

در جستجوی امنیت

علی اصغر جعفری لاری

انتشارات گروه مهندسی - پژوهشی ساحر
انتشارات پارسه

سرشناسه	جعفری لاری، علی اصغر، ۱۳۶۷ -
عنوان و پدیدآور	در جستجوی امنیت/مؤلف علی اصغر جعفری لاری
مشخصات نشر	تهران : گروه مهندسی - پژوهشی ساحر، ۱۳۹۲
مشخصات ظاهری	۵۱۶ ص : نمودار، جدول، مصور.
شابک	978-964-2971-52-7
وضعیت فهرست نویسی	فبیا
موضوع	اینترنت-اقدامات تأمینی شبکه‌های کامپیوتری-اقدامات تأمینی کامپیوترها-ایمنی اطلاعات پایگاه‌های اطلاعاتی-امنیت حفاظت اطلاعات
رده بندی کنگره	۱۳۹۱ ۶۴۵/TK5105
رده بندی دیوئی	005/8
شماره کتابخانه ملی	2906893



● در جستجوی امنیت

- ناشر : انتشارات گروه مهندسی - پژوهشی ساحر
- ناشر همکار : انتشارات پارسه
- مؤلف : علی اصغر جعفری لاری
- چاپ اول : ۱۳۹۲
- تیراژ : ۱۰۰۰ جلد
- قیمت : ۳۰۰۰۰ تومان
- صفحه آرائی : گروه مهندسی - پژوهشی ساحر
- چاپ : مجید
- صحافی : مجید
- شابک : ۹۷۸-۹۶۴-۲۹۷۱-۵۲-۷

مراکز پخش:

۶۶۹۱۹۲۶۷ - ۶۶۰۶۵۹۹۶ - ۰۹۱۲۳۴۴۷۳۵۸

۷۷۲۶۳۶۵۹ - ۰۹۱۲۲۰۷۳۰۸۴

www.paarseh.com

✓ گروه مهندسی - پژوهشی ساحر

✓ انتشارات پارسه

www.saaher.com

بنام خدا

آنچه در تقابل انسان و اطلاعات اهمیت می یابد، دسترسی به دریایی از اطلاعات جامع و کامل است که برای نیل به این مهم، نیاز به اخذ تدابیری میباشد تا نتیجه مطلوب حاصل گردد.

در این راستا، هدف **گروه مهندسی - پژوهشی ساحر** این است تا با عنایت پروردگار و همت و همکاری استادان و دانشجویان متعهد و دلسوز به مطالعات و تحقیقات لازم پرداخته و به تالیف و ترجمه منابع دروس اصلی، فرعی و جنبی علوم دانشگاهی اقدام نماید و صد البته دشواری چنین کاری برداشتمندان و صاحبان نظر پوشیده نیست و به همین جهت مرحله کمال مطلوب آن، باید بتدریج و پس از انتقادات و یادآوریهای پیاپی بدست آید و انتظار می رود که این بزرگواران از این همکاری دریغ نورزند.

دراین میان از استادان و دانشجویان ارجمند تقاضا میشود تا با همکاری، راهنمایی و پیشنهادهای اصلاحی خود، این گروه را در جهت ارائه دیگر آثار مورد نیاز جامعه دانشگاهی یاری دهند.

در خاتمه جای دارد تا از همکاری تمامی اعضای گروه مهندسی - پژوهشی ساحر مخصوصاً برادر عزیزم جناب آقای مهندس سعید هراتیان که در این حرکت و تلاش ما را همراهی نمودند، تشکر و قدردانی نمایم.

مدیر گروه مهندسی - پژوهشی ساحر

مهرداد توانا

سختی با خوانندگان

امروزه با گسترش استفاده مردم از اینترنت و صفحات وب، مباحث مربوط به امنیت در شبکه و وب بیش از پیش مورد توجه کارشناسان و متخصصین رایانه قرار گرفته است. افزایش روزافزون حملات اینترنتی و سرقت اطلاعات، کارشناسان را بر آن داشته تا همواره تمرکز خود را بر روی مقابله با این حملات آماده سازند.

این حملات که اساس آن، شکل گرفته از آسیب پذیری ها و حفره های امنیتی می باشد توسط نفوذگران و متخصصین امنیتی شناسایی و کشف می گردد. با توجه به اینکه، از یک طرف روزانه، آسیب پذیری های جدیدی کشف و ثبت می گردد و از طرف دیگر انگیزه های نفوذگران مخرب تر را بر آن می دارد که با بهره گیری از توصیه های امنیتی و استفاده از این اصل که امنیت نسبی است، به ارتقاء امنیت سیستم ها و شبکه های خود بپردازیم.

نفوذگران بدنبال هدف هایی با آسیب پذیری های خطرناک و اطلاعات مهم و حساس هستند تا با دسترسی داشتن به آن اهداف، انگیزه های بدخواهانه خود را پیاده نمایند. لذا مقوله امنیت باید اساس و بنیان سازمان ها، مراکز مهم و حتی کاربران عادی قرار گرفته تا با اجرای رویه ها و سیاست های ویژه ای در مقابل نفوذ نفوذگران خطرناک مصون بمانند.

برای یک نفوذگر، نفوذ به هر هدفی ممکن بوده چرا که غیر ممکن آن سیستمی است که خاموش، از برق جدا و در یک محفظه مقاوم نگهداری شده باشد، البته باز هم اعتمادی به امنیت آن سیستم نیست. نفوذگر با صرف کردن ساعتها و گاه ماهها تلاش به اهداف خود دست می‌یابد و امنیت شبکه و دانش مدیران آن را زیر سؤال می‌برد چرا که امنیت ثابت نمی‌باشد. بنابراین با توجه به جولان نفوذگران در حریم‌های خصوصی و بی‌توجهی بعضی از مدیران و کاربران به امنیت شبکه، لازم می‌دانم در کنار مقالات و کتب دیگری که در زمینه امنیت اطلاعات منتشر گردیده، با نگارش کتابی با عنوان **در جستجوی امنیت**، گامی کوچک به منظور ارتقاء آگاهی و دانش خوانندگان برداشته باشم.

از این رو که اکثر کتاب‌های موجود دیدگاه هکری داشته و مطالب آن از مراجع خارجی برگرفته شده است بر این هدف مصمم گشتم که با نگارش کتابی با دیدگاه کاملاً امنیتی که به پشتوانه تجربیات و تخصص اینجانب در مقوله امنیت و آشنایی با شبکه‌های سازمان‌ها و وبسایت‌های اینترنتی بوده، به اهداف خود که در زیر ذکر شده است، نائل شوم:

- اطلاع رسانی و آگاهی عموم افراد در سطوح مختلف علمی، از امنیت اینترنت و شناخت خطرات آن.
 - آشنایی با اهداف نفوذگران، وظایف مدیران و مشاوران امنیتی
 - تحلیل آسیب پذیری‌ها و شناخت آنها
 - بررسی امنیت و ارتقاء آن در بخش‌های کامل و مجزا
- پس از سپاس و ستایش به درگاه پروردگار از تمام دوستان و اساتید محترم از جمله مهندس توانا و مهندس هراتیان که مهربانانه دست مرا در انجام این هدف مهم فشرده تشکر و قدردانی می‌نمایم.

علی اصغر جعفری لاری

[Http://Parsing.Ir](http://Parsing.Ir)
admin@Parsing.ir

فهرست

فصل یکم: مروری بر امنیت



۲۷	 مقدمه
۲۸	 مروری کلی بر امنیت
۲۸	 جایگاه امنیت در اینترنت
۲۸	 اهمیت امنیت در اینترنت
۲۹	 انواع تهدیدات
۲۹	 نحوه حفاظت
۳۰	 مروری بر اهداف نفوذگران
۳۱	 مروری بر وظایف مدیران و مشاوران امنیتی

فصل دوم: مروری بر حملات و آسیب پذیری‌ها



۳۳	 آشنایی با حملات و انواع آن
۳۵	 فهرست حملات (Attacks)
۳۵	 آشنایی با آسیب‌پذیری‌ها
۳۸	 چگونه آسیب‌پذیری‌های منتشر شده را پیدا کنیم؟

فصل سوم: در جستجوی امنیت



۴۴	 مقدمه
۴۴	 نکاتی چند با خوانندگان
۴۴	 آشنایی با امنیت
۴۵	 امنیت فیزیکی (Physical Security)

- تعریف..... ۴۵
- تقسیم بندی امنیت فیزیکی ۴۶
- چگونه امنیت فیزیکی را فراهم آوریم ؟..... ۴۷
- امنیت فیزیکی کامپیوترهای همراه..... ۴۸
- تهدیدات ۴۹
- توصیه‌هایی به منظور حفاظت کامپیوترهای لپ‌تاپ..... ۴۹
- اقدامات لازم در صورت سرقت کامپیوتر ۵۰
- امنیت در انتخاب کلمات عبور ۵۲
- امنیت در انتخاب کلمات عبور..... ۵۴
- کشف کلمه عبور سیستم عامل XP و Windows 2000..... ۵۷
- نحوه کار با Pwdump2 ۵۷
- نحوه کار با John The Ripper..... ۵۷
- کلمات عبور شما چقدر شکننده اند ؟..... ۵۸
- امنیت سیستم عامل ها..... ۵۸
- امتیازدهی آسیب پذیری سیستم عامل ها..... ۵۹
- نمودار آسیب پذیری سیستم عامل‌های ایستگاه‌های کاری ۶۰
- نمودار آسیب پذیری سیستم عامل سرور..... ۶۰
- سیستم عامل Windows..... ۶۱
- آنچه نیاز است بدانید ۶۱
- ارزیابی امنیتی سیستم عامل ویندوز ۶۳
- آشنایی با یک اصطلاح..... ۶۳
- Patch چیست ؟ ۶۳
- نحوه آگاهی از پیچ مورد نیاز ۶۴
- HotFix و Service Pack ۶۴
- سنجش امنیت در ویندوز ۲۰۰۰..... ۶۵
- برنامه‌های مایکروسافت ۶۷
- مهم ترین نقاط آسیب پذیری ویندوز ۶۷
- اولین نقطه آسیب پذیر IIS-Internet Information Services..... ۶۸
- نحوه تشخیص آسیب پذیری سیستم ۶۹
- نحوه حفاظت در مقابل نقطه آسیب پذیر ۶۹
- دومین نقطه آسیب پذیر : (Microsoft SQL Server (MSSQL ۷۰
- سیستم عامل‌های در معرض تهدید :..... ۷۳
- نحوه تشخیص آسیب پذیری سیستم ۷۳

۷۳	نحوه حفاظت در مقابل نقطه آسیب پذیر
۷۳	Windows Authentication سومین نقطه آسیب پذیر
۷۵	پیشگیری از ارسال LM hashes بر روی شبکه
۸۲	SAM و بانک اطلاعاتی Hash - ممانعت و پیشگیری از تکثیر
۸۳	چهارمین نقطه آسیب پذیر: Internet Explorer (IE)
۸۳	سیستم عامل‌های در معرض تهدید
۸۳	نحوه تشخیص آسیب پذیری سیستم
۸۴	نحوه حفاظت در مقابل نقطه آسیب پذیر
۸۴	ایمن سازی IE
۸۵	پنجمین نقطه آسیب پذیر: Windows Remote Access Services
۸۵	Anonymouse Logon
۸۶	دستیابی از راه دور به رجیستری ویندوز
۸۶	فراخوانی از راه دور (RPC: Remote Procedure Calls)
۸۶	سیستم عامل‌های در معرض آسیب
۸۶	نحوه تشخیص آسیب پذیری سیستم
۸۷	نحوه تشخیص آسیب پذیری سیستم در مقابل Anonymouse Logon و مسائل مرتبط با آن
۸۸	نحوه تشخیص آسیب پذیری سیستم در مقابل دستیابی از راه دور به رجیستری
۸۸	نحوه تشخیص آسیب پذیری سیستم در مقابل RPC و مسائل مربوطه
۸۸	نحوه حفاظت در مقابل نقاط آسیب پذیر
۸۸	نحوه حفاظت در مقابل مسائل Anonymouse Logon
۸۹	نحوه حفاظت در مقابل دستیابی به رجیستری سیستم
۹۱	نحوه حفاظت سیستم در مقابل مسائل مرتبط با RPC
۹۱	ششمین نقطه آسیب پذیر: Microsoft Data Access Components (MDAC)
۹۱	سیستم عامل‌های در معرض تهدید
۹۲	نحوه تشخیص آسیب پذیری سیستم
۹۲	نحوه حفاظت در مقابل نقطه آسیب پذیر
۹۲	هفتمین نقطه آسیب پذیر: Windows Scripting Host (WSH)
۹۳	سیستم عامل‌های در معرض تهدید
۹۳	نحوه تشخیص آسیب پذیری سیستم
۹۳	نحوه حفاظت در مقابل نقطه آسیب پذیر
۹۳	غیرفعال نمودن WSH
۹۴	تغییر در رفتار پیش فرض WSH

- ۹۴..... آنتی ویروس ها
- ۹۴..... بروزرسانی موتور (هسته) اسکرپت
- ۹۴..... مجوزهای NTFS
- ۹۵..... هشتمین نقطه آسیب پذیر : Outlook Express, Microsoft Outlook
- ۹۶..... سیستم عامل های در معرض تهدید
- ۹۶..... نحوه تشخیص آسیب پذیری سیستم
- ۹۶..... نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۹۶..... ایمن سازی Outlook و Outlook Express
- ۹۷..... آموزش کاربران
- ۹۷..... آنتی ویروس
- ۹۸..... بروزرسانی Outlook و Outlook Express
- ۹۸..... Uninstall نمودن Outlook و Outlook Express
- ۹۸..... نهمین نقطه آسیب پذیر : Windows Peer to Peer File Sharing (P2P)
- ۹۹..... سیستم عامل های در معرض تهدید
- ۹۹..... نحوه تشخیص آسیب پذیری سیستم
- ۹۹..... نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۱۰۰..... دهمین نقطه آسیب پذیر : (SNMP) Simple Network Management Protocol
- ۱۰۱..... سیستم عامل های در معرض تهدید
- ۱۰۱..... نحوه تشخیص آسیب پذیری سیستم
- ۱۰۲..... نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۱۰۳..... ضرورت بررسی تنظیمات امنیتی مرورگرها
- ۱۰۳..... چرا تنظیمات امنیتی برای مرورگرها مهم است ؟
- ۱۰۳..... نحوه انجام تنظیمات امنیتی به چه صورت است ؟
- ۱۰۴..... چگونه می توان از تنظیمات ایده آل و مناسب برای یک مرورگر اطمینان حاصل نمود ؟
- ۱۰۴..... برخی واژه ها و اصطلاحات در ارتباط با تنظیمات امنیتی
- ۱۰۵..... متداولترین نقاط آسیب پذیر مرورگرها
- ۱۰۵..... عوامل تاثیر گذار در نحوه عملکرد ایمن مرورگر IE
- ۱۰۷..... مهمترین نقاط آسیب پذیر یونیکس
- ۱۰۷..... اولین نقطه آسیب پذیر : BIND Domain Name System
- ۱۰۸..... سیستم عامل های در معرض تهدید
- ۱۰۸..... نحوه تشخیص آسیب پذیری سیستم
- ۱۰۸..... نحوه حفاظت در مقابل نقطه آسیب پذیر
- ۱۰۹..... دومین نقطه آسیب پذیر : (RPC) Remote Procedure Calls

۱۱۰	سیستم عامل‌های در معرض تهدید
۱۱۰	نحوه تشخیص آسیب پذیری سیستم
۱۱۰	نحوه حفاظت در مقابل نقطه آسیب پذیر
۱۱۲	سومین نقطه آسیب پذیر : Apache Web Server
۱۱۲	سیستم عامل‌های در معرض تهدید
۱۱۲	نحوه تشخیص آسیب پذیری سیستم
۱۱۲	نحوه حفاظت در مقابل نقطه آسیب پذیر
۱۱۵	چهارمین نقطه آسیب پذیر : حساب‌هایی با رمز عبور ضعیف و یا فاقد رمز عبور
۱۱۶	سیستم‌های در معرض آسیب پذیری
۱۱۶	نحوه تشخیص آسیب پذیری سیستم
۱۱۷	نحوه حفاظت در مقابل نقطه آسیب پذیر
۱۱۹	پنجمین نقطه آسیب پذیر : Clear Text Services
۱۲۰	سیستم عامل‌های در معرض تهدید
۱۲۰	نحوه تشخیص آسیب پذیری سیستم
۱۲۱	نحوه حفاظت در مقابل نقطه آسیب پذیر
۱۲۱	ششمین نقطه آسیب پذیر : Sendmail
۱۲۲	سیستم عامل‌های در معرض تهدید
۱۲۲	نحوه تشخیص آسیب پذیری سیستم
۱۲۲	نحوه حفاظت در مقابل نقطه آسیب پذیر
۱۲۳	هفتمین نقطه آسیب پذیر : Simple Network Management Protocol (SNMP)
۱۲۴	سیستم عامل‌های در معرض تهدید
۱۲۴	نحوه تشخیص آسیب پذیری سیستم
۱۲۵	نحوه حفاظت در مقابل نقطه آسیب پذیر
۱۲۶	هشتمین نقطه آسیب پذیر : Secure Shell (SSH)
۱۲۶	SSH2، ابزاری قدرتمند
۱۲۷	سیستم عامل‌های در معرض تهدید
۱۲۷	نحوه تشخیص آسیب پذیری سیستم
۱۲۷	نحوه حفاظت در مقابل نقطه آسیب پذیر
۱۲۸	نهمین نقطه آسیب پذیر : عدم پیکربندی مناسب سرویس‌های NIS/NFS
۱۲۸	سیستم عامل‌های در معرض تهدید
۱۲۹	نحوه تشخیص آسیب پذیری سیستم
۱۲۹	نحوه حفاظت در مقابل نقطه آسیب پذیر

۱۳۱	 دهمین نقطه آسیب پذیر : Open Secure Sockets Layer (SSL)
۱۳۱	 سیستم عاملهای در معرض تهدید
۱۳۱	 نحوه تشخیص آسیب پذیری سیستم
۱۳۱	 نحوه حفاظت در مقابل نقطه آسیب پذیر
۱۳۲	 امنیت سرویس پست الکترونیکی
۱۳۲	 امنیت نامه‌های الکترونیکی
۱۳۳	 پیشگیری‌ها
۱۳۳	 پیشگیری اول : پیج‌های برنامه پست الکترونیکی مایکروسافت
۱۳۶	 پیشگیری دوم : استفاده از نواحی امنیتی Internet Explorer
۱۳۸	 نمونه‌هایی از حملات اینترنتی توسط نامه‌های الکترونیکی
۱۳۹	 بررسی عملکرد نرم ILOVEYOU
۱۴۰	 بررسی عملکرد ویروس Melissa
۱۴۱	 بررسی عملکرد ویروس BubbleBoy
۱۴۱	 خلاصه
۱۴۲	 پیشگیری سوم : تغییر فایل مرتبط و یا غیر فعال نمودن WSH
۱۴۳	 پیشگیری چهارم : حفاظت ماکروهای آفیس و آموزش کاربران
۱۴۴	 پیشگیری پنجم : نمایش و انتشار فایل
۱۴۵	 پیشگیری ششم : از پیج‌های بروزرسانی شده استفاده گردد
۱۴۵	 پیشگیری هفتم : محصولات آنتی ویروس
۱۴۵	 پیشگیری هشتم : رعایت و پایبندی به اصل " کمترین امتیاز "
۱۴۶	 پیشگیری نهم : امنیت سیستم عامل
۱۴۶	 پیشگیری نهم - رویکرد اول : ایمن سازی رجیستری سیستم
۱۴۷	 پیشگیری نهم - رویکرد دوم : ایمن سازی اشیاء پایه
۱۴۷	 پیشگیری نهم - رویکرد سوم : ایمن سازی دایرکتوری‌های سیستم
۱۴۸	 برخی از روش‌هایی که یک نفوذگر به پست الکترونیکی نفوذ می‌نماید؟
۱۴۸	 چگونه یک نفوذگر ایمیل جعلی می‌فرستد؟
۱۵۰	 مقدمه
۱۵۰	 چگونه یک اکانت پست الکترونیکی هک می‌شود
۱۵۰	 ثبت کلید زنی (Keylogging)
۱۵۰	 آسیب پذیری‌های سیستم عامل
۱۵۰	 کمین‌گر جاسوسی (SniperSpy)
۱۵۱	 فیشینگ (Phishing)
۱۵۱	 فرایند استاندارد حملات فیشینگ در پنج مرحله
۱۵۲	 تروجان‌ها و ابزارهای دیگر دسترسی غیرمجاز

۱۵۲	نفوذگر شماره یک - استفاده از نرم افزار ثبت کلیدزنی
۱۵۳	نفوذگر شماره دو - استفاده از صفحات تقلبی
۱۵۵	نفوذگر شماره سه - استفاده از برنامه های تروجان
۱۵۵	دفاع در برابر این حملات
۱۵۶	از کلمه عبور ساده استفاده نکنید
۱۵۶	امنیت شبکه داخلی
۱۵۶	کلیات
۱۵۶	منابع شبکه
۱۵۷	تهدیدات علیه امنیت شبکه
۱۵۷	هدف امنیت
۱۵۷	تحلیل خطر
۱۵۷	سیاست امنیتی
۱۵۸	نواحی امنیتی
۱۵۹	امنیت شبکه داخلی
۱۵۹	چکیده
۱۵۹	معرفی شبکه
۱۵۹	شبکه چیست ؟
۱۵۹	مدل مرجع ISO/OSI
۱۶۰	برخی از شبکه های رایج و عمومی چه هستند ؟
۱۶۰	UUCP
۱۶۱	دسته پردازش گرا
۱۶۱	محیط پیاده سازی
۱۶۱	محبوبیت
۱۶۲	امنیت
۱۶۲	اینترنت
۱۶۲	اینترنت چیست ؟
۱۶۴	TCP/IP: زبان اینترنت
۱۶۴	IP
۱۶۴	آشنایی با IP
۱۶۴	حمله علیه IP
۱۶۴	جعل IP (IP Spoofing)
۱۶۵	ربودن نشست IP (IP Session Hijacking)
۱۶۶	TCP
۱۶۶	تحويل بسته تضمین شده

۱۶۷	UDP
۱۶۷	سر بار پایین تر از TCP
۱۶۷	مدیریت ریسک : بازی امنیتی
۱۶۸	انواع و منابع تهدیدات شبکه
۱۶۹	حملات تحت شبکه
۱۷۲	این حملات از کجا می آیند
۱۷۲	تجربیات و درسهای آموخته شده
۱۷۳	دیوار آتش یا Firewall
۱۷۴	دستگاههای امن شبکه
۱۷۵	معرفی MRTG به عنوان نرم افزار مانیتورینگ شبکه
۱۷۷	امنیت در برنامه های کاربردی وب
۱۷۸	باگ چیست ؟
۱۷۹	حملات Disclosure
۱۷۹	انواع حملات کسب آگاهی
۱۷۹	حملات کسب آگاهی چگونه صورت می گیرند ؟
۱۸۰	نمونه ای از آسیب پذیری کسب آگاهی php-cgi
۱۸۱	حملات Exposure
۱۸۲	چگونه سایت خود را در برابر این حملات حفظ کنیم ؟
۱۸۲	حمله تزریق اسکریپت (Script Injection)
۱۸۴	حمله Cross-Site-Scripting (CSS/XSS)
۱۸۵	به چه دلیل یک سایت نسبت به XSS آسیب پذیر است ؟
۱۸۷	آسیب پذیری در مدیریت محتوای وب Pligg
۱۸۸	آسیب پذیری در برنامه تحت وب PragmaMX
۱۸۸	آسیب پذیری در برنامه تحت وب PHP-Fusion v5.01
۱۸۹	آسیب پذیری در برنامه تحت وب PHPOpenChat v3.x
۱۸۹	آسیب پذیری در برنامه تحت وب Ublog v1.0.4
۱۹۰	آسیب پذیری در برنامه FreeNAC
۱۹۰	آسیب پذیری در PHP Address Book 7.0
۱۹۰	آسیب پذیری در Hosting Controller
۱۹۰	آسیب پذیری در تالار گفتمان نرم افزار Vanilla
۱۹۱	آسیب پذیری در برنامه Axous 1.1.1
۱۹۱	آسیب پذیری در XOOPS
۱۹۱	آسیب پذیری در SyndeoCMS

۱۹۲		مقابله با حملات Cross-Site-Scripting CSS/XSS
۱۹۲		CSRF چیست؟
۱۹۲		آسیب پذیری در برنامه Axous 1.1.1
۱۹۳		آسیب پذیری در برنامه X7 Chat 2.0.5.1
۱۹۳		آسیب پذیری در برنامه تحت وب Simple PHP Agenda
۱۹۴		آسیب پذیری در برنامه تحت وب Utopia News Pro 1.4.0
۱۹۵		آسیب پذیری در مدیریت محتوای وب NetworX
۱۹۵		آسیب پذیری در برنامه Wordpress 3.3.1
۱۹۶		SQL چیست؟
۲۰۶		برنامه‌های خودکار برای حملات SQL Injection
۲۰۶		تشریح یک نفوذ با استفاده از ابزار هویج
۲۰۸		مقابله با حملات SQL Injection
۲۰۸		کد نویسی دفاعی
۲۰۹		بررسی نوع ورودی
۲۰۹		رمزگذاری ورودی‌ها
۲۰۹		انطباق با الگوی مثبت (Matching Positive Pattern)
۲۰۹		شناسایی تمامی منابع ورودی
۲۱۰		تکنیک‌های تشخیص و جلوگیری
۲۱۰		تست جعبه سیاه
۲۱۰		بررسی کننده‌های کد استاتیک
۲۱۱		تحلیل ترکیبی استاتیک و پویا
۲۱۱		LFI/RFI چیست؟
۲۱۲		آسیب پذیری در مدیریت محتوای وب AneCMS v.2e2c583
۲۱۲		آسیب پذیری در برنامه ی کاربردی تحت وب Jcow 4.2.1
۲۱۳		آسیب پذیری در پورتال ایرانی Saman
۲۱۳		آسیب پذیری در مدیریت محتوای وب Fork CMS v.3.2.4
۲۱۳		بررسی آسیب پذیری RFI/LFI از دید یک نفوذگر
۲۱۴		Shell و Shell Code چیست؟
۲۱۶		Buffer Overflow (BOF) چیست؟
۲۱۷		راه‌های مقابله با آسیب پذیری Buffer Overflow
۲۱۷		Arbitrary File Upload چیست ؟
۲۱۷		آسیب پذیری در مدیریت محتوای وب Pragyan

- ۲۱۸..... Wordpress grapefile plugin 1.1 آسیب پذیری در
- ۲۱۸..... RazorCMS 1.2.1 آسیب پذیری در مدیریت محتوای وب
- ۲۱۸..... Joomla com_remository در کامپوننت آسیب پذیری در
- ۲۱۸..... Privilege Escalation چیست؟
- ۲۱۹..... Liferay Portal 6.1 آسیب پذیری در
- ۲۱۹..... Linux Kernel 2.6.36.2 آسیب پذیری در
- ۲۲۰..... PHPizabi v0.848b آسیب پذیری در
- ۲۲۰..... Remote Admin Password Change چیست؟
- ۲۲۱..... Joomla در آسیب پذیری در
- ۲۲۲..... Event Ticket PORTAL آسیب پذیری در
- ۲۲۳..... Remote Command Execution چیست؟
- ۲۲۳..... AWStats در برنامه آسیب پذیری در
- ۲۲۴..... A WStats v5.7 - v6.2 Multiple Remote آسیب پذیری در
- ۲۲۴..... کد آسیب پذیری: ۸۴
- ۲۲۵..... CGI در آسیب پذیری در
- ۲۲۵..... CGI آزمون آسیب پذیری در
- ۲۲۶..... نفوذگری در انجمن‌ها
- ۲۲۷..... JForum 2.1.8 آسیب پذیری در
- ۲۲۷..... TR Forum 1.5 آسیب پذیری در
- ۲۲۸..... ABB v1.1 Forum آسیب پذیری در
- ۲۲۸..... Uiga Fan Club 1.0 آسیب پذیری در
- ۲۲۹..... PHP Forum ohne My SQL آسیب پذیری در
- ۲۲۹..... Web Wiz Forum آسیب پذیری در
- ۲۳۱..... myPHPNuke 1.8.8_8rc2 آسیب پذیری در
- ۲۳۱..... vBulletin3.6.8 در پورتال cchatbox آسیب پذیری در
- ۲۳۳..... PHPRunner آسیب پذیری در
- ۲۳۳..... ASP-RIDER آسیب پذیری در
- ۲۳۳..... BrewBlogger 2.3.2 آسیب پذیری در
- ۲۳۶..... JPORTAL آسیب پذیری در
- ۲۳۶..... Guestbook 2.2 آسیب پذیری در
- ۲۳۸..... امنیت سرورهای وب
- ۲۳۸..... سرور وب IIS
- ۲۳۹..... تهدیدهای وب با تکیه بر IIS

۲۴۰	برخی نقاط آسیب پذیر (حفره) در سرور وب IIS
۲۴۱	حمله علیه مولفه های IIS
۲۴۲	حفره امنیتی افشاسازی منابع Translate:f
۲۴۳	روش مقابله با حفره امنیتی افشاسازی منابع Translate:f
۲۴۳	تزریق دستورات در پرس و جوهای پایگاه داده MDAC/RDS
۲۴۴	روش مقابله با تزریق دستورات در پرس و جوهای پایگاه داده MDAC/RDS
۲۴۵	حفره امنیتی Showcode.asp و Codebrws.asp
۲۴۵	روش مقابله با حفره امنیتی Showcode.asp و Codebrws.asp
۲۴۵	آسیب پذیری در Frontpage Server Extensions (FPSE)
۲۴۶	آسیب پذیری موجود در Null.htw
۲۴۶	آسیب پذیری جریان داده متناوب (ASP Alternate Data Streams)
۲۴۷	روش مقابله با آسیب پذیری جریان داده متناوب
۲۴۷	آسیب پذیری موجود در Webhits.dll و فایل های htw
۲۴۸	روش مقابله با آسیب پذیری موجود در Webhits.dll و فایل های htw
۲۴۹	آسیب پذیری در Microsoft IIS FTP 5.0
۲۴۹	آسیب پذیری ASP DOT BUG
۲۵۰	آسیب پذیری محدودسازی بافر ISM.DLL
۲۵۰	آسیب پذیری موجود در IDA و IDC
۲۵۱	آسیب پذیری AdSamples در سایت های با سرور NT
۲۵۱	تشریح یک نفوذ با استفاده از دایرکتوری IISADMPWD
۲۵۱	حمله علیه خود IIS
۲۵۱	پیمایش دایرکتوری IIS
۲۵۸	دانلود کردن فایل ها با استفاده از TFTP , FTP , SMB
۲۵۹	استفاده از echo>file برای ایجاد کردن فایل ها
۲۵۹	روش مقابله با آسیب پذیری های موجود در پیمایش دایرکتوری IIS
۲۶۱	تشریح یک نفوذ: نفوذگری در وب سرور
۲۶۲	پیکربندی IIS با رعایت مسائل امنیتی
۲۶۴	موارد زیر در زمان نصب IIS پیشنهاد می گردند
۲۶۵	عملیات قبل از نصب IIS
۲۶۵	گروه هائی برای فایل دایرکتوری و اهداف مدیریتی
۲۶۶	مدیریت IIS با چندین گروه
۲۶۶	نصب تمام پچ برای سیستم عامل و IIS

۲۶۶	دایرکتوری پیش فرض نصب IIS
۲۶۸	سرویس‌های IIS
۲۶۹	ایمن سازی Metabase
۲۷۰	پیشنهادهای تکمیلی در رابطه با امنیت برنامه IIS
۲۷۱	معرفی برنامه Internet Service Manager (ISM)
۲۷۲	سرویس WWW
۲۷۵	سرویس FTP
۲۷۶	Server Property Server Extensions
۲۷۷	خلاصه
۲۷۸	سرور وب Apache
۲۷۸	فایل‌های حیاتی در پیکربندی سرور وب Apache
۲۷۹	فایل پیکربندی httpd.conf
۲۸۲	کنترل دسترسی‌ها در Apache
۲۸۴	Virtual Hosting در Apache
۲۸۵	فایل پیکربندی modules.conf
۲۸۵	برخی نقاط آسیب پذیر در سرور وب Apache
۲۸۵	سیستم عامل‌های در معرض تهدید
۲۸۶	نحوه تشخیص آسیب پذیری سیستم
۲۸۶	نحوه حفاظت در مقابل نقطه آسیب پذیر
۲۸۸	حمله علیه وب سرور Apache
۲۸۹	لیست کردن دایرکتوری‌ها بوسیله اسلش‌های طولانی
۲۸۹	روش مقابله با لیست کردن دایرکتوری‌ها بوسیله اسلش‌های طولانی
۲۹۰	روش مقابله با Multiview
۲۹۱	تزریق mod_auth_sql
۲۹۱	امنیت مسیر یاب‌ها
۲۹۱	Router چیست ؟
۲۹۱	نحوه عملکرد روتر
۲۹۳	روتر دستور کارش را از کجا تهیه میکند ؟
۲۹۴	ارسال بسته‌های اطلاعاتی
۲۹۶	آگاهی از مقصد یک پیام
۲۹۷	پروتکل‌ها
۲۹۷	ردیابی یک پیام
۲۹۸	مهم ترین ویژگی‌های یک مسیر یاب

۲۹۹	 روتر و جایگاه آن
۳۰۰	 جایگاه روتر در شبکه‌های LAN و WAN
۳۰۱	 جایگاه روتر در شبکه‌های WAN
۳۰۲	 استانداردها و پروتکل‌های لایه فیزیکی و data link در شبکه‌های WAN
۳۰۲	 اساسنامه امنیتی برای مسیریاب‌ها
۳۰۴	 مسیریاب‌های Cisco
۳۰۷	 تشریح یک نفوذ؛ ایجاد درب‌های پشتی در مسیریاب‌های Cisco با استفاده از زبان TCL
۳۰۸	 مراقبت از شبکه خود در مقابل این نفوذ
۳۰۹	 تشریح یک نفوذ؛ نفوذ به مسیریاب بوسیله SolarWinds
۳۱۱	 امنیت پایگاه داده‌ها
۳۱۲	 پایگاه داده SQL Server
۳۱۳	 امنیت در پایگاه داده‌ها
۳۱۴	 معماری امن شبکه با نگاه به پایگاه داده
۳۱۵	 امنیت SQL Server 2000
۳۱۵	 شناختن مدهای امنیت
۳۱۶	 بررسی نقاط آسیب پذیر SQL Server و طریقه مقابله با آنها
۳۱۷	 سیستم عامل‌های در معرض تهدید جفرهای SQL Server
۳۱۷	 نحوه تشخیص آسیب پذیری سیستم
۳۱۷	 نحوه حفاظت در مقابل نقطه آسیب پذیر موجود در SQL Server
۳۱۸	 آسیب پذیری اجازه اجرای کد از راه دور در Microsoft SQL Server
۳۱۸	 ده روش برتر بهره برداری از آسیب پذیری‌های سیستم SQL Server
۳۲۱	 پایگاه داده MySQL
۳۲۱	 پیکربندی سرویس دهنده بانک اطلاعاتی MySQL
۳۲۲	 پیکربندی اصلی و مدیریت سرویس دهنده MySQL
۳۲۳	 آشنایی بیشتر با کنسول MySQL
۳۲۴	 مدیریت سرویس دهنده MySQL
۳۲۶	 تشریح یک نفوذ: ASPX:SQL Injection
۳۲۹	 تشریح یک نفوذ: ASP:SQL Injection
۳۳۱	 تشریح یک نفوذ: PHP:SQL Injection
۳۳۳	 امنیت شبکه‌های بی سیم
۳۳۴	 مفاهیم کلی در شبکه‌های بی سیم
۳۳۶	 فناوری WAP (Wireless Application Protocol)

۳۳۷	 فناوری SWAP(HomeRF)
۳۳۷	 فناوری Wi-Fi (WECA)
۳۳۸	 فناوری WiMax
۳۳۸	 انواع شبکه‌های بی سیم از دیدگاه مقیاس بزرگی
۳۳۹	 بررسی معماری و امنیت شبکه‌های محلی بی سیم
۳۳۹	 عناصر موجود در شبکه‌های محلی بی سیم
۳۳۹	 حملات مبتنی بر شبکه‌های محلی بی سیم
۳۴۰	 حملات غیرفعال
۳۴۰	 شنود
۳۴۰	 نرم افزار WireShark
۳۴۱	 موارد استفاده
۳۴۱	 امکانات
۳۴۲	 آنالیز ترافیک
۳۴۳	 حملات فعال
۳۴۳	 تغییر هویت
۳۴۳	 پاسخ‌های جعلی
۳۴۴	 تغییر پیام
۳۴۴	 حملات نوع Denial-Of-Service (DoS)
۳۴۴	 Jamming
۳۴۴	 Man in the Middle
۳۴۵	 نفوذ به شبکه‌های بی سیم
۳۴۶	 ردیابی بی سیم
۳۴۶	 تجهیزات
۳۴۷	 اصطلاحات کلی
۳۴۷	 بررسی ابزارهای معروف جهت پیاده سازی حملات بی سیم
۳۴۸	 ابزار War-Driving
۳۴۸	 ابزار Net Stumbler
۳۴۹	 روش مقابله در برابر ابزار Net Stumbler
۳۴۹	 ابزار Kismet
۳۵۰	 ابزار Change MAC Address
۳۵۱	 ابزار Wireless WEP Key Spy
۳۵۲	 ابزار Passmark WirelessMon
۳۵۲	 نقاط دسترسی جعلی

۳۵۳		اساس ضعف‌های امنیتی در شبکه‌های بی سیم
۳۵۴		حفره‌های امنیتی مهم در شبکه‌های بی سیم 802.11
۳۵۴		مساله شماره ۱ : دسترسی آسان
۳۵۴		راه حل شماره ۱ : تقویت کنترل دسترسی قوی
۳۵۵		مساله شماره ۲ : نقاط دسترسی نامطلوب
۳۵۵		راه حل شماره ۲ : رسیدگی منظم به سایت
۳۵۶		مساله شماره ۳ : استفاده غیرمجاز از سرویس
۳۵۶		راه حل شماره ۳ : طراحی و نظارت برای تایید هویت محکم
۳۵۷		مساله شماره ۴ : محدودیت‌های سرویس و کارایی
۳۵۸		راه حل شماره ۴ : دیدبانی شبکه
۳۵۸		نکاتی در خصوص بهبود امنیت شبکه‌های بی سیم
۳۶۰		AirMagnet Distributed 4.0
		فصل چهارم: سناریوی نفوذگری
۳۶۱		مختصری بر شناسایی نفوذگران
۳۶۲		Firewall یا دیوار آتش
۳۶۲		مقدمه
۳۶۲		خصوصیات برجسته فایروال‌های امروزی
۳۶۳		ویژگی‌ها
۳۶۴		انواع فایروال
۳۶۴		مزایا و معایب استفاده از فایروال
۳۶۴		انواع فایروال‌ها از حیث ساختاری
۳۶۵		توپولوژی‌های فایروال
۳۶۵		سناریوی اول : یک فایروال Dual-Homed
۳۶۶		سناریوی دوم : یک شبکه Two-Legged به همراه قابلیت استفاده از یک ناحیه DMZ
۳۶۷		سناریوی سوم : فایروال Three-Legged
۳۶۸		مقدمه‌ای بر IDS و IPS
۳۶۹		IDS (Intrusion Detection System) چیست؟
۳۶۹		چرا دیواره آتش به تنهایی کافی نیست ؟
۳۷۰		انواع IDS
۳۷۰		سرچشمه اطلاعات
۳۷۰		(۱) Network Based IDS (NIDS)
۳۷۱		(۲) Host-Based IDS (HIDS)
۳۷۲		(۳) Application-Based IDS

۳۷۲	استراتژی کنترل
۳۷۴	نوع زمانبندی (Timing)
۳۷۴	نوع آنالیز
۳۷۴	نوع پاسخ
۳۷۵	ابزارهای مکمل
۳۷۵	۱- ابزارهای ارزیابی آسیب پذیری
۳۷۶	۲- ابزار بررسی صحت و درستی اطلاعات فایل ها
۳۷۶	۳- Honey Pot (ظرف غسل)
۳۷۸	Honeypot های با تعامل کم
۳۷۹	مثالی از Honeypot های با تعامل کم: Honeyd
۳۸۰	Honeypot های با تعامل زیاد
۳۸۰	مثالی از Honeypot های با تعامل زیاد: Symantec Decoy Server
۳۸۱	مقایسه Honeypot های با تعامل کم Honeypot های با تعامل زیاد
۳۸۱	Honeypot های با تعامل کم (شبیه سازی کننده سیستم عاملها و سرویسها)
۳۸۱	Honeypot های با تعامل زیاد (بدون شبیه سازی. با استفاده از سیستم عاملها و سرویسهای حقیقی)
۳۸۱	مزایای استفاده از Honeypot
۳۸۳	معایب استفاده از Honeypot
۳۸۳	مقایسه IPS با IDS
۳۸۳	تفاوت شکلی تشخیص با پیشگیری
۳۸۴	تشخیص نفوذ
۳۸۴	پیشگیری از نفوذ
۳۸۵	نتیجه نهایی
۳۸۵	Snort, نمونه‌ای از یک ابزار تشخیص نفوذ شبکه‌ای
۳۸۶	تشریح نفوذ به برنامه‌های کاربردی در مقابل IDS
۳۸۶	Encoding چیست؟
۳۸۷	محیط تجزیه و تحلیل ما
۳۹۰	چگونه نفوذگر ردپای خود را پاک می‌کند؟
۳۹۴	تست نفوذپذیری
۳۹۴	کلیات تست نفوذپذیری
۳۹۴	چرا سازمان‌ها به تست نفوذپذیری نیاز دارند؟
۳۹۵	تست نفوذ چه چیزی نیست؟
۳۹۵	چه چیزهایی باید تست شوند؟
۳۹۵	روش‌های اجرایی تست نفوذپذیری
۳۹۷	انواع تست نفوذپذیری

۳۹۸	روال اجرای تست نفوذ ، پیش نیاز اجرای تست نفوذ
۳۹۹	برنامه ریزی تست نفوذ
۴۰۰	جمع آوری اطلاعات (شناسایی)
۴۰۰	Footprinting (ردگیری)
۴۰۱	Scanning (پویش)
۴۰۱	Enumerating
۴۰۲	بکارگیری آسیب پذیری‌ها با هدف نفوذ
۴۰۳	پاکسازی
۴۰۳	ارائه نتایج تست
۴۰۳	آزمایش آسیب پذیری در برنامه کاربردی وب با ابزار Acunetix
۴۰۴	ساختار سایت (Site Structure) و کوکی‌ها (Cookies)
۴۰۶	ابزار Metasploit
۴۰۷	رابط کنسول
۴۰۹	تشریح یک نفوذ: با استفاده از کنسول ابزار متاسپلویت
۴۱۰	رابط گرافیکی
۴۱۲	مراحل استفاده از ابزار متاسپلویت
۴۱۳	رابط وب
۴۱۴	تشریح چند سناریوی نفوذ
۴۱۴	سناریوی اول : نفوذ به شبکه‌های بی‌سیم با Back Track
۴۱۵	ابزار مورد نیاز نفوذگر
۴۱۵	شروع نفوذگر
۴۱۹	سناریوی دوم: نفوذ به سرور (Back Connect)
۴۲۴	سناریوی سوم: نفوذ به سرور با استفاده از آسیب پذیری Microsoft IIS Malformed Local Filename Security Bypass
۴۲۹	سناریوی چهارم: پشت پرده صفحات وب
۴۳۱	سناریوی پنجم: نفوذ به یک سیستم عامل
ضمائم:	
۴۳۶	توصیه‌های امنیتی
۴۳۶	(۱) ده قانون تغییرناپذیر در رابطه با امنیت اطلاعات
۴۳۸	(۲) توصیه‌هایی برای کاهش Spam
۴۳۸	Spam چیست ؟
۴۳۹	چگونه می‌توان میزان Spam را کاهش داد ؟
۴۴۰	(۳) توصیه‌هایی برای تشخیص و پیشگیری از نرم افزارهای جاسوسی



- ۴۴۱..... Spyware چیست ؟
- ۴۴۱..... نحوه تشخیص Spyware
- ۴۴۱..... نحوه پیشگیری از نصب Spyware
- ۴۴۲..... نحوه حذف Spyware
- ۴۴۲..... ۴) توصیه هایی برای حفاظت از داده ها
- ۴۴۶..... ۵) توصیه هایی برای محافظت از خودتان در مقابل حملات phishing
- ۴۴۷..... ۶) توصیه هایی برای پیاده سازی شبکه های بی سیم امن
- ۴۴۸..... انتخاب یک مسیریاب بی سیم
- ۴۴۹..... مسیریاب خود را تنظیم کنید
- ۴۵۰..... Client ها را به هم متصل کنید
- ۴۵۱..... ارتباطات client را با فیلتر کردن آدرس MAC کنترل کنید
- ۴۵۱..... امنیت فایروال
- ۴۵۲..... از یک سوئیچ برای افزودن پورتهای بیشتر استفاده کنید
- ۴۵۲..... شبکه بی سیم را به یک وسیله سیمی متصل کنید
- ۴۵۳..... نکات طلایی امنیت در Wireless
- ۴۵۴..... ۷) توصیه های اجرایی برای گزینش فایروال
- ۴۵۴..... ۸) توصیه های امنیتی مشهورترین هکر جهان یا نام مستعار hacker poster boy
- ۴۵۵..... معرفی ابزارهای امنیتی
- ۴۵۵..... -فصل سوم<بخش امنیت در انتخاب کلمات عبور
- ۴۵۶..... -فصل سوم<بخش امنیت سیستم های عامل
- ۴۵۶..... -فصل سوم<بخش امنیت سرویس پست الکترونیکی
- ۴۵۶..... -فصل سوم<بخش امنیت شبکه داخلی
- ۴۵۶..... -فصل سوم<بخش امنیت برنامه های کاربردی وب
- ۴۵۶..... -فصل سوم<بخش امنیت مسیریاب ها
- ۴۵۶..... -فصل سوم<بخش امنیت شبکه های بی سیم
- ۴۵۷..... -فصل چهارم<تشریح چند سناریوی نفوذ
- ۴۵۷..... -فصل چهارم<شناسایی و ردیابی نفوذگران
- ۴۵۷..... -فصل چهارم<تست نفوذپذیری
- ۴۵۸..... فهرستی از DORK ها
- ۵۰۸..... نام کاربری و کلمه عبورهای پیش فرض مسیریاب ها