به نام خدا

نعیم اصفهانی
۸۴۲۰۱۰۰۳

تمرین اول
امنیت پایگاه داده‌ها

۱.

در حمله‌ی مردی در وسط به گونه‌ای پس از نقض محرمانگی (دسترسی به بسته‌ی اطلاعاتی) شخص می‌تواند تمامیت را نقض کند (اطلاعات جدید را به عنوان اطلاعات قبلی بفرستد). عملا نقض تمامیت متوقف نقض محرمانگی است.

۲.

a. اطلاعات حساب بانکی
b. پیدا کردن پردازه‌ی غیر مجازی که در سیستم وارد شده
c. برگرداندن اطلاعات یک سرور که توسط نفوذگر پاک شده است

۳.

همان طور که می‌دانیم زبان SQL زبانی است که توسط آن درخواست‌هایی به پایگاه داده‌ها فرستاده می‌شود. در این زبان مانند بسیاری از زبان‌های دیگر مفهوم کامنت وجود دارد.

در نرم‌افزاری که مستقیما قسمت‌هایی از درخواست خود را از کاربر می‌گیرد امکان سوء استفاده از این زبان وجود دارد؛ به این ترتیب که ما می‌دانیم که این اطلاع در قسمت WHERE یک درخواست وارد می‌شود و مثلا برای داده‌های رشته‌ای بین دو عدد ″ قرار می‌گیرد. ما می‌توانیم با قرار دادن اطلاعات مورد نظر و بستن ″ و ادامه دادن درخواست مطابق میلمان هر کاری که دلمان می‌خواهد انجام دهیم. برای مثال در شکل زیر تکه کدی را می‌بینیم که کار بسیار ساده ای را انجام می‌دهد و با گرفتن نام دانشجو و گذرواژه نمره‌ی او را به او نشان می‌دهد:

```
String usr, pass;
input usr, pass;
String query = "Select Garde From Students Where Name='";
query += usr;
query += "' and Password='";
query += pass;
query += "';";
Show (Database.doQuery(query));
```

حال در این برنامه‌ی اگر مقدار متغیرها به صورت زیر باشد درخواست را بازنویسی می‌کنیم.

usr: hehe' **Or** 1=1; --
pass: a

query:

Select Garde **From** Students **Where** Name='hehe' **Or** 1=1; --*' and Password='a';*

عملا در این درخواست ما بدون داشتن حتی یک نام کاربری و گذرواژه توانسته‌ایم نمرات تمام دانشجوها را ببینیم (و این یک اتفاق واقعی است!!!!). البته اگر از رویه‌های ذخیره شده و یا جمله‌های آماده استفاده شود این مشکل وجود ندارد. برای حل ساده‌ی این مشکل هم می‌توان تمام ″ های ورودی را با فاصله‌ی خالی جایگزین نمود.

۴.

a.

۱.

	S1	S2	S3	O1	O2	O3
S1				o,r,w,c		w,c
S2				r	o,r	r
S3				r	w,c	r,o

۲.

	S1	S2	S3	O1	O2	O3
S1				o,r,w,c		w,c
S2				r	o,r	r
S3				r	w,c	r,o

۳.

	S1	S2	S3	O1	O2	O3
S1				o,r,w,c		w,c
S2				r	o,r	r
S3				r	w,c	r,o

۴.

	S1	S2	S3	O1	O2	O3
S1				o,r,w,c		w,c
S2				r	o,r	r
S3				r,w	w,c	r,o

۵.

	S1	S2	S3	O1	O2	O3
S1				o,r,w,c		w,c
S2				r	o,r	r
S3				o,r,w	w,c	r,o

۶.

	S1	S2	S3	O1	O2	O3
S1				o,r,c		w,c
S2				r	o,r	r
S3				o,r,w	w,c	r,o

۷.

	S1	S2	S3	O1	O2	O3
S1				o,c		w,c
S2				r	o,r	r
S3				o,r,w	w,c	r,o

۸.

	S1	S2	S3	O1	O2	O3
S1				o,c	w	w,c
S2				r	o,r	r
S3				o,r,w	w,c	r,o

۹.

	S1	S2	S3	O1	O2	O3
S1				o,c	w	w,c
S2				r	o,r	r
S3				o,r,w	w,c	r,w,o

۱۰.

	S1	S2	S3	O1	O2	O3
S1				o,c	w	w,c
S2				r	o,r	r,w
S3				o,r,w	w,c	r,w,o

.۱۱

	S1	S2	S3	O1	O2	O3
S1				o,c	w	w,c
S2				r	o,r	r,w
S3				o,r,w	w,c	r,w,o

b. بله، همین ترتیب قبل یک حق نوشتن روی شیئ سوم به کاربر دوم داده است.

c. اولا آن حرف شرطی داشت و آن این که اعمال یکنواخت نباشند که این‌جا هستند. دوما آن حرف کلی بود و با یک مثال نقض قابل رد کردن نیست. در آن‌جا گفته شد به طور کلی این‌طوری است.

.۵

a. بله

take(C,S,"r on A")

b. بله

take(C,S,"r on A")
grant(C,D, "r on A")

c. خیر

take(M,S,"r on A")

d. خیر می‌توانند

create(H,"C has t", "T has g")
grant(T,H, "r on B")
take(C,H, "r on B")