

به نام ایزد یکتا.

تزریق SQL، حمله و دفاع



www.ketab.ir

Justin Clarke

ترجمه: مهندس محسن کجباف

انتشارات پندار پارس

سرشناسه	: کلارک، جاستین
عنوان و نام پدیدآور	: Clarke, Justin
مشخصات نشر	: تهران : پندار پارس، ۱۳۹۴.
مشخصات ظاهری	: ۳۱۲ ص.: مصور، جدول.
شابک	: ۹۷۸-۶۰۰-۶۵۲۹-۸۹-۹ : ۲۸۰۰۰۰ ریال
وضعیت فهرست نویسی	: فیبا
یادداشت	: عنوان اصلی: SQL injection attacks and defense, ۲۰۱۲.
موضوع	: کامپیوترها -- ایمنی اطلاعات
موضوع	: اس. کیو. ال. (زبان برنامه نویسی کامپیوتر)
موضوع	: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	: نرم‌افزار کاربردی -- تدابیر ایمنی
شناسه افرو	: کجیاف، محسن، ۱۳۶۵، - مترجم
رده بندی دیره	: ۹۷۷ ۱۳۹۴۹۵/ ۹/۷۶۴۹۸
رده بند دیره	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۳۹۹۷۶۱۶

انتشارات پندار پارس



دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوچه شستن، شماره ۱۴، واحد ۱۶ www.pendarepars.com
 تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۴۵۷۸، ۹۲۱۲۷۱۹۰ info@pendarepars.com

نام کتاب	: تزریق SQL، حمله و دفاع
ناشر	: انتشارات پندار پارس
تالیف	: جاستین کلارک
ترجمه	: محسن کجیاف
چاپ نخست	: دی ماه ۹۴
شمارگان	: ۵۰۰ نسخه
طرح جلد و صفحه‌آرایی	: سارا یعسوبی
چاپ، صحافی	: روز

قیمت : ۲۸۰۰۰ تومان شابک : ۹۷۸-۶۰۰-۶۵۲۹-۸۹-۹

هرگونه کپی برداری، تکثیر و چاپ کاغذی یا الکترونیکی از این کتاب بدون اجازه ناشر تخلف بوده و پیگرد قانونی دارد

مقدمه

امروزه یکی از متداول‌ترین روش‌های نفوذ به وب سایت‌ها و بانک‌های اطلاعاتی حملات تزریق کد SQL است. در این گونه حملات شخص نفوذگر یا کدهای مخرب را از طریق ورودی‌هایی که برنامه‌های تحت وب می‌گیرند، اجرا می‌کند که باعث اختلال در سیستم وب سایت‌ها می‌شوند. اهداف نفوذگران در این گونه حملات سرقت اطلاعات یا تغییر اطلاعات بانک اطلاعات است که گاهی این دسترسی تا نفوذ به سرور و دسترسی به کل فایل‌ها و اطلاعات سرور ختم می‌شود که از این جنبه بسیار خطرناک است. در این حملات نفوذگر با یک سری دستورهای SQL عملیاتی را (متفاوت با عملیات عادی موردنظر طراح وب‌سایت) در پایگاه داده وب‌سایت آسیب‌پذیر انجام می‌دهد. تزریق sql از زمانی که برنامه‌های کاربردی وب بوجود آمده‌اند، وجود داشته و یکی از آسیب‌دهی‌های غربی است که یک کسب و کار را تهدید می‌کند، زیرا می‌تواند موجب افشای اطلاعات حساس سازمان‌ها و شرکت‌ها شود. براین داشتن اطلاعاتی کامل درباره شیوه‌های حمله از طریق تزریق SQL و همچنین دفاع در برابر این حملات برای برنامه نویسان ضروری است.

به دلیل اهمیت این موضوع، تصمیم گرفتم تنها مرجع تخصصی تزریق SQL، اثر پرفسور جاستین کلارک را ترجمه کنم. امیدوارم این اثر برای دانش‌خوانندگان محترم در زمینه حملات تزریق SQL مفید واقع شود. این کتاب بهترین و کاربردی‌ترین مرجع برای درس امنیت پایگاه داده برای دانشجویان رشته مهندسی فن آوری اطلاعات گرایش امنیت می‌باشد.

با توجه به اینکه هیچ ترجمه‌ای عاری از نقص نیست، از خوانندگان عزیز تقاضا دارم نقص‌های مشاهده شده و پیشنهاد‌های خود را از طریق پست الکترونیکی M_Kajbaf@yahoo.com و همچنین از طریق وب سایت انتشارات پندار پارس با اینجانب درمیان بگذارند.

در پایان از جناب آقای مهندس حسین یعسوبی که با چاپ این اثر انتشارات پندارپارس موافقت نمودند، کمال تشکر و سپاسگزاری را دارم.

محسن کجیاف

آذرماه ۹۴

فهرست

۱	فصل نخست: تزریق SQL چیست؟
۱-۱-۱	مقدمه
۱-۲-۱	درک چگونگی کار نرم افزارهای وب
۱-۳-۱	ساختار یک برنامه ساده
۱-۴-۱	معماری پیچیده تر
۱-۵-۱	تایید تزریق SQL
۱-۶-۱	ملاحظات مهم در زمینه امنیت وب
۱-۷-۱	درک چگونگی روش های آن
۱-۸-۱	ایجاد رشت
۱-۹-۱	استفاده نادرست از اکثرای SQL
۱-۱۰-۱	انواع استفاده های نادرست
۱-۱۰-۱-۱	استفاده نادرست از کوئری
۱-۱۰-۱-۲	استفاده نادرست از پیام های
۱-۱۰-۱-۳	استفاده نادرست از پیشنهاد های چنگانه
۱-۱۱-۱	پیکربندی نا امن پایگاه داده
۱-۱۲-۱	پاسخ های سریع
۱-۱۲-۱-۱	درک چگونگی کار برنامه های کاربردی وب
۱-۱۲-۲	درک مفهوم SQL
۱-۱۲-۳	درک چگونگی روی دادن آن
۱-۲۵	پرسش های متداول
۲۷	فصل دوم: آزمون های تزریق SQL
۲-۱-۱	مقدمه
۲-۲-۱	یافتن تزریق SQL
۲-۳-۱	آزمون از طریق استنتاج

۲۸	۱-۳-۲ شناسایی داده های ورودی
۲۹	۱-۳-۲ درخواست های GET
۲۹	۲-۳-۲ درخواست های POST
۳۲	۴-۲ جریان کاری اطلاعات
۳۴	۵-۲ خطاهای پایگاه داده
۳۵	۶-۲ نمایش خطاهای متداول SQL
۳۵	۱-۶-۲ خطاهای SQL Server
۴۰	۲۰-۲ پاسخ برنامه کاربردی
۴۱	۲۰-۲ خطاهای عمومی
۴۳	۷-۲ خطای کد HTTP
۴۵	۸-۲ انداز های پاسخ مختلف
۴۶	۹-۲ تشخیص تزریق
۵۰	۱۰-۲ تأیید تزریق SQL
۵۰	۱۱-۲ تفکیک اعداد و رشته ها
۵۱	۱۲-۲ تزریق درون خطی SQL
۵۱	۱-۱۲-۲ تزریق درون خطی رشته ها
۵۵	۲-۱۲-۲ تزریق درون خطی مقادیر عددی
۵۸	۱۳-۲ خاتمه تزریق SQL
۵۸	۱-۱۳-۲ نحو کامنت پایگاه داده
۶۰	۲-۱۳-۲ استفاده از کامنت ها
۶۴	۳-۱۳-۲ اجرای گزاره های چندتایی
۶۸	۱۴-۲ تأخیرهای زمانی
۷۰	۱۵-۲ خودکارسازی کشف تزریق SQL
۷۱	۱۶-۲ ابزار یافتن خودکار تزریق SQL
۷۱	۱-۱۶-۲ WebInspect HP
۷۳	۲-۱۶-۲ AppScan منطقی IBM
۷۵	۳-۱۶-۲ HP Scrawlr

۷۷	SQLiX -۴-۱۶-۲
۷۹	Paros پروکسی -۵-۱۶-۲
۸۲	۱۷-۲- مرور سریع
۸۲	۱۷-۲-۱- یافتن تزریق SQL
۸۲	۱۷-۲-۲- تأیید تزریق SQL
۸۲	۱۷-۲-۳- خودکارسازی کشف تزریق SQL
۸۳	پرش‌های متداول
۸۵	فصل سوم: بررسی کد برای شناسایی تزریق SQL
۸۵	۱-۳- روشی
۸۵	۲-۳- بررسی کد منبع برای تزریق SQL
۸۸	۳-۳- رفتارهای شناسایی خطرناک
۹۶	۴-۳- توابع خطرناک
۹۹	۵-۳- تعقیب داده‌ها
۱۰۰	۶-۳- تعقیب داده‌ها در جاوا
۱۰۲	۷-۳- تعقیب داده‌ها در C#
۱۰۳	۸-۳- بررسی کد PL/SQL و T-SQL
۱۱۱	۹-۳- بررسی خودکار کد منبع
۱۱۳	۱۰-۳- یاسکا (YASCA)
۱۱۴	۱۱-۳- Pixy
۱۱۵	۱۲-۳- AppCodeScan
۱۱۵	۱۳-۳- LAPSE
۱۱۶	۱۴-۳- ابزار تحلیل حیطه امنیتی برنامه‌های کاربردی وب (SWAAT)
۱۱۶	۱۵-۳- تحلیلگر کد منبع مایکروسافت برای تزریق SQL
۱۱۷	۱۶-۳- ابزار تحلیل کد مایکروسافت .NET (CAT.NET)
۱۱۷	۱۷-۳- ابزارهای تجاری بررسی منبع کد
۱۱۹	۱۸-۳- اونس (OUNCE)
۱۱۹	۱۹-۳- تقویت تحلیلگر کد منبع

۱۲۰.....	CodeSecure -۲۰-۳
۱۲۰.....	خلاصه بحث
۱۲۱.....	۲۱-۳ مرور سریع
۱۲۱.....	۱-۲۱-۳ بررسی کد منبع برای تزریق SQL
۱۲۲.....	۲-۲۱-۳ بررسی کد منبع به صورت خودکار
۱۲۳.....	پرسش‌های متداول
۱۲۵.....	فصل چهارم: بهره برداری از تزریق SQL
۱۲۵.....	۴- مقدمه
۱۲۶.....	۲-۲ درک تکنیک‌های عمومی بهره‌برداری
۱۲۸.....	۳-۴ استفاده از جست‌یوهای انباشته (stacked)
۱۲۹.....	۴-۴ شناسایی پایگاه داده (بانک اطلاعات)
۱۲۹.....	۵-۴ اثر انگشت رکور (Non-Blind Fingerprint)
۱۳۱.....	۶-۴ روش Banner Grabbing
۱۳۳.....	۷-۴ اثر انگشت کور
۱۳۵.....	۸-۴ استخراج اطلاعات از طریق دستورات UNION
۱۳۵.....	۹-۴ تطبیق ستون‌ها
۱۳۷.....	۱۰-۴ تطبیق انواع داده‌ها
۱۴۳.....	۱۱-۴ استفاده از گزاره‌های شرطی
۱۴۴.....	رویکرد ۱: مبتنی بر زمان
۱۴۶.....	رویکرد ۲: مبتنی بر خطا
۱۴۸.....	رویکرد ۳: مبتنی بر محتوا
۱۴۸.....	۱۲-۴ کار با رشته‌ها
۱۵۰.....	۱۳-۴ بسط و توسعه حمله
۱۵۲.....	۱۴-۴ برشماری شمای پایگاه داده
۱۶۳.....	۱۵-۴ افزایش اختیارات بر روی سرورهای آسیب پذیر اصلاح نشده (unpatched)
۱۶۵.....	۱۶-۴ ارتباط خارج از گروه (OOB)
۱۶۶.....	۱۷-۴ ایمیل

۱۶۹.....	HTTP/DNS - ۱۸-۴
۱۷۰.....	سیستم فایل (File System) - ۱۹-۴
۱۷۳.....	خودکارسازی بهره برداری تزریق SQL - ۲۰-۴
۱۷۳.....	Sqlmap - ۱-۲۰-۴
۱۷۴.....	مثالهایی از Sqlmap - ۲-۲۰-۴
۱۷۶.....	بابکت (Bobcat) - ۳-۲۰-۴
۱۷۷.....	BSQL - ۴-۲۰-۴
۱۷۹.....	سایر ابزارها - ۵-۲۰-۴
۱۸۰.....	خلاصه بحث
۱۸۰.....	مرور سریع - ۲۱-۴
۱۸۰.....	درک تکنیک‌های معمول بهره برداری - ۱-۲۱-۴
۱۸۱.....	شناسایی پایگاه داده - ۲-۲۱-۴
۱۸۱.....	استخراج داده از طریق UNION - ۳-۲۱-۴
۱۸۱.....	استفاده از گزاره های برطی - ۴-۲۱-۴
۱۸۱.....	برشماری شمای پایگاه داده - ۵-۲۱-۴
۱۸۲.....	افزایش اختیارات - ۶-۲۱-۴
۱۸۲.....	سرقت هُش های گذرواژه - ۷-۲۱-۴
۱۸۲.....	ارتباطات خارج از گروه (OOB) - ۸-۲۱-۴
۱۸۲.....	خودکارسازی بهره برداری تزریق SQL - ۹-۲۱-۴
۱۸۲.....	پرسش‌های متداول
۱۸۵.....	فصل پنجم: بهره برداری از تزریق SQL کور
۱۸۵.....	۱-۵- مقدمه
۱۸۶.....	۲-۵- یافتن و تأیید کردن تزریق SQL کور
۱۸۶.....	۳-۵- اجبار خطاهای عمومی
۱۸۷.....	۴-۵- تزریق جست‌وجوها با عوارض جانبی
۱۸۷.....	۵-۵- جداسازی و بالانس کردن
۱۹۰.....	۶-۵- سناریوهای رایج تزریق SQL کور

۱۹۱.....	۷-۵- تکنیک‌های تزریق SQL کور
۱۹۱.....	۷-۵- ۱- تکنیک‌های استنباطی
۱۹۵.....	افزایش پیچیدگی‌های تکنیک‌های استنباط
۱۹۹.....	۷-۵- ۲- تکنیک‌های کانال‌های جایگزین
۲۰۰.....	۵-۸- استفاده از تکنیک‌های مبتنی بر زمان
۲۰۰.....	۵-۸- ۱- تأخیرات SQL Server
۲۰۲.....	۵-۸- ۲- بهره برداری استنباط جست‌وجوی دودویی SQL Server عمومی
۲۰۲.....	۵-۸- ۳- بهره برداری استنباط جست‌وجوی بیت به بیت SQL Server عمومی
۲۰۲.....	۵-۸- ۴- ملاحظات استنباط مبتنی بر زمان
۲۰۳.....	۵-۸- ۵- استفاده از تکنیک‌های مبتنی بر پاسخ
۲۰۳.....	۵-۸- تکنیک‌های پاسخ SQL Server
۲۰۶.....	۵-۸- ۷- بازگرداندن پاسخ از یک بیت از اطلاعات
۲۰۸.....	۵-۸- ۸- استفاده از کانال‌های جایگزین
۲۰۸.....	۵-۸- ۹- اتصال‌های پایگاه داده
۲۰۹.....	۵-۸- ۱۰- فیلتر خروج DNS
۲۱۳.....	۵-۹- فیلتر خروج ایمیل
۲۱۴.....	۵-۱۰- فیلتر خروج HTTP
۲۱۶.....	۵-۱۱- خودکارسازی بهره برداری از تزریق SQL کور
۲۱۷.....	۵-۱۱- ۱- Absinthe
۲۱۸.....	۵-۱۱- ۲- هکر BSQL
۲۲۱.....	۵-۱۱- ۳- SQLBrute
۲۲۲.....	۵-۱۱- ۴- SQLninja
۲۲۳.....	۵-۱۱- ۵- Squeeza
۲۲۴.....	خلاصه بحث
۲۲۵.....	۵-۱۲- مرور سریع
۲۲۵.....	۵-۱۲- ۱- یافتن و تأیید کردن تزریق SQL کور
۲۲۵.....	۵-۱۲- ۲- استفاده از تکنیک‌های مبتنی بر زمان

۲۲۵.....	۵-۱۲-۳- استفاده از تکنیک‌های مبتنی بر پاسخ
۲۲۵.....	۵-۱۲-۴- استفاده از کانال‌های جایگزین
۲۲۶.....	۵-۱۲-۵- خودکارسازی بهره برداری از تزریق SQL کور
۲۲۶.....	سؤالات متداول
۲۲۹.....	فصل ششم: بهره برداری از سیستم عامل
۲۲۹.....	۶-۱- مقدمه
۲۳۰.....	۶-۲- دسترسی به سیستم فایل
۲۳۰.....	۶-۳- خواندن فایلها
۲۳۱.....	SQL Server
۲۳۸.....	Oracle
۲۴۱.....	۶-۴- نوشتن فایلها
۲۴۳.....	SQL Server
۲۴۹.....	۶-۵- اجرای دستورات سیستم عامل
۲۴۹.....	۶-۵-۱- اجرای مستقیم
۲۴۹.....	۶-۵-۲- احتمالات دیگر
۲۵۰.....	۶-۵-۳- جایگزینی رویدادهای مجموعه سیستم
۲۵۰.....	PL/SQL Native 9i
۲۵۰.....	۶-۵-۴- سرورز بافر
۲۵۰.....	۶-۵-۵- کد سفارشی برنامه
۲۵۵.....	۶-۶- افزایش دسترسی
۲۵۷.....	خلاصه بحث
۲۵۸.....	۶-۷- مرور سریع
۲۵۸.....	۶-۷-۱- دسترسی به سیستم فایل
۲۵۸.....	۶-۷-۲- اجرای دستورات سیستم عامل
۲۵۹.....	۶-۷-۳- افزایش دسترسی
۲۵۹.....	پرسش‌های متداول
۲۶۱.....	فصل هفتم: مباحث پیشرفته

۲۶۱.....	۱-۷- مقدمه.....
۲۶۱.....	۲-۷- دور زدن فیلترهای ورودی.....
۲۶۲.....	۳-۷- استفاده از تنوع حرف.....
۲۶۲.....	۴-۷- استفاده از کامتهای SQL.....
۲۶۳.....	۵-۷- استفاده از رمزگذاری URL.....
۲۶۷.....	۶-۷- استفاده از اجرای کوثری داینامیک.....
۲۶۸.....	۷-۷- استفاده از بایتهای پوچ (Null).....
۲۶۹.....	۱-۷- قراردادن عبارات رشته ای.....
۲۶۹.....	۹-۷- بهره برداری از کوتاه سازی.....
۲۷۱.....	۱۰-۷- دور زدن فیلترهای سفارشی.....
۲۷۲.....	۱۱-۷- استفاده از اسقاط داده‌ی غیر استاندارد.....
۲۷۴.....	۱۲-۷- بهره برداری از تریق SQL مرتبه دوم.....
۲۷۶.....	۱۳-۷- یافتن آسیب پذیرهای مرتبه دوم.....
۲۷۹.....	۱۴-۷- استفاده از حملات ترکیبی.....
۲۷۹.....	۱۵-۷- اعمال فشار با استفاده از داده های گفته شده.....
۲۷۹.....	۱۶-۷- ایجاد اسکریپت نویسی cross site.....
۲۸۰.....	۱۷-۷- اجرای دستورات سیستم عامل بر روی Oracle.....
۲۸۱.....	۱۸-۷- بهره برداری از آسیب پذیریهایی تأییدشده.....
۲۸۲.....	خلاصه بحث.....
۲۸۳.....	۱۹-۷- مرور سریع.....
۲۸۳.....	۱-۱۹-۷- دور زدن فیلترهای ورودی.....
۲۸۳.....	۲-۱۹-۷- بهره برداری از تریق SQL مرتبه دوم.....
۲۸۳.....	۳-۱۹-۷- استفاده از حملات ترکیبی.....
۲۸۴.....	پرسش های متداول.....
۲۸۵.....	فصل هشتم: دفاع سطح-کد.....
۲۸۵.....	۱-۸- مقدمه.....
۲۸۶.....	۲-۸- استفاده از گزاره های پارامتری شده (parameterized).....

۲۸۷.....	۳-۸- گزاره های پارامتری شده در جاوا
۲۸۹.....	۴-۸- گزاره های پارامتری شده در (C#) .NET
۲۹۱.....	۵-۸- اعتبارسنجی ورودی
۲۹۲.....	۶-۸- تهیه لیست سفید
۲۹۴.....	۷-۸- تهیه لیست سیاه
۲۹۵.....	۸-۸- تأیید اعتبار ورودی در جاوا
۲۹۷.....	۹-۸- تأیید اعتبار ورودی در .NET
۲۹۷.....	۱۰-۸- رمزگذاری خروجی
۲۹۸.....	۱۱-۸- رمزگذاری برای پایگاه داده
۲۹۸.....	۱۲-۸- رمزگذاری برای SQL Server
۳۰۰.....	۱۳-۸- استاندارد سازی
۳۰۱.....	۱۴-۸- رویکردهای استاندارد سازی
۳۰۲.....	۱۵-۸- کار با یونیکدها
۳۰۳.....	۱۶-۸- طراحی برای جلوگیری از خرابی ناشی از تزریق SQL
۳۰۴.....	۱۷-۸- استفاده از رویه های ذخیره شده
۳۰۵.....	۱۸-۸- استفاده از لایه های انتزاع
۳۰۵.....	۱۹-۸- چگونگی رفتار با داده های حساس
۳۰۷.....	۲۰-۸- منع استفاده از اسامی هدف آشکار
۳۰۸.....	۲۱-۸- ایجاد هانی پاتهای پایگاه داده
۳۰۹.....	۲۲-۸- منابع دیگر توسعه ایمن
۳۱۰.....	خلاصه بحث
۳۱۰.....	۲۳-۸- مرور سریع
۳۱۰.....	۱-۲۳-۸- استفاده از گزاره های پارامتری شده
۳۱۱.....	۲-۲۳-۸- تأیید اعتبار ورودی ها
۳۱۱.....	۳-۲۳-۸- رمزگذاری خروجی
۳۱۱.....	۴-۲۳-۸- استاندارد سازی
۳۱۲.....	۵-۲۳-۸- تدابیری برای جلوگیری از خطرات ناشی از تزریق SQL

۳۱۲.....	پرسش‌های متداول.....
۳۱۵.....	فصل نهم: شیوه‌های دفاع در سطح پلتفرم.....
۳۱۵.....	۱-۹- مقدمه.....
۳۱۶.....	۲-۹- استفاده از حفاظت زمان اجرا.....
۳۱۷.....	۳-۹- فایروال‌های برنامه‌های وب.....
۳۱۷.....	۴-۹- استفاده از ModSecurity.....
۳۱۸.....	۵-۹- مجموعه دستورات قابل پیکربندی.....
۳۲۰.....	۶-۹- پوشش درخواست.....
۳۲۱.....	۷-۹- نرمال سازی درخواست.....
۳۲۲.....	۸-۹- آنالیز سطح.....
۳۲۳.....	۹-۹- قابلیت‌های تشخیص نفوذ.....
۳۲۴.....	۱۰-۹- متوقف کردن فید ها.....
۳۲۴.....	۱۱-۹- فیلترهای وب سرور.....
۳۲۷.....	۱۲-۹- فیلترهای برنامه کاربردی.....
۳۲۸.....	۱۳-۹- پیاده سازی الگوی فیلتر در زبانهای اسکریپت.....
۳۲۹.....	۱۴-۹- فیلتر کردن پیامهای سرویس وب.....
۳۲۹.....	۱۵-۹- حفاظت ورودی قابل ویرایش در مقابل حفاظت ورودی غیر قابل ویرایش.....
۳۳۰.....	۱۶-۹- استراتژیها در سطح صفحه/URL.....
۳۳۰.....	۱-۱۶-۹- جایگزینکردن صفحه (page overriding).....
۳۳۱.....	۲-۱۶-۹- بازنویسی URL.....
۳۳۲.....	۳-۱۶-۹- Proxying/Wrapping منابع.....
۳۳۲.....	۴-۱۶-۹- برنامه نویسی جنبه گرا (AOP).....
۳۳۲.....	۱۷-۹- سیستمهای تشخیص نفوذ به نرم افزار (IDS ها).....
۳۳۳.....	۱۸-۹- دیوار آتش (فایروال) پایگاه داده.....
۳۳۳.....	۱۹-۹- ایمن سازی پایگاه داده.....
۳۳۴.....	۲۰-۹- قفل کردن داده های برنامه.....
۳۳۴.....	۱-۲۰-۹- استفاده از ورود به سیستم (login) با کمترین اختیارات پایگاه داده.....

۲۲۵.....	۲-۲۰-۹- لغو مجوزهای PUBLIC
۲۲۵.....	۳-۲۰-۹- استفاده از رویه های ذخیره شده
۲۲۵.....	۴-۲۰-۹- استفاده از رمزنگاری قوی برای حفاظت از داده های حساس ذخیره شده
۲۲۶.....	۵-۲۰-۹- حفظ یک دنباله ممیزی
۲۲۷.....	۲۱-۹- قفل کردن (ایمن کردن) سرور پایگاه داده
۲۲۷.....	۱-۲۱-۹- قفل کردن (ایمن کردن) دیگر اشیای سیستم
۲۲۸.....	۲-۲۱-۹- محدود کردن کوئری های Ad-Hoc
۲۲۸.....	۲۰-۱-۹- تقویت کنترل محیط احراز هویت
۲۲۸.....	۱-۲۱-۹- اجرا در متن حساب کاربری سیستم عامل دارای حداقل اختیارات
۲۲۹.....	۲۱-۹- اطلاع رسانی به مدیران نرم افزار سرور پایگاه داده، پچ (اصلاح) شده است
۲۴۰.....	۶-۲۱-۹- اسناد و پیش فرض های وب سایت
۲۴۱.....	۷-۲۱-۹- استفاده از راه های ساختگر یزبان برای جستجوهای DNS معکوس
۲۴۱.....	۸-۲۱-۹- استفاده از گواهی های خاتمه SSL
۲۴۱.....	۹-۲۱-۹- محدود کردن کشف از طریق موتور جستجو
۲۴۲.....	۱۰-۲۱-۹- غیرفعال کردن اطلاعات زبان ترجمه و سرویس (WSDL)
۲۴۳.....	۱۱-۲۱-۹- افزایش اضافه نویسی لاگ های سرور وب
۲۴۳.....	۱۲-۲۱-۹- استقرار سرورهای پایگاه داده و وب بر روی هاردهای جداگانه
۲۴۴.....	۱۳-۲۱-۹- تنظیم کنترل دسترسی به شبکه
۲۴۴.....	خلاصه بحث
۲۴۴.....	۲۲-۹- مرور سریع
۲۴۴.....	۱-۲۲-۹- استفاده از حفاظت زمان اجرا
۲۴۵.....	۲-۲۲-۹- تأمین امنیت پایگاه داده
۲۴۵.....	۳-۲۲-۹- دیگر ملاحظات استقرار
۲۴۵.....	بررسی های متداول