

Task: Web-Anwendungen

Inhalt

- [Einfachen Scan von Webanwendungen ausführen](#)
- [Fine-Tuning für Scan von Web-Anwendungen](#)
- [Anpassung Scanner Preferences](#)
- [Anpassung NVT Preferences](#)

Einleitung

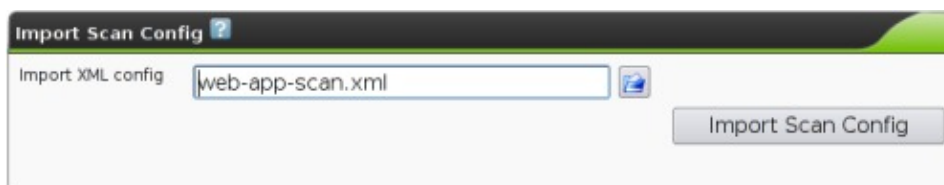
Der Greenbone Security Manager unterstützt die Prüfung von Web-Anwendungen auf 2 Arten:

- Durch eigene Network Vulnerability Tests (NVTs, etwas über 1500 haben Relevanz für Web-Anwendungen)
- Durch den integrierten Web-Anwendungs-Scanner [w3af](#)

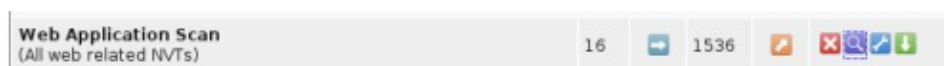
Einfachen Scan von Webanwendungen ausführen

Dieses Beispiel führt eine breit angelegte Prüfung von Web-Anwendungen aus. Ein erfahrener Anwender wird auf einer solchen Basis in eine vertiefte Prüfung mit angepassten Parametern einsteigen.

1. Importieren Sie die Scan Configuration [Web-Application Scan](#).



2. Diese Konfiguration beinhaltet alle Network Vulnerability Tests (NVT's), die in irgendeiner Weise relevant für die Prüfung von Web-Anwendungen sind. Dabei reichen die Überprüfungen von Webserver-Versionen über bekannte Schwachstellen in Web-Applikationen bis hin zu rudimentärer generischer Suche (Fuzzing).



Dies hat den Vorteil, dass kein zeitintensives Auswählen relevanter NVT's nötig ist. Auf der anderen Seite wird dieser allgemeine Scan länger dauern und ggf. zuviel Informationen zusammenstellen als eigentlich notwendig.

Es ist also eine Konfiguration um eine noch nicht tiefgreifend analysierte Web-Anwendung kennen zu lernen um anschließend die Punkte zu identifizieren die eine tiefere Analyse notwendig erscheinen lassen.

3. Legen Sie die Zielsysteme (Targets) fest.

New Target ?

Name:

Comment (optional):

Hosts:

Credential (optional):

4. Nun können Sie die Aufgabe (Task) erstellen. Dafür kombinieren Sie die oben importierte Scan Configuration mit den entsprechend erstellten Zielsystemen.



New Task ?


Name:

Scan Config:

Scan Targets:

Escalator (optional):

5. Die Suche wird gestartet in dem Sie für den eben erstellten Task auf  klicken. Es kann einige Zeit dauern, bis der Scan abgeschlossen ist. Den aktuellen Stand des Scans erhalten Sie indem Sie auf  klicken.


Task Summary ? 

Name: **Web Application Scan Task** [Back to Tasks](#)


Config: [Web Application Scan](#)



Escalator:

Target: [Web Application Server](#)

Status:  48 %

Reports: 1 (Finished: 0)

Reports for "Web Application Scan Task" ? 

Report	Threat	Scan Results				Download	Actions
		Critical	Medium	Low	Log		
Mon Feb 15 22:59:04 2010 Running	Medium	0	2	70	3	PDF <input type="button" value="Download"/>	 

6. Sobald der Status auf "Done" wechselt, ist der vollständige Bericht verfügbar. Sie können aber auch schon während des Scans die bereits gefundenen Ergebnisse einsehen.

Filtered Results

Host	High	Medium	Low	Log	Total
192.168.2.4	26	129	0	0	155
192.168.2.6	4	5	0	0	9
Total: 2	30	134	0	0	164

Port summary for host "192.168.2.4"

Service (Port)	Threat
general/tcp	High
http (80/tcp)	High
https (443/tcp)	High
cvspserver (2401/tcp)	Medium
ipp (631/tcp)	Medium
ndl-aas (3128/tcp)	Medium
netbios-ns (137/udp)	Medium
rsync (873/tcp)	Medium

Security Issues reported for 192.168.2.4

High general/tcp
NVT: [moziloCMS Multiple Cross Site Scripting Vulnerabilities \(OID: 1.3.6.1.4.1.25623.1.0.801076\)](#)

Overview: The host is running moziloCMS and is prone to Multiple Cross Site Scripting Vulnerabilities

Vulnerability Insight:
 The flaws are due to an error in 'admin/index.php'. The input values are not properly verified before being used via 'cat' and file parameters in an 'editsite' action.

Impact:
 Successful exploitation will allow remote attackers to execute arbitrary HTML and script code in a user's browser session in the context of an affected site.

Impact Level: Application.

Affected Software/OS:
 moziloCMS version 1.11.1 and prior on all running platform.

Fix:
 No solution or patch is available as on 07th December, 2009. Information regarding this issue will be updated once the solution details are available. For updates refer, http://cms.mozilo.de/index.php?cat=10_moziloCMS&page=50_Download


References:
<http://en.securitylab.ru/nvd/388498.php>
<http://downloads.securityfocus.com/vulnerabilities/exploits/35212.txt>

Fine-Tuning für Scan von Web-Anwendungen

Die im obigen Beispiel importierte Scan Configuration auch als Grundlage für speziell angepasst Scans verwendet werden.

Konkret kann zum einen eine individuelle Unterauswahl der NVT's erstellt werden. Zum anderen kann die Parametrisierung ausgestaltet werden.

Anpassung Scanner Preferences

Klicken Sie in der Übersicht der Scan Configurations auf das Icon  um die Scan-Parameter je nach Bedarf im Abschnitt "Edit Scanner Preferences" anzupassen.

Die hier gemachten Justierungen werden von allgemeinen NVT's berücksichtigt, nicht aber von w3af. Das integrierte Werkzeug erlaubt eine eigenen, unabhangige Parametrisierung.

- *cgi-path*: Falls bekannt, konnen Sie hier weitere Pfade angeben um sie beim Scan zu beruckichtigen.

cgi_path	/cgi-bin:/scripts
----------	-------------------

Die einzelnen Pfade werden jeweils mit einem Doppelpunkt getrennt.



- *port_range*: Liegen die Ports fest auf denen die Web-Anwendung lauft, kann hier durch eine Einschrankung die Zahl nicht-relevanter Scan-Ergebnisse deutlich reduziert werden (z.B. nur "80, 8080, 8443").

port_range	80, 443, 8080, 8443
------------	---------------------



Diese Einschrankung macht vor allem deshalb Sinn, weil es eine Reihe von Standard-Diensten gibt die auf HTTP-Basis funktionieren. Sie laufen auf irgendwelchen anderen Ports und werden beim Scan-Vorgang (richtigerweise) als eine Web-Anwendung identifiziert und dann im Detail gepruft.

Mit dem "Save Config"-Knopf am Ende dieses Abschnittes werden die anderungen ubernommen.

Anpassung NVT Preferences

Klicken Sie in der bersicht der Scan Configurations auf das Icon  und gehen Sie zum Abschnitt "Network Vulnerability Test Preferences". Dort kann man direkt uber das Icon  zum NVT-Editor springen dessen Parameter einstellen.



- *Global variable settings (Enable CGI scanning)*: Schaltet den Test von CGI's ein.

Global variable settings	Enable CGI scanning	yes	 
--------------------------	---------------------	-----	---

Dies ist auch voreingestellt. Wenn keine solchen Tests gemacht werden sollen, schalten Sie hier um von "yes" auf "no".

Enable CGI scanning	<input checked="" type="radio"/> yes <input type="radio"/> no
---------------------	---

- *Global variable settings (HTTP User-Agent)*: Jedes Programm welches einen Web-Server anspricht sendet dabei eine eigene Kennzeichnung mit. Auch beim Scan wird eine solche Kennung mitgesendet und sie kann hier eingestellt werden.

Global variable settings	HTTP User-Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)	 
--------------------------	-----------------	--	---

In einigen Fallen verhalt sich eine Web-Anwendung unterschiedlich je nach dem ob sich beispielsweise ein Mozilla Browser oder ein Internet Explorer meldet. Insofern kann eine Variation notwendig werden um ein bestimmtes Verhalten zu testen.

Ein weitere Aspekt ist, dass eine spezielle Kennung erlaubt, in den Logeintragen des Web-Servers die Auswirkungen des Scans leichter zu finden.

HTTP User-Agent Mozilla/4.0 (compatible; MSIE 6.0; Windc

- **HTTP login page (Login form, Login form fields, Login page):** Diese Einstellungen helfen der Scan-Engine sich bei anmeldepflichtigen Web-Anwendungen einzuloggen um dann erst die Tests auszuführen. Andernfalls würden die Tests mangels Authorisierung abgewiesen werden.

HTTP login page	Login form :		 
HTTP login page	Login form fields :	user=%USER%&pass=%PASS%	 
HTTP login page	Login page :	/	 

Mit *Login form* wird die URL zur Aktion der Web-Anwendung für das einloggen gesetzt. Wenn Sie die Web-Anwendung im Browser aufrufen können Sie die URL zumeist direkt ablesen.

Die *Login page* bezeichnet die URL auf der die Aktion zum einloggen ausgelöst werden kann.

Schliesslich kann mit *Login form fields* für URL-basierte Web-Anmeldungen über die Platzhalter "%USER%" und "%PASS%" das Benutzerkonto mit Passwort übermittelt werden. Das konkrete Format müssen Sie auch hier aus der zu prüfenden Web-Anwendung ermitteln. Die konkreten Zugangsdaten lassen sich über das NVT "Login configurations" (siehe unten) einstellen.

Login page :	/login.html
Login form :	/authenticate.php
Login form fields :	user=%USER%&pass=%PASS%

- **Login configurations (HTTP account, HTTP password):** Mit diesen beiden Parameter werden Zugangsdaten definiert die benutzt werden um auf den entsprechend konfigurierten Login-Seiten (siehe oben) eine Anmeldung durchzuführen und der Scan damit über die Login-Seite hinaus in die eigentliche Anwendung wirksam wird.



Login configurations	HTTP account :	 
Login configurations	HTTP password (sent in clear) :	 

Es sollten hierfür nur Test-Zugänge verwendet werden. Beachten Sie, dass ggf. das Passwort im Klartext gesendet wird.

Wenn die Änderung des Passworts in Kraft treten soll, so muss "Replace old value" explizit angeschaltet werden. Ansonsten wird das eingegebenen Passwort bei der Aktion "Save Config" wieder verworfen.

HTTP account :	<input type="text"/>
HTTP password (sent in clear) :	<input type="text"/> <input type="checkbox"/> Replace old value





- **Nmap (NASL wrapper) (Service scan):** Eine Umstellung auf "yes" kann die Informationsgewinnung vor dem eigentlichen Schwachstellen-Scan erhöhen.

Nmap (NASL wrapper)	Service scan	no	 
---------------------	--------------	----	---

Das macht nur dann Sinn, falls noch unklar ist auf welchen Systemen und an welchem Port Web-Anwendung arbeiten. Ggf. macht es auch Sinn, falls die Web-Anwendung ansonsten nicht auf Anrieb als solche erkannt wird.

Service scan yes no


























- *Web mirroring (Number of pages to mirror, Start page)*: Für den Scan einer Webanwendung wird ein Spiegel (also eine Kopie in Form einer Momentaufnahme) erstellt. Während des Scans arbeitet sich die Scan-Engine systemtisch durch die Verweisstruktur.

Web mirroring	Number of pages to mirror :	200	 
Web mirroring	Start page :	/	 

Diese beiden Einstellungen beschreiben wieviele Webseiten gespiegelt und wo damit gestartet werden soll. Die Voreinstellungen sind in der Regel ausreichend für eine erste Prüfung. Je nach Web-Anwendung kann es jedoch notwendig werden entsprechend nachzustimmen.

Number of pages to mirror :	<input type="text" value="200"/>
Start page :	<input type="text" value="/"/>


- *HTTP NIDS evasion*: Falls versucht werden soll ein Intrusion Detection System (IDS), Intrusion Prevention System (IPS) oder eine vorgeschaltete Web Application Firewall (WAF) zu umgehen, bietet dieses NVT eine Reihe von Einstellungen.

HTTP NIDS evasion	CGI.pm semicolon separator	no	 
HTTP NIDS evasion	Dos/Windows syntax	no	 
HTTP NIDS evasion	Double slashes	no	 
HTTP NIDS evasion	HTTP/0.9 requests	no	 
HTTP NIDS evasion	Null method	no	 
HTTP NIDS evasion	Parameter hiding	no	 
HTTP NIDS evasion	Premature request ending	no	 
HTTP NIDS evasion	Random case sensitivity (Nikto only)	no	 
HTTP NIDS evasion	Self-reference directories	no	 
HTTP NIDS evasion	TAB separator	no	 
HTTP NIDS evasion	Use HTTP HEAD instead of GET	no	 
HTTP NIDS evasion	Force protocol string :		 
HTTP NIDS evasion	HTTP User-Agent		 
HTTP NIDS evasion	Absolute URI host	none	 
HTTP NIDS evasion	Absolute URI type	none	 
HTTP NIDS evasion	Reverse traversal	none	 
HTTP NIDS evasion	URL encoding	none	 

Die Justierung dieser Einstellungen sollte mit Kenntnis der IDS/IPS/WAF Technologien erfolgen.

HTTP User-Agent	<input type="text"/>
Use HTTP HEAD instead of GET	<input type="radio"/> yes <input checked="" type="radio"/> no
URL encoding	<input checked="" type="radio"/> none <input type="radio"/> Hex <input type="radio"/> UTF-16 (double byte) <input type="radio"/> UTF-16 (MS %u) <input type="radio"/> Incorrect UTF-8
Absolute URI type	<input checked="" type="radio"/> none <input type="radio"/> file <input type="radio"/> gopher <input type="radio"/> http
Absolute URI host	<input checked="" type="radio"/> none <input type="radio"/> host name <input type="radio"/> host IP <input type="radio"/> random name <input type="radio"/> random IP
Double slashes	<input type="radio"/> yes <input checked="" type="radio"/> no
Reverse traversal	<input checked="" type="radio"/> none <input type="radio"/> Basic <input type="radio"/> Long URL
Self-reference directories	<input type="radio"/> yes <input checked="" type="radio"/> no
Premature request ending	<input type="radio"/> yes <input checked="" type="radio"/> no
CGI.pm semicolon separator	<input type="radio"/> yes <input checked="" type="radio"/> no
Parameter hiding	<input type="radio"/> yes <input checked="" type="radio"/> no
Dos/Windows syntax	<input type="radio"/> yes <input checked="" type="radio"/> no
Null method	<input type="radio"/> yes <input checked="" type="radio"/> no
TAB separator	<input type="radio"/> yes <input checked="" type="radio"/> no
HTTP/0.9 requests	<input type="radio"/> yes <input checked="" type="radio"/> no
Force protocol string :	<input type="text"/>

- *w3af (NASL wrapper) (Profile)*: Der integrierte Web-Anwendungsscanner "w3af" erlaubt unterschiedliche Profile für einen Scan.

w3af (NASL wrapper)	Profile	full_audit	 
---------------------	---------	------------	---

Das voreingestellte Profil "full_audit" sorgt für einen umfassenden Scan. Für weitere Profile und Anpassungsmöglichkeiten bietet die Dokumentation von w3af Unterstützung.

Profile	<input type="text" value="full_audit"/>
---------	---