设置 FortiDB 漏洞扫描

说明：

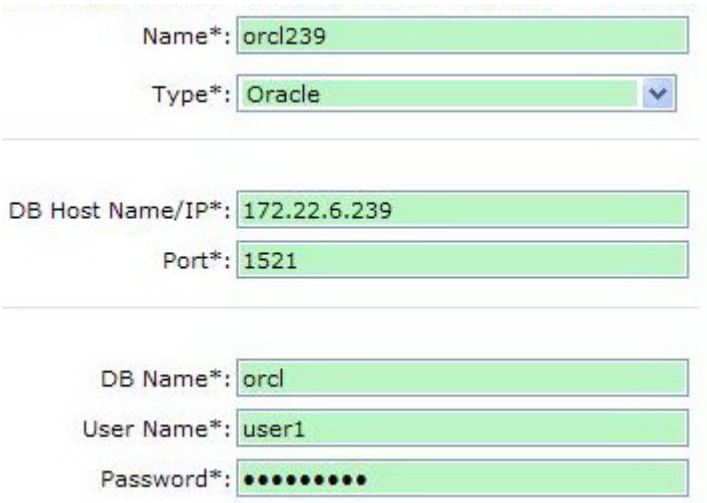
本文档针对 FortiDB 漏洞扫描配置进行说明。FortiDB 可以对目标数据库进行三种功能的漏洞扫描：数据库补丁漏洞、数据库配置漏洞和操作系统漏洞。FortiDB 还可以对扫描结果生成详细报告，方便数据库管理员了解现有数据库的安全隐患。

环境介绍：

本文使用 FortiDB1000B 做演示。本文使用的系统版本为 4.0。本文以 Oracle 10g 为例说明漏扫过程。

步骤一：配置目标数据库

在左侧菜单 Target Management—Targets 中点击 Add 按钮，填写目标数据库信息



Name：目标数据库名称，自定义一个名称

Type：数据库类型，本例为 Oracle

DB Host Name/IP：目标数据库 IP 地址，本例为 172.22.6.239

Port：目标数据库端口，默认是 1521

DB Name：数据库实例名，一个数据库软件可以开多个实例，FortiDB 认为一个实例就是一个目标数据库

User Name：连接到目标数据库的用户名

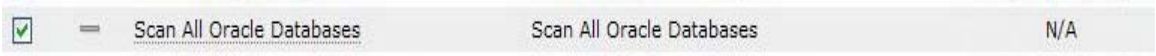
Password：连接到目标数据库的密码

以上信息可以让数据库管理员协助完成。

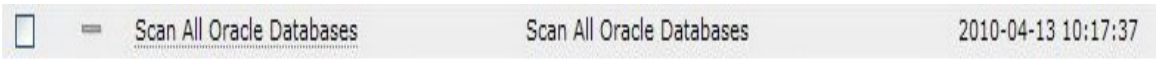
点击左下角的 Test Connection 按钮测试连接。在左上角出现 • Success 表明连接正确，否则会出现红色报错信息。点击右下角的 Save 按钮保存信息。

步骤二：扫描数据库漏洞

在 Assessment Management—Assessments 中勾选扫描所有 Oracle 数据库



点击 Run 按钮执行扫描，约需要五分钟。完成后可以看到上一次扫描时间



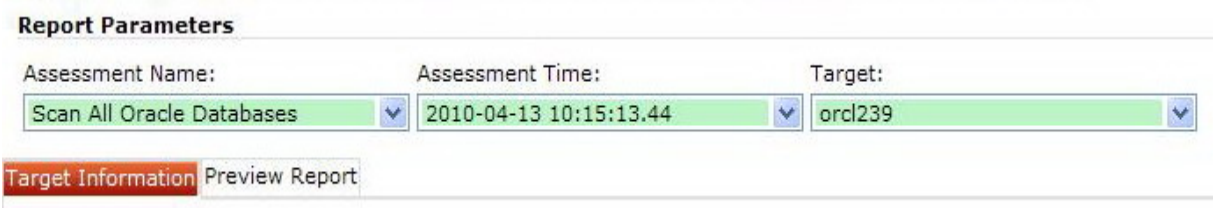
步骤三：查看扫描报告

在 Report Management—Pre-Defined VA Reports 中可以看到漏洞扫描报告。FortiDB 预定义了一些报告内容：

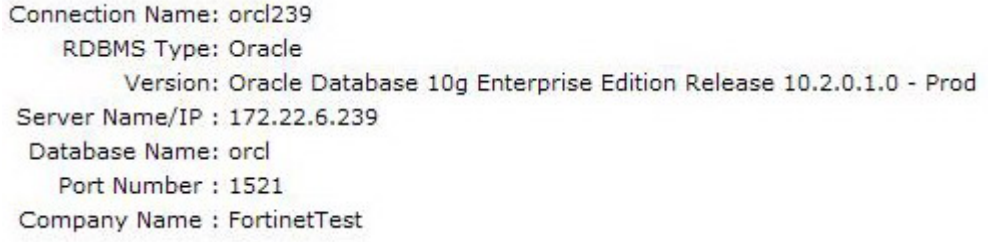
Detailed Report：给出所有已打补丁和未打补丁的漏洞数量、分类和详细信息描述

Detailed Failed Report：给出所有未打补丁的漏洞数量、分类和详细信息描述

Summary Report：给出所有已打补丁和未打补丁的漏洞汇总信息描述
Summary Failed Report：给出所有未打补丁的漏洞汇总信息描述
Score Report：以图形界面表示所有已打补丁和未打补丁的漏洞信息
点击 Detailed Report 查看报告：



Assessment Name：任务名称，本例选择 Scan All Oracle Database
Assessment Time：任务时间，选择上次执行漏扫的时间
Target：目标名称，选择漏扫数据库名称
在 Target Information 中可以看到数据库基本信息



点击 Preview Report 可以看到详细内容

Severity:

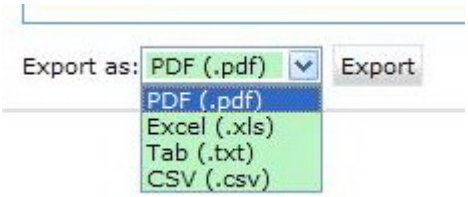
	Critical	Major	Minor	Cautionary	Informational	Total
PASSED	33	22	5	10	0	70
FAILED	13	12	8	4	0	37
INFORMATIONAL	0	0	0	0	56	56
ERROR	0	0	0	0	0	0
TOTAL	46	34	13	14	56	163

Classification:

	Host System	DB Server	Privilege	Password	Configuration	Unclassified	Total
PASSED	1	34	7	4	24	0	70
FAILED	2	2	15	5	13	0	37
INFORMATIONAL	0	0	5	1	50	0	56
ERROR	0	0	0	0	0	0	0
TOTAL	3	36	27	10	87	0	163

- [+] Critical Vulnerabilities - (46)
- [+] Major Vulnerabilities - (34)
- [+] Minor Vulnerabilities - (13)
- [+] Cautionary Vulnerabilities - (14)
- [+] Informational Vulnerabilities - (56)

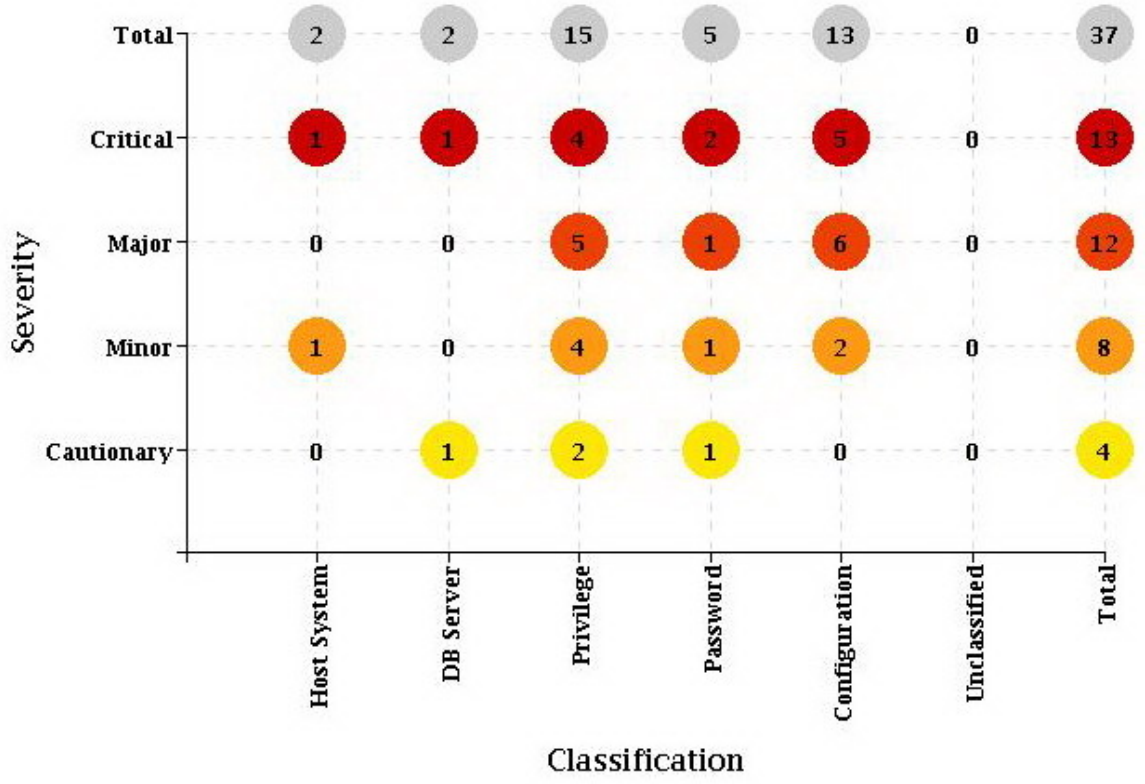
在 Preview Report 页面的最下面点击 Export 可以导出报告，支持的格式为 PDF，Excel，Tab，CSV

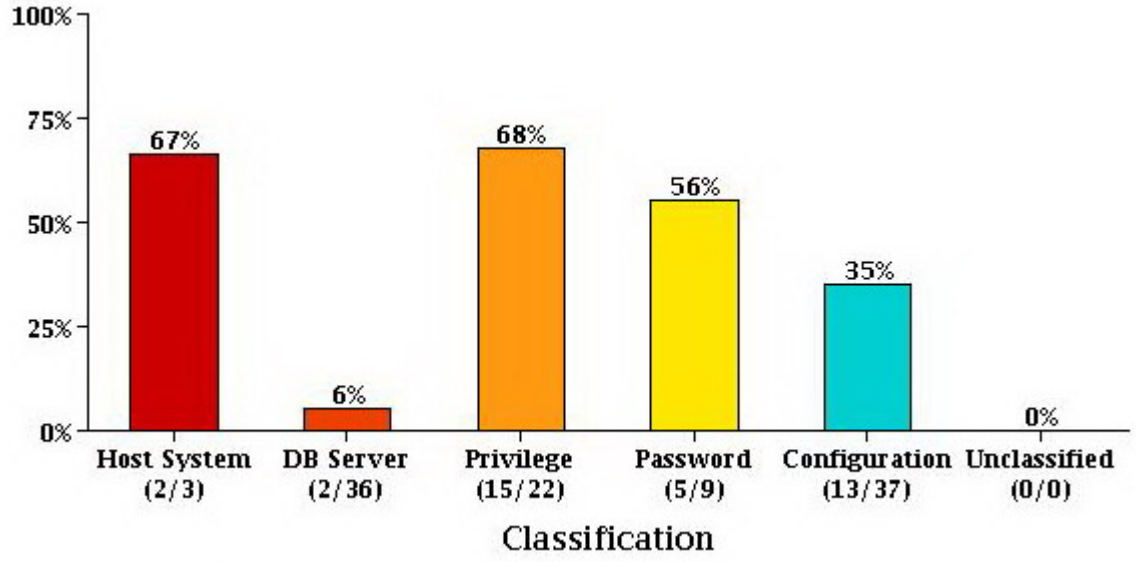


报告样例

下面是导出报告的部分信息

FAIL	DBSERVER	DVA ORCL 01.31 Restrict UTL_FILE_DIR	1 Pre-Defined Policy violation(s) found. Overview: Report on UTL_File_Dir access. Policy Reference: CVE-2006-7141 Versions Impacted: Oracle 8i, Oracle 9i, Oracle 10g and Oracle 11g Description: The UTL_FILE package allows for the ability to access files outside of the Oracle database server. This package can read/write files in directories that are defined to it either via the UTL_FILE_DIR init.ora parameter, or the CREATE DIRECTORY SQL statement. There are associated vulnerabilities with this feature as well (see above CVE). Assessment Results: • Name -: utl_file_dir Value -: /home/oracle/oracle/product/10.2.0/db_1/testlog Remediation Advice: UTL_FILE access should not be used. The privilege CREATE DIRECTORY should be used to provide access to directories outside the database (restricted). Review and revoke access on UTL_FILE where possible. Other References:


Total
Critical
Major
Minor
Cautionary
Severity
2 2 15 5 13 0 37
1 1 4 2 5 0 13
0 0 5 1 6 0 12
1 0 4 1 2 0 8
0 1 2 1 0 0 4
Host System
DB Server
Privilege
Password
Configuration
Unclassified
Total
Classification


100%
75%
50%
25%
0%
67%
6%
68%
56%
35%
0%
Host System (2/3)
DB Server (2/36)
Privilege (15/22)
Password (5/9)
Configuration (13/37)
Unclassified (0/0)
Classification