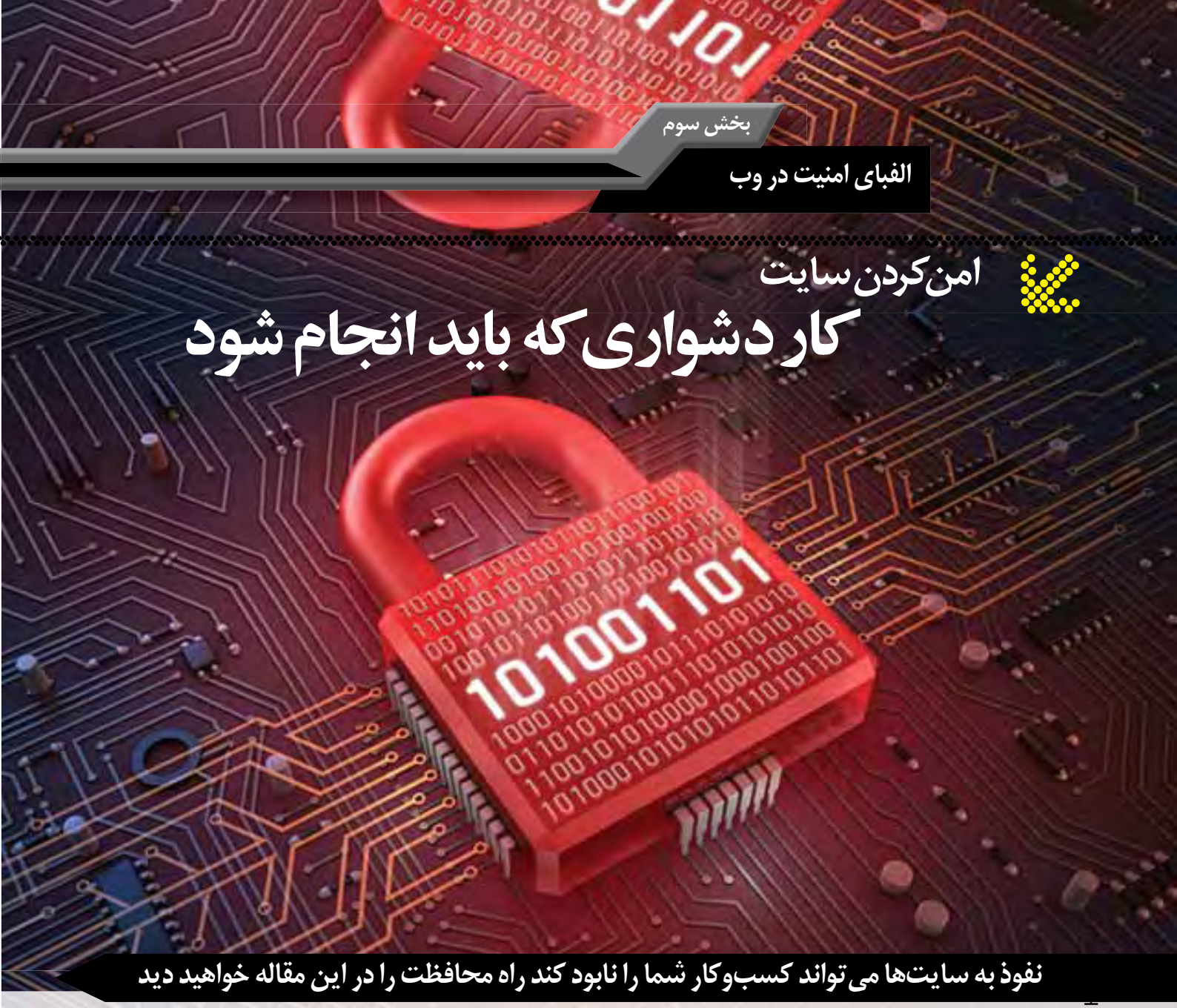
امن‌کردن سایت

کار دشواری که باید انجام شود



نفوذ به سایت‌ها می‌تواند کسب‌وکار شما را نابود کند راه محافظت را در این مقاله خواهید دید

در سال ۲۰۰۶ اعضای یکی از گروه‌های مجرمانه فروشگاه‌های آنلاین شرکت‌هایی نظیر Hannaford Brothers، 7-Eleven و چندین خرده‌فروشی دیگر را هک کردند. هدف آن‌ها پیداکردن رخنه‌ای بود که به حلقه کلاه‌برداری کارت‌های خریدشان امکان جمع‌آوری اطلاعات کافی برای انجام یک کلاه‌برداری بزرگ را بدهد. در روزهای آغازین آن سال، به‌لطف هکرهای روسی که در میان آژانس‌های امنیتی به هکر ۱ و هکر ۲ مشهور بودند، آن‌ها دستبرد به خزانه اصلی را انجام دادند. هکرها که در هلند و کالیفرنیا مستقر بودند، توانستند نقطه‌ضعفی را در سایت سیستم پرداخت هارت‌لند (Heartland Payment System) پیدا کنند. این سرویس ماهانه ۱۰۰ میلیون تراکنش را برای حدود ۲۵۰ هزار مشتری به انجام می‌رساند. با استفاده از سیستم نفوذی که به‌اصطلاح تزریق سیکوئل (SQL Injection) نامیده می‌شود، توانستند در این شبکه پرداخت آنلاین جای پایی برای خود فراهم کنند و نفوذی را رقم زدند که برای هارت‌لند زیانی در حدود ۱۲/۶ میلیون دلار به‌همراه داشت.

مغز متفکر این هک، هکر شناخته شده آلبرت گونزالس بود. این هک به یکی از نمونه‌های به یادماندنی خرابکاری‌هایی تبدیل شد که ممکن است در نتیجه نفوذپذیری‌های معمولی که در همه کامپیوترهای سرور وجود دارد، اتفاق بیفتد. متخصصان امنیت نرم‌افزارهای وب مدت‌ها است که درباره هزینه‌ای که این باگ‌ها می‌توانند برای کسب‌وکارها به‌وجود آورند، هشدار می‌دهند اما انگار در بیش‌تر مواقع این هشدارها نادیده گرفته می‌شوند. با این حال، پس از هک هارتلند، هیچ‌کس نمی‌توانست اهمیت کنترل این باگ‌ها و میزان خسارت ناشی از آن‌ها را انکار کند. علاوه‌بر میلیون‌ها دلاری که این حمله به هارتلند ضرر زد، شرکت با از دست دادن اعتبارش در میان مشتریان و سرمایه‌گذاران نیز زیان قابل ملاحظه‌ای را تجربه کرد.

این حادثــه به هیچ وجــه رخدادی اســتثنایی یا غیرمعمول نیســت. در ســال‌های بعد از آن، ســایت‌های کوچک و بزرگ زیــادی در دام چنین حمله‌هایی که ناشی از SQL Injection، Cross-site Scripting و دیگر باگ‌ها بودند، گرفتار شــدند. این حفره‌های کوچک به نفوذکنندگان اجازه می‌دهد که کدهای مخرب خــود را در مرورگر یک کاربر نهایی تزریق کرده یا کل یک وب ســرور را در اختیار بگیرند. در ژانویه ۲۰۱۳، حمله‌کنندگان سایت خبرنــگاران بدون مرز را دراختیار گرفته و توانســتند به‌صورتی مخفیانه بدافزارهایی را روی کامپیوترهای بازدیدکنندگان نصب کنند. حمله‌هایی که از این نفوذپذیری‌های ســاده استفاده کرده و به مجرمان اجازه آلوده‌کردن بازدیدکنندگان را می‌داد به حدی معمول شده‌اند که اصطلاح «حمله‌های راه آب» (watering hole attack) برای آن‌ها مورد استفاده گرفت. این اصطلاح به این دلیل ســر زبان‌ها افتاد که هکرها درســت مانند شــکارچیانی رفتار می‌کنند که بر سر آبگیرها کمین کرده و منتظر صیدهای تشنه‌ای می‌مانند که به دنبال چیزی برای نوشیدن می‌گردند.

احتمالات این است...

تمام این‌هــا تنها یک معنــی دارد: اگر به تازگی گروهی از متخصصان امنیت ســایت شما را بررسی نکرده‌اند، به احتمال زیاد سایت شــما هم می‌تواند به منبعی برای گســترش آلودگی تبدیل شود.

براساس رده‌بندی ۱۰ نفوذپذیری مخرب که به تازگی توسط پروژه امنیت نرم‌افزارهای وب بــاز OWASP (ســرنام Open Web Application Security Project) منتشــر شده است، تهدیدهایی که بیش از بقیه سایت‌ها را تهدید می‌کنند به شرح زیر است:

۱- تزریق (Injection)

ایــن نفوذپذیری‌ها زمانی اتفــاق می‌افتند کــه نرم‌افزارهای تحت وب ورودی‌های کاربر را به همراه سایر داده‌های غیرقابل اعتماد برای یک مفسر (Interpreter) ماننــد یک پایگاه داده SQL ارســال می‌کنند. حمله‌کنندگانی نظیــر هکرهایی که برای گونزالــس کار می‌کردند، ایــن باگ‌ها را به کمک اســکرهایی یافته و از آن‌ها برای سرقت جدول‌های گذرواژه‌ها یا داده‌های حساس اســتفاده می‌کنند. از این آســیب‌پذیری‌ها می‌توان برای حمله‌های «رد دسترســی» یــا Denial of access یا حتی دراختیارگرفتن کنترل کامل وب‌ســرور اســتفاده کرد. چنین نفوذپذیری‌هایی ممکن است آن‌قدر متعدد باشند که درست همانند علف‌های هرز یک باغ ریشه‌کن کردن‌شان ناممکن باشد. بهترین روش برای از بین بردن این راه‌های نفوذ، تکیه بر برنامه‌های وبی است که ورودی‌های کاربر را پیش از ارسال به سرور کنترل و اصلاح کنند. راه مورد علاقه OWASP برای جلوگیری از حمله‌های تزریقی این است که «از یک API اســتفاده شود که در کل از مفسر استفاده نمی‌کند یا نوعی اینترفیس پارامتری برای مفسر به‌وجود می‌آورد.»

۲- اسکریپت‌های بین‌سایتی (Cross-site Scripting)

این نوع حملات که به اختصار XSS نامیده می‌شوند زمانی اتفاق می‌افتند که برنامه‌های وب داده‌های کاربر را بدون اعتبارسنجی یا حتی صرف‌نظر از آن داده‌ها به یک مرورگر ارسال می‌کنند. حمله‌کنندگان از این نفوذپذیری استفاده کرده و قطعه‌کدهای جاوااسکریپتی را ارسال می‌کنند که کوکی‌های مرورگر را می‌دزدند. کوکی‌هایی که برای اعتبارســنجی کاربر نهایی برای ورود به حســاب کاربری ایمیل یا سایر ســرویس‌های نیازمند رمزعبور مورد اســتفاده قرار می‌گیرند. از این حفره‌هــا می‌توان برای دیفیس کردن سایت‌ها نیز استفاده کرده و کاربران را به دیگر سایت‌ها هدایت کرد یا حتی از بدافزارها برای دراختیارگرفتن کنتــرل مرورگر کاربر کمک گرفت. تنها زمانی می‌توان نگرانی از باگ‌های XSS را فراموش کرد که مطمئن باشیم که تمام داده‌هایی که کاربر وارد می‌کند مورد ارزیابی قرار می‌گیرند یا از آن‌ها صرف‌نظر می‌شود و در نتیجه دیگر خطرناک نیستند.

۳- اعتبارسنجی از کار افتاده و مدیریت نشست (Broken Authentication and Session Management)

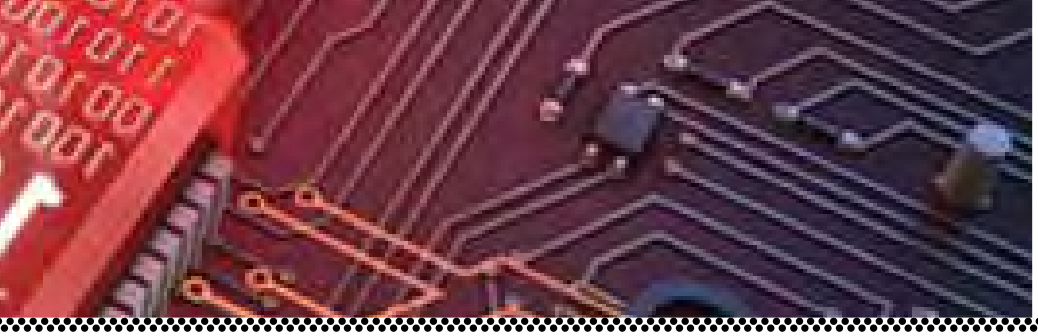
این خطاها به‌طور معمول، در برنامه‌هایی وجود دارند که کارشــان وارد کردن (Login) کاربر بــه بخش‌هــای با دسترســی محدود سایت (مثلاً حســاب‌های ایمیل) است. معمولاً این خطاها در برنامه‌هایی یافت می‌شــوند که به‌صورت اختصاصی توســعه داده شده‌اند و در آن‌ها اشــتباه‌های حیاتی و خطرناک وجود دارد. مثلاً ممکن است شماره نشست (Session ID) مورد اســتفاده به‌سادگی قابل حدس زدن باشد یا در URL سایت دیده شود. همان‌طور که نام این دسته نشان می‌دهد پیامد چنین اشتباهاتی این است که این الگوهای اعتبارســنجی آن‌طوری که ما فکــر می‌کنیم کار نمی‌کننــد و در نتیجه به حمله‌کنندگان اجازه می‌دهند بدون اعتبارسنجی کنترل حساب‌های کاربری را دراختیــار گرفتــه و کارهایی را انجام دهند کــه درواقع یک کاربر مجاز می‌تواند انجام دهد. مثلاً حمله‌کننده می‌تواند داده‌های حساس یا ایمیل‌های کاربر را پاک کند. بهترین راه در امان ماندن از چنین حفره‌هایی این اســت که از الگوها و برنامه‌هایی که به‌صورت اختصاصی توسعه می‌یابند پرهیز کرده و در عوض به برنامه‌هایی روی آورد که قبلاً به صورت کامل امتحان شده‌اند.

۴- ارجاع مستقیم به شئ ناامن (Insecure Direct Object Reference)

ایــن حفره‌ها ریشــه در برنامه‌های وبی دارند کــه در هنگام تولید یک صفحه وب از نام واقعی یا کلید یک شئ در URL صفحه استفاده می‌کنند. در برخی موارد حمله‌کننده‌ها می‌توانند با استفاده از این رخنه‌ها و تنها با تغییر دادن متــن یک URL مجوزهای قدرتمند مدیر سیســتم را دراختیار بگیرند. برای جلوگیری از این خطاها سایت‌ها باید از ارجاع‌های غیرمستقیم به اشیا یا ارجاع‌های جداگانه برای هر کاربر اســتفاده کنند، زیرا این ارجاع‌ها قابل دستکاری نیستند.

۵- جعل درخواست بین‌سایتی (Cross-site Request Forgery)

حفره‌های CSRF از ســایت‌های تقلبی برای تولید درخواست‌های HTTP جعلی اســتفاده می‌کنند تا به کاربرانی که از ســایت‌های نفوذپذیر بازدید



شکل ۲

می‌کنند، حمله کنند. حمله‌کننده‌ها از این حفره‌ها اســتفاده می‌کنند تا کاربر نهایی را وادار کنند که در سایتی که در آن وارد شده کارهای ناخواسته‌ای را به اجبــار انجام دهد. این آســیب‌پذیری‌ها می‌تواننــد قربانی را مجبور کننــد تا ســهواً ایمیلی را پاک کند یا کار دیگری را انجــام دهد که انجام آن توســط هکر نیازمند تأیید هویت است. این حمله‌ها به‌ویژه زمانی که کاربر قربانی مجوزهای مدیریت سیســتم را دراختیار داشــته باشــد، می‌توانند بســیار مخرب باشند. برای بســتن حفره‌های مربوط به CSRF برنامه‌های وب بایــد از توکن‌های غیرقابل پیش‌بینی در بدنه (BODY) یا URL هر یک از درخواست‌های HTTP استفاده کنند و این توکن‌ها باید در هر نشست کاربر و هر درخواست منحصربه‌فرد باشند.

در ادامه پنج تله و دامی که سایت‌ها به لحاظ امنیتی گرفتار آن می‌شوند و مواردی که باید برای پیشگیری از آن‌ها رعایت شوند را خواهید دید.

۶- تنظیمات نادرست امنیتی

این باگ‌ها به‌طور عمومی، به حمله‌کننده‌ها اجازه می‌دهند به عملکردهای قدرتمند سیستم یا داده‌های حســاس دسترسی پیدا کنند. این باگ‌ها اغلب نتیجه تنظیمات نادرست وب سرورها، برنامه‌های وبی یا کدهای اختصاصی هستند. مســتحکم کردن محیط وب (مثلاً به‌روز نگه داشتن سیستم‌عامل، برنامه‌ها و سایر نرم‌افزارها)، غیرفعال‌کردن یا حذف سرویس‌های ناخواسته و همچنین از کارانداختن تمام حساب‌های کاربری و گذرواژه‌های پیش‌فرض از جمله راه‌های مبارزه با این باگ‌ها است.

۷- رمزنگاری نا امن سیستم ذخیره‌سازی

این مجموعه شامل نمونه باگ‌هایی است که به‌تازگی برخی متخصصان امنیتی در ســرویس ذخیره‌ســازی ابری کیم دات کام یعنی Mega کشف کرده‌اند. سیستم ذخیره‌سازی رمزنگاری‌شده ناامن ممکن است شکل‌های مختلفی به خود بگیرد. از موفق نبــودن در رمزنگاری اطلاعات کارت‌های اعتباری یا ســایر داده‌های حســاس گرفته تا اســتفاده از پیاده‌سازی‌های ناامن رمزنگاری که بــه حمله‌کنندگان اجازه می‌دهــد محتوای رمزنگاری شــده را رمزگشایی کنند. Mega با ناتوانی در امن نگاه داشتن کلید مورد اســتفاده در الگوریتم برخی از کدهای رمزنــگاری‌اش، درس مهمی را در زمینه ذخیره‌ســازی رمزنگاری شده به توسعه‌دهندگان وب داد. یکی دیگر از بی‌توجهی‌های مهمی که در این زمینه اتفاق می‌افتد، مشــکل در حفاظت از پایگاه‌های داده حاوی گذرواژه‌های کاربران ســایت در زمانی اســت که یک ســایت مورد نفوذ قرار می‌گیرد. بــا این‌که هش‌کردن گذرواژه‌ها برای رمزنگاری الزامی است، اما به تنهایی کافی نیست. نکته مهم دیگر این است که الگوریتم استفاده شده به‌صورت اختصاصی برای رمزنگاری گذرواژه‌ها طراحی شده باشد. الگوریتم‌هایی نظیر PBKDF2، Bcrypt یا SHA512crypt انتخاب‌های خوبی هستند. اما نمونه‌هایی نظیر SHA3، SHA1 و MD5 چندان مناســب نیستند. (نکته: یکی دیگر از روش‌های دفاع اساسی این است که به جز در مــوارد ضروری از اطلاعات کارت‌های اعتباری و ســایر اطلاعات حساس صرف‌نظر کنیم.)

۸- ناتوانی در محدود کردن دسترسی URL

ایــن خطاهــا زمانی اتفــاق می‌افتنــد که یــک برنامه به درســتی از درخواســت‌های دریافت صفحات محافظت نکنــد. این وضعیت به کاربران غیرمجاز اجازه می‌دهد که با دســتکاری URL به صفحاتی که برای‌شــان ممنوع اســت دسترســی پیدا کنند. زمانی که حمله‌کننده از چنین حفره‌ای اســتفاده کنــد، می‌تواند تمام کارهایــی را که در حــدود مجوزهای کاربر مجــاز قرار دارند به انجام برســاند. راه‌های مختلفی بــرای برطرف‌کردن چنیــن مشــکلاتی وجود دارد کــه از جمله آن‌هــا می‌توان به اســتفاده از اجــزای مربوط به اعتبارســنجی در خــارج از برنامــه وب در حال اجرا اشاره کرد.

۹- حفاظت ناکافی از لایه نقل‌وانتقال شبکه (Transport Layer)

پروتکل SSL (ســرنام Secure Sockets Layer) و دیگر نمونه مشابه‌اش یعنــی TLS (ســرنام Transport Layer Security) در واقــع مبنــای تمــام رمزنگاری‌هایی هستند که برای اعتبارسنجی سایت‌ها و رمزنگاری داده‌های جابه‌جا شــده میان آن‌ها و کاربر نهایی، مورد استفاده قرار می‌گیرند. نکته عجیب اینجا اســت که این پروتکل‌ها اغلب به‌درســتی مورد اســتفاده قرار نمی‌گیرند. به‌عنوان مثال، ســرویس هات‌میل مایکروسافت تازه در نوامبر ســال گذشــته بود که امکان امن کردن کل نشست سیستم ایمیل تحت وب از طریــق SSL را برای کاربران فراهم کرد. تا پیــش از آن کاربران پس از عبور از صفحه لاگین، راهی برای حفاظت از نشست خود در برابر حمله‌های man-in-the-middle نداشتند. اما وجود نداشتن یک سیستم حفاظتی SSL یا TLS از ابتدا تا انتهای مســیر تنها یکــی از نمونه‌های محافظت ناکافی از لایه نقل و انتقال شبکه اســت. کوکی‌های مرورگرها که برای اعتبارسنجی و سایر موارد حســاس مورد استفاده قرار می‌گیرند، باید از یک flag امن استفاده کنند. همچنین گواهی‌های تأیید اعتبار (Certificateها) نباید توسط خود سایت استفاده کننده امضا شده باشند و همچنین نباید به آن‌ها اجازه انقضا داده شود.

از همــه مهم‌تر این‌که پیاده‌ســازی‌های SSL و TLS بایــد در برابر انواع حمله‌هــای جدیدی که در چند ســال اخیر انجام شــده‌اند مقاوم باشــند. به‌عنــوان نمونــه‌ای از این حمله‌ها می‌تــوان به حمله‌های مذاکــره دوباره (Renegotiation Attack) و حفره‌ای که Beast نامیده می‌شــود اشاره کرد. SSL Pulse سایتی است که توسط شرکت امنیتی Qualys پشتیبانی می‌شود و کارایی حدود دویست‌هزار سایت پرکاربردی را که از SSL استفاده می‌کنند، پایش می‌کند. به گزارش این سایت، متأسفانه تخمین زده می‌شود که حدود دو سوم سایت‌هایی که از SSL و TLS استفاده می‌کنند، هنوز در برابر Beast مقاوم نشده‌اند.

۱۰- ارجاع و انتقال نامعتبر
(Unvalidated redirects and forwards)

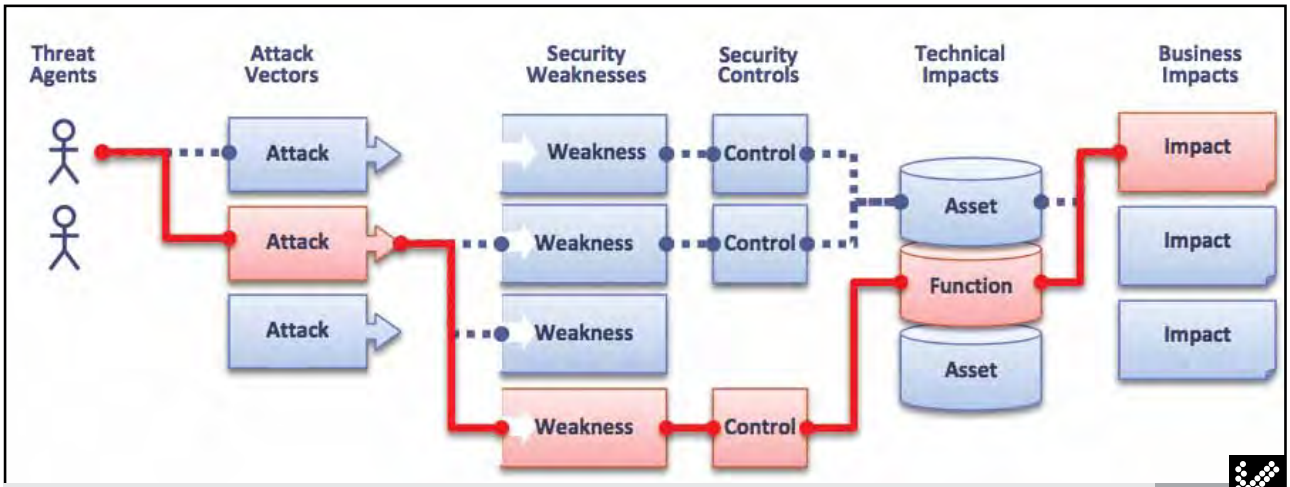
باگ‌های این دسته باعث می‌شوند که بازدیدکنندگان به سایر بخش‌های یک سایت یا سایتی در کل متفاوت هدایت شوند. در طی این فرآیند آن‌ها در معرض حمله‌های فیشینگ یا توزیع‌کنندگان بدافزارها قرار می‌گیرند. این توزیع‌کنندگان بدافزار اغلب با لینکی به سایت‌های مشهور مثلاً گوگل یا بانک امریکا، کاربران را فریفته و آن‌ها را به سایت‌های آلوده هدایت می‌کنند.(شکل۳)

تصور کنید که نفوذپذیر هستید

با پیچیدگی فزاینده سرورها و برنامه‌های وب خوانندگان این مقاله باید این طور فرض کنند که سایت‌شان حداقل در معرض برخی از آسیب‌پذیری‌هایی که به آن‌ها اشاره کردیم قرار دارد. به این ترتیب، ارزشمندترین دارایی‌های تجاری شما تنها چند کلیک با دانلود شدن توسط مجرمان سخت‌کوش یا نفوذگران فاصله دارد. اگر فکر می‌کنید این مطلب اغراق‌آمیز است، نگاهی به داستان هشداردهنده HBGary Federal بیاندازید. این شرکت حدود دو سال پیش توسط اعضای گروه انانیموس هک شد. با این که خود این شرکت سرویس‌های امنیت وب را نمی‌بود.برای بدتر کردن اوضاع هش‌های گذرواژه لو رفته با الگوریتم MD5 رمزنگاری شده بودند، الگوریتمی که متخصصان امنیتی مدت‌ها است اشاره می‌کنند که برای نگه‌داری گذرواژه‌ها اصلاً مناسب نیست. دلیل این امر آن است که این الگوریتم‌ها سریع بوده و به محاسبات چندان احتیاج ندارند و همین باعث می‌شود که شکستن این هش‌ها بسیار ساده‌تر شود.

هدف این نیست که HBGary را مورد انتقاد قرار دهیم، بلکه هدف این است که آسیب‌پذیری سایت‌ها استثنا نیست بلکه یک قاعده عمومی است! اگر شرکتی که در زمینه امنیت فعالیت می‌کند می‌تواند چنین اشتباهاتی را مرتکب شود، تصور کنید که اوضاع در یک استارت‌آپ در حوزه تجارت‌الکترونیک یا برنامه‌نویسی موبایل چگونه خواهد بود!

مشکلات سایت‌ها علاوه‌بر این‌که اسرار تجاری و سایر داده‌های اختصاصی را در معرض خطر قرار می‌دهند، اعتبار یک شرکت را نیز (با دلایلی واضح و روشن) از بین می‌برند. یک سایت ناامن علاوه‌بر آسیبی که متوجه بازدیدکنندگانش می‌کند، می‌تواند تعداد بی‌شماری از کاربران اینترنت که حتی درباره شما چیزی نشنیده‌اند را نیز تهدید کند. زیرا در بیش‌تر موارد، سایت‌های نفوذپذیر برای انجام حملات سیادی، توزیع بدافزار و سایر انواع حمله‌ها مورد استفاده واقع می‌شود.



شکل ۳ حمله‌کنندگان می‌توانند از راه‌های متفاوت و متعددی و از طریق برنامه‌های شما، به شما و کسب‌وکار یا سازمان‌تان لطمه بزنند. هر یک از این مسیرها نشان‌دهنده ریسکی است که ممکن است به‌اندازه‌ای مهم به‌نظر نرسد که باعث جلب توجه شود.

به شرکت‌های معتبر فهرست فورچون ۵۰۰ و آژانس‌های دولتی عرضه می‌کرد، چندان به امن کردن سایت خودش توجه نکرده بود. سیستم مدیریت محتوای این سایت در برابر حمله‌های تزریق SQL آسیب‌پذیر بود و به لینک‌های به ظاهر بی‌ضرری مانند http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27 اجازه می‌داد که کوئری‌های اعتبارسنجی نشده‌ای را روی پایگاه داده سایت اجرا کنند.

در نتیجه پایگاه داده لیستی از نام‌های کاربری، آدرس‌های ایمیل و هش‌های گذرواژه‌ها را بیرون می‌ریخت که متعلق به کارکنان برخی از قدرتمندترین سازمان‌های دنیا بودند. اگر سیستم مدیریت محتوای مورد استفاده در برابر حمله‌های تزریقی امن شده بود، شاید نفوذ به صورت کامل هیچ‌گاه امکان‌پذیر (یا حداقل ویران‌کننده)

به‌یقین مهم‌ترین کاری که یک مدیر وب می‌تواند برای مستحکم نگه‌داشتن یک سایت انجام دهد به روز نگه‌داشتن سیستم‌عامل و کل برنامه‌های در حال اجرا روی آن است. به‌روز نگه‌داشتن در اینجا یعنی تمام وصله‌های امنیتی ظرف ۲۴ ساعت یا کمتر نصب شوند. اما به درنظر گرفتن، پیچیدگی پلتفرم‌های اغلب سایت‌ها، نصب وصله‌ها به تنهایی کافی نیست. لازم است که ادمین‌ها نیز در زمینه امنیت مهارت‌هایی را کسب کنند. OWASP محل خوبی برای شروع این کار است.درنهایت، بررسی‌های دوره‌ای و منظم توسط شرکت‌های تخصصی حوزه امنیت برای سایت‌هایی که اطلاعات گذرواژه‌ها، کارت‌های اعتباری و سایر داده‌های حساس را نگه‌داری می‌کنند، یک الزام است. اینترنت پر از سایت‌هایی مانند هارتلند و HBGary است. چیدن علف‌های هرزی که آن‌ها را به دردسر انداخت ساده نیست، اما ارزشش را دارد.