ITRC
مرکز تحقیقات مخابرات ایران

دانشگاه شیراز

مرکز تخصصی آپا درزمینه اختلالات امنیتی مرتبط با بد افزارها

cert@shirazu.ac.ir

امن سازی مرورگر اینترنت اکسپلورر

تنظیم کننده:

صابر نوروزپورلاری

ویرایش: ۱

شماره سند: T-89/5-4

www.ircert.cc

چکیده :

امروزه مرورگرهای وب یکی از ابزارهای بسیار پرطرفدار و پر استفاده می باشند. به دلیل آسان بودن نفوذ مهاجمان به اینگونه نرم افزارها بسیاری از این مرورگرها در معرض آسیب هایی از سوی مهاجمان می باشند که باید راه حلی برای آنها پیدا کرد در این مقاله ما شما را با یک سری ترفندهایی آشنا می کنیم که بتوانید از سیستم خود در برابر این آسیب ها محافظت کنید.

واژه های کلیدی:

web browser security، security ، internet explorer ، browser setting ، Plug-in،Cookie

آپا ؟؟؟

چگونه می توان مرورگر وب خود را امن کرد:

برخی نرم افزارها که برای مرورگر وب وظایفی را مقرر می کنند مانند active X ، java ، برنامه های تحت وب (java scripting , VB scriptin و غیره) ممکن است به سیستم آسیب برسانند. این مشکل ممکن است ناشی از پیاده سازی ضعیف طراحی ضعیف و یا پیکر بندی ناامن باشد. به این دلایل باید فهمید که کدام مرورگر ها چه ویژگی هایی دارند و خطرات ناشی از آنها چیست. برخی مرورگرهای وب به شما اجازه غیر فعال کردن کلیه ی این تکنولوژی ها را می دهند در حالیکه بقیه ممکن است اجازه فعال کردن برای برخی سایت ها را بدهند.

این بخش به شما نحوه برقراری امنیت را در بیشتر مرورگرهای پر طرفدار آموزش می دهد.

ممکن است روی رایانه شما چندین مرورگر نصب شده باشد. دیگر برنامه های کاربردی شما از جمله برنامه های مربوط به نامه های الکترونیکی و یا برنامه های نشان دهنده متن ممکن است از مرورگرهای دیگری غیر از آنچه شما برای دسترسی به وب دارید استفاده کنند. اگر چه ممکن است برخی فایل ها طوری ذخیره شده باشند که با مرورگر دیگری اجرا شوند، استفاده از این مرورگر برای وب سایت ها به معنی این نیست که دیگر برنامه ها نیز به طور خودکار ازآن مرورگر استفاده کنند. به همین دلیل امن کردن همه مرورگرهایی که بر روی سیستم نصب می شوند مهم است. یکی از فواید استفاده از چندین مرورگر این است که می توان از یک مرورگر برای کارهای حساس مثل کارهای بانکی و از مرورگر دیگر

برای کارهای عادی استفاده کرد. این کار شانس استفاده از آسیب پذیری در یک مرورگر وب ، وب سایت و یا نرم افزارهای مربوطه را برای کشف اطلاعات مهم کاهش می دهد.

مرورگرهای وب باید مرتبا بروز شوند اختیارات و مشخصه های نرم افزارها وابسته به نسخه نرم افزار تغییر می کنند، یا عوض می شوند.

ماکروسافت اینترنت اکسپلورر:

Microsoft Internet Explorer(IE) یک مرورگر وب است که در سیستم عامل ماکروسافت ویندوز ، قرار داده شده است. حذف این نرم افزار سودمند نیست.

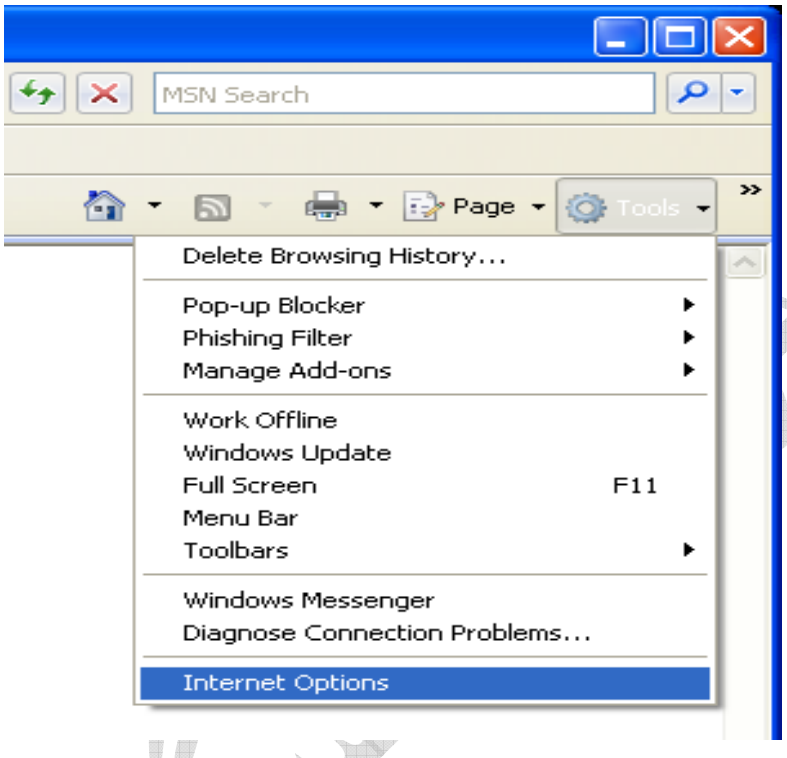
اینترنت اکسپلورر علاوه بر پشتیبانی java، scripting و غیره تکنولوژی Active X را هم دارد. در حالیکه همه نرم افزارهای کاربردی در برابر مهاجمان آسیب پذیر هستند ممکن است استفاده از مرورگری که active X را پشتیبانی نکند میزان آسیب پذیری را کاهش دهد، هر چند ممکن است استفاده از مرورگر جایگزین بر روی کارایی برخی سایت ها که نیاز به استفاده از active X control دارند تاثیر بگذارد.

توجه داشته باشید که استفاده از مرورگر وب دیگر ، باعث حذف IE و یا دیگر مولفه های ویندوز نمی شود. دیگر نرم افزارها از جمله نرم افزار های مربوط به نامه های الکترونیکی ممکن است از IE ، مرورگر وب Active X control (WebOc) و یا ماشین مترجم IE HTML (MS HTML) استفاده کنند.

نتایج حاصل از کارگاه بررسی Active X در سال ۲۰۰۰ بر روی لینک http://www.cert.org/reports/activeX_report.pdf قرار دارد.

در ادامه مراحلی برای غیر فعال کردن مشخصه های متفاوتی در نسخه ۷ اینترنت اکسپلورر آمده است. توجه داشته باشید که ممکن است شکل منوها در نسخه های متفاوت اینترنت اکسپلورر متفاوت باشد. بنابراین باید مراحل زیر را مناسب هر نسخه تغییر داد.

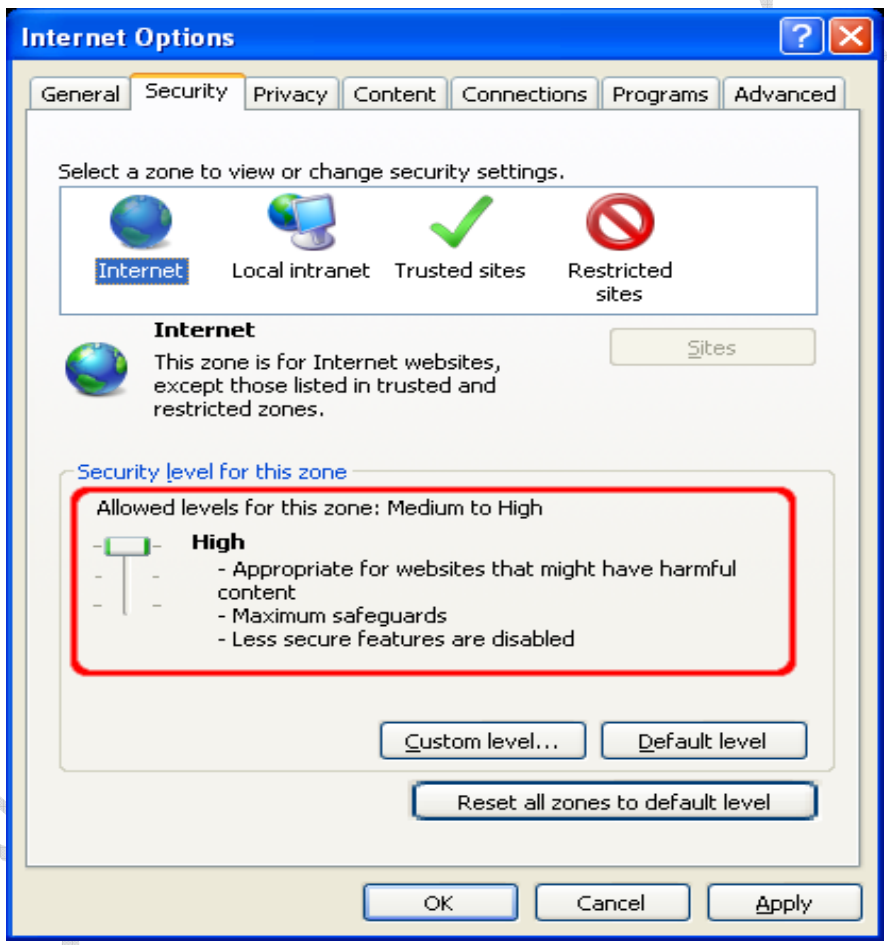
برای تغییر در تنظیمات اینترنت اکسپلورر، Tools را انتخاب کنید ، سپس بر روی Internet Options کلیک کنید.



پنجره security را انتخاب کنید. در بالای این پنجره ، لیستی از حوزه های امنیتی که اینترنت اکسپلورر از آنها استفاده می کند وجود دارد. اطلاعات بیشتر درباره حوزه های امنیتی اینترنت اکسپلورر در لینک Setting Up Security Zone وجود دارد. برای هر یک از این حوزه ها، می توان سطح حفاظت تعیین کرد. با کلیک بر روی دکمه custom control دو پنجره باز می شود که اجازه انتخاب تنظیمات متفاوت را برای حوزه های مختلف به شما می دهد . حوزه های امنیتی جایی است که همه ی سایت ها در ابتدا ... .

تنظیمات امنیتی برای این ناحیه بر روی همه وب سایت هایی که در لیست دیگر ناحیه های امنیتی قرار ندارند اعمال می شود. توصیه ما این است که از بالاترین سطح امنیت برای این نواحی استفاده کنید. با انتخاب بالاترین سطح امنیت ، چندین مشخصه از جمله Active X ، Active scripting و

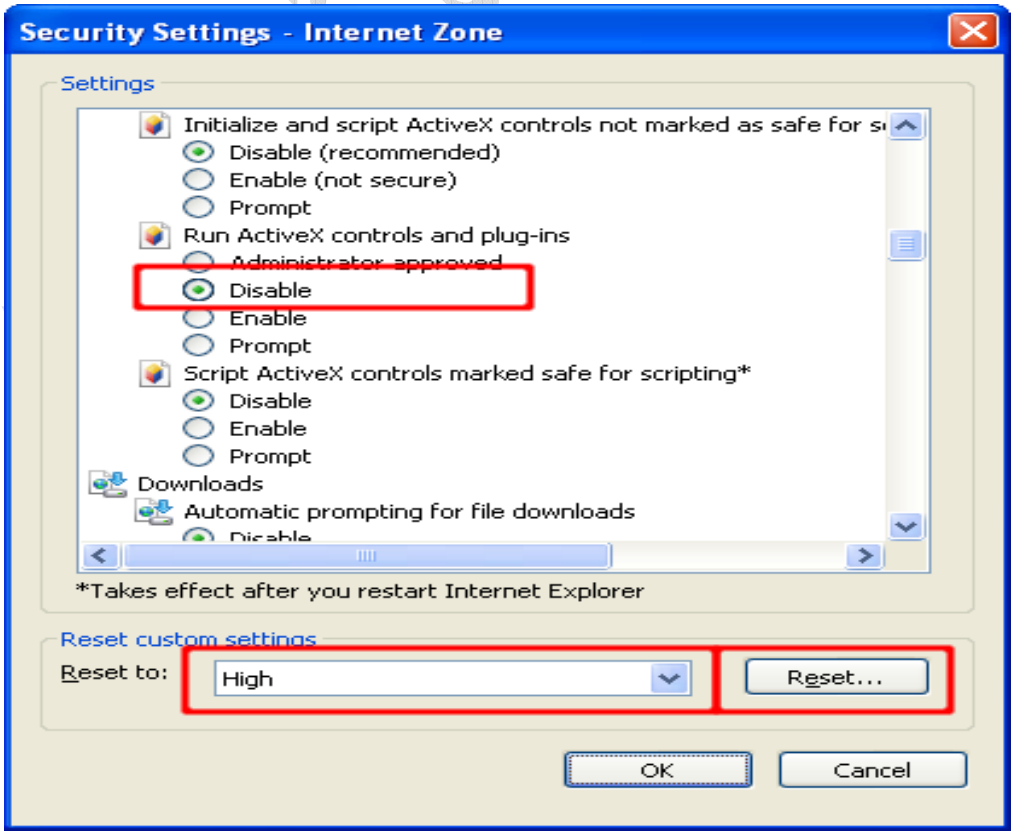
java غیر فعال می شوند. وقتی این موارد غیر فعال می شوند، مرورگر بیشترین امنیت را دارد. بر روی دکمه Default Level کلیک کنید و کلید لغزنده را در بالاترین سطح قرار دهید.

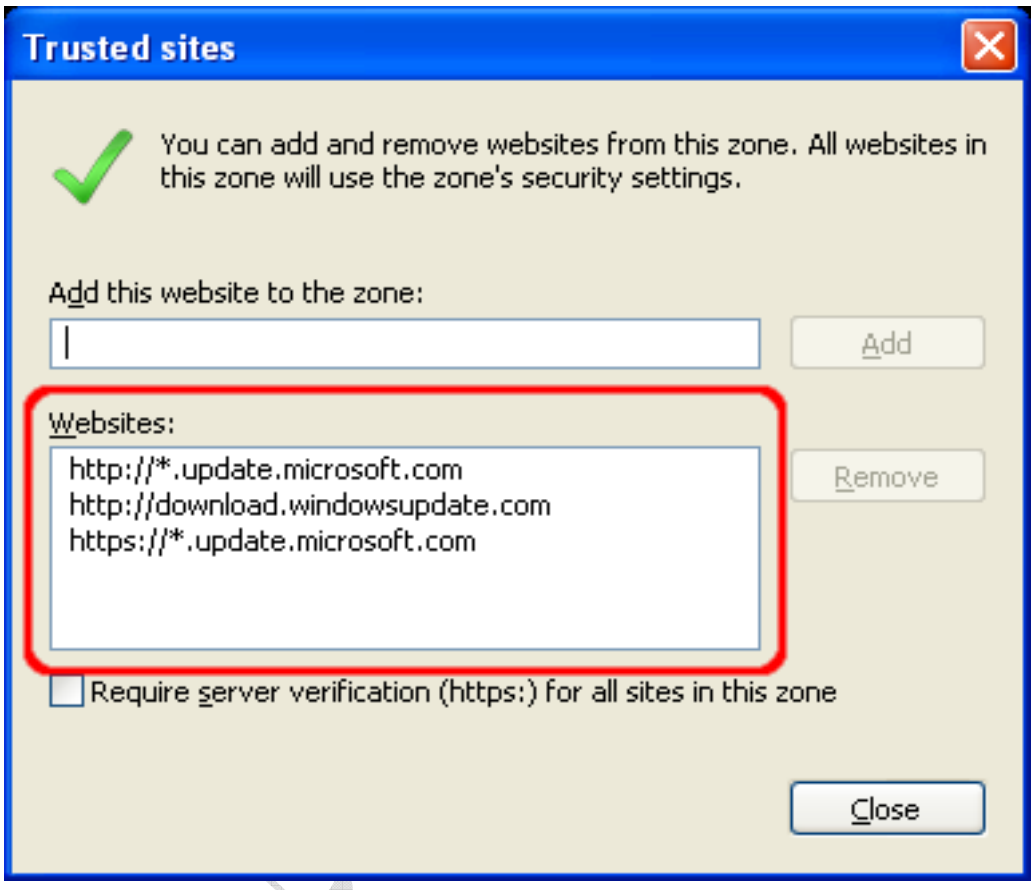


برای کنترل بیشتر بر روی آن مشخصه هایی که در ناحیه اجازه کار دارند ، بر روی دکمه custom level کلیک کنید. اینجا شما می توانید موارد امنیتی خاص را کنترل کنید. مثلا active X را می توان با

انتخاب Disable در قسمت Run ActiveX controls and plug-ins غیر فعال کرد. مقادیر پیش فرض برای داشتن بالاترین سطح امنیت را می توان با انتخاب High و کلیک بر روی دکمه Reset اعمال کرد.

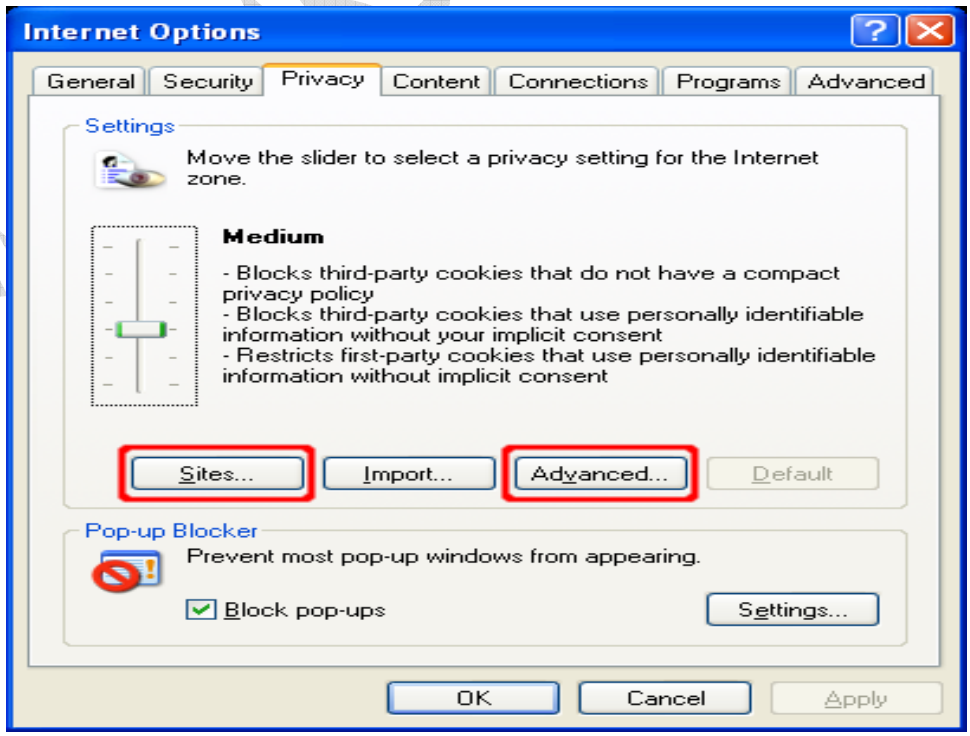
ناحیه Trusted sites یک ناحیه امنیتی برای سایت هایی است که فکر می کنید ایمن هستند. وقتی شما به ایمن بودن یک سایت بخصوص باور دارید و می دانید که دارای محتویات مخرب نیست آن را در این قسمت قرار می دهید. برای اضافه و یا حذف سایت ها از این حوزه می توانید بر روی دکمه Sites... کلیک کنید. با کلیک بر روی این دکمه پنجره جدیدی باز می شود که در آن پنجره امکان حذف و اضافه کردن سایت ها به شما داده شده است. همچنین شما ممکن است بخواهید فقط سایت های بازبینی شده (HTTPS) در این لیست قرار بگیرد. این موضوع اطمینان بیشتری درباره امن بودن این سایت ها به شما می دهد.



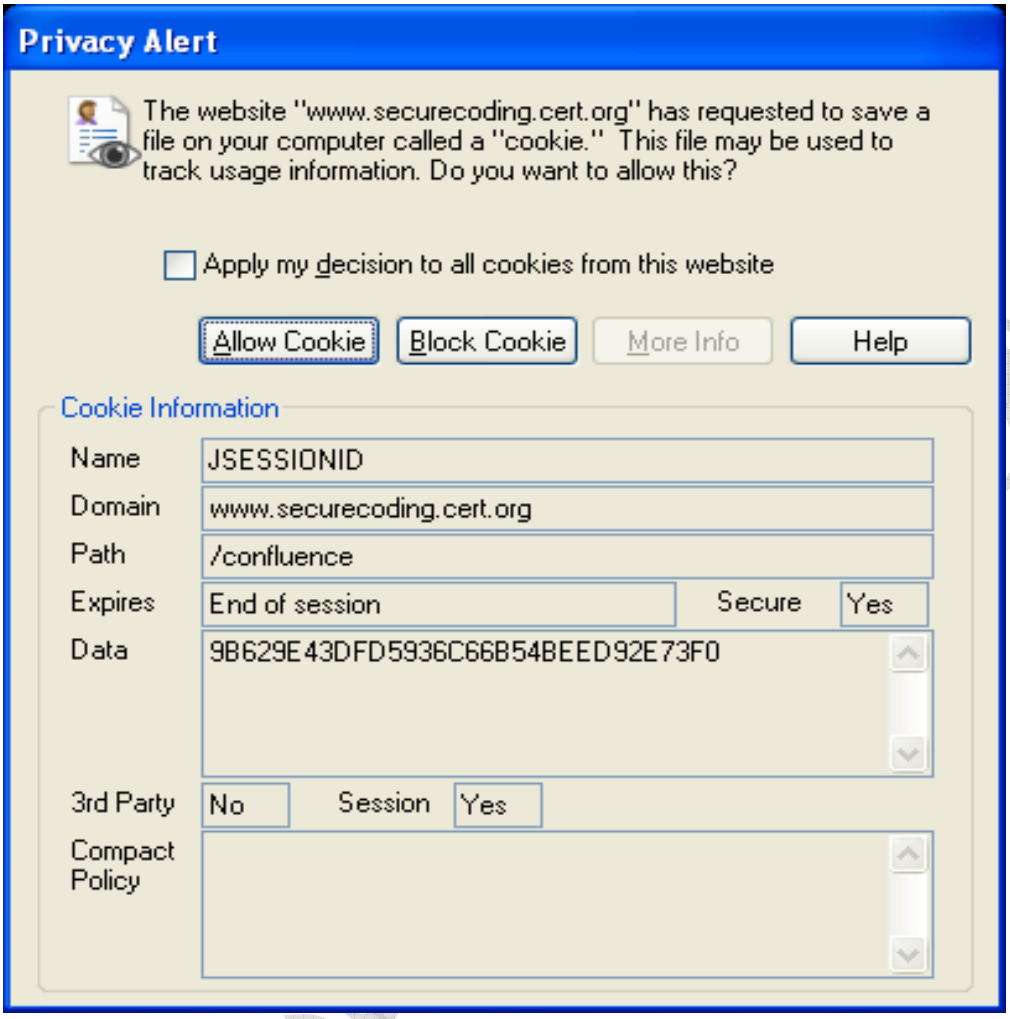


توصیه می کنیم که سطح امنیت برای ناحیه Trusted zone را بر روی Medium-High (یا برای IE6 و نسخه های قبل از آن بر روی Medium) قراردهید. وقتی امنیت حوزه های اینترنت را در بالاترین وضعیت قرار دهیم ، ممکن است با وب سایت هایی مواجه شویم که درست کار نمی کنند که به دلیل تنظیمات امنیتی انجام شده می باشد. اینجا همان جایی است که، Trusted zone می تواند کمک کند. اگر مطمئن باشید که سایت محتویات مخرب ندارد می توانید آن را به لیست Trusted zone ها اضافه کنید. فقط وقتی سایت به لیست اضافه می شود، مواردی همچون Active X و Active Scripting برای سایت فعال خواهد شد. فایده این کار این است که IE از ابتدا بسیار امن خواهد بود، و سایت ها می توانند در قسمت Trusted zone برای داشتن کارایی بیشتر قرار بگیرند.

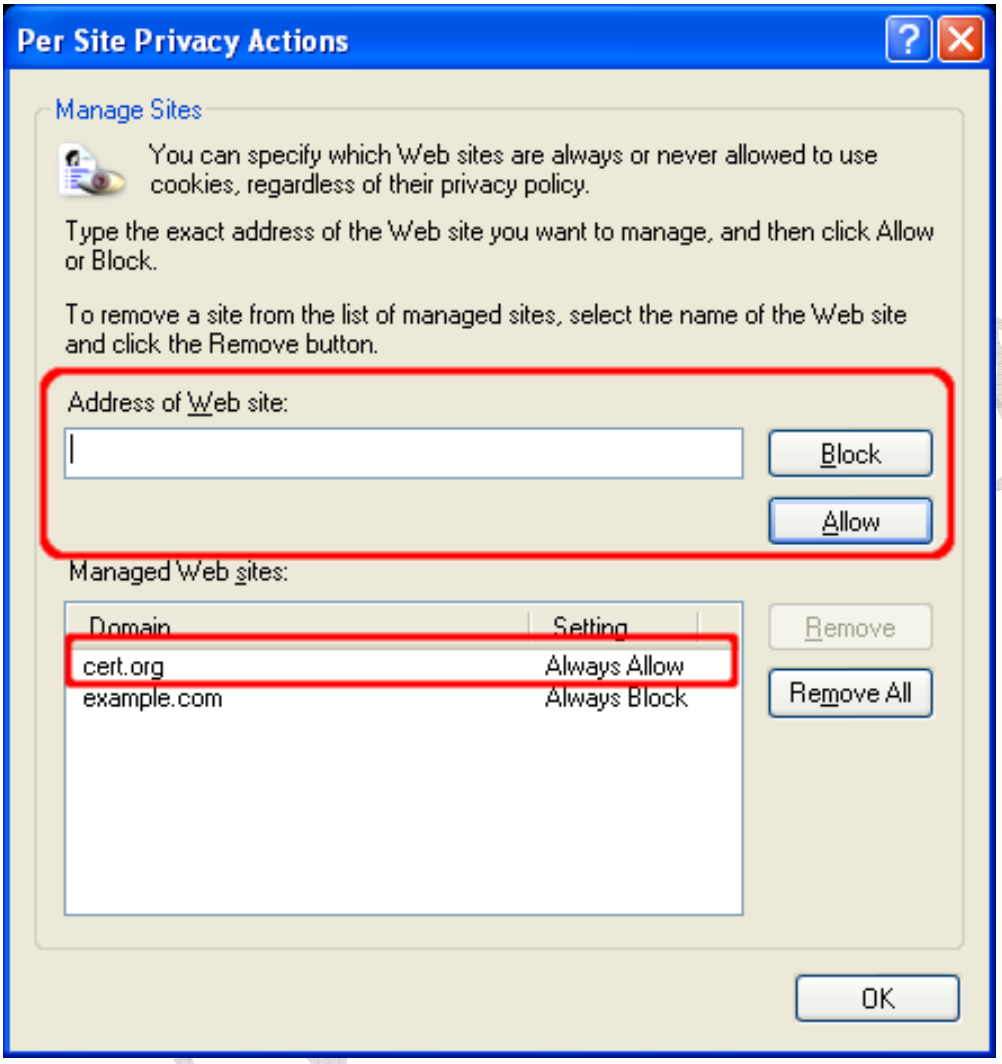
پنجره Privacy شامل تنظیماتی برای Cookie ها می باشد. Cookie ها فایل هایی هستند که توسط سایت های مختلف به طور مستقیم یا غیر مستقیم بر روی رایانه شما قرار گرفته اند. یک Cookie می تواند شامل هر اطلاعاتی که برای ذخیره کردن یک سایت نیاز است ، باشد. اغلب از Cookieها برای دنبال کردن رایانه شما در حین گردش در اینترنت و ذخیره برخی اطلاعات از جمله اطلاعات اعتباری شما استفاده می شود. توصیه ما این است که بر روی دکمه Advanced کلیک کرده و Override automatic cookie handling را انتخاب کنید. آنگاه برای Cookieهایی که به طور مستقیم (first-party) یا غیر مستقیم (third-party) ذخیره شده گزینه prompt را انتخاب کنید. با این کار هنگامی که یک سایت تلاش می کند تا cookie بر روی رایانه شما قرار دهد به شما هشدار داده می شود. اگر تعداد Cookieهایی که با هشدار همراه بودند بیش از اندازه شود، گزینه Always allow session cookies می تواند فعال شود. با این کار cookie هایی که بر روی رایانه ماندگار نیستند بدون اجازه کاربر اجازه کار پیدا می کنند. Session cookie ها خطر کمتری نسبت به persistent cookie ها دارند.



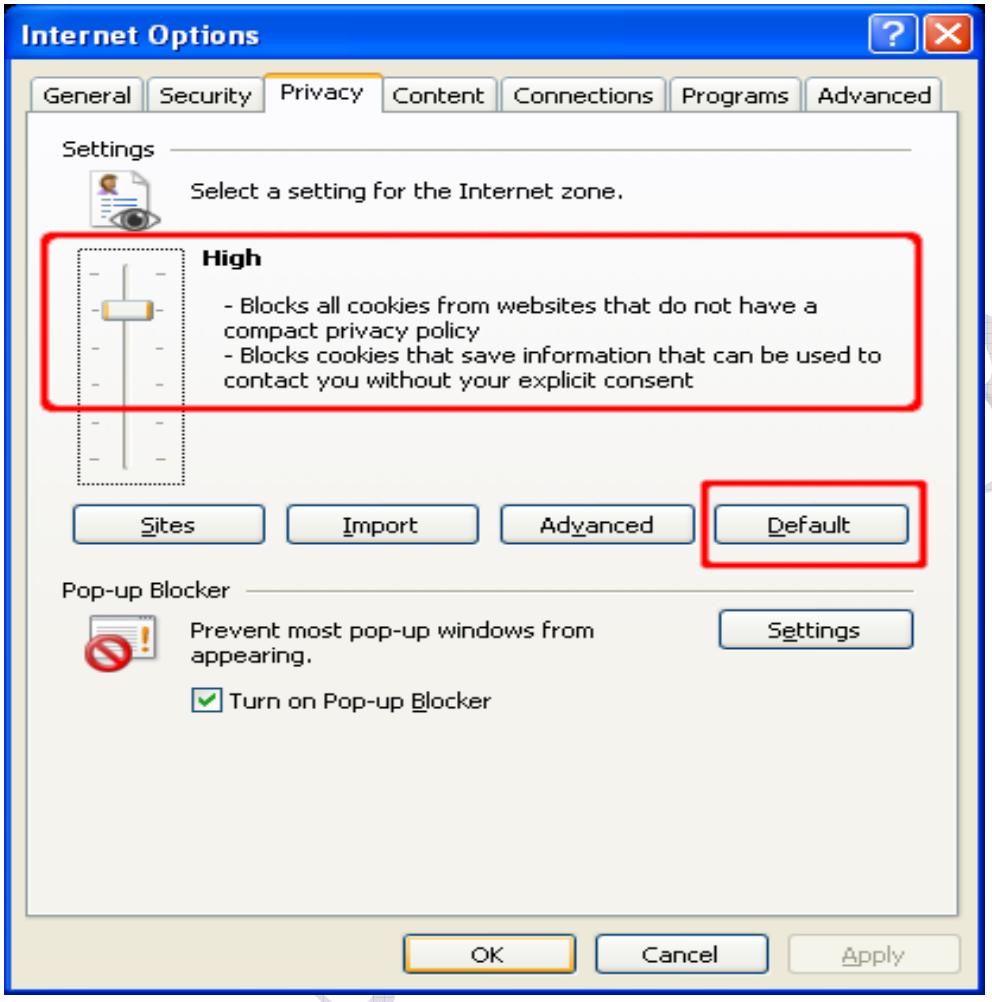
آنگاه شما می توانید با توجه به قبول و یا رد شدن cookie ها و عملی که اتفاق می افتد (رد کردن و یا اجازه دادن به وسیله گزینه ای که تصمیمات گرفته شده برای cookie های یک وب سایت را ذخیره می کند) یک سایت را بررسی کنید. برای مثال اگر در حین بازدید از یک سایت با یک هشدار مربوط به cookie های تبلیغاتی مواجه شوید دوست دارید که با کلیک بر روی block cookie از ذخیره شدن آن cookie جلوگیری کنید.



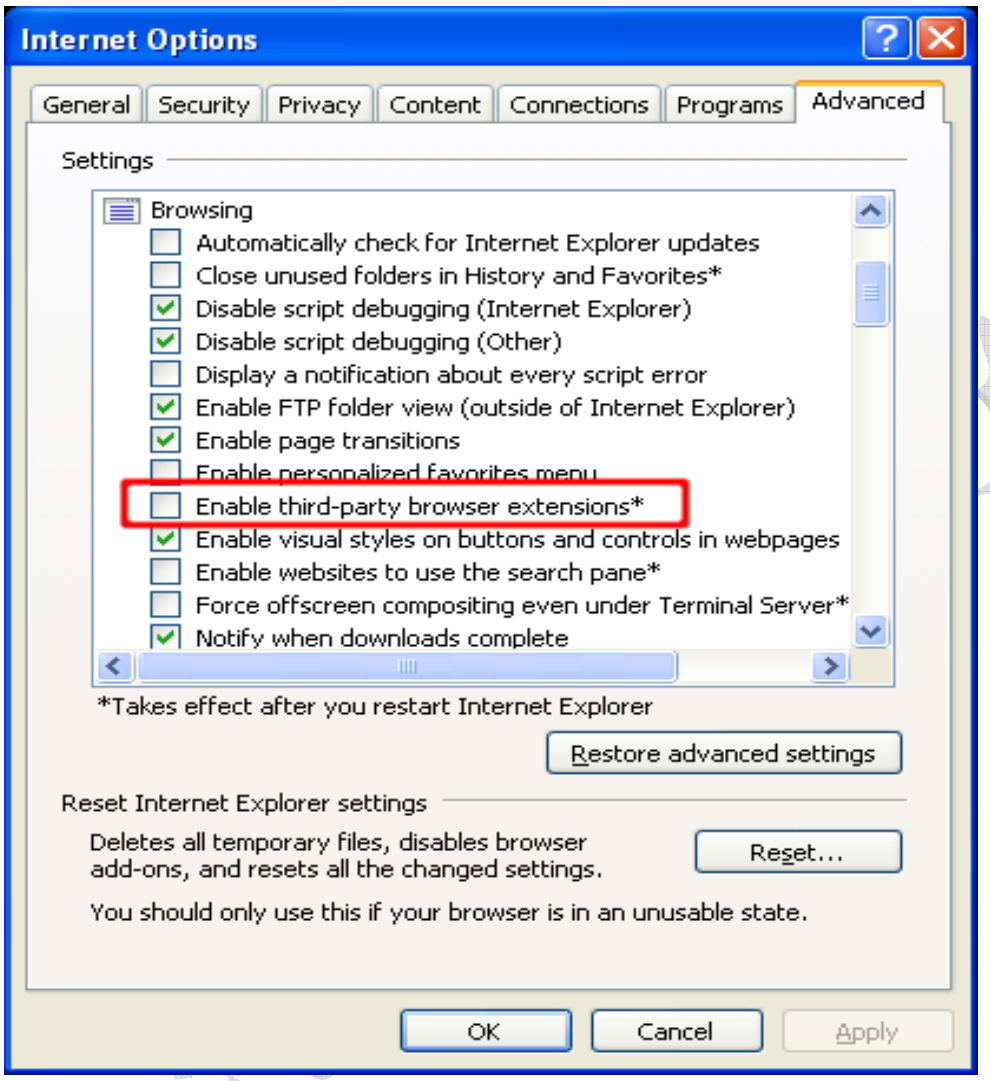
با انتخاب کلید ...site ، می توانید تنظیمات cookie را برای برخی سایت های خاص مدیریت کنید. می توانید سایت ها را حذف و یا اضافه کنید، و می توانید تنظیمات جاری را برای سایت مورد نظر تغییر دهید. قسمت پایین این پنجره مربوط به domain سایت و عکس العمل انجام شده توسط سیستم هنگامی که سایت می خواهد cookie را بر روی رایانه قرار دهد می باشد. همچنین شما می توانید از قسمت بالای این پنجره برای تغییر تنظیمات استفاده کنید.



متناوبا، اگر می خواهید وقتی که یک سایت تلاش دارد cookie را بر روی رایانه قرار دهد هشداری دریافت نکنید می توانید از قانون pre-set privacy در IE استفاده کنید. بر روی کلید default کلیک کنید و کلید لغزنده را در بالاترین سطح قرار دهید. توجه داشته باشید که برخی وب سایت ها در این حالت به خوبی کار نمی کنند . در این حالت می توانید سایت را به لیستی که مربوط به cookie های اجازه داده شده می باشد اضافه کنید همانطور که پیش از این گفته شد.

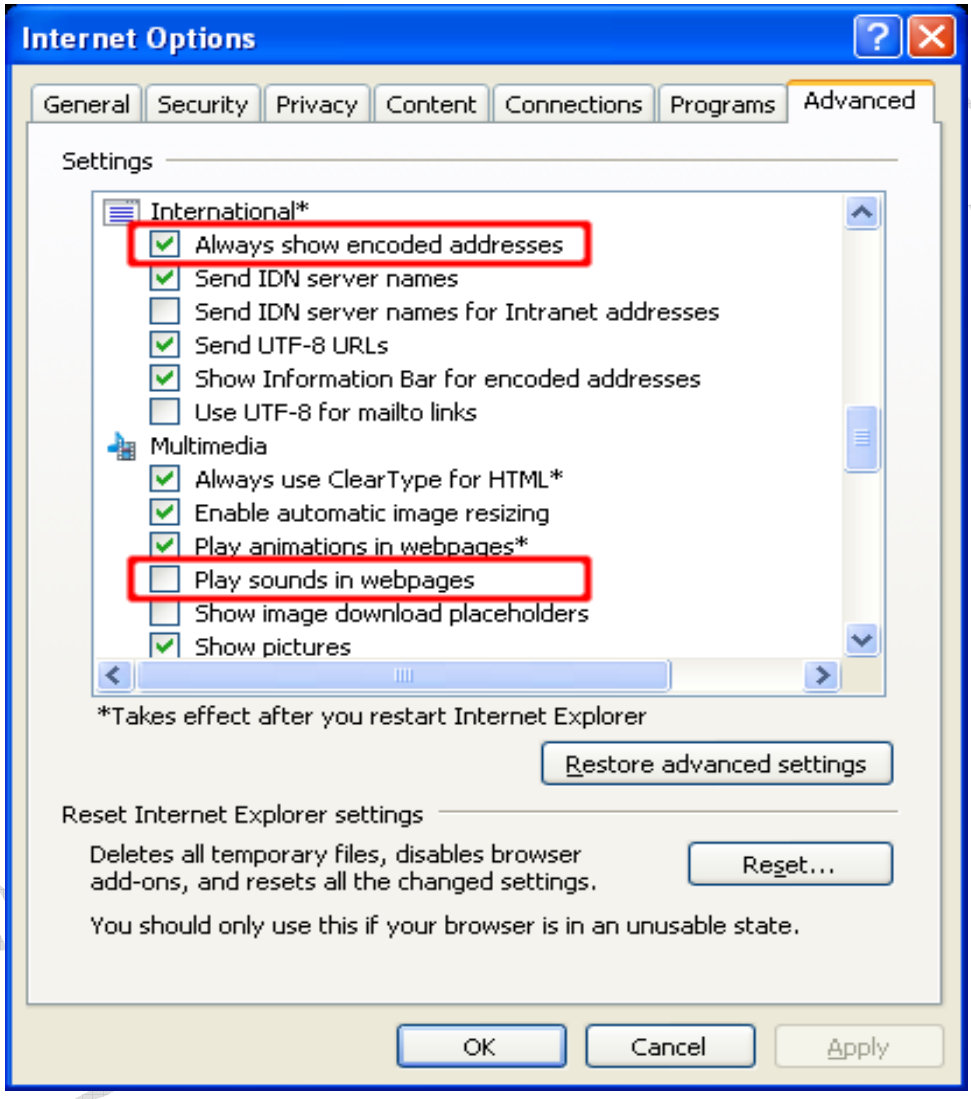


پنجره Advanced شامل تنظیماتی است که بر روی تمام حوزه های امنیتی اعمال می شود. توصیه ما این است که گزینه Enable third-party browser extensions را غیر فعال کنید. این مورد شامل نوار ابزار و کمک رسان به مرورگرها (BHO) می باشد. با اینکه برخی افزودنی ها به نرم افزار مفید هستند اما برخی مواقع کارها را مختل می کنند. برای مثال یک برنامه افزوده شده به مرورگر ممکن است صفحات وب شما را ذخیره کند و یا حتی محتویات صفحه وب را برای بدست اوردن اطلاعات شخصی شما تغییر دهد.

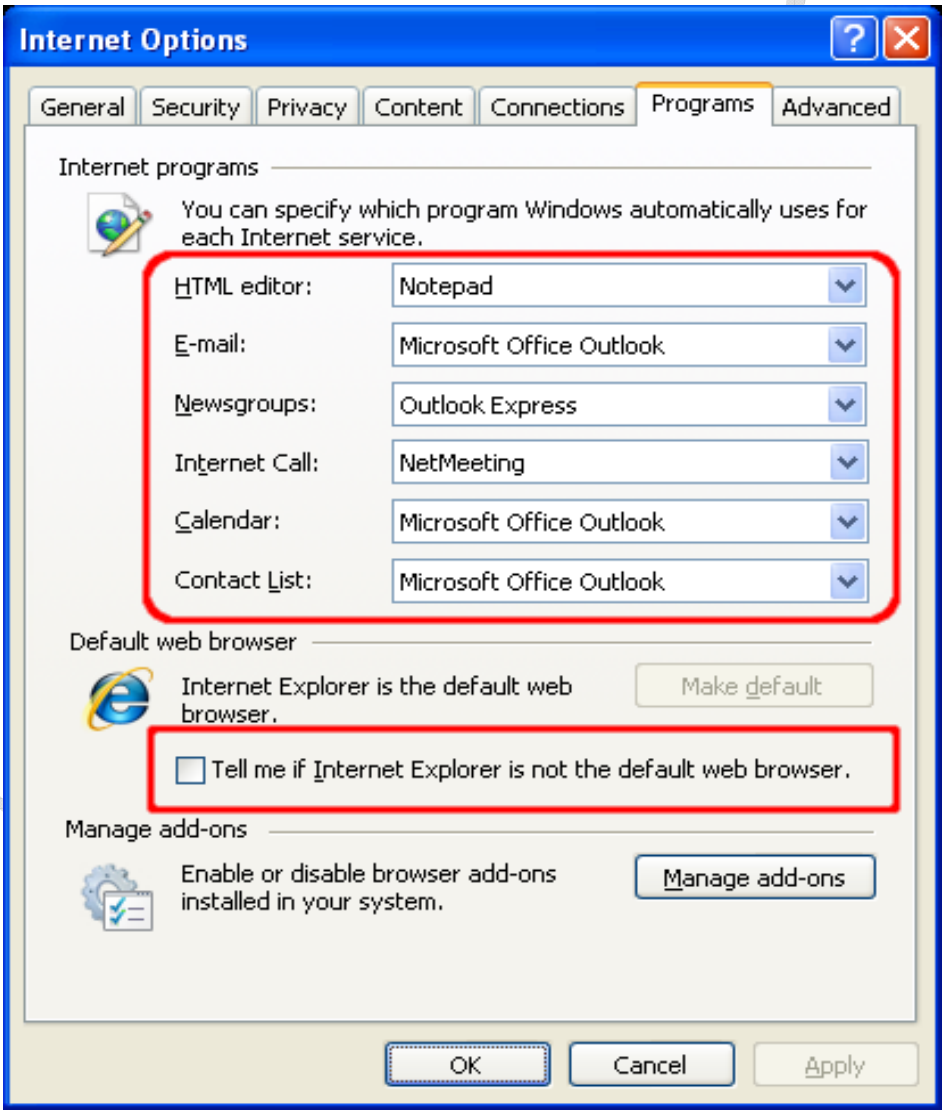


نام domainهای بین المللی شده (IDN) می تواند طوری استفاده شود که اجازه کلاهبرداری به وسیله آدرس های صفحات وب را بدهد. برای محافظت در برابر کلاهبرداری های IDN در internet explorer ، گزینه Always show encoded addresses را فعال کنید. این کار باعث می شود که آدرس های IDN در نوار آدرس و نوار وضعیت Internet explorer به شکل رمز گشایی شده نمایش داده شوند ، و آدرس هایی که با آدرس های کلاهبردار شباهت دارند را حذف کرد.

همچنین توصیه می کنیم که گزینه play sounds in web pages را غیر فعال کنید. صداها در صفحات وب به ندرت مربوط به خود آن سایت هستند و باعث ایجاد خطراتی می شوند.



در پنجره program ، می توانید نرم افزارهای کاربردی را برای نمایش وب سایت ها نامه های الکترونیکی و دیگر کارهای مربوط به شبکه انتخاب کنید. همچنین می توانید در صورتی که می خواهید Internet explorer مرورگر وب پیش فرض شما باشد پرسش IE را در این مورد غیر فعال کنید.



منابع:

http://www.microsoft.com/windows/ie/using/howto/security/setup.mspx

http://support.microsoft.com/?kbid=182569

http://www.us-cert.gov/cas/tips/ST04-022.html

http://www.us-cert.gov/cas/tips/ST05-001.html

http://www.us-cert.gov/cas/tips/ST04-012.html

http://www.cert.org/tech_tips/home_networks.html

http://www.cert.org/homeusers/HomeComputerSecurity/

http://www.cert.org/archive/pdf/spyware2005.pdf

http://www.cert.org/reports/activeX_report.pdf

http://www.opera.com/support/tutorials/security

http://www.mozilla.org/projects/seamonkey

http://www.konqueror.org

http://browser.netscape.com

مرکز ایمنی دانشگاه شیراز