

Gi i thu t mã hóa m t kh u Oracle

Gi i thi u

Ngày 08/07/1993, Bob Baldwin; ng i c gi nh là tác gi thi t k gi i thu t mã hóa m t kh u Oracle ,--1--, ã ng bài vi t v i tiêu “Gi i thu t mã hóa m t kh u Oracle” trên trang comp.security.misc. Bài vi t c a Bob Baldwin ã mô t các yêu c u mà gi i thu t mã hóa c n th a mãn và các b c hi n th c gi i thu t.

Gi i thu t mã hóa phân tích trong ch này ng d ng cho phiên b n Oracle6 n Oracle10g, phiên b n Oracle11g ã ng d ng gi i thu t mã hóa m i.

Yêu c u v gi i thu t mã hóa

1. Ph i có th thi hành c trên m i thi t b u cu i
2. Tên truy nh p và m t kh u ph i h tr c nh ng ký t ngoài b ng mã ASCII ,--2--
3. Tr ng h p các tài kho n có cùng m t kh u thì m t kh u mã hóa ph i khác nhau
4. M t kh u ph i có dài l n

Gi i thu t mã hóa m t kh u Oracle

T các c t yêu c u gi i thu t nh n c, Bob Baldwin ã thi t k gi i thu t mã hóa g m các b c nh sau:

1. Ghép tên truy nh p và m t kh u thành m t giá tr chu i ph ng
2. Chuy n chu i ký t ph ng thành chu i ch hoa
3. Chuy n chu i ký t ph ng sang nh d ng l u tr nhi u byte
4. Mã hóa chu i ký t k t qu b c (3) dùng thu t toán DES-CBC ,--3--, v i khóa mã hóa c nh là **0x0123456789ABCDEF**
5. Mã hóa m t l n n a chu i ký t k t qu b c (3) dùng thu t toán DES-CBC, nh ng khóa mã hóa l n này là kh i d li u cu i c trích t k t qu b c (4). Kh i d li u cu i c a b c (5) sau khi chuy n sang nh d ng in c chính là m t kh u mã hóa k t qu .

Ví d t hai hình d i ây minh h a tính úng c a gi i thu t mã hóa trên:

```

oracle@localhost:~
SQL> CREATE USER viet IDENTIFIED BY pace;

User created.

SQL> SELECT password FROM DBA_USERS WHERE username='VIET';

PASSWORD
-----
EB077F3A1EA4B1BB

SQL>

```

Hình 1 - Mật mã kết nối chính Oracle Database có giá trị là **EB077F3A1EA4B1BB**

Trình tự mã hóa mật khẩu Oracle



```

SQL> exec oracle_pwd_encrypt('viet','pace');

=====
THUAT TOAN MA HOA MAT KHAU TAI KHOAN ORACLE
USERNAME: viet
PASSWORD: pace
=====

Buc 1: Ghep chuoai Username va Password.
vietpace
Buc 2: Chuyen chuoai thanh chu hoa.
VIETPACE
Buc 3: Chuyen dinh dang luu tru chuoai.
00560049004500540050004100430045
Buc 4: Ma hoa DES-CBC lan 1.
(00560049004500540050004100430045 , 0123456789ABCDEF) ==> DB01AB66DCF39BEA171861676481F451
Buc 5: Ma hoa DES-CBC lan 2.
(00560049004500540050004100430045 , 171861676481F451) ==> 6AA0F6CBCD9BFC80EB077F3A1EA4B1BB

=====
Mat khau Oracle da duoc ma hoa: EB077F3A1EA4B1BB
Thoi gian ma hoa = [0 Seconds]

=====

PL/SQL procedure successfully completed.

```

Hình 2 - Mật khẩu kết nối có kết quả thu thập mã hóa một trình tự mật khẩu do chính Oracle Database tạo ra. (trích tài liệu khóa học “[Ngày hội bảo mật Oracle – Day1](#)”)

Y u i m m t kh u Oracle

Gi i thu t mã hóa m t kh u Oracle tuy th a m ả n các c t ban u, nh ng ả b c l nhi u y u i m c b n.

1. M t kh u không phân bi t ch hoa th ng.

- Giá trị Salt, dùng cho giá trị thu thập mã hóa chính là “Tên truy nhập”.
- Số ngẫu nhiên khóa mã hóa không phải là **0x0123456789ABCDEF** cho giá trị thu thập mã

Chú thích

- [Bob Baldwin](#), trình diễn án “Trusted Oracle”, có xem là người thi đấu giá trị thu thập mã hóa mật khẩu Oracle dùng cho các phiên bản Oracle6 và Oracle10g. Bài viết ngày 08/07/1993 của Ông nhằm mục đích giúp mọi người biết về thuật toán mã hóa và có thể kiểm tra tính đúng đắn của mật khẩu Oracle. Theo Bob Baldwin, nội dung bài viết được đăng trên tạp chí công bố và trình bày ở Ông đã trình bày nội dung này tại hội nghị BATSS (Bay Area Trusted Systems Symposium)
 - [ASCII](#): Chuỗi mã trao đổi thông tin Hoa Kỳ
 - [DES-CBC](#): Giá trị thu thập mã hóa DES thể hiện chế độ Cipher-Block-Chaining
 - [Salt](#): Chuỗi giá trị ngẫu nhiên dài, tăng độ khó và thời gian phá mã mật khẩu
- Tài liệu tham khảo: [An Assessment of the Oracle Password Hashing Algorithm](#)

hiểu rõ hơn về chúng, các bạn có thể tham gia chuyên [Xác thực các cách trình Ngày hôm nay](#) [Oracle](#), hoặc liên hệ theo thông tin dưới đây:

Trung tâm đào tạo VietPace

VietPace Training Center

123 Trường Chinh, Quận 3, TP. HCM.

Phone: (+84) 8 39.325.977

Fax: (+84) 8 9.321.042

Email: tamntt@vietpace.com --- cucntt@vietpace.com

Web: www.vietpace.com, www.baomatoracle.com