

Análise em Aplicações Web

+ Dessa vez, usaremos o Template: Web Application Tests

+ Modo de uso:

New Scan / Web Application Tests

[← Back to Scan Templates](#)

Settings

Credentials

Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

Host 172.16.1.7 - Web

Description

Folder

My Scans

Targets

172.16.1.7

Upload Targets

Add File

Save Cancel

→ As configurações de scan estarão bem diferentes, por se tratar de um scan diferente do básico.

→ Esse já demorou mais de uma hora para ser realizado

+ Um fato interessante é que podemos ocultar ou modificar os resultados apresentados no relatório da ferramenta.

Host 172.16.1.7 - Web / 172.16.1.7

[← Back to Hosts](#) [Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

Vulnerabilities 29

Filter Search Vulnerabilities 29 Vulnerabilities

Sev	Name	Family	Count	
High	CGI Generic Remote File Inclusion	CGI abuses	1	
High	CGI Generic SQL Injection	CGI abuses	1	
High	CGI Generic SQL Injection (2nd pass)	CGI abuses	1	
High	Free Articles Directory index.php page Parameter Remote File Inclusion	CGI abuses	1	
Misc	PHP (Multiple Issues)	Web Servers	3	
Medium	Browsable Web Directories	CGI abuses	1	
Medium	CGI Generic Cookie Injection Scripting	CGI abuses	1	
Medium	CGI Generic HTML Injections (quick test)	CGI abuses : XSS	1	
Medium	CGI Generic XSS (comprehensive test)	CGI abuses : XSS	1	
Medium	SQL Dump Files Disclosed via Web Server	CGI abuses	1	
Medium	Web Application Information Disclosure	CGI abuses	1	

Host Details

IP: 172.16.1.7
OS: Linux Kernel 2.6 on Debian 5.0 (squeeze)
Start: Today at 12:56 AM
End: Today at 1:44 AM
Elapsed: an hour
KB: [Download](#)



→ Pode ser útil quando encontramos um falso positivo (daí ocultamos)

→ Ou quando queremos modificar a gravidade da vulnerabilidade conforme

algum sucesso que obtivemos ao explorá-la