مرکز آپا قم

مرکز تخصصی آپا قم
دانشگاه قم، ساختمان کتابخانه مرکزی
cert.qom.ac.ir

مرداد ماه ۹۷
ماهنامه خبری

عناوین خواندنی های این شماره

آگاهی | پشتیبانی | امداد

۳۰ مرداد ۹۷

اخبار امنیتی

حمله هکر ها به پمپ بنزین

هکرها گاز پمپ بنزین را در معرض خطر قرار داده و ۶۰۰ گالن گاز را با استفاده از دستگاه و از راه دور سرقت کردند. این حادثه در ایستگاه گاز ماراتون در دیترویت اتفاق افتاد و حدودا ۹۰ دقیقه طول کشید و در این مدت وسایل نقلیه می توانستند از گازی که به صورت آزاد جریان داشت، سوخت گیری کنند.

ادامه مطلب

اصلاحیه‌های امنیتی مایکروسافت

سه‌شنبه، ۲۳ مرداد ماه، شرکت مایکروسافت اصلاحیه‌های امنیتی ماهانه خود را برای ماه میلادی آگوست منتشر کرد.

ادامه مطلب

تولید نسل جدید بدافزارها بوسیله هوش مصنوعی

هوش مصنوعی (AI) به عنوان یک راه حل بالقوه برای مبارزه با نرم‌افزارهای مخرب و جلوگیری از حملات سایبری قبل از بروز هر گونه اختلال در عملکرد سازمان، دیده می شود. با این حال، همان فناوری همچنین می‌تواند توسط هکرها برای استفاده از نسل جدیدی از نرم‌افزارهای مخرب استفاده شود.

ادامه مطلب

انتشار باج‌افزار KeyPass

نوع جدیدی از باج‌افزار STOP با نام KeyPass در حال انتشار است. اطلاعات زیادی از چگونگی انتشار آن در دست نیست اما برخی کاربران گفته‌اند که باج‌افزار پس از دانلود و نصب کرک‌هایی مانند KMSpico شروع به کار کرده است. گزارش‌های دیگر نشان می‌دهند که باج‌افزار بصورت خودکار و بدون نصب برنامه‌ای نمایان شده است. براساس اطلاعات ثبت شده از ۲۰ کشور مختلف در ID Ransomware، از روز هشتم ماه جاری میلادی (۱۷ مرداد)، میزان گسترش این باج‌افزار افزایش یافته است. لازم به ذکر است که این باج‌افزار هیچ ارتباطی با ابزار مدیریت رمزعبور KeePass ندارد.

ادامه مطلب

ملاحظات امنیتی چارچوب‌های اینترنت اشیا بر اساس مستندات OWASP

اینترنت اشیا (Internet of Things) شبکه‌ای از اشیای فیزیکی نظیر وسایل نقلیه، ساختمان‌ها و موارد دیگر است که به وسایل الکترونیکی، نرم‌افزارها و سنسورها مجهز شده‌اند و قادرند با اتصال به شبکه‌ی ارتباطی داده‌های مختلفی را جمع‌آوری و مبادله کنند. به دلیل گستردگی اینترنت اشیا، برای توسعه برنامه‌های کاربردی و اتصال دستگاه‌ها به یکدیگر از چارچوبهای مختلف استفاده می‌شود. یکی از اصلی‌ترین چالش‌های موجود در IOT رعایت نکات امنیتی و به حداقل رساندن آسیب‌پذیری‌ها است.

از این رو مرکز تخصصی آپا دانشگاه قم با بررسی گزارش‌های OWASP، به انتشار مستندی به منظور تعریف مجموعه‌ای از معیارهای ارزیابی امنیتی برای ارزیابی توانایی‌ها و نقاط قوت و ضعف امنیتی چارچوبهای IOT پرداخته است.

این سند می‌تواند به‌عنوان خط مبنای سودمند مورد استفاده قرار گیرد، همچنین می‌تواند محرکی برای فروشندگان چارچوبهای اینترنت اشیاء به‌منظور توسعه‌ی چارچوب‌های قدرتمندتر برای پاسخگویی به نیازهای امنیتی IOT باشد. معیارهای ارزیابی به چهار دسته‌ی مجزای زیر تقسیم‌بندی می‌شوند. هرکدام از این موارد یکی از بخش‌های اکوسیستم اینترنت اشیاء هستند و ویژگی‌های امنیتی مختص به خود را دارند.

الف- Edge

به دستگاه‌های فیزیکی که اکوسیستم اینترنت اشیاء را ایجاد می‌کنند edge گفته می‌شود. نکته‌ی مهم این است که در بسیاری از محیط‌های توسعه، دستگاه‌های edge ناهمگون هستند بدین معنا که شامل انواع مختلفی از دستگاه‌ها با سخت‌افزارها، سیستم‌عامل‌ها و قابلیت و منابع ارتباطی یا شبکه‌ای مختلف می‌شوند

ب- Gateway

gateway معمولاً از دستگاه‌های ضعیف سمت edge پشتیبانی می‌کند، همچنین امکان ارتباط دستگاه‌های edge را با مؤلفه‌های ابری فراهم می‌کند. gateway می‌تواند به‌عنوان تجمیع کننده‌ی ارتباطات و کنترل تنگناها استفاده شود و می‌تواند رابطی بین شبکه محلی قابل اعتماد ولی ناامن با شبکه جهانی اینترنت غیرقابل‌اعتماد از طریق ارتباطی امن ایجاد کند.

ج- Cloud

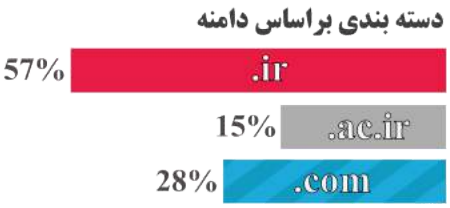
مؤلفه‌ی cloud در یک اکوسیستم اینترنت اشیاء به بخش مرکزی مدیریت و تجمیع داده‌ها در اکوسیستم اشاره دارد. مؤلفه‌ی cloud معمولاً شامل یک لایه ذخیره‌سازی داده‌ها(نظیر پایگاه داده)، بخش تحلیل و گزارش دهی، مدیریت اکوسیستم، رابط کاربری تحت وب و سایر اجزا نظیر سرویس ایمیل و پشتیبان گیری و ... می‌شود.

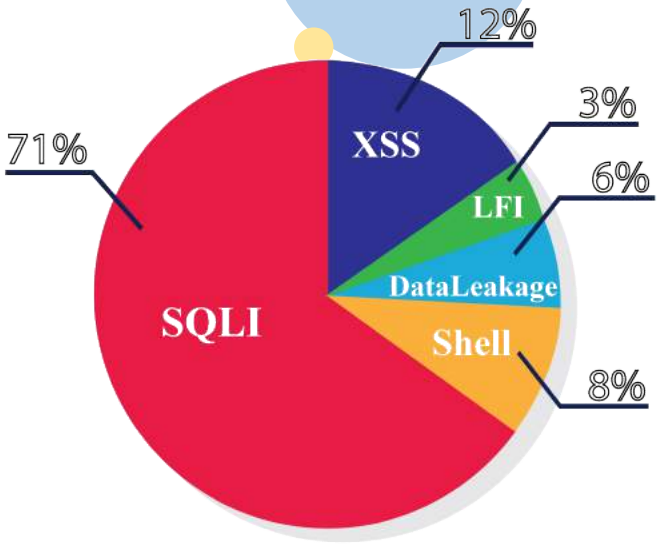
د- Mobile

توانایی‌های تلفن همراه در اکوسیستم اینترنت اشیاء بسیار متفاوت است. برخی برنامه‌های کاربردی تلفن‌های همراه صرفاً قابلیت گزارش‌گیری محدود از دستگاه‌های edge را فراهم می‌کنند، برخی امکان دستکاری و ایجاد تغییرات در مؤلفه‌های edge را فراهم کرده و برخی نیز توانایی مدیریت ابر و مشاهده‌ی تحلیل‌ها و آنالیزهای کامل را ارائه می‌دهند.

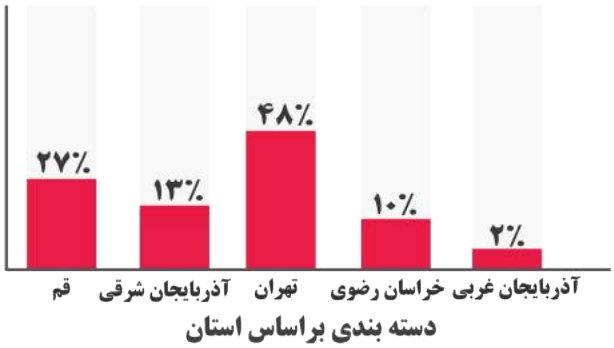
مطالعه متن کامل مقاله

نگاهی بر آمار آسیب پذیری های کشف شده

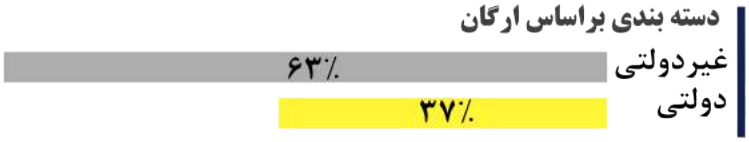




دسته بندی براساس نوع حمله



دسته بندی براساس استان



نمودارهای بالا آمار آسیب پذیری‌های کشف شده در دوره گذشته توسط مرکز آپا دانشگاه قم است. این نمودارها می‌تواند توسط متخصصان جهت راهنمایی برای شناسایی بهتر آسیب پذیری های احتمالی سازمان خود مورد استفاده قرار گیرد.

SQLinjection تکنیکی است که هکرها از آن استفاده کرده تا از طریق ورودی های صفحه وب دستورات SQL را در عبارات SQL تزریق کنند. دستورات تزریق شده می‌تواند پایگاه داده را تغییر داده و امنیت web application را به خطر اندازد.

باگ LFI مخفف Local File Inclusion می‌باشد به این معنی که امکان خواندن فایل های سرور را می‌دهد که بسیاری از فایل های مهم توسط آن خوانده می‌شود. همچنین در مواردی باعث می‌شود، تمامی سایت‌های مستقر روی سرور مورد نفوذ قرار گیرند.

Cross-site scripting از روش‌های نفوذ و گرفتن دسترسی غیر مجاز از یک وب‌گاه است که توسط یک هکر به کار می‌رود. در XSS تلاش می‌شود تا یک اسکریپت اجرایی (همچون جاواسکریپت) یا کد HTML نامطلوب از لایه‌های امنیتی احتمالی یک وب‌گاه گذر داده شود و همراه با کد HTML و اسکریپتهای اجرایی اصلی وب‌گاه دوباره به سمت کاربر بازگردانده شود. در نتیجه مرورگر این کد جدید را با این فرض که متعلق به وب‌گاه است اجرا کرده و تغییراتی در ظاهر و کارکرد وب‌گاه حاصل می‌شود. در گونه خطرناک‌تر این حمله، اسکریپت، در سمت کارگزار ذخیره می‌شود (همچون بخشی از متن یک وبلاگ) تا در آینده توسط همه کاربرهایی که به آن وب‌گاه مراجعه می‌کنند دریافت و اجرا شود.

اخبار داخلی مرکز آپا قم

صدور گواهی نامه امنیتی برای محصولات توسط مرکز آپا

فضای تبادل اطلاعات بیش از پیش رشد کرده و مورد استفاده قرار می‌گیرد، همچنین آسیب‌های ناشی از آن نیز افزایش می‌یابند، از جمله حمله به بانک‌های اطلاعاتی و صفحات خدماتی، باج‌افزارها، شنود و ... ، غافل‌شدن از این آسیب‌ها می‌تواند تبعات جبران‌ناپذیری داشته باشد.

مرکز تخصصی آپا قم با ارزیابی امنیتی دقیق توسط تیم حرفه‌ای این مرکز به سازمان‌ها، شرکت‌ها و ادارات کمک می‌کند تا از خطرات و حملات فضای تبادل اطلاعات در امان بمانند. از جمله خدمات ارائه شده توسط مرکز تخصصی آپا می‌توان به موارد زیر اشاره کرد:

- ارزیابی زیرساخت: بررسی سخت‌افزار، میان‌افزار و نرم‌افزار، تنظیم router، firewall و server ها
- تست نفوذ: انجام تست سیستماتیک و برنامه‌ریزی شده به منظور شناخت آسیب‌پذیری نرم‌افزار

همکاری بین مرکز آپا و نظام صنفی رایانه‌ای استان قم

اردیبهشت ۳ ,۱۳۹۷

در راستای نیازمندی‌های امنیتی بخش خصوصی فعال در حوزه فناوری اطلاعات استان قم، تفاهم‌نامه‌ای بین مرکز تخصصی آپا دانشگاه قم و و نظام صنفی رایانه‌ای استان قم منعقد شد. طبق این قرارداد، مرکز آپا به عنوان مرجع رسمی امنیت حوزه فناوری اطلاعات به بخش خصوصی فعال در استان معرفی گردید و آمادگی خود را جهت ارائه خدمات امنیتی مورد نیاز شرکت‌ها و مراکز تحت نظر نظام صنفی، اطلاع‌رسانی آسیب‌پذیری‌های روز صفر، برگزاری همایش‌های مشترک در سطح استان و استفاده متقابل از کارشناسان اعلام داشت.

شرکت‌های متقاضی خدمات امنیتی مانند گواهی‌نامه‌های امنیتی می‌توانند با معرفی‌نامه نظام صنفی از خدمات مرکز آپا طبق این تفاهم‌نامه بهره‌مند شوند.

دعوت جهت پروژه های کسری خدمت و امریه

به استحضار میرساند مرکز تخصصی آپای دانشگاه قم جهت انجام پروژه های خود از فارغ التحصیلان ارشد و دکتری پژوهشی در قالب امریه و پروژه کسری خدمت دعوت به عمل می آورد.

دعوت جهت کارآموزی در مرکز تخصصی آپا دانشگاه قم

از دانشجویان مستعد و علاقه‌مند جهت گذراندن واحد کاراموزی در این مرکز دعوت به عمل می آیند.

لازم به ذکر است قبل از هرگونه انجام کارهای اداری جهت اخذ واحد کارآموزی از دانشگاه خود به مرکز تخصصی آپا مراجعه کرده ثبت نام نمائید.

صاحب امتیاز: مرکز تخصصی آپا دانشگاه قم
مدیر مسئول و سردبیر: دکتر امیر جلالی بیدگلی
به زحمت: خانم صفیه موسوی، خانم سارا امیری، آقای متین لطیفی و آقای عیسی نودهی

مرکز تخصصی آپا قم
دانشگاه قم، ساختمان کتابخانه مرکزی
(+۹۸) ۲۵ ۳۲۸۵۰۹۶۵
http://cert.qom.ac.ir/
apaoffice@qom.ac.ir