بخش پایانی

چگونه از برنامه خود در برابر هکرها محافظت کنیم؟

محمد غفاری

در بخش‌های قبلی این مقاله، به بررسی حملات SQL Injection و XSS علیه برنامه‌های تحت وب پرداختیم. در این بخش، شما را با دو دسته دیگر از حملات علیه برنامه‌های وب، تحت عنوان «تغییر متغیر» و «سرریزی بافر» آشنا می‌کنیم.

Variable manipulation

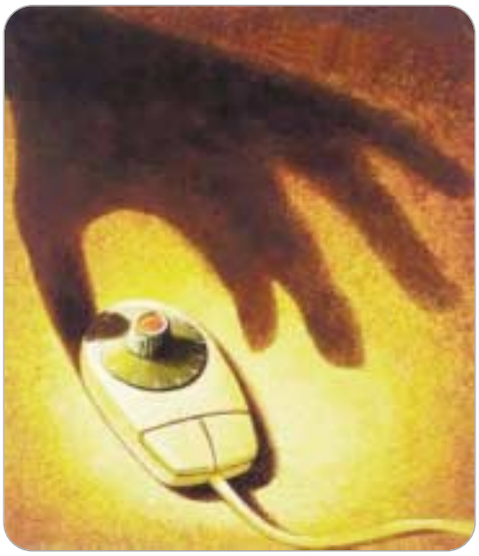
در این تکنیک، مهاجم سعی بر تغییر متغیرهای موجود در برنامه دارد. در نتیجه این تغییرات، منطق برنامه دچار مشکل می‌شود. مثال کلاسیک این نوع حمله eShoplifting نام دارد که در آن مهاجم با دسترسی به یک یا چند متغیر قیمت در وب سایت فروش آنلاین و تغییر مقدار آنها، منطق برنامه را فریب داده و منجر به محاسبه اشتباه قیمت محصول توسط برنامه می‌شود. در نتیجه مهاجم می‌تواند اقدام به خرید یک آیتم گران قیمت با قیمت بسیار پایین کند. در اکثر موارد برنامه قادر به تشخیص تغییر قیمت نیست و روند کار در حالت عادی انجام خواهد شد.

برای بررسی وجود چنین رخنه‌پذیری در وب‌سایت خود، به‌صورت زیر عمل کنید:

کد HTML صفحه فروش را وقتی در پروسه پرداخت قرار دارید، باز کنید. اگر در میان کدهای شما متغیری شامل مقدار و یا مبلغ کالای درخواستی وجود دارد، سایت شما مستعد این نوع حملات خواهد بود.

راهکار برخورد با این مشکل عبارتست از:

- اعتبارسنجی پارامترهای فروش قبل از انجام هر نوع محاسبه قیمت
- رمزگذاری پارامترهای فروش.



Buffer overflow

همانطورکه می‌دانید، یک برنامه حجم مشخصی از حافظه را اشغال می‌کند. درصورتی‌که اطلاعاتی بیشتر از فضای اختصاص یافته به برنامه (حتی باندازه یک بایت)، وارد حافظه شود، منجر به سرریزی خواهد شد. در زیر به بیان دو نوع رایج سرریز به‌نام‌های «سرریزی پشته» و «سرریزی هیپ» می‌پردازیم:

Stack Overflow

پشته، بخشی از حافظه است. رایانه اطلاعاتی را که نمی‌تواند در رجیسترهای خود ذخیره کند، در پشته ذخیره می‌کند. در این تکنیک مهاجم با آگاهی از عدم کنترل نوع و سایز مقادیر ورودی یک تابع توسط برنامه، اقدام به ارسال مقادیر بیشتر از فضای حافظه و نهایتا بازنویسی آدرس تابع مخرب خود به‌جای آدرس بازگشت تابع اصلی می‌کند (تابع مخرب عبارتست از هرآن‌چه منجر به خطرپذیری برنامه و سرور می‌شود، مثلا در محیط لینوکس دستور ساده EXEC("sh") منجر به باز شدن پنجره دستورات و خطرپذیری بسیار برای سرور می‌شود)، حال وقتی برنامه قفل می‌شود، اقدام به بازیابی توسط آدرس بازگشت می‌کند و چون این آدرس به دستور مخرب مشخص شده از سوی مهاجم تغییر کرده است، منجر به اجرای دستور مخرب خواهد شد.

Heap Overflow

وقتی یک برنامه با حجم بزرگی از اطلاعات نیازمند پردازش مواجه می‌شود، بخشی از حافظه به نام هیپ به‌منظور مدیریت اطلاعات فوق در نظر گرفته می‌شود. در زبان‌های سطح پایینی چون C و C++ برنامه‌نویس مسوول تعیین میزان حافظه اختصاص یافته است، حال در صورتی که حجم اطلاعات بارشده بیش از مقدار مشخص شده برای هیپ باشد، برنامه قفل خواهد کرد.

راهکار برخورد با این مشکل نیز در مرحله نخست، استفاده از زبان‌های برنامه‌نویسی چون Java، .NET، Perl، Python و Ruby است که اجازه دسترسی مستقیم برنامه‌نویس به حافظه را نمی‌دهند و خود کنترل حافظه را برعهده می‌گیرند.

توجه به این نکته لازم است که گاه برنامه‌نویس اقدام به پیاده‌سازی برنامه با یکی از زبان‌های فوق می‌کند، ولی در بخشی از برنامه خود اقدام به استفاده از برنامه یا ابزارهای غیرایمنی می‌کند که توسط زبان‌های برنامه نویسی ناامن نوشته شده‌اند، که این نیز منجر به افزایش خطرپذیری برنامه خواهد شد.

- مقادیر ورودی را قبل از هرگونه پردازش اعتبارسنجی کنید.
- در صورت استفاده از توابع سیستمی یا ابزارهای نوشته شده با این زبان‌ها، از کامپایلرهای ایمن در برابر سرریز استفاده کنید
- برنامه را به‌طور مداوم توسط اسکنرهای تشخیص سرریز بررسی کنید.
- در صورت استفاده از زبان‌های ناامن چون C، C++، کوبول و اسمبلی، قبل از کپی اطلاعات در پشته مقصد، از فضای کافی آن مطمئن شوید.

منابع: acunetix.com، owasp.org و whitehatsec.com

پرسش و پاسخ

برنامه‌ها پیغام خطا می‌دهد. چگونه باید آنها را از Add Or Remove پاک کنم؟ و همچنین روش یا برنامه‌ای معرفی کنید تا بتوان محدودیت زمانی نرم‌افزارها را از بین برد.

همچنین چگونه می‌شود کامپیوتر را خاموش کرد و پس از روشن کردن آن تمام برنامه‌هایی که هنگام خاموش کردن در حال اجرا بودند دوباره به‌کار بیفتند (مانند stand by اما کامپیوتر کاملا خاموش شود)؟

پاسخ سوال اول: چنانچه امکان نصب مجدد آن نرم‌افزارها را دارید، با نصب دوباره آنها در همان پوشه‌که قبلا نصب شده بودند نسبت به Uninstall آنها اقدام کنید. اما چنانچه امکان نصب مجدد ندارید، می‌توانید از نرم‌افزارهایی که به همین منظور (مانند Perfect Uninstaller) طراحی شده‌اند استفاده کنید. راه دیگر استفاده از رجیستری است که چنانچه اطلاعات کافی دارید می‌توانید از این روش نیز استفاده کنید. از منوی Start گزینه Run را انتخاب کرده و عبارت Regedit را تایپ و تایید کنید. از پنجره باز شده در قسمت چپ به آدرس زیر بروید:

HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall

حال در قسمت سمت راست، فهرست برنامه‌های نصب شده بر روی سیستم را می‌بینید. برنامه‌ای را که می‌خواهید Uninstall کنید، انتخاب کرده و آن را Delete کنید.

پاسخ سوال دوم: برنامه‌هایی که محدودیت زمانی دارند، از طرف شرکت تهیه‌کننده آنها برای معرفی محصول خود به‌صورت رایگان در اختیار کاربران قرار می‌گیرد و به منظور معرفی محصول شرکت است. یعنی این نسخه ضمن اینکه محدودیت زمانی دارد، ممکن است تمام امکانات نسخه اصلی را نیز نداشته باشد. بنابراین با تهیه نسخه اصلی (Original) این محدودیت زمانی و محدودیت دسترسی به امکانات از بین خواهد رفت. البته هستند افراد یا شرکت‌هایی که با استفاده از کرک همین نسخه‌ها، محدودیت‌های زمانی یا دسترسی به امکانات را از بین می‌برند و در حقیقت حقوق تهیه‌کنندگان این نرم‌افزارها را از بین می‌برند.

پاسخ سوال سوم: در سیستم امکانی با عنوان Hibernate تعبیه شده است که با استفاده از آن می‌توان سیستم را خاموش کرد ولی برنامه‌های در حال اجرا را از کار نینداخت و زمانی که سیستم را دوباره به کار می‌اندازید، برنامه‌ها نیز در حال اجرا باشند.

برای فعال کردن امکان Hibernate بر روی Desktop کلیک راست کنید و گزینه Properties را انتخاب کنید.

لبه Screen Saver را انتخاب کنید و گزینه ...Power را انتخاب کنید.

از پنجره بازشده (Properties Power Options) لبه Hibernate را انتخاب کرده و تیک گزینه Enable Hibernation را بزنید.

سیستم خود را دوباره راه‌اندازی کنید. از این پس چنانچه بخواهید سیستم را خاموش کنید، هنگامی‌که پنجره Shut Down ظاهر می‌شود، با نگهداشتن دکمه Shift عبارت Stand By تبدیل به Hibernate خواهد شد و با انتخاب آن می‌توانید سیستم خود را در حالت Hibernate قرار دهید.