امنیت تجارت الکترونیک

فصل شانزدهم:
امنیت سرویس دهنده وب

تهیه و تنظیم: دکتر آرش حبیبی لشکری
منبع: کتاب "اصول امنیت برای تجارت الکترونیکی"

اولین نسخه: دی 1393
بروزرسانی: فروردین 1396

فهرست:

- مقدمه
- واسط دروازه عمومی (CGI)
- Servletها
- انتشار گمنام در وب یا Rewebber
- امنیت پایگاه داده
- حفاظت از حق‌نشر

امنیت سرویس دهنده وب

مقدمه

مدیریت کنترل دسترسی در سوی سرویس‌دهنده وب مشکل‌تر از سمت سرویس‌گیرنده وب است.

یک سرویس‌گیرنده (یک کاربر) معمولا تعداد محدودی رابطه قابل اعتماد با شرکتها و موسسات (بانکها) دارد که خود به عنوان یک مشتری شناخته می‌شود و می‌تواند توسط یک گواهی احرازهویت شود. در اکثر موارد سرویس‌گیرنده می‌تواند به راحتی یک گواهی از سرویس‌دهنده موسسات یا شرکتها دریافت کند.

بیشتر سرویس‌دهنده‌های تجاری با کاربران کاملا ناشناخته و حتی گمنام در ارتباط هستند. بنابراین آنها در کل نمی‌توانند با تقاضای احرازهویت سرویس‌دهنده از خودشان محافظت کنند، بلکه با بکارگیری مکانیزم-های کنترل‌دسترسی با دقت پیکربندی شده می‌توانند این کار را انجام دهند.

این حوزه از مکانیزم‌های دیوارآتش و امنیت سیستم عامل شروع شده و تا محیطهای اجرایی ایمن شده برای کدهای سیار ادامه دارد. عموما، تمام مکانیزم‌هایی که به یک سرویس‌گیرنده اجازه اجرای دستورات روی سرویس‌دهنده را می‌دهند یا باید کاملا غیرفعال شده یا تنها برای مقدار محدودی مهیا شده باشند.

واسط دروازه عمومی (CGI)

یک سرویس‌دهنده وب علاوه بر برگرداندن اسناد ایستای HTML، می‌تواند به صورت پویا اسناد پویا خلق نماید که باید به عنوان ورودی اطلاعات کاربر در درخواست سرویس‌گیرنده با روش POST ارسال شود.

روش GET نیز، همانطور که در فصل قبلی شرح داده شد، می‌تواند استفاده شود اما باید بدلایل امنیتی از آن اجتناب شود، البته بجز برای پرس و جوهای غیرخود توان خیلی ساده که استفاده از آن مشکل ساز نخواهد بود.

دراصل CGI پروتکلی است که بوسیله آن یک سرویس‌دهنده وب و یک برنامه که با هر زبان برنامه-نویسی نوشته شده باشد، می‌توانند با هم ارتباط برقرار کنند. سرویس‌دهنده در پاسخ بعدی HTTPباید خروجی را به سرویس‌گیرنده ارسال نماید.

به عبارت دیگر CGI در حال حاضر مکانیزمی است که به همه اجازه اجرای مجازی یک برنامه از راه دور را با انتخاب آزادانه ورودی روی یک سرویس‌دهنده وب، می‌دهد

Servletها

سرولت‌ها (Servlet) برای سرویس‌دهنده‌ها همانند اپلت‌ها (applet) برای مرورگرهای وب هستند

درحالیکه اپلت‌های جاوا به سرویس‌گیرنده‌های وب که جاوا در آنها فعال شده است، کاربردهایی اضافه می‌کنند، البته سرولت‌ها نیز به سرویس‌دهنده‌های وب که جاوا در آنها فعال شده است و از API سرولت‌ها پشتیبانی می‌کنند نیز کاربردهایی اضافه می‌کنند

یک سرولت ممکن است برای گسترش کاربرد یک سرویس‌دهنده و مدیریت کردن درخواستهای HTTP استفاده شود، برای مثال، برای خواندن داده از یک فرم HTML از نوع order-entry و بکار گیری منطق تجاری استفاده شده برای به روز رسانی پایگاه‌داده سفارشات شرکت

شبیه به اپلت‌های جاوا، سرولت‌ها متشکل هستند از کلاسهای جاوا در قالب بایت-ک

انتشار گمنام در وب یا Rewebber

دلایل زیادی وجود دارند که چرا یک سرویس‌دهنده وب ترجیح می‌دهد تا گمنام و غیرقابل ردیابی باقی بماند، برای مثال، اگر محتوی صفحات وب آن برای گروه خاصی از افراد عصبانی کننده باشد.

Rewebber (یا نام قبلی JANUS) سرویس وبی است که هم برای سرویس‌گیرنده‌ها و هم برای سرویس‌دهنده‌ها گمنامی فراهم می‌کند

Rewebber به سادگی بخش آدرس یک URL را با کلیدعمومی RSA رمز می‌کند (پس فقط Rewebber می‌تواند آنرا رمزگشایی کند).

بخش رمزشده آدرس و باقی URL بصورت base64 رمز می‌شوند.

به عبارت دیگر، با سرویس‌دهنده وب گمنام می‌توان فقط توسط یه سرویس‌دهنده Rewebber در تماس بود

امنیت پایگاه داده

پایگاه‌داده‌های بزرگ معمولا روی کامپیوترهای اختصاصی به نام سرویس‌دهنده‌های پایگاه‌داده قرار می‌گیرند.

در یک پیکربندی معمولی، یک سرویس‌دهنده وب در یک DMZ قرار می‌گیرد که از اینترنت فابل دسترسی باشد (بخش 10. 8 را ببینید).

برای مثال ممکن است دو پایگاه‌داده متفاوت موجود باشد، یکی برای عموم (مشتری بالقوه)، و دیگری فقط برای مشتریان واجد شرایط.

دراین مورد هر کدام از پایگاه‌های داده می‌توانند در DMZ های جداگانه قرار گیرند

یک سیستم تجارت الکترونیکی در بیشتر موارد، برای ذخیره انواع گوناگون اطلاعات نیازمند یک پایگاه-داده است:

- اطلاعات احراز هویت کاربر؛
- اطلاعات مجوزدهی کاربر؛
- اطلاعات داد و ستد؛
- اطلاعات تراکنش تجاری.

علاوه بر ایمن بودن، خیلی از پایگاه‌های داده تجارت الکترونیکی باید *real time* باشند. به این معنی که تراکنش‌های پایگاه‌داده باید قبل از آخرین مهلت منقضی شود، کامل شده باشد

حفاظت از حق‌نشر

سرویس دهندگان وب اطلاعاتی از قبیل نرم افزار کامپیوتر، موسیقی، روزنامه، تصاویر، یا فیلم را در قالب دیجیتالی توزیع یا به فروش می‌رسانند.

متاسفانه، محتوای دیجیتال، می‌تواند به سادگی رونوشت برداری شود بدون این که سرویس‌دهنده مبدا اطلاع یابد، مگر اینکه تدابیر خاصی اندیشیده شود.

واترمارکینگ یا نهان‌سازی (watermarking) دیجیتالی برای حفاظت از دارایی های موجود در محتوای چندرسانه‌ای بکار می‌رود.

از لحاظ فنی یک نهان‌سازی به صورت دیجیتال، علامت یا الگویی است که به محتوی دیجیتال افزوده می‌شود (از جانب مالک) تا بتواند ادعایی در مورد محتوی داشته باشد.

نیازمندی کلی این است که یک نهان‌سازی باید مقاوم باشد (با وجود ایجاد تغییرات عمدی یا غیرعمدی روی محتوی بازیافتنی باشد). بعلاوه، نهان‌سازی نباید کیفیت محتوییات (نهان‌سازی شده) را تغییر دهد، و البته باید غیرقابل انکار نیز باشد (باید برای هرکس قابل اثبات باشد که آنها جاسازی شده‌اند و معنی آنها چیست).

حفاظت از حق‌نشر

علامت نهان‌سازی‌های دیجیتال می‌توانند برای انواع مختلفی از سرویس‌های محافظت از رسانه دیجیتال استفاده شوند:

- ادعای مالکیت برای ایجاد مالکیت روی محتوی؛
- انگشت نگاری برای افشای ویرایش برداری بدون مجوز و توزیع محتوی با وارد کردن یک نهان-سازی متمایز به هر رونوشت از محتوی؛
- احراز هویت و تایید یکپارچگی پیوند زدن جدا نشدنی مولف به محتوی، برای احراز هویت مولف و حصول اطمینان ازاینکه محتوی تغییر نکرده است؛
- کنترل مصرف برای کنترل رونوشت برداری و مشاهده محتوی است (با اشاره به نهان‌سازی تعداد رونوشتها اجازه داده می‌شوند)؛
- حفاظت از محتوی برای مهرگذاری محتوی و غیرفعال کردن استفاده غیرقانونی (با جاسازی یک نهان‌سازی آشکار در یک محتوایی که مجانی قابل مشاهده است، آنرا از لحاظ تجاری بی ارزش می‌کند).

بحث در باب حملات مرتبط: هدف *حملات کاهش قدرت یا مقاومت (robustness)*، حملات *ارائه محتوی* (presentation)، *حملات تفسیر (interpretation)*

خلاصه: مقدمه، واسط دروازه عمومی (CGI)، Servletها، انتشار گمنام در وب یا Rewebber، امنیت پایگاه داده، حفاظت از حق‌نشر

جلسه بعدی: امنیت سرویس گیرنده وب

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.