مرکز تخصصی آپا
دانشگاه قم

خرداد ماه ۱۳۹۸

آمار آسیب پذیری های کشف شده

بررسی آخرین اخبار دنیای امنیت سایبری

اخبار داخلی مرکز تخصصی آپا قم

گزارش تحلیلی

فیشینگ

اخبار امنیتی

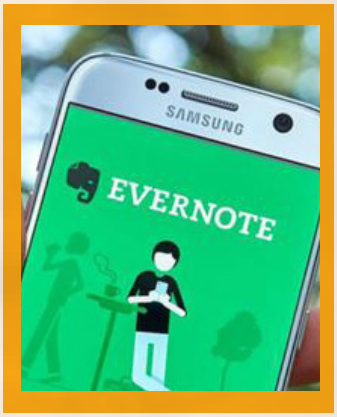
آخرین اخبار دنیای امنیت سایبری

سرقت اطلاعات حساب ارز دیجیتال کاربران توسط برنامه‌های اندرویدی

تاریخ: ۲ تیر ماه ۱۳۹۸
http://cert.qom.ac.ir/?p=2632

محققان امنیتی دو برنامه مخرب اندرویدی را کشف کرده‌اند که با وجود استفاده از احراز هویت دو مرحله‌ای (۲FA)، شگردی هوشمندانه برای ورود به حساب ارز دیجیتال کاربران استفاده می‌کنند.

ESET دو برنامه مخرب را کشف کرد که قادر به گمراه کردن کاربران در استفاده از ۲FA شده بودند و در فروشگاه Google Play منتشر شدند. اولین برنامه به نام BTCTurk Pro Beta در ۷ ژوئن و دومین برنامه، با نام sBtcTurk .....

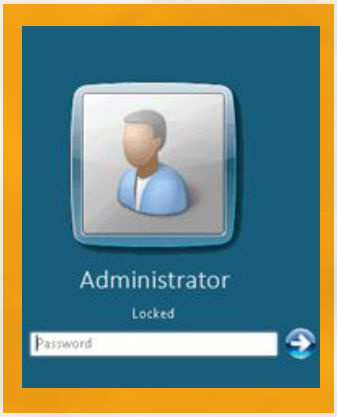


افزونه‌ی برنامه‌ی EVERNOTE و آسیب‌پذیری میلیون‌ها کاربر

تاریخ: ۲۷ خرداد ماه ۱۳۹۸
http://cert.qom.ac.ir/?p=2612

آسیب پذیری Evernote Web Clipper منجر به سرقت اطلاعات میلیون‌ها کاربر این سرویس شد.

مشکل امنیتی کشف شده که از نوع UXSS در افزونه‌ی برنامه‌ی Evernote نصب شده بر روی مرورگر کروم باعث می‌شود که مهاجمان بتوانند اطلاعات کاربر را بدست آوردند و مورد سوء استفاده قرار دهند. بر طبق گزارش شرکت امنیتی گاردیو (Guard.io)، آسیب‌پذیری درماه گذشته کشف شده است و میلیون‌ها نفر را تحت تاثیر قرار می‌دهد....



دور زدن قفل ویندوز در RDP

تاریخ: ۲۱ خرداد ماه ۱۳۹۸
http://cert.qom.ac.ir/?p=2604

یک محقق امنیتی اخیرا جزئیاتی از آسیب پذیری ویندوز در بخش Remote Desktop Protocol (RDP) منتشر و با شناسه CVE-۲۰۱۹-۹۵۱۰ ثبت کرده است که در آن مهاجمان می توانند از lock screen در Remote Desktop عبور کنند.

این آسیب پذیری توسط Joe Tammariello در موسسه مهندسی نرم افزار دانشگاه Carnegie Mellon کشف شده است، این شکاف زمانی اتفاق افتاد که مایکروسافت....

تلویزیون‌های هوشمند در دست هکرها

تاریخ: ۱۸ خرداد ماه ۱۳۹۸
http://cert.qom.ac.ir/?p=2601

تلویزیون‌های هوشمند یکی از دستگاه‌های به شدت تکامل یافته محسوب می‌شوند مخصوصا وقتی آن‌ها را به اینترنت متصل می‌کنیم. قابلیت‌هایی همچون پخش رسانه، گشت و گذار در اینترنت، بازی و همچنین ذخیره‌ی فایل‌ها در cloud؛ تلویزیون‌های هوشمند را به کامپیوترهایی تمام عیار تبدیل کرده است. در حالی که دستگاه‌های هوشمند بیشتری در سراسر جهان فروخته می‌شوند، مصرف کنندگان باید از خطرات امنیتی...

فضای سایبری کنونی ایران، در مقابله با حملات صفحات جعلی بسیار آسیب‌پذیر است. ضعف در تکنیک و روش‌های مقابله و نبود حداقل‌های مهارتی در کاربران و استفاده کنندگان از فضای سایبری باعث شده است که فضا برای مهاجمان و سارقان به شدت مساعد باشد. مقاله‌ی پیشرو، تلاشی است که فضای کنونی را به همراه ضعف‌ها و نواقص موجود تشریح کند و پیشنهادهای بهبود را ارائه دهد

گزارش تحلیلی فیشینگ

فیشینگ، حملاتی با رویکرد فریفتن کاربران با صفحات جعلی است که با هدف سرقت اطلاعات هویتی و پرداختی صورت می‌گیرد. مهاجمان با استفاده از تکنیک‌های مهندسی اجتماعی و فنی جعل صفحات و برنامه‌های مورد استفاده‌ی قربانیان، سعی در جمع‌آوری اطلاعات دارند. فیشینگ راهی است که تبهکاران، اطلاعاتی نظیر کلمه کاربری، رمز عبور، شماره ۱۶ رقمی عابر بانک، رمز دوم و cvv2 را از طریق ابزارهای الکترونیکی ارتباطات به سرقت می‌برند. شبکه‌های اجتماعی، سایت‌های حراجی و درگاه‌های پرداخت آنلاین نمونه‌ای از ابزارهای الکترونیکی ارتباطات می‌باشند. کلاهبرداری فیشینگ از طریق ایمیل‌ها ، وبسایت‌ها و پیام‌ها صورت می‌پذیرد و قربانیان به صورت مستقیم اطلاعات حساس و محرمانه خود را در وب سایت‌ها و صفحات جعلی که در ظاهر کاملا شبیه وب سایت‌های سالم و قانونی می‌باشد وارد می‌نمایند. حقه‌ی فیشینگ یکی از تکنیک‌های مهندسی اجتماعی برای فریب کاربران می‌باشد که کلاهبرداران از ضعف امنیتی یک وب سایت برای انجام عملیات مجرمانه خود استفاده می‌کنند.

انواع فیشینگ

افرادی که در فضای مجازی سعی در فریب دادن کاربران دارند. برای مثال اشخاصی که با هدف فریب دادن کاربران با هویت جعلی به سراغ کاربران رفته و با ترفند هایی از قبیل دوستی ، درخواست کمک ، درخواست شارژ و ... سعی در فریب دادن کاربران و سرقت اطلاعات کارت بانکی ان ها مینمایند. کاربران میتوانند با پرهیز از اعتماد کردن به چنین افرادی از اطلاعات خود محافظت نموده و با هشدار دادن به بقیه افراد و کاربران از به سرقت رفتن اطلاعات آنان نیز محافظت نمایند .

فیشینگ با ایمیل های فریبنده

در این روش از حمله‌های فیشینگ، شخص کلاهبردار با ارسال ایمیل‌های فریبنده به قربانیانش می‌کوشد با بیان دلایل مجاب کننده مخاطبان را به وارد کردن اطلاعات بانکی خود وادار میکند. ممکن است ایمیل به ظاهر از طرف بانک اشخاص، یک شرکت معتبر و یا حتی بانک مرکزی ارسال شود و از کاربران درخواست کند ظرف مدت زمان معینی اطلاعات بانکی خود را ارسال کنند. نکته قابل بیان این است که سیستم مالی و بانکی هیچگاه از طریق ایمیل از شما درخواست نمی‌کند اطلاعات بانکی‌تان را برای آن‌ها ارسال کنید، شما حتی مجاز به اعلام رمز بانکی خود به کارکنان بانک هم نیستید.

فیشینگ تلفنی

کلاهبرداران در این روش از طریق تلفن با طعمه های خود ارتباط برقرار می‌کنند و ضمن اینکه خود را نماینده بانک، شرکت معتبر و یا سازمانی که شما می‌شناسید معرفی می‌کنند از شما می خواهند جهت دریافت جایزه خود اطلاعات بانکی خود را در اختیار ایشان قرار دهید. برای واریز هر گونه وجه به حساب شما اعم از جایزه، پاداش و مزایا نیازی به اعلام رمز بانکی شما نخواهد بود.

طراحی صفحه‌ای نظیر درگاه پرداخت بانکی

کلاهبرداران در این روش صفحه‌ای مشابه درگاه پرداخت آنلاین بانک‌ها طراحی می‌کنند و با قرار دادن این صفحه جعلی در فروشگاه‌های جعلی و با ارائه پیشنهادهای بسیار مناسب سعی در فریب دادن کاربران میکنند و انان را وادار به وارد کردن اطلاعات خود داخل درگاه جعلی مینمایند. به محض ورود کاربران به صفحات جعلی و ارائه اطلاعات بانکی کاربران، اطلاعات به صورت خودکار برای کلاهبردار ارسال میگردد.

فیشینگ با دستگاه‌های POS و ATM تقلبی

برخی کلاهبرداران با استفاده از POS و ATM های تقلبی(Skimmer) کارت‌های بانکی طعمه های خود را کپی کرده و به بهانه فروش محصول و کالا رمز عبور آن‌ها را پرسیده و سپس به حساب وی دسترسی پیدا میکنند. پیشرفت تکنولوژی شیوه‌های پرداخت متنوعی در اختیار کاربران قرار گرفته که با کمک آن می‌توان استفاده از POS و ATM را به میزان قابل توجهی کاهش داد.

ربات‌های تلگرام

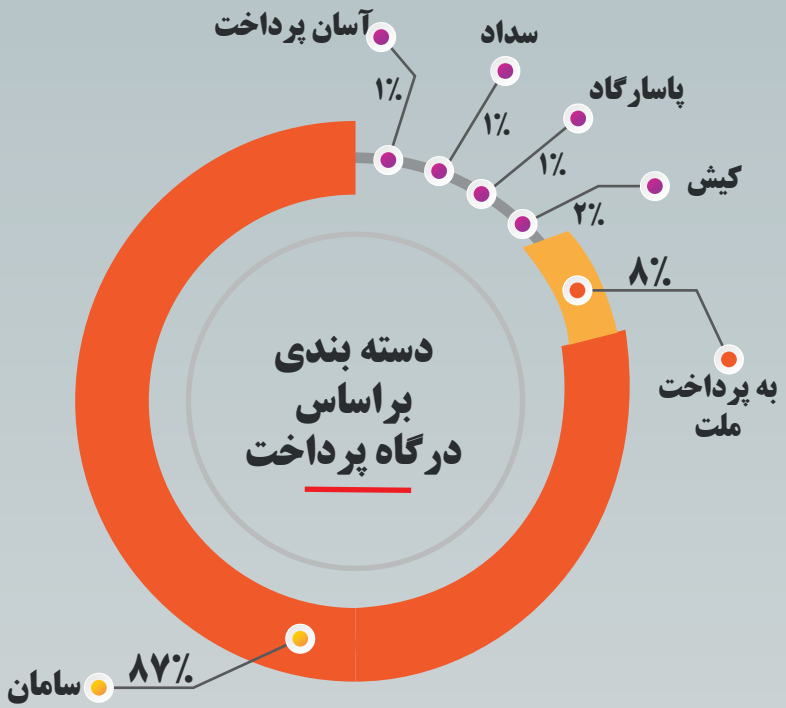
ربات‌های تلگرام میتوانند بسیار پر کاربرد و پر استفاده باشند، اما به هر روی تلگرام بستر مناسبی برای انتقال وجه نیست کاربران برای انجام معاملات و انتقال وجه کافی است هنگام استفاده از این خدمات نکات امنیتی را رعایت نموده و همواره با مراجعه به مراکز معتبر و شناخته شده سعی در انجام تراکنش نمایند.

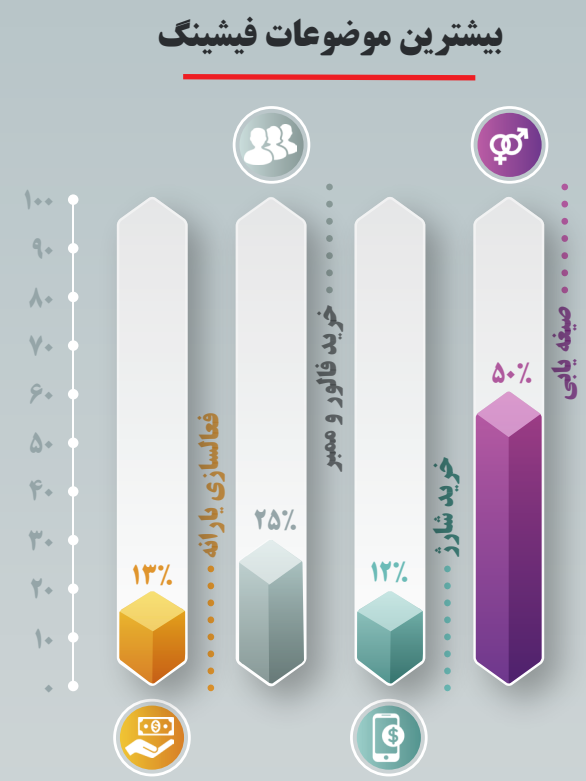
دام‌های فیشینگ

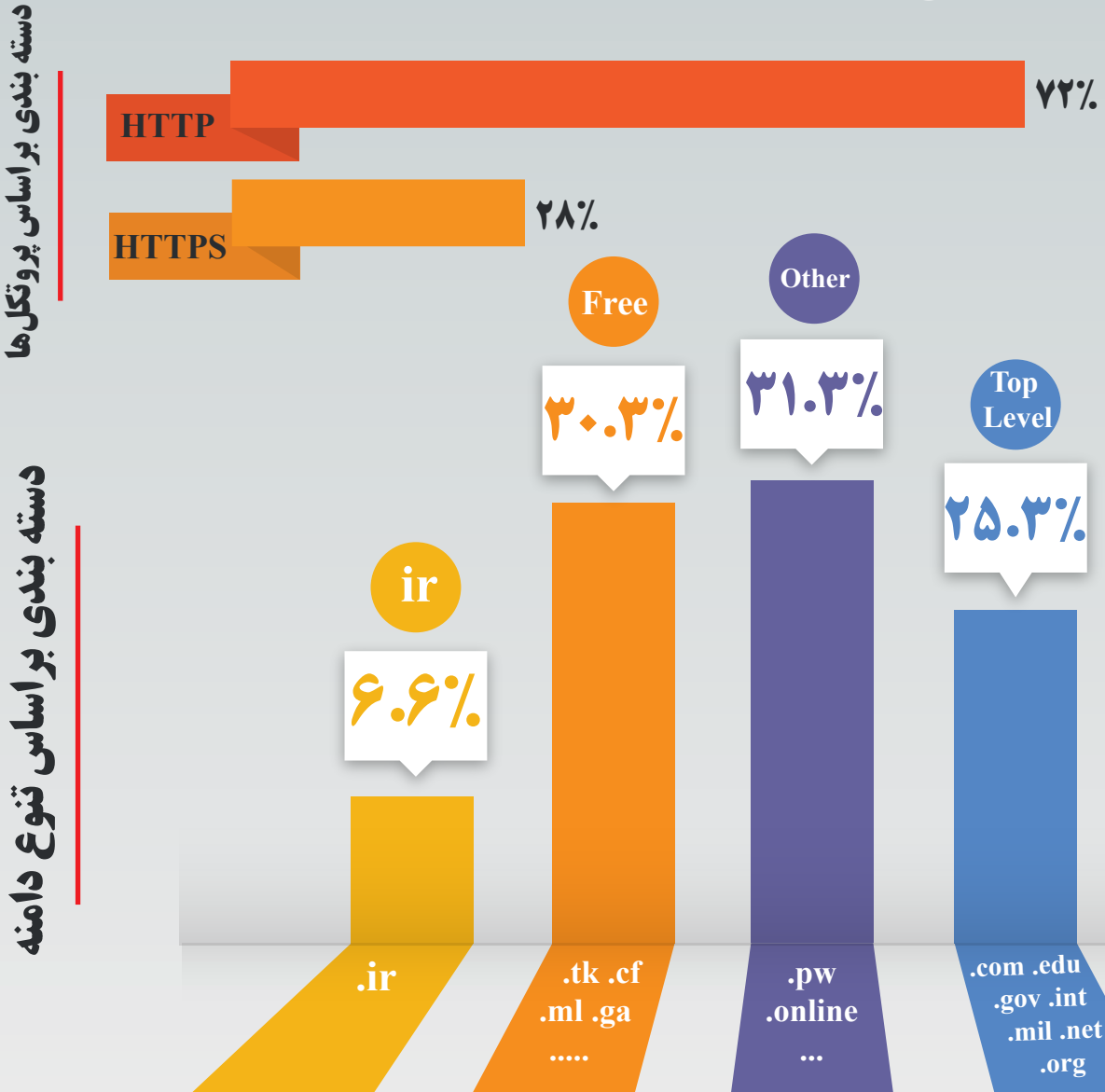
در فیشینگ، قربانیان با استفاده از موضوع‌های مختلفی به دام می‌افتند. موضوع باید به قدر جذاب و واقعی باشد که جای شک و شبهه‌ای برای کاربران فضای مجازی باقی نگذارد.....

مطالعه بیشتر: http://cert.qom.ac.ir

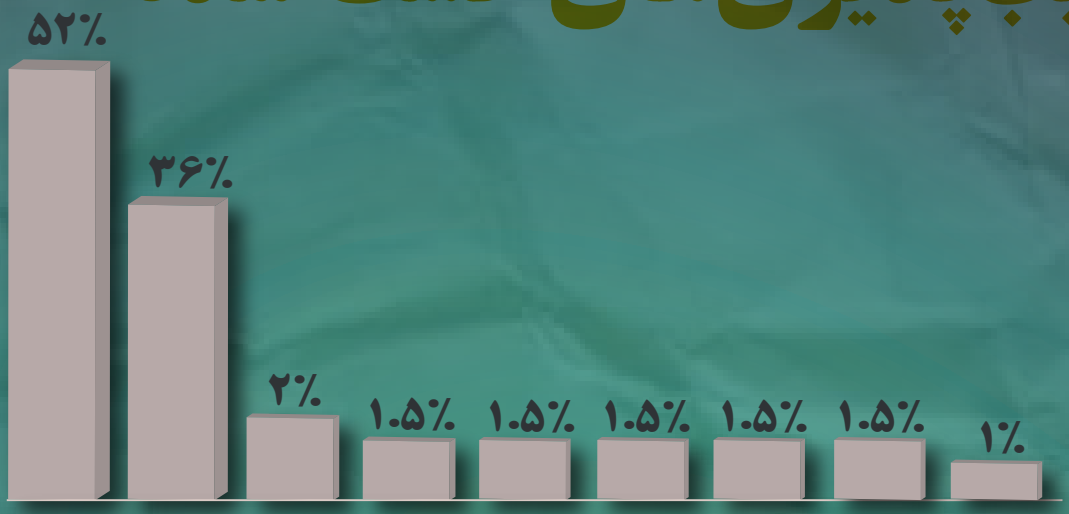
اینفوگراف آمار تحلیلی فیشینگ





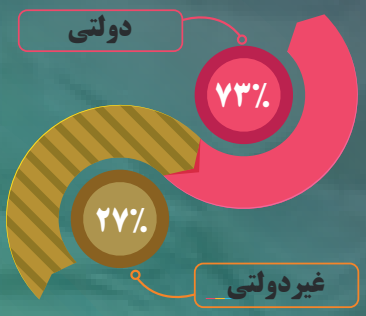


آمار آسیب‌پذیری‌های کشف شده

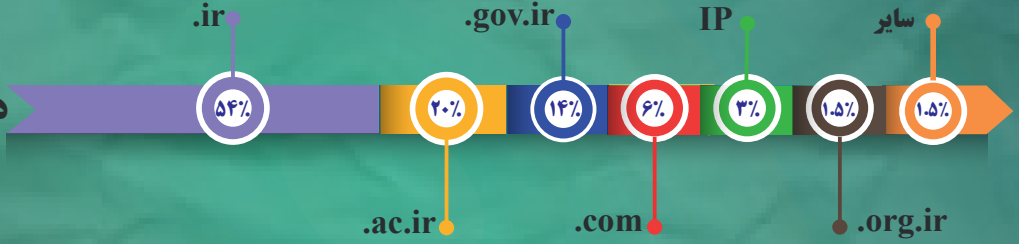


دسته بندی براساس استان

دسته بندی براساس ارگان

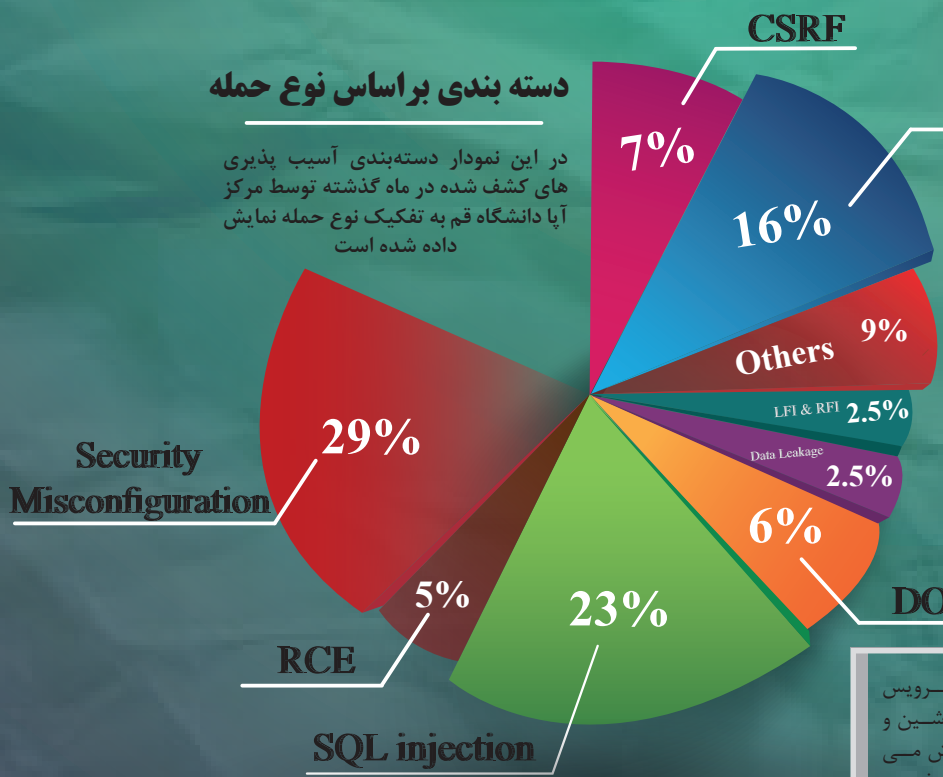


دسته بندی براساس دامنه



دسته بندی براساس نوع حمله

در این نمودار دسته‌بندی آسیب پذیری های کشف شده در ماه گذشته توسط مرکز آپا دانشگاه قم به تفکیک نوع حمله نمایش داده شده است



XSS

از روش‌های نفوذ و گرفتن دسترسی غیر مجاز از یک وب‌گاه است. 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.

DOS

حمله منع سرویس یا حمله منع سرویس توزیع شده، تلاش برای خارج کردن ماشین و منابع شبکه از دسترس کاربران مجازش می باشد. در واقع هر حمله‌ای علیه دسترس پذیری به عنوان حمله منع سرویس تلقی می‌شود. اگرچه منظور از حمله DOS و انگیزه انجام آن ممکن است متفاوت باشد، اما به‌طور کلی شامل تلاش برای قطع موقت یا دائمی یا تعلیق خدمات یک میزبان متصل به اینترنت است.

SQL injection

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

اخبار داخلی

برگزاری دوره های ضمن خدمت در حوزه امنیت فناوری اطلاعات

با عنایت به الزام آموزش کارکنان دستگاه های اجرایی در حوزه امنیت فناوری اطلاعات و به منظور جلوگیری از خسارات ناشی از عدم آگاهی و دانش کافی، مرکز آپا دانشگاه قم با همکاری سازمان مدیریت و برنامه‌ریزی استان و گروه آموزش‌های آزاد دانشگاه قم اقدام به برگزاری دوره های آموزشی «بنیان مدیریت امنیت اطلاعات (بما)» و «امنیت کاربری فناوری اطلاعات (اکفا)» نموده است. هدف کلی این دوره ها ارتقاء سطح آگاهی و دانش مدیران و عموم کارکنان دولت نسبت به امنیت فناوری اطلاعات و مدیریت مؤثر آن در به کارگیری منابع فناوری اطلاعاتی در سازمان ها می باشد و از سرفصل‌های این دوره‌ها می توان به شناخت امنیت سایبری در سازمان‌ها، امنیت شبکه های اجتماعی، مسائل حقوقی در امنیت و استانداردهای امنیت و آشنایی کاربردی با ابزارهای افزایش امنیت فناوری اطلاعات اشاره کرد.

این دوره از جمله دوره های ضمن خدمت مصوب مدیران ادارات دولتی می باشد و سازمان اداری و استخدامی کشور هم در طرح بازبینی دوره های آموزشی، مطابق بخشنامه مربوطه، دوره های آموزشی موردنظر را نیمه مهرماه گذشته تصویب و برای اجرا به کلیه دستگاه های اجرایی کشور ابلاغ نمود. در این خصوص با توجه به اهمیت حفظ امنیت سایبری سازمان‌ها، لازم است دستگاه‌های اجرایی استان برپایه نظام آموزشی کارمندان دولت نسبت به برنامه ریزی و اجرای آنها اقدام نمایند.

علاقه مندان جهت ثبت نام به وبسایت مرکز آموزشهای آزاد دانشگاه قم به آدرس http://oe.qom.ac.ir مراجعه نمایند و یا در ساعت اداری به جز روزهای تعطیل و پنجشنبه با کارشناسان مرکز آپا به شماره تلفن های ۰۲۵۳۲۱۰۳۳۸۷ یا ۰۲۵۳۲۸۵۰۹۶۵ تماس حاصل فرمایند.

برگزاری دوره آموزشی Security+

همه ما می دانیم در عصر کنونی امنیت فضای سایبری یکی از مهم ترین موضوعات در حوزه مهندسی IT بوده و یکی از دغدغه های اصلی همه سازمان ها و نهادها می باشد. موسسه CompTIA دوره استاندارد و پایه ای را با نام Security+ برای علاقمندان حوزه امنیت سایبری طراحی کرده است تا به صورت ابتدایی و ریشه ای به حوزه های مختلف امنیت پرداخته و مهارت‌های علاقمندان این حوزه را افزایش دهد Security+ اولین دوره ای است که در دنیای امنیت مطرح می‌شود و گام نخستی است به دنیای امنیت سایبری. گواهینامه این دوره مورد قبول جهانی واقع شده و دانش بنیادی شخص را در حوزه امنیت افزایش می‌دهد.

طول این دوره ۳۰ ساعت و پیش نیاز آن داشتن دانش مقدماتی شبکه در محدوده Network+ است. کلاس به محض رسیدن به حد نصاب تشکیل می‌شود و به ثبت نام کنندگان اطلاع رسانی می‌گردد. شماره تلفن تماس جهت پیگیری و پشتیبانی، ۰۲۵۳۲۱۰۳۵۵۶ از ساعت ۱۱:۳۰ تا ۱۳:۰۰ می باشد. همچنین متقاضیان می توانند سؤالات و پیگیری های خود را از طریق ارسال پیام در بحش نظرات انجام دهند.

مدرس این دوره مهندس مجتبی زارع، دانشجوی دکتری مهندسی فناوری اطلاعات و مدرس دانشگاه و عضو مرکز تخصصی آپا دانشگاه قم می باشد. حوزه تخصصی ایشان، امنیت اطلاعات و اینترنت اشیاء است.

برای ثبت نام در این دوره می توانید به وبسایت مرکز آموزش‌های آزاد دانشگاه قم به آدرس http://oe.qom.ac.ir/course/41 مراجعه نمایید.

مرکز تخصصی آپای دانشگاه قم
آگاهی، آمادگی، پشتیبانی، اقدام

صاحب امتیاز:
مرکز تخصصی آپا دانشگاه قم

مدیر مسئول و سردبیر:
دکتر امیر جلالی بیدگلی

طراحی و صفحه آرایی:
محمد معین فاضلی

تماس با ما

قم، دانشگاه قم
۰۲۵۳۲۸۵۰۹۶۵
apa@qom.ac.ir
http://cert.qom.ac.ir