

Acunetix Web Vulnerability Scanner 맞보기

작성날짜: 2010년 5월 21일 금요일

메일주소: <u>boangongbu@naver.com</u>

Acunetix Web Vulnerability Scanner 모르시는분들이 있을지 모르겠지만. 보안에 관심이있거 나 보안업계에 몸을 담고있다면 모르시는분이 없으리라고 믿구있구요. 해커의 컴퓨터라면 거의 다 깔려있을법한 아큐네틱스. 그럼 아래에 간략한 사용법을 소개해드리도록 하겠습니 다.

다운로드: <u>http://rapidshare.com/files/356407862/2010_02_10_01_webvulnscan65.exe</u> 크랙파일: http://rapidshare.com/files/356414045/web.vulnerability.scanner.6.5.patch.rar

위 링크에서 설치파일과 크랙파일을 받으시구요. 먼저 프로그램을 설치하고 크랙파일을 설 치폴더에 위치한다음 patch 를 클릭하면 크랙은 완료.

Acunetix Web Vulnerability Sca	anner (Enterprise Edition)	×
File Actions Tools Configu	juration Help	
New Scan 🕓 🌶 🔎 🗟		
Tools Explorer 🏨	🗋 😂 🌸 🛃 🐨 🕼 Report 🔊 Start URL: http://testphp.acunetix.com 🗸 offie: default 💽 J	Start
Web Vulnerability Scanner	Concentration set	URITY
⊡⊡ Tools 	Web Scanner	
Configuration	No data to display. You have either not performed a scan or need to load a saved scan results. To start a new scan: File > New > Web site scan To load the results of a saved scan: File > Load scan results 	
🔂 Settings Scanning Profiles □/┌── General	Acunetix Ltd © 2010 All rights reserved. Acunetix WVS v6.5 Build 20	100210
Program Updates	Activity Window	<u>t</u>
- 1.0 Version Information - 2 Licensing - 2 Support Center - 2 Purchase - 2 User Manual (html) - 2 User Manual (html)	5월 21 10:19.34, Load module "Web Services - Multirequest parameter manipulation" 5월 21 10:19.34, 14 modules loaded. 5월 21 10:19.37, Determining necessary updates 5월 21 10:20.01, Canceled.	•
AcuSensor	Application Log Error Log	
Ready		11

프로그램을 실행하면 아래와 같은 프로그램창을 확인가능.

제일 처음 해야될건 프로그램 업그레이드.

메뉴바에서 "Help" -> "Check for updates" 를 실행하여 업데이트파일 존재여부를 확인.

만약 업데이트 가능한 파일들이 존재한다면 아래처럼 파일리스트가 보여질꺼구요.

Acunetix Web Vulnerability Sc	anner (Enterprise Edition)		_	
File Actions Tools Config	juration Help			
🛾 🗋 New Scan 🔂 🎯 🔑 🍭	💿 🔜 🗞 💿 👌 🔛 🖡	2 🛃 🖻 2 🖓 🖬		
Tools Explorer 4	🔕 Check for Updates 🛛 👔	Download and Install Updates	🙃 Download and Install New Build	
Web Vulnerability Scanner	🚸 New build is available (Buil	d number 20100419, Filename 2010_	_04_19_01_webvulnscan65.exe).	
🚊 🔂 Tools	Date	File Name	File Size	Progress
🥸 Site Crawler	🔂 목요일, 2월 11, 2010	patch_20-21.cab	364 Kb	
Target Finder	Updated CSA (bugfixed	es).		
Blind SOL Triestor	🗄 🕖 Changes (1)			
HTTP Editor	🐞 금요일, 2월 12, 2010	patch_21-22.cab	365 Kb	
HTTP Sniffer	Updated CSA (bugfixe	es).		
HTTP Fuzzer	E OPL a S a seco			
	[] 수요일, 3월 3, 2010 □ 004 free and added	patch_22-23.cab	466 KD	
Compare Results	CSA fixes and added	a check for XML External Entity Injec	tion.	
Web Services Scapper		patch 22.24 cab	265 Mb	
Web Services Editor	Undated CSA	patch_25-24.cab	303 KD	
	the changes (1)			
🔂 Settings	·····································	patch 24-25.cab	2 KP	
Scanning Profiles	Added compliance ren	part for Owasp Top 10 2010.	E ND	
General				
Version Information	Activity Window			
	5월 21 10:19.34, Load mod	lule "Web Services - Multireque	est parameter manipulation"	
Support Center	5월 21 10:19.34, 14 modules l	oaded.		
Purchase	5월 21 10:19.37, Determining	necessary updates		
User Manual (html)	5월 21 10:20.01, Canceled.			
User Manual (pdf)	Application Log Error Log			
Beadu				
(in stay				

"Download and Install Updates" 를 실행하여 이들을 설치.

옆메뉴에서 "Download and Install New Build" 버튼이 활성화 되었을시는 새로운 프로그램이 발표되었다는 얘기구요. 우선 새로운 버전의 크랙파일이 공개되었는지를 확인하고 업그레이 드하는 것을 추천. 만약 그렇지 않다면 업그레이드후 프로그램이 실행안되는 불상사가 발생. (아큐네틱스는 프로그램 업그레이드가 빈번하다.)

그럼 타겟을 하나 잡고 스캔을 해보도록 하겠습니다.



메뉴바에서 "File -> New -> Web Site Scan" 을 클릭 혹은.



그럼 아래와 같은 창이 뜰건데요.

Scan Wizard		23				
Scan Type Select Targets Crawling Options	Scan Type Select whether you want to scan a single website, a list or range of websites or whether you want to the results of a previous crawl.) analyze				
Scan Options Login Error Pages Finish	Scan type Scan type Here you can scan a single website. In case you want to scan a single web application and whole site you can enter the full path below. The application supports HTTP and HTTPS we Scan single website					
	Website URL: http://testphp.acunetix.com If you saved the site structure using the site crawler tool you can use the saved results here. Th Scan will load this data from the file instead of crawling the site again. Scan using saved crawling results					
	In case you want to scan a list of websites, you need to choose this option. Prepare a text fil containing the list of websites and indicate the path of this file below. Scan a list of websites from a file	3				
	Filename: You can also scan a range of computers. This wizard will inspect this range looking for HTTF HTTPS websites. You may select individual websites later after the discovery was finished.	4				
acunetix	IP range: 192.168.0.1-30 List of ports: 80,443	▼▼				
	< <u>B</u> ack <u>N</u> ext > Ca	incel				

1번: 특정타겟 웹사이트의 도메인을 입력.

2번: "Site Crawler" 프로그램으로 스캔가능한 웹사이트주소를 수집하였고 또 이를 저장하였을시 해당파일을 선택하여 다수스캔이 가능. (Site Crawler툴은 뒤에서 설명드릴꺼구요)
3번: 텍스트파일에 저장된 웹사이트들을 스캔하려고 할시. 이를 선택.
4번: 직접 특정 아이피대역을 입력하여 스캔을 하려고 할시 4번을 선택.

선택완료후 "Next"를 클릭하여 다음페이지로 이동함.

Scan Wizard			23
Scan Type Select Targets Crawling Options	Select Targets Please wait until the scanning is finished and then s For every target you can enter details such as oper path. By entering these details you can reduce the	select the targets you want to scan from the list be ating system, webserver, technology or change th scanning time.	elow. ne base
Scan Options	List of targets		
Finish	E testphp.acunetix.com:80 Base path Server banner Target URL Operating system WebServer	Apache/2.0.55 (Ubuntu) mod_python/3.1.4 Pythttp://testphp.acunetix.com:80/ Unix Apache 2.x	thon/2.4.
	Detected custom 404 error page	No [PHP, Perl, mod_ssl, mod_perl, mod_python, Op	penSSL]
acunetix	Status : Done		
		< Back Next Car	ncel

이 페이지 에서는 타겟 웹사이트의 간략한 정보를 보여줌. 상관말고 "Next"

Scan Wizard		23		
Scan Type	Crawling Options Here you can set crawling options.			
Select Targets Free you can set clawing options. Crawling Options Crawling options Login Image: Start HTTP shifter for manual crawling at the end of the process Get first URL only Image: Do not fetch anything above start folder Image: Fetch files below base folder Image: Fetch files below base folder Image: Start HTTP shifter forms Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter forms Image: Below base folder Image: Start HTTP shifter formshifter for m				
acunetix				
	< Back Next Car	ncel		

스캔시 각종 옵션들인데 그냥 상관없이 "Next"



 Scan options 	
🎯 These option general sca	ons will define the behaviour of the an behaviour, you should go to setti
Scanning mode: [Heuristic
Test known w (For a large n	Heuristic Extensive amber or anectones, enabling this o

여기는 스캔속도설정, 빠르게? 일반? 아니면 느리게? 스캔결과의 정확도에 영향주는거니깐 그냥 일반적으로 "Heuristic" 그대로 두시면 되구요.

Scan Wizard		23			
Scan Type Select Targets Crawling Options	Scan Options Here you can set scan options.				
Scanning profile Login Finish Scanning profile will enable/disable different tests (or group of tests) from the test database. Use this scanning profile: default					
Scan options These options will define the behaviour of the scan for the current scans. If you want to mo general scan behaviour, you should go to settings.					
Scanning mode: Heuristic <u>Help</u> Test known web application vulnerabilities in all directories (For a large number of directories, enabling this option will generate a lot of HTTP requests.)					
	 Enable Port Scanning Enable <u>AcuSensor Technology</u> 				
acunetix					
	< <u>B</u> ack Next Can	cel			

역시 "Next"

	A . dla andia a'	tions -	
HIIF	Authentica	lion	
<u>8</u>	If your web you need to	site requires HTTP authentication (Basic or N p provide the credentials below.	ΓLM),
💌 Au	uthenticate v	with this username and password combination	:
ι ι	Jsername :	OFOICI	
F	^o assword :	*******	

그다음 페이지로 넘어왔을 때 로그인이 필요한 사이트라면 설정해야될 옵션들이죠. HTTP인증이 필요한 웹페이지라면 체크를 하시고 아이디 하고 패스워드를 입력.

Form:	 Forms Authentication (Login Sequence) 					
<u> </u>	If your website rea website. This will You can also spe links that will log y	If your website requires forms authentication, you need to record website. This will be saved as a login sequence file and can be You can also specify a section of the website which you do not links that will log you out from the website).				
	Login sequence <no login="" sequence=""></no>					
Record New Login Sequence						

만약 웹로그인이 필요하다면 위에 버튼을 클릭하면 오픈되는 웹사이트에서 로그인하시고 세 션을 저장.

Scan Wizard	
Scan Type Select Targets Crawling Options	Login Configure input/login details for password protected areas or HTML forms
📃 Scan Options	THTTP Authentication
Login Finish	If your website requires HTTP authentication (Basic or NTLM), you need to provide the credentials below.
	Authenticate with this username and password combination :
	Username : 0;0;0;[]
	Password : XXXXXXXXX
	 Forms Authentication (Login Sequence) If your website requires forms authentication, you need to record the steps required to login on the website. This will be saved as a login sequence file and can be used later. You can also specify a section of the website which you do not want to be crawled (for example links that will log you out from the website). Login sequence <no login="" sequence=""></no> Record New Login Sequence
acunetix	
	< <u>B</u> ack <u>N</u> ext Cancel

저장이 끝났다면 저장된 세션을 선택하고 "Next" 클릭.

【실전으로 배워보는 인터넷보안】

Scan Wizard		x
Scan Type Select Targets Crawling Options Scan Options Login	Finish Here you can review your scanning details. Verify if everything is in order and then click Finish. Scan Summary	
Finish	List of targets selected for scanning	^
	Profile	
	default	
	Targets • http://testphp.acunetix.com:80/ OS: Unix Server: Apache 2.x Technologies: PHP,Perl,mod_ssl,mod_perl,mod_python,OpenSSL	
acunetix	The Source coordinate to detablish for report constraints	Ŧ
	Save scan results to database for report generation. < <u>Back</u> <u>Finist</u> Cancel	

여기까지 오면 설정 완료. 그냥 "Finish" 를 클릭하시면 스캔이 시작됩니다.

【실전으로 배워보는 인터넷보안】



스캔이 시작되면 위에 상태로 보여지는데요.

- 1) 여러가지 보조용 해킹툴
- 2) 웹사이트 파일리스트와 존재하는 버그들
- 3) 위험레벨
- 4) 현재 진행상태

스캔이 완료되었다면 2번창에서는 아래와 유사한 정보를 확인가능.



현재 존재하는 버그들을 그 위험도에 따라 색상별로 정리가 됨. 그리고 스캔옵션 설정시 포 트스캔설정도 체크를 하였다면 현재 서버에 오픈된 포트가 아래에 보여짐. (개인적으로 이 옵션은 닫아두는 것을 추천함.) 그리고 그 아래에는 사이트 폴더와 파일구조를 확인할수있 구요 이는 실정 해킹에 많은 도움이 되죠.

【실전으로 배워보는 인터넷보안】

Acunetix Web Vulnerability Sc	anner (Enterprise Edition)							
File Actions Tools Config	guration Help							
📲 New Scan 🕓 🎯 🔎 🔍	💿 🗟 🌒 🕘 🖉 🛃	2 🖉	a					
Tools Explorer 4	IP Range: 192.168.1.1-30				✓ List of Po	rts: 80,443	-	
Web Vulnerability Scanner	Server	Hostname	Ba	nner		Web Server		3
Web Scather Tools Site Crawler Target Finder Subdomain Scather Bind SQL Injector HITP Editor	C http://192.168.1.1:80/		A	thentication required.				
	Response Headers Response Data	View Page						
HIP Shifter HIP Starter Web Services Scamer Web Services Caning Profiles Graning Profiles								
	Activity Window							4
	[5] 23 14:42.01, Parameter manipula [5] 28 14:42.43, Find targets (loc [5] 28 14:42.50, Done [5] 28 14:42.55, Find targets (loc [5] 28 14:43.03, Done [6] Application Log [7] Part Log	tion is executing or oking for HTTP) . oking for HTTP) .	n script "/redir.php (9 of 14)" 					-
Ready								11

왼쪽 프로그램리스트에서 "Target Finder" 는 일정한 IP대역에 대한 스캔을 통하여 현재 웹 서버가 실행중인 아이피를 확인.

Acunetix Web Vulnerability Scanner (Enterprise Edition)	
File Actions Tools Configuration Help	
- Mew Scan 🔼 🌚 🔎 🖲 👔	
Tools Explorer 4	
Web Vulnerability Scanner	
Web Scanner	HIP Kequest Setting Tools
Tools D	erault value: 1 🔹
Site Crawler Starget Finder Subdomain Scamer Subdomain Scamer Subdomain Scamer Mitthe Starget Mitthe Starget Mitthe Starget Mitthe Starget Subdomain Scamer Web Services Scamer Results Configuration General Orgam Updates Version Information Westion	1 GET http://testphp.acunetix.com:80/artists.php?artist=\$(injectHere) HTTP/1.0 2 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322) 4 Host: testphp.acunetix.com 5 Connection: Close 7 Fragma: no-cache 8 Acunetix-Froduct: WV5/6.0 (Acunetix Web Vulnerability Scanner - NORMAL) 9 Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED 10 Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm Look for: Image: State Stype: MySQL Image: State Stype: MySQL Image: State Stype: MySQL
Support Center	Current database: acuart
User Manual (html)	Current user: acuart@localhost
User Manual (pdf)	
	5.0.22-Debian_Oubuntu6.06.6-logacuartacuart@localhost
A	Activity Window
5	월 28 14:43.20, URL redirection "/redir.php" on parameter "r" <
5	² ² ² ¹
5	2 20 14-13.2 (LEF induced in Figure 1) (February 1) (Febr
5	월 28 14:43.34, CRLF injection/HTTP response splitting "/redir.php" on parameter "r"
	Andreation Los Strong Los
-	Approximiting
Ready	

"Blind SQL Injection" 툴은 SQL인젝션 버그가 존재하는 페이지에 대한 침투테스트를 도와주 는 기능이구요. 위에 화면처럼 현재 서버에 사용된 디비서버 유형과 버전. 그리고 현재 웹사 이트에 사용된 디비유저등 정보를 확인하실수있구요.

그외에도 다른기능들이 있지만 다음기회에 소개해드리는거로 하구요 일단 여기까지만 아셔 도 자신이 운영하고 있는 웹사이트에 대한 보안체킹이 가능하니깐 한번씩은 프로그램을 다 운받으셔서 웹서버의 보안상태를 점검해보시는 것을 추천합니다.

더욱 상세한 정보는 아큐네틱스 공식홈페이지(<u>http://www.acunetix.com</u>) 을 확인하시거나 매 뉴얼 파일을 다운받아 보시는 것을 추천드립니다. **매뉴얼 파일:** http://www.acunetix.com/vulnerability-scanner/wvsmanual.pdf

그리고 마지막으로 acunetix 는 유료 프로그램이기에 여건이 되시는분들은 최대한 정품을 사용하시길 바랍니다. ^^

그럼 다음강좌에서 봐요~