp	house	✗	✓	✗	
Cross Site Scripting (XSS)	join.asp	street	✗	✓	✗	
Cross Site Scripting (XSS)	join.asp	name	✗	✓	✗	
Cross Site Scripting (XSS)	forgot2.asp	msg	✗	✓	✗	
Cross Site Scripting (XSS)	login/login.asp	UserName	✗	✓	✓	
Cross Site Scripting (XSS)	testing/pcomboindex.asp	cboPage	✓	✓	✓	
Cross Site Scripting (XSS)	pcomboindex.asp	referer (Header)	✗	✗	✓	
Cross Site Scripting (XSS)	pcomboindex.asp	user-agent (Header)	✗	✗	✓	
Cross Site Scripting (XSS)	cookietest/ShowCookies.asp	Second (Cookie)	✗	✓	✗	
Cross Site Scripting (XSS)	cookietest/ShowCookies.asp	FirstCookie (Cookie)	✗	✓	✗	

Cross Site Scripting (XSS)	cookietest/ShowCookies.asp	userid (Cookie)	✗	✓	✗	
Cross Site Scripting (XSS)	cookietest/ShowCookies.asp	username (Cookie)	✗	✓	✗	
Cross Site Scripting (XSS)	cookietest/ShowCookies.asp	State (Cookie)	✗	✓	✗	
Cross Site Scripting (XSS)	cookietest/ShowCookies.asp	Keyed (Cookie)	✗	✓	✗	
Cross Site Scripting (XSS)	banklogin.asp	err	✓	✓	✓	
Cross Site Scripting (XSS)	plink.asp	a	✓	✓	✓	
Cross Site Scripting (XSS)	plink.asp	c	✓	✓	✓	
SQL Injection	login1.asp	login	✓	✓	✓	
SQL Injection	forgot1.asp	get	✗	✓	✗	
Local File Inclusion	rootlogin.asp	txtName	✗	✓	✗	
HTTP Response Splitting	login1.asp	login	✓	✗	✓	
Summary			27 missed 7 found	3 missed 31 found	24 missed 10 found	
Score			-100	140	-70	

False positives

Non-Vulnerability	File	Parameter	AppScan	WebInspect	Acunetix	Acunetix + AcuSensor
SQL Injection	plink.asp	a	⊖			N/A
SQL Injection	plink.asp	c	⊖			
Summary			2 reported	0 reported	0 reported	
Score			-2	0	0	
Total score			**-102**	**140**	**-70**	

Notes:
pcomboindex.asp will dump the HTTP request so any header can be used to cause an XSS vulnerability.

Summary results for all tested applications

Best scores / application						
Nr.	**Tested application**	**Platform**	**AppScan**	**WebInspect**	**Acunetix**	**Acunetix + AcuSensor**
1	Javascript tests	N/A		✓		
2	Vanilla-1.1.4	PHP				✓
3	VivvoCMS-3.4	PHP				✓
4	fttss-2.0	PHP				✓
5	Wordpress-2.6.5	PHP	No clear winner			
6	vbulletin_v3.6.8	PHP	No clear winner			
7	riotpix v0.61	PHP				✓
8	javabb_v0.99	Java			✓	
9	Yazd Discussion Forum_v3.0	Java	✓	✓		
10	pebble_v2.3.1	Java	No clear winner			
11	TriptychBlog_v.9.0	ASP.NET	No clear winner			
12	DMG Forums_v3.1	ASP.NET				✓
13	Dave's CMS_v2.0.2	ASP.NET	No clear winner			
14	Acunetix Demo Application - Acunetix Acuart	PHP				✓
15	AppScan Demo Application - Altoro Mutual	ASP.NET	✓			
16	WebInspect Demo Application - free Bank online	ASP		✓		
	Summary		**2 wins**	**3 wins**	**7 wins**	

Conclusions

Before starting this evaluation my favorite scanner was AppScan. They have a nice interface and I had the impression they are very fast.
After the evaluation, I've radically changed my opinion: AppScan scored worst in almost all the cases.
They are finishing the scan quickly because they don't do a comprehensive test.
And they have a huge rate of false positives. Almost all scans contain some false positives (most of the times for applications that are not even installed on the machine). They have a lot of space for improvement.

Acunetix WVS and WebInspect are relatively good scanners.
If you are in the position to use the AcuSensor technology (PHP, ASP.NET and you are not required to do a blackbox testing) then Acunetix WVS + AcuSensor is the better choice.

As these results show, blackbox testing is not enough anymore.

If you cannot use AcuSensor then you should decide between WebInspect and Acunetix WVS.
Both have their advantages and disadvantages. Browse the results and decide for yourself.

Final words

I've included enough information in this report (the javascript files used for testing, exact version and URL for all the tested applications) so anybody with enough patience can verify and reproduce the results presented here.

Therefore, I will not respond to emails for vendors.
You have the information, fix your scanners!