در آخرین بخش از سری مقالات مروری بر امنیت مرورگرها به توضیح ویژگی های امنیتی اپرا می پردازیم.

اپرا

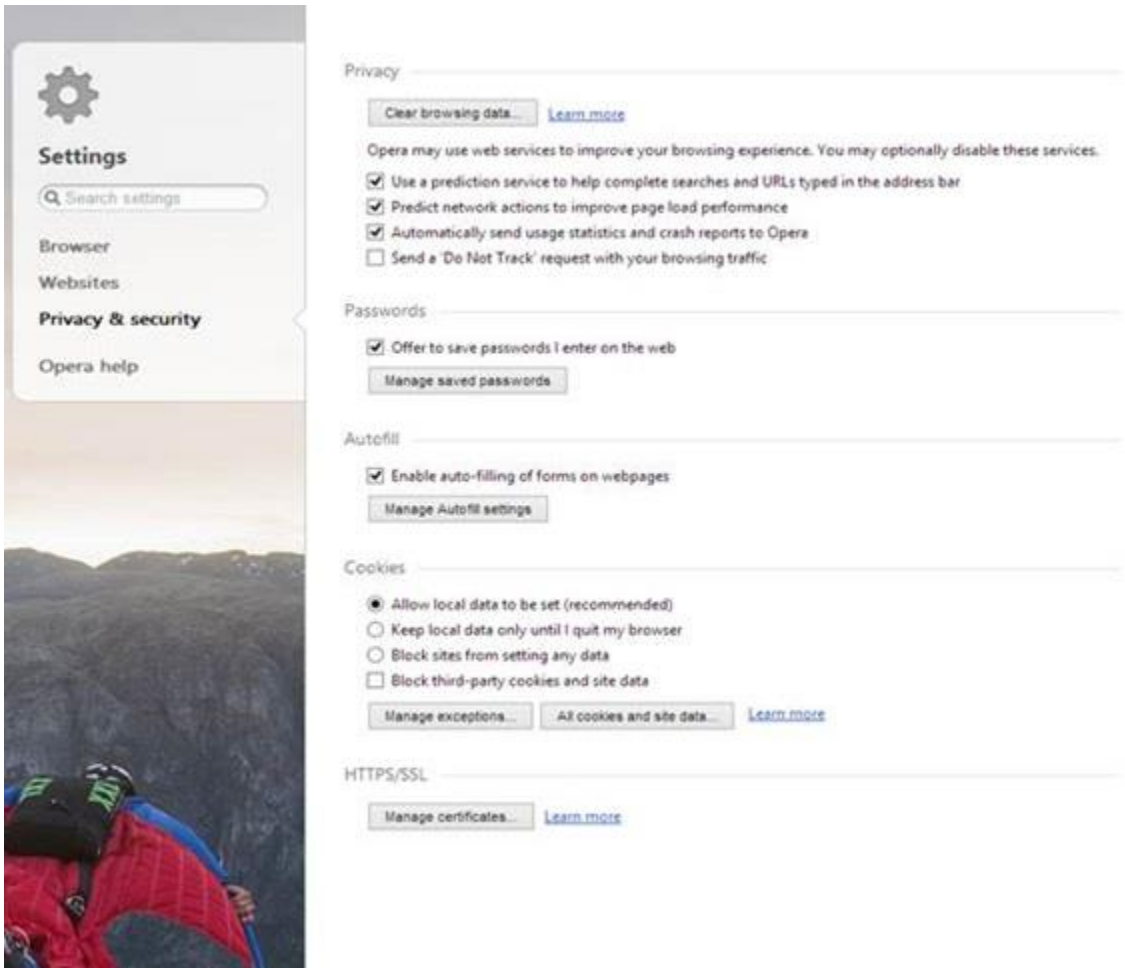
نظرسنجی که سال ۲۰۱۲ توسط Naked Security برگزار شد نشان داد که شرکت کنندگان بر این باور هستند که مرورگر اپرا امن ترین مرورگر می باشد. اما این نظر در سال ۲۰۱۳ زمانیکه گروه امنیتی اپرا اعلام کرد که یک حمله هدفمند در شبکه داخلی آن ها اتفاق افتاده است و مهاجمان گواهینامه امضای کد را به سرقت برده اند تغییر کرد. مهاجمان با این گواهینامه ها بدافزارها را امضاء کرده و این امکان وجود داشت که کاربران این بدافزار را با این باور که یک به روز رسانی برای مرورگر است نصب نمایند.

ویژگی های امنیتی اپرا

اپرا نیز مانند سایر مرورگرهای معروف دارای ویژگی های امنیتی است. در این مرورگر ویژگی حفاظت در برابر بدافزار به طور پیش فرض فعال می باشد و هم چنین دارای لیست سیاهی از سایت های سرقت هویت شناخته شده و سایر سایت های خرابکار است. این مرورگر از گواهینامه های EV پشتیبانی می کند و به کاربر اجازه می دهد تا رفتار پلاگین ها، ذخیره اطلاعات، دسترسی سایت های وب به رایانه کاربر یا سخت افزار دستگاه و داده های محلی را کنترل نماید.

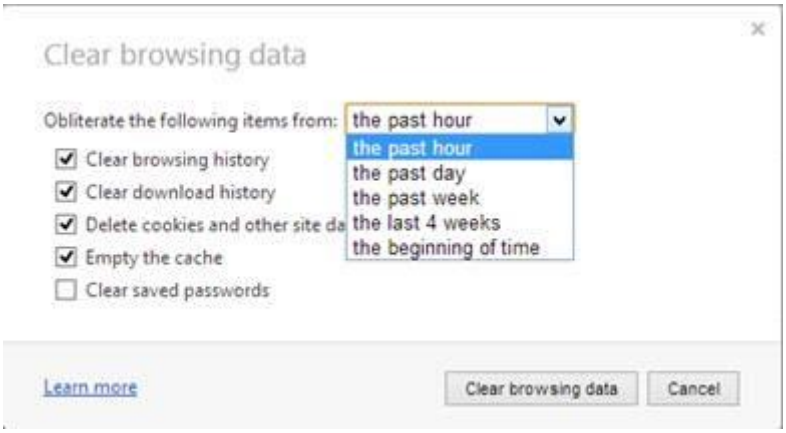
بهترین پیکربندی اپرا

همانطور که در شکل ۱ مشاهده می شود، مرورگر اپرا گزینه هایی را برای پیکربندی حریم خصوصی و تنظیمات امنیتی از طریق مسیر Opera button ا Settings ا Privacy & security ارائه می دهد.



شکل ۱

در این قسمت می توان اقداماتی از قبیل پاک کردن تاریخچه مرورگر، دانلود تاریخچه، کوکی ها، حافظه نهان و رمزهای عبور ذخیره شده را انجام داد. بهترین ویژگی این قسمت آن است که اپرا به کاربر اجازه می دهد تا بر اساس یک جدول زمانی اقدامات فوق را انجام دهد. همانطور که در شکل ۲ مشاهده می شود، کاربر می تواند اقدامات فوق را بر اساس یکساعت پیش، یک روز پیش، یک هفته پیش، ۴ هفته پیش و از زمان شروع به کار مرورگر انجام دهد.



شکل ۲

می توان گزینه "ردگیری نشود" را فعال کرد و هم چنین می توان استفاده از خدمات پیش بینی و ارسال خودکار گزارش های آماری و خرابی برای اپرا را غیر فعال کرد (این ویژگی به طور پیش فرض فعال است).

به طور پیش فرض، رمزهای عبور برای دسترسی به وب سایت ها ذخیره می شود. از نظر امنیتی، بهتر است این گزینه غیرفعال شود. هم چنین می توان مانع از آن شد که وب سایت های خاص رمز عبور کاربر را ذخیره نمایند. اگر کاربر بخواهد رمزهای عبور خود را ذخیره نماید می توان مکان ذخیره فایل را تغییر داد و بدین وسیله احتمال دسترسی مهاجمان به سایت را کمی کاهش داد.

در مرورگر اپرا برای مدیریت کوکی های مرورگر، گزینه هایی وجود دارد. به طور پیش فرض، وب سایت ها می توانند داده های محلی تنظیم نمایند اما می توان هنگام بستن مرورگر این داده ها را حذف نمود، اجازه تنظیم داده ها توسط سایت را مسدود نمود یا دانلود کوکی های ثالث و داده ها را مسدود نمود. هم چنین می توان برای این محدودیت ها از طریق گزینه Manage exceptions استثنائاتی را برای برخی از وب سایت ها تنظیم نمود.

جاوا اسکرپیت و سایر پلاگین ها را می توان از طریق بخش وب سایت ها در Settings پیکربندی کرد. در این قسمت می توان گزینه ها را به گونه ای انتخاب نمود که پلاگین ها به طور خودکار اجرا شوند، می توان آن ها را مسدود کرد یا می توان آن ها را به گونه ای تنظیم کرد که با کلیک کردن بر روی آن ها اجرا شوند. در این بخش نیز می توان استثنائاتی را برای وب سایت های خاص تعریف کرد. باید توجه داشت که ممکن است کاربر بخواهد دسترسی سایت ها را به وبکم و میکروفون مسدود کند. این کار را می توان از طریق بخش مدیا در صفحه وب سایت ها انجام داد.

اگر وب سایتی از سرویس های مبتنی بر موقعیت استفاده می کند، هنگام مشاهده چنین وب سایت هایی با مرورگر اپرا، پیامی در نوار آدرس نمایش داده می شود که از کاربر درخصوص اجازه داشتن یا نداشتن دسترسی وب سایت به اطلاعات موقعیت جغرافیایی که ممکن است مبتنی بر GPS، آدرس IP، اطلاعات وای فای یا IDS نزدیک برج های سلولی باشد، سوال می شود. می توان تنظیمات به گونه ای انجام شود که همیشه اجازه دسترسی به سایت ها بدهد، همین یکبار اجازه دسترسی دهد یا به طور کل به هیچ سایتی اجازه دسترسی ندهد. اگر گزینه اجازه دسترسی انتخاب شود، آیکون موقعیت جغرافیایی در نوار آدرس نمایش داده می شود و به کاربر یادآوری می کند که موقعیت او به اشتراک گذارده

می شود. می توان از طریق Settings | Preferences | Advanced | Network امکان دسترسی به موقعیت جغرافیایی را برای تمامی وب سایت ها مسدود نمود.

خلاصه

در سری مقالات مروری بر امنیت مرورگرهای وب سعی شد تا اقدامات لازم در خصوص استفاده از بهترین ویژگی ها و قابلیت های مرورگرها برای داشتن امنیت بیشتر شرح داده شود. روشن است که تنظیمات مرورگرهای وبی که توسط کاربران رایانه مورد استفاده قرار می گیرد باید مورد توجه متخصصان IT قرار داشته باشد. متخصصان IT می توانند با بهره گیری از ویژگی های مرورگرها نقش موثری در کاهش مخاطرات امنیتی داشته باشند.