

امنیت نشست‌های وب با قابلیت مدیریت نشست چارگون

نشست‌های وب، دنباله‌ای از مذاکرات درخواست‌ها (Request) و پاسخ‌های (Response) پروتکل HTTP شبکه هستند که برای یک کاربر خاص به ازای یک بار لاگین در نظر گرفته می‌شوند. برنامه‌های کاربردی مدرن و پیچیده وب، نیازمند حفظ و نگهداری اطلاعات و وضعیت هر کاربر برای مدت درخواست‌های متعدد آن کاربر هستند. نشست‌ها این امکان را فراهم می‌کنند تا متغیرهایی مانند حقوق دسترسی و تنظیمات محلی ایجاد و برای هر یک از مذاکرات و تعاملات کاربر با برنامه کاربردی وب اعمال شوند.

اهمیت نشست‌های وب

پس از احراز هویت کاربر در هنگام ورود و اختصاص نشست جدید، برنامه‌های کاربردی وب برای شناسایی کاربر در هر درخواست بعدی، اعمال کنترل‌های دسترسی امنیتی، مجوز دسترسی به داده‌های خصوصی و افزایش قابلیت استفاده از برنامه، از قابلیت‌های نشست و مقادیر ذخیره‌شده در آن استفاده می‌کنند. شناسه نشست یا Session ID در طول عمر نشست، معادل با قوی‌ترین روش احراز هویت استفاده‌شده توسط برنامه کاربردی وب خواهد بود. یک حمله موفق برای به دست آوردن نشست

کاربر می‌تواند منجر به دسترسی مهاجم به همه دسترسی‌های آن کاربر در طول نشست شود. حملاتی مانند Session Hijacking، Session Reuse و Session Fixation می‌توانند اثرات مخربی به همراه داشته باشند.

راهکار چارگون: سرویس مدیریت نشست

سرویس مدیریت نشست چارگون، با هدف جلوگیری از این حملات طراحی و به تدریج تکمیل شده است. این سرویس امروز علاوه بر اهداف اولیه خود، امکانات فراوانی را در اختیار کاربران و مدیران قرار می‌دهد تا به بهبود عملکردهای امنیتی در سازمان‌ها کمک کند. مهم‌ترین این امکانات عبارتند از:

تعیین تعداد نشست‌های هم‌زمان مجاز

مدیر سیستم می‌تواند برای همه کاربران یا کاربران خاص حداکثر تعداد نشست‌های هم‌زمان مجاز را تعیین کند.

واکنش سیستم هنگام رسیدن به سقف مجاز

برای ایجاد امنیت، سیستم باید بر روی ورود قطعی قرار گیرد. به این ترتیب بعد از رسیدن به سقف تعداد نشست‌های مجاز، ایجاد نشست جدید توسط کاربر باعث از بین رفتن تمامی نشست‌های پیشین می‌شود.

زمان اعتبار نشست غیرفعال

امکان تعیین زمان اعتبار نشست غیرفعال برای ختم نشست در صورت عدم فعالیت کاربر (به عنوان مثال، 60 دقیقه).

زمان اعتبار نشست

مشخص کردن مدت زمان اعتبار نشست فعال یا غیرفعال (مثلاً 120 دقیقه). به این ترتیب کاربر هر 120 دقیقه از نرم افزار خارج شده و باید مجدداً احراز هویت شود.

اطلاع رسانی نشست های فعال

به محض اینکه نام کاربری یک کاربر برای ورود به نرم افزار استفاده شود، به همه نشست های فعال او اطلاع رسانی می شود.

مشاهده وضعیت لاگین کاربران

مدیر سیستم می تواند وضعیت لاگین یا غیرلاگین بودن کاربران را مشاهده کند.

مدیریت نشست های کاربران

مدیر سیستم می تواند همه نشست های کاربران را ببیند و در صورت گزارش عملکرد مشکوک، آن ها را ببندد.

کنترل ایجاد نشست

مدیر سیستم می‌تواند اجازه ایجاد نشست و در نتیجه ورود کاربر را بگیرد.

مدیریت نشست‌های خود کاربران

هر کاربر می‌تواند لیست همه نشست‌های خود را ببیند و آن‌ها را ببندد.

بستن نشست‌های موجود

مدیر سیستم می‌تواند با اهداف امنیتی یا در فرآیندهای نگهداری سامانه همه نشست‌های موجود را ببندد و جلوی ایجاد نشست و در نتیجه ورود همه کاربران را بگیرد.

تعیین رفتار سیستم در رسیدن به حداکثر نشست‌های مجاز

مدیر سیستم می‌تواند انواع رفتارهای سیستم را در هنگام رسیدن کاربر به حداکثر تعداد نشست‌های مجاز تعیین کند.

تعیین طول عمر نشست‌ها

مدیر سیستم می‌تواند برای طول عمر نشست‌ها به تفکیک فعال بودن و غیرفعال بودن کاربر، بازه مجاز تعیین کند.

جمع بندی

با بهره‌گیری از سرویس مدیریت نشست چارگون، سازمان‌ها می‌توانند امنیت نشست‌های وب خود را تضمین کرده و از حملات مختلف جلوگیری کنند. این سرویس با امکانات فراوان خود، به بهبود عملکردهای امنیتی در سازمان‌ها کمک می‌کند و اطمینان کاربران را به امنیت داده‌های خود افزایش می‌دهد.