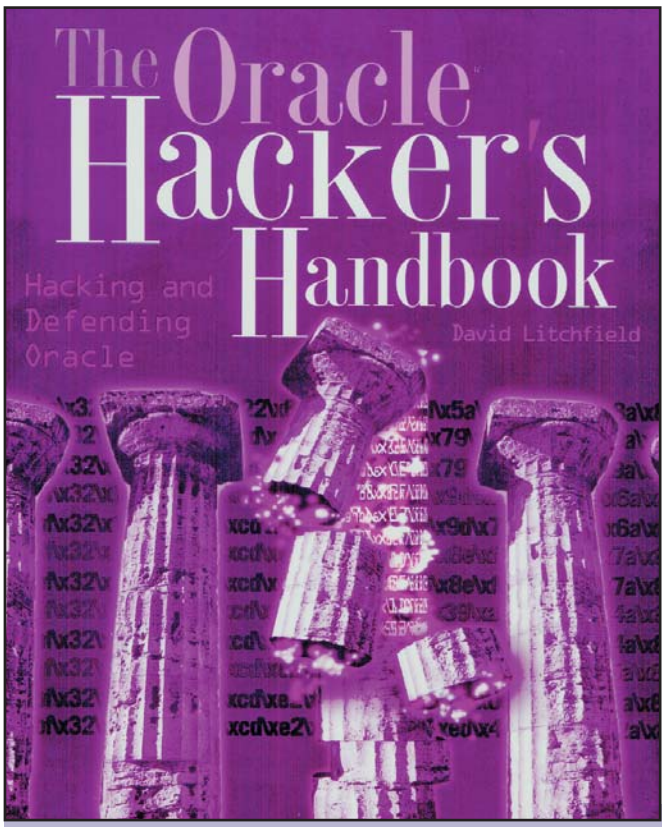
BOEKBESPREKING

The Oracle Hackers Handbook

door David Litchfield

Over de auteur

De naam van David Litchfield (geen familie van Nial Litchfield, medelid van het Oaktable Network) is de laatste jaren verbonden aan soms uitgebreide publiciteit over de beveiligingslekken van de Oracle Database. Niet alleen Oracle software, maar beveiliging van software en systemen in het algemeen heeft zijn interesse. Litchfield spreekt regelmatig op conferenties gewijd aan security, en onderhoudt onder andere de interessante website www.databasesecurity.com. Op deze site zijn interessante tools en whitepapers te vinden rondom de beveiliging van (onder andere) Oracle databases.



Boek:	The Oracle Hacker's Handbook
Schrijver:	David Litchfield
Uitgever:	Wiley
ISBN	978-0-470-08022-1

Grote bekendheid verwierf Litchfield kort nadat Oracle in december 2001 de 'unbreakable'-marketing campagne startte. Binnen enkele dagen na de start van deze campagne wist Litchfield samen met zijn broer Mark een lijst met zwakheden aan Oracle te presenteren.

Het boek

Het boek is een paperback van 190 bladzijden. Wat mij interesseert (maar wat ik nog niet heb kunnen achterhalen): waarom is dit boek uitgegeven bij de relatief onbekende uitgever Wiley? In 2006 en 2007 zijn bij deze uitgever volgens hun website maar drie boeken verschenen, die gerelateerd zijn aan Oracle. Heeft het te maken met de onbarmhartige uitspraken over gebrek aan beveiliging van de Oracle-database beveiliging? Het zou me niets verbazen als de bekende uitgevers van Oracle het conflict liever uit de weg gaan, en zich er niet aan wagen.

In de inleiding wordt direct de toon gezet als Litchfield de aanvaring tussen Oracle's security officer Mary-Ann Davidson en hemzelf beschrijft. Davidson beschouwt de onderzoekers van beveiligingslekken zèlf als risico. Litchfield is het daar uiteraard niet mee eens: hun doel is om sámen met de softwareleveranciers tot een beter beveiligd product te komen.

In hoofdstuk 1 wordt begonnen met de beschrijving van de architectuur van Oracle. Op bladzijde 3 wordt direct al een listing gepresenteerd van een C-programma waarmee een lek wordt blootgelegd en gebruikt.

In hoofdstuk 2 wordt de netwerkarchitectuur behandeld. Daarbij wordt uitgebreid ingegaan op de interne structuur van de datapakketten die over het netwerk worden verstuurd. Als voorbeeld wordt aangegeven hoe het versienummer van

een database uit deze pakketten kan worden afgeleid. Op zich is dat versienummer geen kritisch gegeven, maar de inbreker krijgt zo wel inzicht in het gebruikte systeem, en kan daarmee nauwkeuriger te werk gaan door bekende lekken van die versie te benutten. Hoofdstuk 3 borduurt hier verder op voort met een beschrijving van aanvallen op de listener en de dispatchers.

Hoofdstuk 4 behandelt het authenticatieproces. In eerste instantie om toegang te krijgen, al blijft het uiteindelijke doel van de hacker om beheerdersrechten te verkrijgen.

Er wordt in hoofdstuk 5 eerst een uitstapje gemaakt naar PL/SQL. Er wordt uitgelegd op welke verschillende manieren PL/SQL kan worden uitgevoerd met rechten van de rol die de code heeft gemaakt, dan wel degene die de functie aanroept. Verder beschrijft Litchfield hoe 'wrapped' PL/SQL code kan worden 'unwrapped'. Het 'wrappen' van PL/SQL is een manier om intellectueel eigendom te beschermen. De bedoeling is dat de code wel kan worden uitgevoerd, maar niet meer voor mensen leesbaar is. Uiteraard is dit slechts schijn. Een kant en klare oplossing om PL/SQL te unwrappen biedt Litchfield niet, maar met de beschikbare informatie is het heel goed mogelijk de benodigde programmatuur hiervoor zelf te schrijven. Verder komt in dit hoofdstuk ook PL/SQL injection aan bod.

Hoofdstuk 6 is erg kort. Het behandelt een aantal zwakheden van triggers.

In hoofdstuk 7 wordt beschreven hoe gebruik gemaakt kan worden van te ruimhartig toegekende rollen, zoals onder andere EXECUTE ANY PROCEDURE en CREATE ANY VIEW.

Een feature die in het bijzonder bedoeld is om gebruikers af te schermen van gegevens die zij niet mogen zien is de 'Virtual Private Database'. Hoofdstuk 8 laat zien hoe ook deze feature nog de nodige lekken vertoont.

De komst van webapplicaties heeft de systemen er niet veiliger op gemaakt. De verschillende varianten van Oracle applicatieservers, zoals onder meer Oracle Portal en de Oracle HTTP server bevatten een PL/SQL gateway, waarmee PL/SQL vanaf het web is uit te voeren. Ook hier bestaat weer een ruime hoeveelheid mogelijkheden tot misbruik, zoals hoofdstuk 9 laat zien.

Hoofdstuk 10 laat zien dat iemand die met behulp van de eerdere hoofdstukken zichzelf de juiste privileges heeft verschaft, vervolgens ook op het niveau van het operating systeem commando's kan uitvoeren. Dat uitstapje naar het OS wordt vervolgens in hoofdstuk 11 uitgebreid naar het filesystem.

Het laatste hoofdstuk tenslotte geeft een paar 'tips' hoe vervolgens de illegaal verkregen gegevens naar buiten gesmokkeld zouden kunnen worden.

Doelgroep

Het boek beschrijft zelf geen duidelijke doelgroep, maar naar mijn mening dient iedere DBA en ontwikkelaar die beveiliging (en zichzelf) serieus neemt, te weten wat de beheerde systemen bedreigt. Alleen door kennis te vergaren hoe inbrekers te werk gaan, kan hen het leven lastiger worden gemaakt. Met boeven vang je boeven.

Conclusie

Dit boek is een must voor iedere beheerder van databases met gegevens die in eenmaal verkeerde handen lastige vragen veroorzaken. Uiteraard zijn de voorbeelden momentopnamen, Oracle zal deze met een recente of nog komende Security Patch wel dichttimmeren. Maar alleen al de denkwijze die dit boek je bijbrengt maakt het de moeite waard.

Carel-Jan Engel werkt als onafhankelijk Oracle-consultant. Hij is lid van het Oak Table Network. E-mail: cjpengel.dbalert@xs4all.nl.