

سیاست امنیتی نرم افزارهای کامپیوتری

مؤلف: یوزیا بار سابر

آفتاب

www.ketab.ir



سرشناسه	: پارسایار، پوریا، ۱۳۷۵-
عنوان و نام پدیدآور	: سیاست امنیتی نرم‌افزارهای کامپیوتری / مولف پوریا پارسایار.
مشخصات نشر	: تهران: آفتاب گیتی، ۱۴۰۳.
مشخصات ظاهری	: ۱۴۹ ص.: مصور.
شابک	: ۹۷۸-۶۲۲-۳۱۴-۷۱۲-۸
وضعیت فهرست نویسی	: فیبا
یادداشت	: کتابنامه.
موضوع	: نرم‌افزار کاربردی — تدابیر ایمنی Application software – Security measures کامپیوترها — ایمنی اطلاعات — تدابیر ایمنی Computer security – Security measures کامپیوترها — ایمنی اطلاعات — سیاست دولت Computer security -- Government policy
رده بندی کنگره	: ۲۶/۵۵۸
رده بندی دیویی	: ۰۰۴/۱۶
شماره کتابشناسی ملی	: ۹۸۶۴۳۵۲
اطلاعات رگورد کتابشناسی	: فیبا

آفتاب‌گیتی

عنوان: سیاست امنیتی نرم‌افزارهای کامپیوتری

مولف: پوریا پارسایار

صفحه‌آرایی: نوژن گرافیک

نشر و پخش: موسسه انتشاراتی آفتاب گیتی

نوبت چاپ: اول، ۱۴۰۳

شمارگان: ۲۰۰ نسخه

چاپ: فدک

قیمت: ۱۵۰۰۰۰۰ ریال

شابک: ۹۷۸-۶۲۲-۳۱۴-۷۱۲-۸

کلیه حقوق برای ناشر محفوظ است.

نشانی: تهران - میدان آتریش خیابان بنفشه دهم مجتمع تجاری و اداری باران طبقه همکف
واحد ۱۴۳ *نشر و پخش همراه: ۰۹۱۲۳۳۴۲۳۶۲-۰۲۱۴۴۷۶۳۶۸۹

فهرست مطالب

۱۳	 مقدمه
۱۴	 فصل اول
۱۴	 کلیات و تعاریف
۱۵	 ۱-۱ مقدمه
۱۵	 ۱-۲ لینوکس
۱۶	 ۱-۳ طراحی لینوکس
۱۸	 ۱-۴ کرنل لینوکس
۲۰	 ۱-۵ رابط کاربری
۲۰	 ۱-۶ توزیع های مختلف لینوکس
۲۲	 ۱-۸ اصول برنامه نویسی امن
۲۲	 اعتبارسنجی ورودی
۲۳	 جدی گرفتن هشدارهای کامپایلر
۲۳	 معماری و طراحی برای به کارگیری سیاست های امنیتی
۲۴	 سادگی
۲۴	 انکار پیش فرض

۲۴	وفادار بودن به اصل حداقل حق دسترسی.....
۲۵	اجرای دفاع در عمق.....
۲۵	استفاده از روش های موثر تضمین کیفیت.....
۲۵	اتخاذ یک استاندارد کدنویسی امن.....
۲۶	تعریف نیازمندیهای امنیتی.....
۲۷	مدل سازی تهدیدها.....
۲۷	۱ - ۹ برنامه های تحت لینکس.....
۲۸	تقلید.....
۳۰	بازی.....
۳۱	گرافیک تصویر:.....
۳۱	چند رسانه ای.....
۳۲	دفتر.....
۳۳	علم.....
۳۳	شناسایی ویروس.....
۳۵	فصل دوم.....
۳۵	آسیب پذیری های حوزه ی نرم افزار.....

۳۶	۲- ۱ مقدمه.....
۳۷	۲- ۲ آسیب پذیری نرم افزار.....
۳۸	سرریز بافر.....
۳۸	ورودی اعتبارسنجی نشده.....
۳۹	ورودی های خط فرمان.....
۳۹	شرایط رقابت.....
۴۰	ارتباطات بین پرداز های.....
۴۰	عملیات فایلی غیر ایمن.....
۴۱	مشکلات مربوط به کنترل دسترسی.....
۴۲	ذخیره سازی امن و رمزنگاری:.....
۴۳	مهندسی اجتماعی:.....
۴۴	۲- ۳ یست و پنج خطای نرم افزاری براسای منبع CWE:.....
۴۷	۲- ۴ آسیب پذیری های مشترک نرم افزارها از دیدگاه.....
۵۳	دو روش برای پیشگیری از آسیب پذیری.....
۵۳	بازرسی نرم افزار.....
۵۳	گراف فعالیت امنیتی.....

- تکنیکهای ثابت: ۵۳
- تکنیک های پویا: ۵۴
- ۲- ۵ حوزه های امنیت نرم افزار ۵۶
- ذخیره و بازیابی اطلاعات در نرم افزار ۵۷
- ۲- ۶ ثبت وقایع و گزارش خطا ۶۱
- ۲- ۷ معماری سیستم ۶۲
- مراحل فرآیند مدل سازی تهدید ۶۳
- ۲- ۸ الگوهای امن در سطح معماری ۶۵
- ۲- ۹ کد منبع ۶۵
- ۲- ۱۰ چک لیست امنیتی در تولید نرم افزار ۶۵
- ۲- ۱۰- ۱ استفاده از حقوق و امتیازات ویژه ۶۶
- ۲- ۱۰- ۲ داده، پیکربندی و فایل های موقتی ۶۹
- ۲- ۱۰- ۳ استفاده از پورت شبکه ۷۱
- شکست به آرامی ۷۲
- ۲- ۱۰- ۴ لاک های بازرسی ۷۳
- فایل رویدادنگاری شخصی ۷۵

- ۷۶ ۲ - ۱۰ - ۵ احراز هویت کلاینت سرور
- ۷۷ حسابهای کاربری غیر فعال شده:
- ۷۸ حساب های کاربری منقضی شده:
- ۷۸ محدودیت در طول کلمه عبور (قابل تنظیم توسط مدیر سیستم):
- ۸۰ ۲ - ۱۰ - ۶ سرریز اعداد صحیح ها و سرریز بافر
- ۸۱ ۲ - ۱۰ - ۷ استفاده از تابع رمزنگاری
- ۸۱ ۲ - ۱۰ - ۸ نصب و بارگذاری
- ۸۳ ۲ - ۱۰ - ۹ استفاده از ابزار و کتابخانه های بیرونی
- ۸۸ ۲ - ۱۱ - ۲ چک لیست برنامه های کاربردی تحت وب از دیدگاه
- ۹۰ چک پوینتها
- ۹۱ احراز هویت:
- ۹۱ چک پوینتها
- ۹۳ اجازه و کنترل دسترسی
- ۹۴ چک پوینتها
- ۹۴ مدیریت نشست
- ۹۵ چک پوینتها

اعتبار سنجی ورودی و داده ها ۹۶

چک پوینتهاء ۹۶

چک پوینت: ۹۷

معایب تزریق دستور: ۹۸

ورود به سیستم: ۱۰۲

فصل سوم ۱۰۵

حفاظت از داده ها و اطلاعات ۱۰۵

۳-۱ مقدمه ۱۰۶

۳-۲ واژه نامه زیر برای حفاظت اطلاعات در کامپیوترها تهیه گردیده است ۱۰۷

۳-۳ اصول پایه در حفاظت اطلاعات: ۱۱۰

۳-۳-۱ ملاحظاتی در حوزه مطالعات مربوط به حفاظت ۱۱۰

۳-۳-۲ سطح عملکرد حفاظت اطلاعات ۱۱۲

۳-۵ چک لیست ها از دید گاههای مختلف ۱۲۹

۱- حفاظت از نشأت اطلاعات ۱۳۰

۱-۱-۱: کشف ۱۳۰

۱-۱-۲: بازیابی ۱۳۰

- ۱-۱-۳: جستجو..... ۱۳۱
- ۱-۳: جرم‌شناسی تحقیقات..... ۱۳۴
- ۱-۴: کنترل دستگاه خارجی..... ۱۳۴
- ۱-۵: پشتیبانی از قوانین DLP..... ۱۳۵
- ۱-۵-۲: ایجاد، توسعه و مدیریت قوانین..... ۱۳۵
- ۲-۳ مدیریت و بازیابی کلیدها..... ۱۳۷
- ۴-۲: مدیریت کدگذاری..... ۱۳۷
- ۴-۱: پروفایل شرکت..... ۱۴۳
- ۴-۲: نگهداری و پشتیبانی..... ۱۴۳
- ۴-۳: قیمت گذاری..... ۱۴۴
- ۵-۳-۲ چک لیست حفاظت داده‌ها از دید منبع..... ۱۴۴
- مسدود کردن دسترسی به انتقال فایل شناخته شده و وب سایت ایمیل..... ۱۴۶
- ۳-۵-۳ چک لیست حفاظت داده از دیدگاه..... ۱۴۶

مقدمه

همواره استفاده از تکنولوژی مانند شمشیر دو لبه است. همانطور که هر تکنولوژی جدیدی می تواند به روند بهبود کار و زندگی انسانها کمک کند، از طرفی می تواند منجر به پیدایش آسیب پذیری ها و خطراتی در کار و زندگی شود. این مقوله شامل همه ی تکنولوژی های موجود در این جهان می شود. شاید یک دلیل عمده برای این قضیه این باشد که هر تکنولوژی از ابتدا تنها برای راحتی و احتمالاً سرعت بخشیدن به کار به وجود می آید و آفرینندگان آن به خطراتی که در آینده به وجود خواهد آورد فکر نمی کنند. موضوعی که ما در این تحقیق به آن خواهیم پرداخت، حفاظت داده، رمزنگاری پایگاه داده، اداره کردن خطا، امنیت نرم افزار و برنامه های دسکتاپی تحت لینوکس است که اگر چه مزایای زیادی داشته و انجام بسیاری از کارها را روان تر ساخته است اما در عین حال باعث به وجود آمدن آسیب پذیری های امنیتی زیادی در کار و حریم خصوصی انسانها شده است.