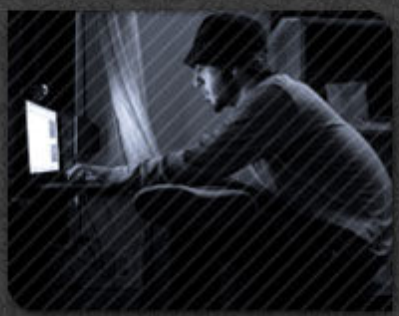
دی ماه ۸۹ / مجله شماره ۲

آشیانه

مجله الکترونیکی هک و امنیت آشیانه

www.Ashiyane.org



آموزش آسیب پذیری XSS

آموزش آسیب پذیری SQL Injection

Network+

شبکه های هدف

آموزش PHP

آموزش C#

امنیت جوملا

هک و امنیت

برنامه نویسی

شبکه

سیستم های مدیریت محتوا

جزئيات موتور جستجوي ملي اعلام شد

کوروش مشگی فارغ التحصیل کارشناسی ارشد دانشگاه صنعتی امیر کبیر که موفق به ارایه مدل ریاضی هوشمند برای عملکرد بخش بینایی مغز به منظور آشکار سازی چهره شده است به خبرنگار باشگاه خبرنگاران گفت: با توجه به آزمایش های گسترده برای شناسایی مغز نیاز به رشته کامپیوتر برای ارایه مدل های مختلف شناسایی مغز برای عصب شناسان است به همین منظور در این مدل برای تعامل بیشتر بین کاربر و رایانه واسطی طراحی شده که کاربر را شناسایی و محل قرار گرفتن وی را نشان می دهد.
رضا تقی پور وزیر ارتباطات در خصوص راه اندازی موتور جستجوی ملی اظهار داشت : ایجاد موتور جستجوی ملی ضرورت است و نگهداری اطلاعات باید در داخل کشور باشد البته جایگزین نیست اما برای جلوگیری از سرقت اطلاعات راه اندازی می شود که امنیت آن بسیار بالاست.
- گسترش زیر ساخت های it در برنامه پنجم توسعه
احمد بزرگیان رئیس کمیته تخصصی دولت الکترونیک در خصوص زیر ساخت های it در برنامه پنجم توسعه بیان داشت: گسترش it در جوامع از ضروریات محسوب می شود و کشور ما هم به سمت ایجاد دولت الکترونیک حرکت کرده که تا کنون ارتباط بین دستگاهی را تا حد ۱۰۰ درصد طراحی کردیم و خدمات دهی به مردم تا ۷۰ درصد الکترونیکی شده و در بخش توسعه باند اینترنتی تا ۵۱۲ kb برنامه ریزی کردیم و بحث پرونده سلامت الکترونیک مردم هم باید تا ۱۰۰ درصد محقق شود.
وی تصریح کرد: کشور به سمتی حرکت می کند که شهروند الکترونیکی می طلبد پس بستر را باید در بخش آموزش، تجهیزات و قوانین فراهم کنیم.
- پایان فضای آدرس دهی اینترنتی در انگلیس
به گفته نایب رئیس گوگل باقیمانده فضای آدرس دهی اینترنتی ipv4 در بهار آینده اختصاص می یابد و این بدان معناست که این فضا تا سال ۲۰۱۲ به پایان خواهد رسید.
گفتنی است: فضای آدرس دهی اینترنتی ipv6 که به زودی ارائه خواهد شد ظرفیت پذیرش ۳۴۰ تریلیون آدرس اینترنتی را خواهد داشت.
- انتشار خطرناک ترین تروجان در اینترنت
شرکت امنیتی بیت دیفندر در مورد یک تروجان خطرناک که به تازگی در فضای مجازی منتشر شده هشدار داد.
بنابراین گزارش؛ این تروجان که trojan.spy.yek نام دارد نرم افزاری برای جاسوسی است و خود را در شبکه های محلی شرکت های مختلف پنهان می کند و در فرصت مناسب نسبت به سرقت اطلاعات اقدام می کند همچنین در زمینه انتقال اطلاعات مسروقه به مهاجمان نیز با دقت عمل کرده و تمامی دیتای ارسالی را رمز گذاری می کند.

مدیر بلاگفا : حدود دو میلیون وبلاگ فارسی فعال وجود دارد که ...

خبرگزاری دانشجویان ایران - تهران سرویس: نگاهی به وبلاگها
مدیر بلاگفا گفت: حدود دو میلیون وبلاگ فارسی فعال وجود دارد که حدود ۲۰۰ هزار مورد آن وبلاگ تاثیرگذار است .
علیرضا شیرازی در گفت وگو با خبرنگار سرویس وبلاگ های خبرگزاری دانشجویان ایران (ایسنا)، اظهار کرد: در حال حاضر ۸۰۰ هزار وبلاگ در بلاگفا وجود دارد که حدود ۳۰۰ هزار وبلاگ طی یک هفته اخیر فعال بوده اند .
وی اظهار کرد: تعداد وبلاگ های ساخته شده با تعداد وبلاگ هایی که محتوا دارد و همچنان فعال است، بسیار متفاوت بوده و وبلاگی که قدمت بالاتری دارد نقش بیشتری نسبت به وبلاگ های جدید خواهد داشت چراکه مخاطب و کاربران بیشتری دارد .
شیرازی اظهار کرد: حدود دو میلیون وبلاگ فارسی فعال وجود دارد که حدود ۲۰۰ هزار مورد آن وبلاگ تاثیرگذار است .
مدیر بلاگفا با بیان اینکه تاکنون چهار میلیون و ۵۰۰ هزار وبلاگ در سرویس بلاگفا ثبت شده است، گفت :تعداد وبلاگ هایی که در یک سرویس ساخته شده مهم نیست بلکه وبلاگ هایی که فعال هستند و سابقه کار دارند، ارزش دارد .
وی با تاکید بر اینکه وبلاگ های غیرفعال مرتب از سرویس بلاگفا حذف می شوند، افزود: در این سرویس، وبلاگی که سه سال فعال نباشد، وجود ندارد و مرتبا وبلاگ های غیرفعال براساس تاریخ ثبت، آخرین مطلب و تعداد مطالب ثبت شده و ... حذف می شوند .
به اعتقاد شیرازی، وبلاگی که یک سال فعالیتی نداشته باشد، وبلاگ غیرفعال؛ وبلاگی که طی شش ماه گذشته فعالیت کرده، وبلاگ نیمه فعال و وبلاگی که طی ۹۰ روز گذشته فعالیت داشته، وبلاگ فعال محسوب می شود .
وی اظهار کرد: هرچه سابقه فعالیت یک سرویس وبلاگ بیشتر می شود، تعداد وبلاگ های غیرفعال آن نیز بیشتر

خواهد شد .
مدیر بلاگفا اظهار کرد: می توان گفت سرویس وبلاگی که بیش از سه سال فعالیت داشته، یک سوم از وبلاگ هایش فعال است .
شیرازی با اشاره به اینکه بلاگفا سرویس وبلاگ اول کشور است، گفت: یک میلیون و نیم وبلاگ فعال در این سرویس وجود دارد که بر اساس فرمول هایمان تاکنون حذف نشده اند .
وی بلاگفا، میهن بلاگ، پرشین بلاگ، وبلاگ اسکای و پارسی بلاگ را سرویس وبلاگ های اصلی کشور عنوان و اظهار کرد: حدود ۳۰ سرویس وبلاگ جدید فعال شده که تعداد کاربران آن بسیار محدود بوده و قابل توجه نیست.

حمله زامبی ها به گوشی های چین

بیش از یک میلیون تلفن همراه در چین به ویروس زامبی آلوده شده اند که به صورت خودکار پیغام های اسپم به تمام شماره های موجود در دفترچه تلفن یک گوشی می فرستد .
بر اساس گزارش خبر گزاریها این ویروس در حال حاضر بیش از ۳۰۰هزار دلار در روز به مشترکان چینی آسیب مالی می زند و از ابتدای ماه سپتامبر تاکنون در شبکه تلفن های همراه چینی وجود دارد و در هفته نخست یک میلیون گوشی را آلوده کرده است .
این ویروس در یک نرم افزار ضدویروس چینی به نام سیچوان قرار دارد و از این طریق خود را منتشر می کند. طبیعتا این شرکت هیچ مسوولیتی در قبال این ویروس نپذیرفته و اعلام کرده است که نمی توان نرم افزار سالم را از نرم افزار ویروسی تشخیص داد. این شرکت همچنین اعلام کرد که شرکت های تجاری نیز با این ویروس دست و پنجه نرم می کنند .
این ویروس با ارسال اطلاعات سیمکارت به هکرها کار خود را آغاز می کند. هکرها سپس کنترل گوشی را از راه دور برعهده می گیرند و به تمام کسانی که در دفترچه تلفن وی وجود دارد، اسپم ارسال می کنند. این روش درست مشابه گسترش هرزنامه از طریق ایمیل است: پیغام شامل معرفی یک وب سایت تبلیغاتی درآمدزایی اینترنتی است که از طرف یکی از اعضای خانواده یا دوست ارسال شده است. با کلیک کردن روی لینک، آن گوشی نیز آلوده می شود و این روند ادامه پیدا می کند .شایان ذکر است با گسترش استفاده از تلفن های همراه موج جدیدی از ویروس ها در تلفن های همراه آغاز شده است، برخی از این ویروس ها حتی نرم افزار ضدویروس موبایل را هم از کار می اندازند.

لزوم مدیریت شرکت های ارایه دهنده ی سیستم امنیت اطلاعات

علی حکیم جوادی در گفت وگو با خبرنگار فن آوری اطلاعات خبرگزاری دانشجویان ایران (ایسنا)، درباره استانداردسازی با امنیت فضای تبادل اطلاعات اظهار کرد: یکسری الزامات در isms تعریف شده است که یک بخشی از آن برای بازرسی و نظارت باید به شرکت ها بروند و ما هم باید به شرکت هایی مجوز بدهیم تا بتوانند مراجعه به سازمان ها کند و کار isms را پیش ببرند.
وی افزود: اکنون کم و بیش برخی شرکت هایی وجود دارند که isms را انجام می دهند اما باید تحت سیستمی مدیریت شوند تا گواهی هایی هم که صادر می کنند قابل قبول باشد.
و گفت: استانداردهای ایزو که مرتبط با isms است، دارای معیارهای بسیاری است که ممکن است طی چند مرحله این معیارها پیاده سازی شوند.
حکیم جوادی با اشاره به اینکه فعالیت پروژه متبا در سازمان فن آوری اطلاعات شروع شده است گفت: افتتاحیه آن هم طبق برنامه زمان بندی خودش به اجرا درخواهد آمد.

زامبی ، یک میلیون گوشی در چین را آلوده کرد

به گزارش اخبار خارجی موبنا، با حمله ویروس زامبی به گوشی های هوشمند در چین، جزییات سیمکارت کاربران برای هکرها ارسال شده، سپس بدون وقفه برای آنها پیامک ارسال می شود.
به این ترتیب لینک هایی شامل بازی و نرم افزار برای کاربران ارسال می شود که با کلیک روی این لینک ها تلفن همراهشان آلوده خواهد شد.
گفته می شود این ویروس از یک نرم افزار آنتی ویروس نشات گرفته است.
اپراتورهای بی سیم در چین در حال کاهش تعداد پیام های آلوده هستند اما کارشناسان مخابراتی اعتقاد دارند بروز رسانی این ویروس ممکن است باعث کاهش پیام ها شود که به این ترتیب مشکلات بیشتری برای هر گونه

فعالیتی به وجود خواهد آمد.
در ماه اوت اولین ویروس تروجان به گوشی های هوشمند مبتنی بر اندرویید وارد شد که هکرها پیشتر این ویروس را در بازی های ویدیویی برای گوشی های مبتنی بر ویندوز موبایل ارایه کرده بودند.
در ماه مه شرکت سیمانتک که آنتی ویروس نورون را تولید می کند یک سری از محصولاتش را برای محافظت از گوشی های هوشمند ارایه کرد.

تولید آنتی ویروس قویتر از مک آفی در ایران

مدیرعامل شرکت فناوری اطلاعات از اتمام فاز فنی پروژه سیستم فیلترینگ یکپارچه در این شرکت خبر داد و گفت: این پروژه در مرکز تحقیقات مخابرات ایران در حال انجام و عملیاتی شدن است و زمان عملیاتی شدن این پروژه باید از سوی این مرکز اعلام شود .
سعید مهدیون در پاسخ خبرنگار مهر در مورد آخرین وضعیت سیستم فیلترینگ یکپارچه که توسط زیرمجموعه وزارت ارتباطات و فناوری اطلاعات در حال انجام است گفت: وظایف شرکت فناوری اطلاعات در مورد این پرو ژه به اتمام رسیده است و این پروژه هم اکنون در مرکز تحقیقات مخابرات ایران در حال انجام است.وی با بیان اینکه شرکت فناوری اطلاعات در مباحث مفهومی، محتوایی و فنی این پروژه فعالیت داشته است گفت: هم اکنون وظایف فناوری اطلاعات در این بخش به اتمام رسیده و مابقی پروژه از سوی دیگر شرکتها باید انجام شود.مهدیون اضافه کرد: زمان عملیاتی شدن این پروژه باید از سوی مرکز تحقیقات مخابرات ایران به عنوان متولی این پروژه اعلام شود.فناوری اطلاعات تا پایان سال شرکتی می ماندمدیرعامل شرکت فناوری اطلاعات با بیان اینکه این شرکت تا پایان سال به صورت شرکتی اداره خواهد شد و به سازمان فناوری اطلاعات تبدیل نمی شود با اشاره به تصویب اساسنامه سازمان فناوری اطلاعات ایران گفت: به دلیل نیمه کاره ماندن برخی پرو ژه ها و با توجه به اینکه شرکت فناوری اطلاعات از ابتدای امسال با ساختار شرکتی فعالیت کرده تا پایان سال این روند به همین ترتیب ادامه می یابد و فعالیت شرکت فناوری اطلاعات متوقف نمی شود.وی با بیان اینکه سازمان فناوری اطلاعات در حال تعیین و تفکیک وظایف حاکمیتی و غیر حاکمیتی برای شروع به کار است ادامه داد: تکلیف پروژه های فناوری اطلاعات نیز پس از این مرحله مشخص می شود.مهدیون با اشاره به اینکه شرح وظایف و اهداف سازمان فناوری اطلاعات باید به تصویب هیئت دولت برسد اضافه کرد: این وظایف به عهده گروه و مشاوران گذاشته شده است .چرا که دولت سه ماه برای تفکیک وظایف سازمان فناوری اطلاعات مهلت مقرر کرده است.به گفته وی تمامی پروژه های شرکت فناوری اطلاعات بیشتر جنبه حاکمیتی دارد و پروژه ای که قابل واگذاری به بخش خصوصی باشد وجود ندارد.تولید آنتی ویروس ایرانی بالاتر از مک آفیمهدیون با اشاره به مسائل امنیت فضای تبادل اطلاعات و با تاکید بر اینکه ۱۰ تا ۱۵ درصد حجم بازار متعلق به نرم افزارهای امنیتی است گفت: هم اکنون آنتی ویروس ایرانی بسیار قوی در کشور داریم که تولید داخل است و حتی در بسیاری موارد در شناسایی بدافزارها از آنتی ویروس مک آفی هم بالاتر قرار گرفته است.مدیرعامل شرکت فناوری اطلاعات با اشاره به ضد بدافزار "ایمن" که نشان از توانمندی کشور در امر تولید نرم افزارهای امنیتی دارد خاطرنشان کرد: توانمندی کشور بیش از یک محصول است و بزودی شرکتهای دیگری هم در این عرصه وارد بازار خواهند شد.وی در مورد آخرین وضعیت مرکز توسعه مدیریت اینترنت (متما) با بیان اینکه این مرکز یکی از ابزارهای اصلی مدیریت بر آدرس های اینترنتی (ip) است، ادامه داد: این مرکز به بهبود توسعه و ایمن سازی شبکه کمک می کند که آیین نامه آن تحت عنوان "چگونگی مدیریت ip در کشور" در نوبت تصویب سازمان تنظیم مقررات و ارتباطات رادیویی قرار گرفته است.توضیحی درباره فیلترینگ یکپارچهمدیرعامل شرکت ارتباطات زیرساخت پیش از این درباره سطح متفاوت خدمات برخی شرکتهای ارائه دهنده اینترنت در مورد دسترسی به سایتها گفت: براساس ماده ۲۱ قانون جرایم رایانه ای فیلترینگ یکپارچه برای تمامی شرکتهای اینترنتی تعریف شده است و isp ها این اجازه را ندارند که به دلخواه برای سایتی محدودیت و عدم محدودیت اعمال کنند.
وی ادامه داد: فیلترینگ یکپارچه در کل کشور و از مسیر "گیت وی "انجام می شود و تعیین سایتهایی که مشمول این طرح قرار می گیرند از سوی کمیته تعیین مصادیق خواهد بود و شرکت ارتباطات زیرساخت آن را اعمال می کند. برابر قانون نیز هر سرویس دهنده اینترنت موظف است که این موارد را اجرا کند.

درآمد دو میلیون دلاری یک ویروس اینترنتی!

بدافزار کوب فیس تاکنون خسارت های مادی و معنوی بسیاری به کاربران سایت های اینترنتی وارد کرده است.
تحقیقات اخیر نشان می دهد کرم نسبتا قدیمی کوب فیس (koobface) که بیشتر برای حمله به کاربران شبکه های اجتماعی از قبیل توییتر، ببو، مای اسپیس و به ویژه فیس بوک طراحی شده است، درآمد سرشاری را روانه جیب سازندگان خود کرده است.

به گزارش ایتنا به نقل از ای ویک، بر اساس یافته های جدید، این کرم اینترنتی فقط در فاصله زمانی ژوئن ۲۰۰۹ تا ژوئن ۲۰۱۰ بیش از دو میلیون دلار درآمد برای نویسندگان خود به همراه داشته است. این بررسی توسط مرکز munk school of global affairsدر دانشگاه تورنتو انجام شده است. کوب فیس که اولین بار در دسامبر سال ۲۰۰۸ شناسایی شد، پس از آلوده کردن رایانه ها، خود را به لیست «دوستان» کاربر در فیس بوک ارسال می نماید و به همین ترتیب با گسترش دایره شیوع خود، اعضای بات نت خود را افزایش می دهد.یکی از نکاتی که در طراحی کوب فیس لحاظ شده این است که کرم مزبور پس از آلوده ساختن رایانه، از وصل شدن آن به وب سایت های امنیتی جلوگیری به عمل می آورد.هکرها با استفاده از این بدافزار می توانند دستورهای خاصی را بر رایانه قربانیان اجرا کنند.

هک موبایل پیگرد قانونی به همراه دارد

سرهنگ مهرداد امیدی در گفت وگو با خبرنگار انتظامی فارس گفت: هک موبایل با توجه به نرم افزارهای موجود، قابل انجام است و لازم شهروندان در این زمینه هوشیار باشند.
وی اظهار داشت: تا به حال شکایتی مبنی بر هک موبایل به پلیس آگاهی ارائه نشده است، شهروندان می توانند شکایات خود را در این زمینه به پلیس آگاهی اعلام کنند تا پیگیری شود.
سرهنگ امیدی درباره غیرقانونی بودن هک افزود: هک موبایل دسترسی غیرمجاز به سیستم های رایانه ای و مخابراتی محسوب می شود که طبق قانون جرائم رایانه ای قابل تعقیب و پیگرد است.
معاون مبارزه با جرائم رایانه ای پلیس آگاهی از شهروندان خواست تا عکس های شخصی، اطلاعات و ... را در موبایل خود نگهداری نکنند و تأکید کرد: حفظ امنیت خصوصی در فضای مجازی و بر روی سیستم های رایانه ای اصل غیرقابل انکاری است.

آموزش آسیب پذیری XSS (قسمت اول)

مقدمه :

در این مقاله شما را با یکي از جدي ترین آسیب پذیري وب سایت ها که داراي ریسك بالا و خطرناك است آشنا خواهیم کرد! این آسیب پذیري همان Cross Site Scripting یا به اختصار XSS نامیده مي شود! و طبق آمار بیش از ٦٩ درصد از وب سایت ها داراي این نوع آسیب پذیري مي باشند!

مباحثي که در این مقاله به آن ها خواهیم پرداخت به این شرح مي باشند:

١- آشنایي با حملات XSS
٢- تست سایت براي پیدا کردن آسیب پذیري XSS روي آن
٣- اجراي کدهاي دلخواه روي سایت آسیب پذیر
٤- آشنایي با کوکي و کوکي گرابر
٥- ساخت کوکي گرابر و دزدیدن کوکي هاي کاربران
٦- استفاده از کوکي دزدیده شده و نفوذ به سایت
٧- مشاهده ي کوکي هاي ذخیره شده در کامپیوتر خود
٨- روش هاي جلوگیري از رخ دادن آسیب پذیري XSS

آشنایي با حملات XSS :

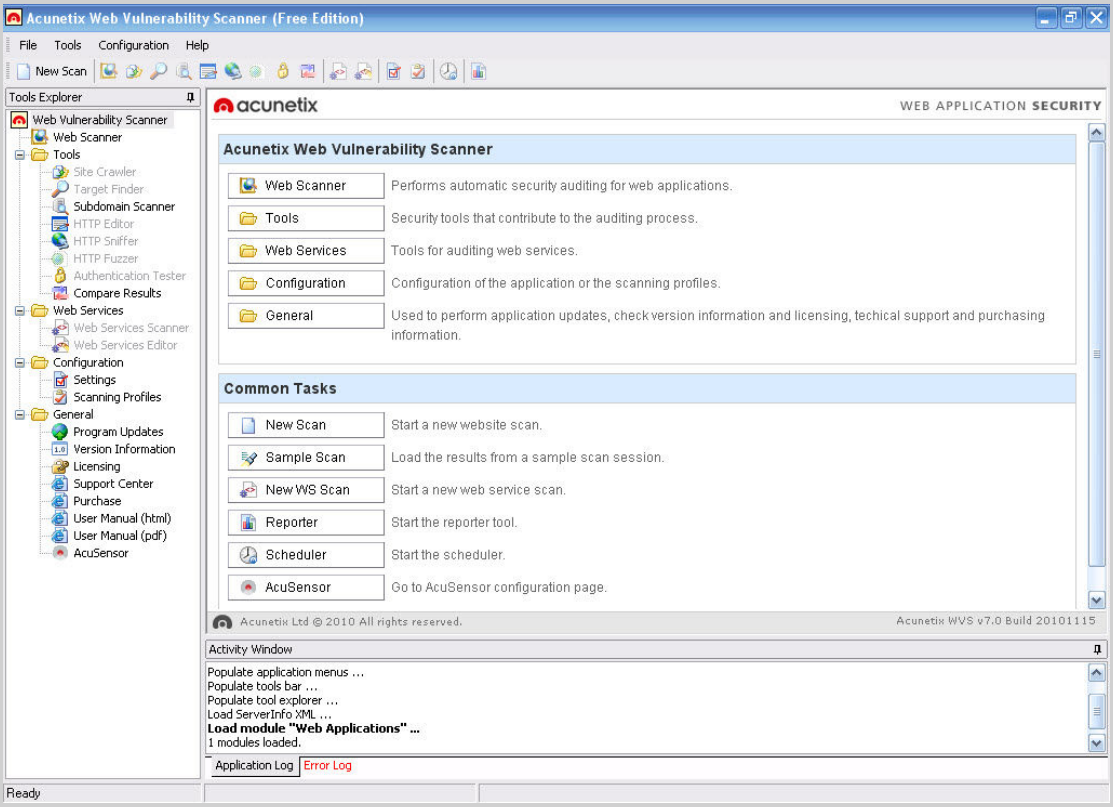
آسیب پذیری های Cross Site Scripting سبکی از حمله هستند که مهاجم را قادر می سازند کدهای مخرب خود را درون صفحات قانونی یک وب سایت بکار بگیرند. حالا بسته به نظر مهاجم این نوع کد ها مي توانند JavaScript, VBScript, ActiveX, HTML و یا Flash باشند!
این نوع حملات وقتي رخ مي دهد که ورودي یك کاربر باید در جایي به نمایش در بیاید!
از این روش حمله فیشرها و سارقان هویت بهره می برند. به عنوان مثال:
فردي که قصد دارد کاربران یك سایت را هك کند با تزریق کد در سایت آسیب پذیر اطلاعات آن ها را بدون آن که خودشان متوجه شوند مي دزدد این اطلاعات مي توانید نام کاربري و کلمه ي عبور کاربران و ... باشد سپس مهاجم با وارد کردن نام کاربري و کلمه ي عبور کاربران در سایت مي تواند به جاي آن ها وارد سایت شود و از هویت آن ها سوء استفاده کند!

تست سایت براي پیدا کردن آسیب پذیري XSS روي آن :

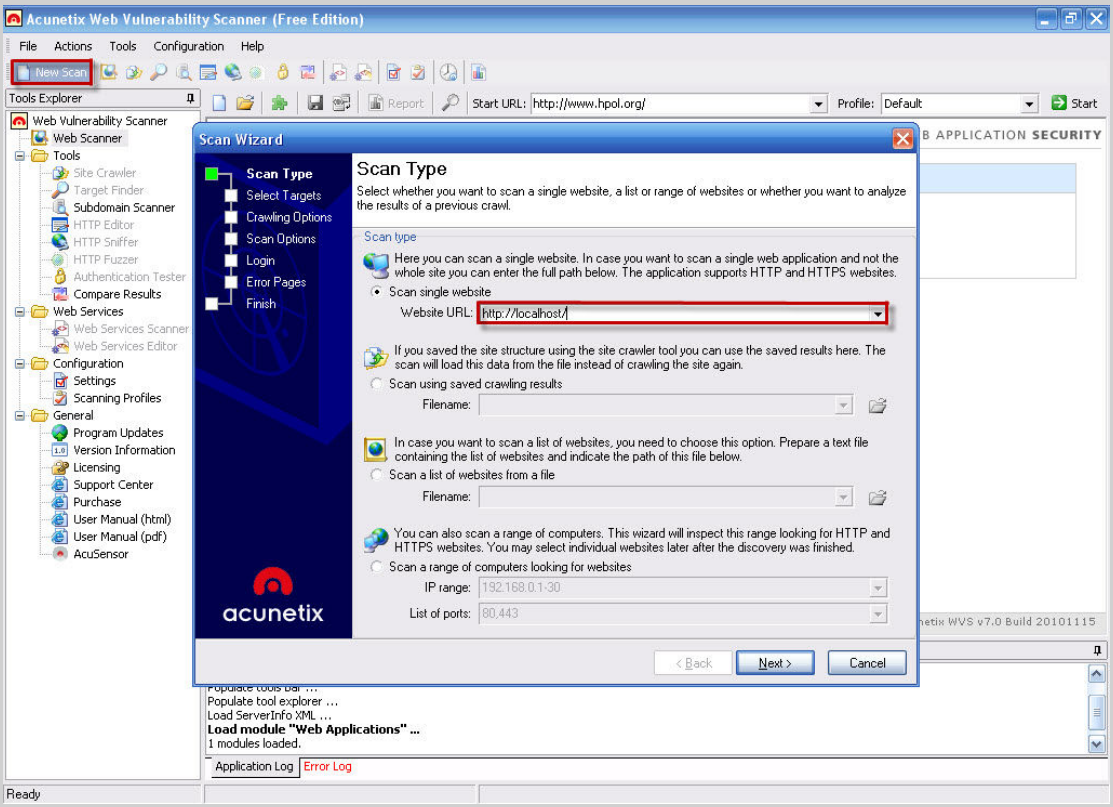
یکي از بهترین روش هاي پیدا کردن آسیب پذیري ها روي سایت استفاده از اسکنرهاي امنیتي مي باشد چون از روش هاي متعدد و پچیده اي براي یافتن آسیب پذیري ها استفاده مي کنند اما خوب گاهي اوقات هم میتوانند حدسي اشتباه را به دنبال داشته باشند!

ما در این مقاله از نرم افزار قدرتمند Acunetix که پویشگري قدرتمند است براي یافتن این آسیب پذیري استفاده خواهیم کرد!

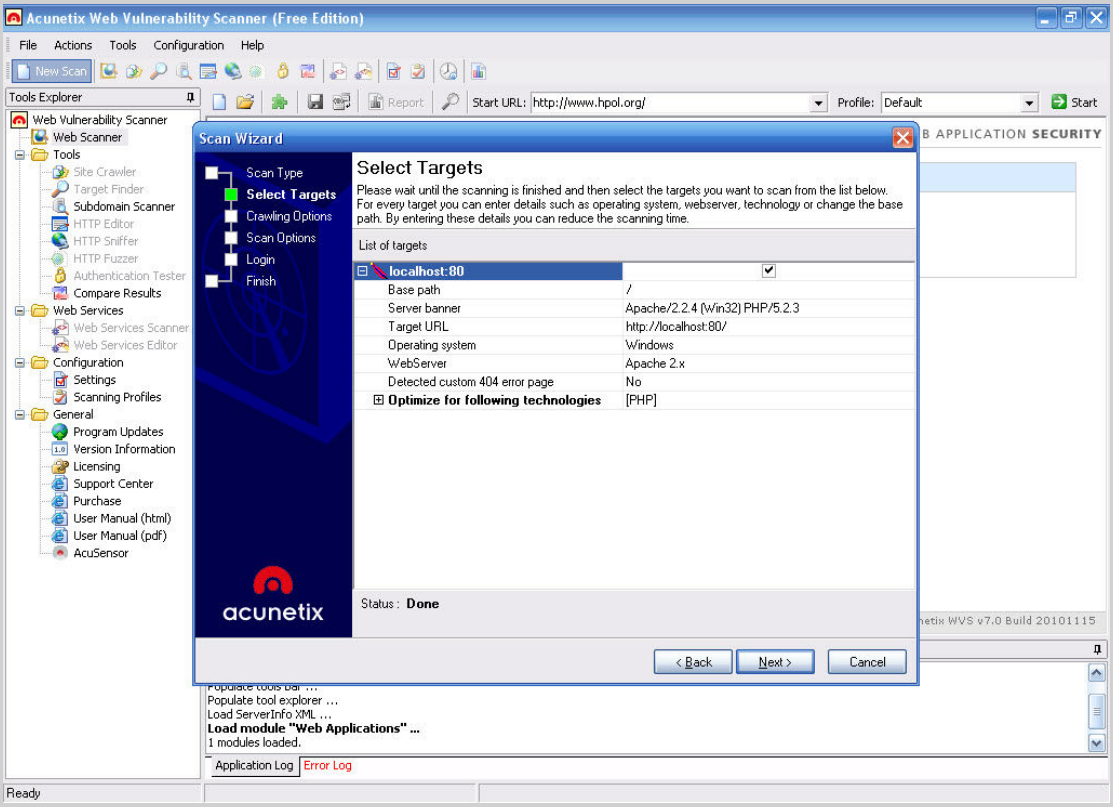
محيط كلي اين نرم افزار :



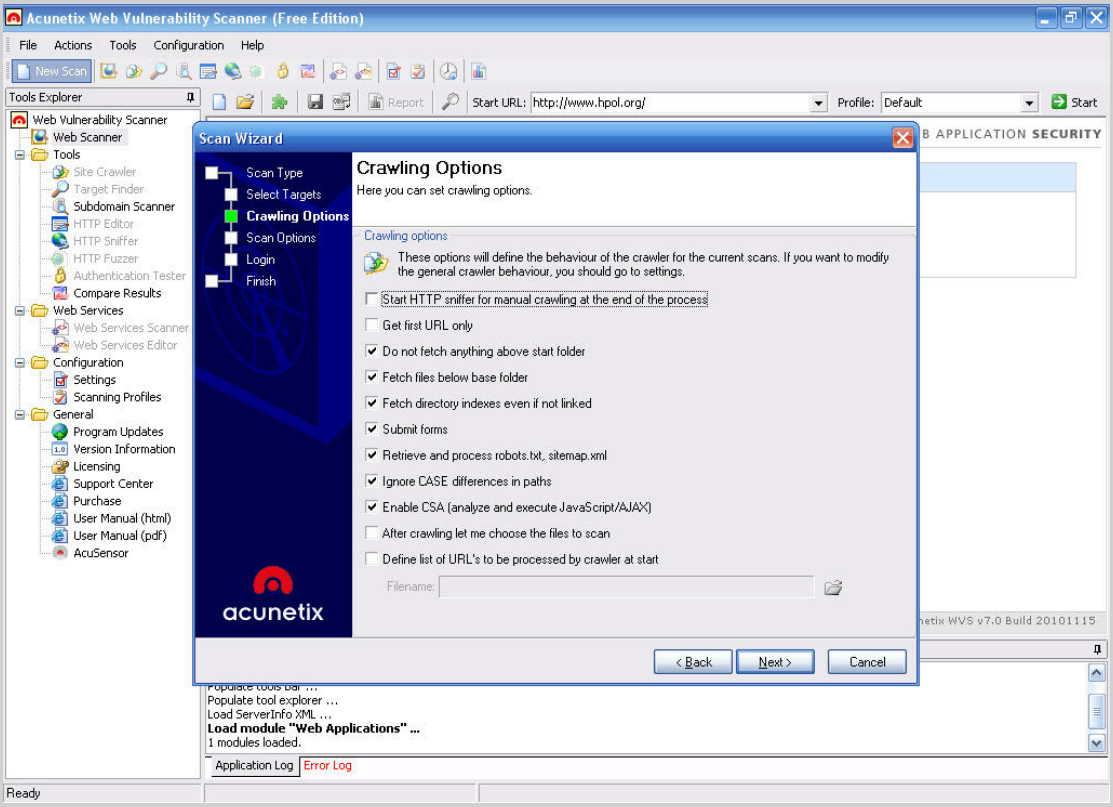
بعد از ورود به محيط نرم افزار مطابق شكل روي New Scan كليك كرده و در پنجره ي باز شده در قسمت Website URL آدرس سايت مورد نظر را براي يافتن آسيب پذيري روي آن وارد كنيد!



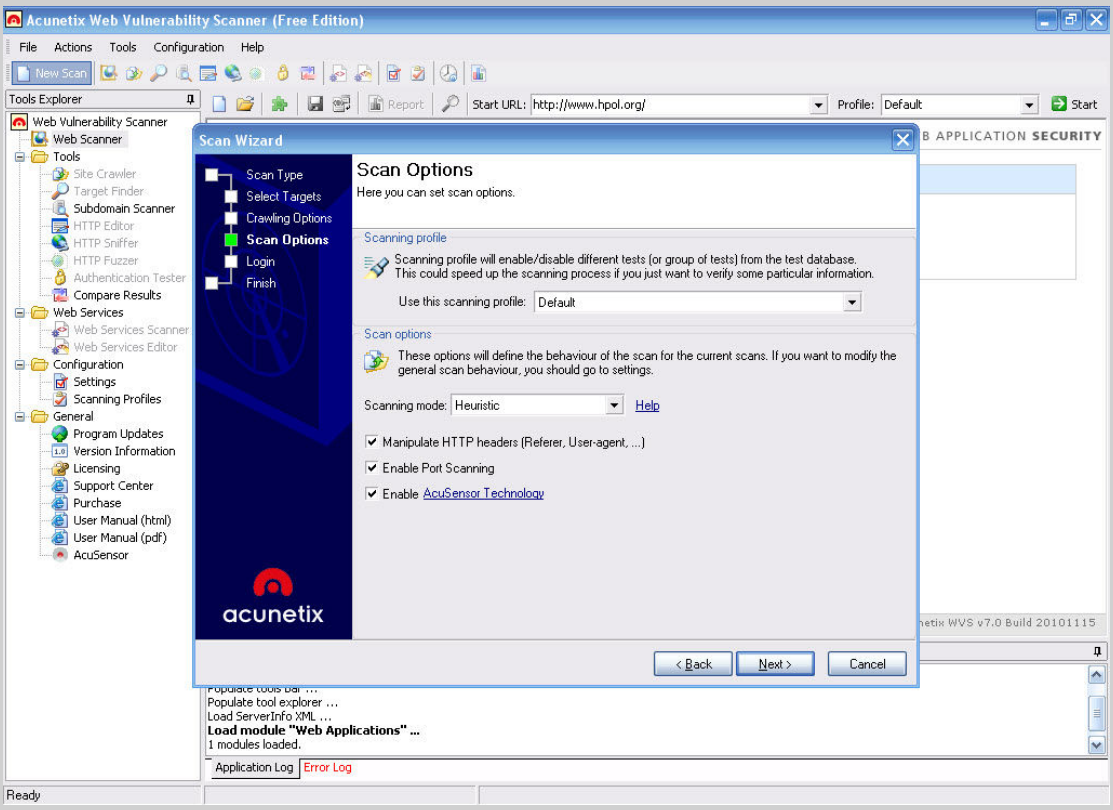
سپس روي دكمه ي Next كليك كنيد تا وارد مرحله ي بعدي شويد!
در اين جا نرم افزار اطلاعاتي از نوع سيستم عامل سايت و نسخه ي وب سرور نصب شده روي آن و ... را به دست مي آورد و به شما نشان مي دهد!



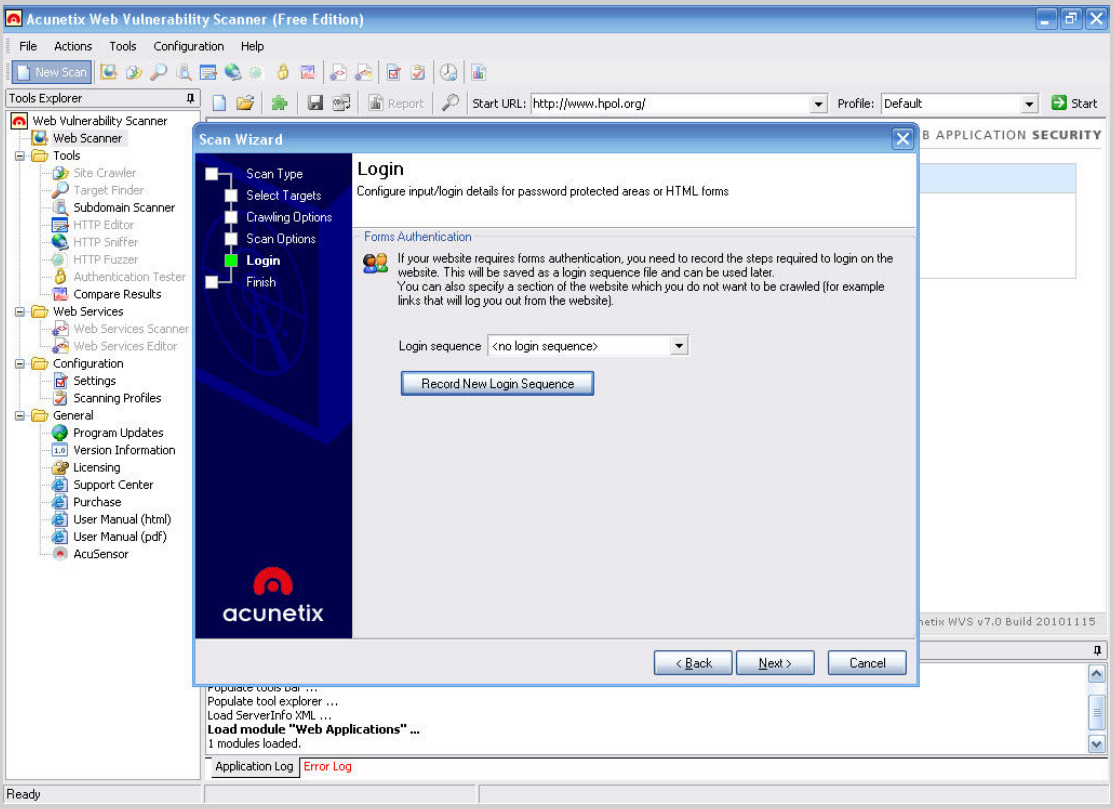
تنظيمات را مطابق شكل انجام دهيد و روي دكمه ي Next كليك كنيد تا وارد مرحله ي بعدي شويد!



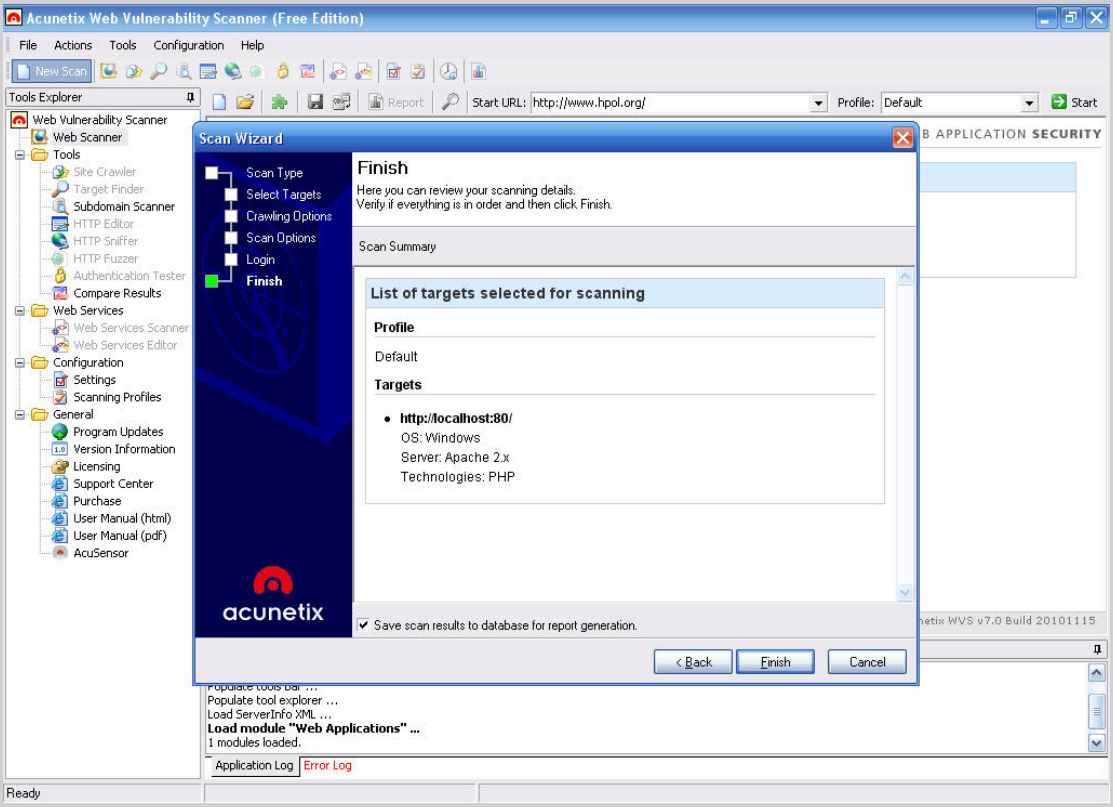
در این مرحله نیز تنظیمات رو مطابق شکل انجام دهید و روي دکمه ي Next کلیك کنید تا وارد مرحله ي بعدي شوید!



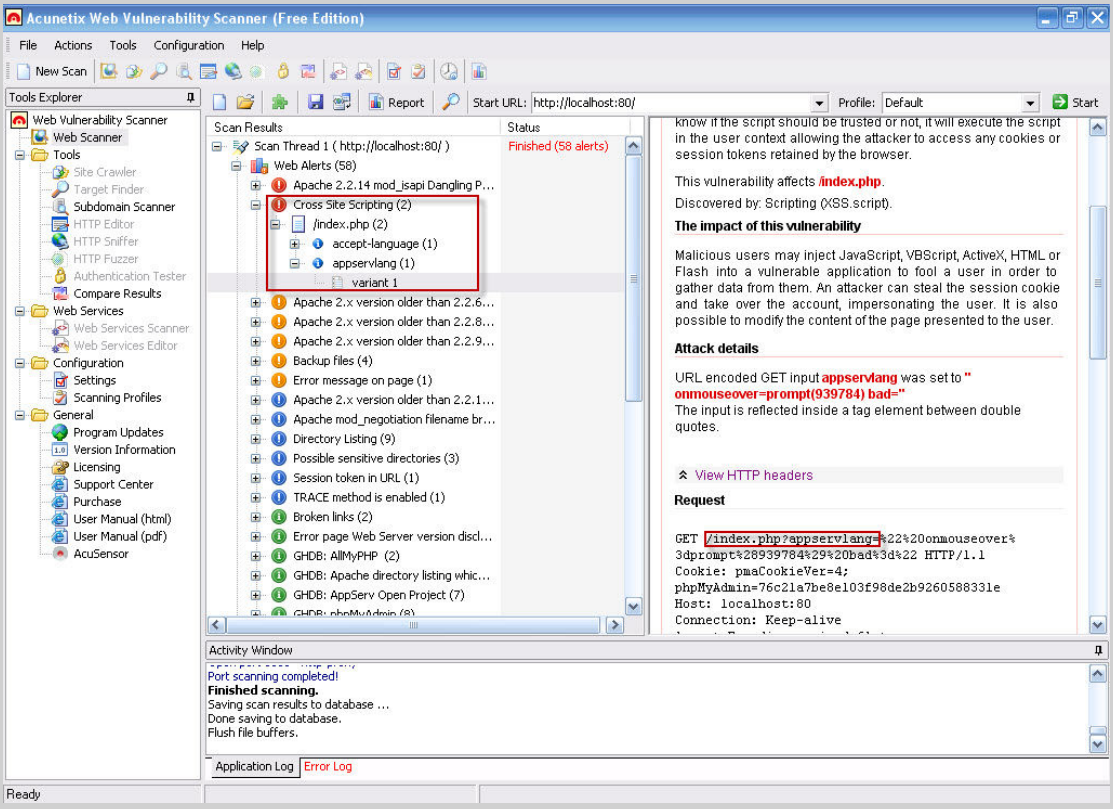
در این مرحله نیز روي دکمه ي Next کلیك کنید تا به مرحله ي بعد بروید!



حالا به قسمت پاياني مرحله رسيديم اكنون روي دكمه Finish كليك كنيد تا عمليات اسكن شروع شود!



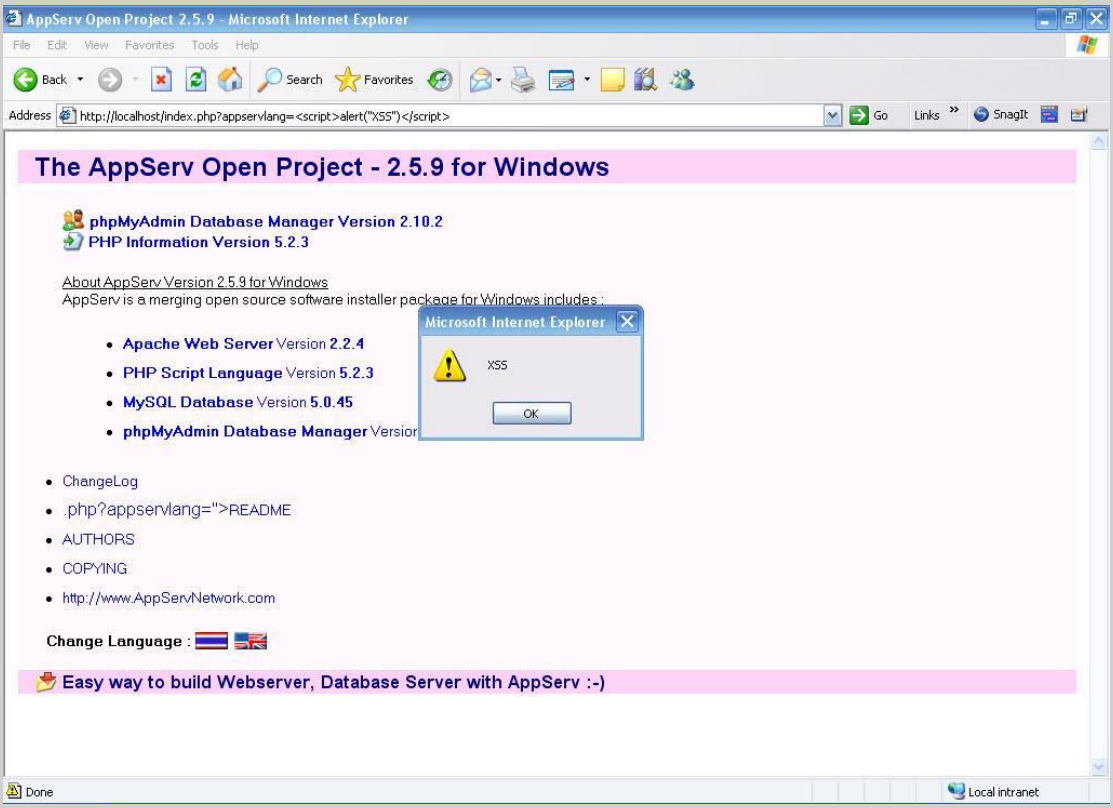
بعد از چند دقيقه اسكنر آسيب پذيري XSS را در سايت مورد نظر پيدا كرده و گزارش داد!



حالا مي رويم كه از صحت اين گزارش مطمئن شويم! براي اين كار ما آدرس تارگت رو به همراه صفحه اي كه باگ در آن گزارش شده است به مرور گر مي دهيم و با تزريق كد:

<script>alert("XSS")</script>

بعد از كلمه ي = يعني در انتهاي آدرس سايت اين آسيب پذيري رو بررسي مي كنيم!



بله! پيغام ظاهر شد بنابراين وجود آسيب پذيري درست گزارش شده است!

(ادامه مقاله در شماره بعد)

آموزش آسيب پذيري SQL Injection (قسمت اول)

مقدمه :

در اين مقاله در مورد جزئيات فنون دستورات SQL Injection و راههايي كه مي توانيم از طريق آنها دستورات SQL را به Applcation ها و Database ها Inject و يا تزريق كنيم , آشنا مي شويم .

آشنايی با مفاهيم پايگاه داده ها :

بسياري از Web Application هاي مدرن براي ذخيره سازي اطلاعات خود از بانكهاي اطلاعاتي استفاده ميكنند.اطلاعات درون بانك هاي اطلاعاتي و يا Database و داخل جداول و يا Table ها ذخيره مي شوند .
پايگاه داده در ساده ترين تعريف به محلي براي ذخيره سازي داده ها به صورت منسجم و ساختاريافته گفته مي شود .براي مديريت پايگاه داده از برنامه هاي رايانه ايي استفاده مي شود كه مديريت و پرسش و پاسخ بين پايگاه‌های را انجام مي دهند كه آنها را مدير سيستم پايگاه داده‌ای يا به اختصار (DBMS) می‌نامند.
يكي از بزرگترين و محبوب ترين Platform ها براي ذخيره سازي اطلاعت در Web (Web Data Source) , SQL مي باشد . در پايگاههاي داده دسترسی به اطلاعات ذخيره شده در جداول از طريق زبان پرس و جوی ساخت يافته يا همان SQL ميسر ميگردد .
از SQL براي ارتباط با يك بانك اطلاعاتي استفاده ميشود . اين زبان كه بر طبق سازمان استاندارد سازي زبانها ANSI American National Standard Institute تنظيم شده است براي مديريت سيستمهاي بانكهاي اطلاعاتي رابطه اي به كار ميرود .

آشنايي با SQL :

SQL به معنای زبان ساخت يافته جستجو يا Structured Query Language ميباشد .با استفاده از اين زبان ميتوان به Database دسترسی داشته و تغييراتي را در داده ها و يا ساختار Database اعمال نمود .بعضی از نرم افزارهاي مديريت بانك اطلاعاتي همچون Access , DB2 , Informix , Oracle , SQL Server , Sybase , Ingres و غيره از اين زبان استفاده ميكنند .
با استفاده از زبان SQL ميتوانيد يكسري جستجو يا Query بر روی Database اجرا نموده و از نتايج آن ها استفاده كرد.
اين جسجو ها ميتوانند برای ذخيره ، بازيابی ، به روز رسانی ، و يا حذف داده ها به كار روند . همچنين يكسري از Query ها را برای انجام مقاصد خاص مثل ايجاد جدول و .. استفاده می كنيم.
دستورات موجود در SQL به چند دسته تقسيم مي شوند :

۱ – DDL
۲ – DCL

DDL و يا Data Definition Language بخش از دستورات SQL مي باشد كه توسط اين دستورات مي توانيم ساختار Database را تغيير دهيم . بخشی از اين دستورات عبارتند از :

CREATE TABLE - ALTER TABLE - DROP TABLE - CREATE INDEX - DROP INDEX

DCLيا Data Control Language بخشي از دستورات SQL است كه به كاربر دسترسي كنترل داده ها (ايجاد ، ويرايش ، حذف)اين دستورات عبارتند از :
CONNECT - SELECT - INSERT - UPDATE - DELETE – USAGE

: SQL Injection

از آنجا كه تمام اطلاعات و داده ها در Database ها ذخيره مي شوند , از اينرو Database ها قلب WebSiteها محصوب مي شوند و از طريق SQL Injection ما مي توانيم به اطلاعات موجود در Database سايت دسترسي پيدا كنيم .
SQL Injection زماني اتفاق مي افتد كه يك حمله كننده و يا يك هكر با توجه به حفره امنيتي كه در Application موجود است , براي Insert و يا وارد كردن يكسري از دستورات SQL به داخل Query ها آماده است و اين كار را بوسيله مديريت و اداره كردن داده هاي ورودي به برنامه انجام مي دهد .

تشخيص Injection :
اولين مرحله در SQL Injection تشخيص آن در Application موجود است . براي اين كار هكر ابتدا مي بايست بعضي مواردي را كه دليل بر وجود خطا در سيستم است را ايجاد نمايد و از خطاهاي نمايش داده شده استفاده نماييد . اگر چه در موارد خود خطا نمايش داده نمي شود , اما هكر مي بايست قدرت تشخيص اين خطا ها را داشته باشد و بتواند از آنها استفاده نمايد .

تشخيص انواع Error :
قبل از عمل SQL Injection ما مي بايست با انواع Error هايي كه ممكن است در حين كار با آنها مواجه شويم , آشنا شويم . يك Web Application مي تواند در مواجه با مشكلات ايجاد شده Error ها را به دو شكل كلي ايجاد نمايد .
اولين نوع Error , خطايي است كه به وسيله Web Server و در اثر يك مشكل توليد مي شود . معمولا SQL Injection هايي كه با استفاده از Syntax اشتباه Inject مي شوند مثل نبستن Quotetion ها , باعث مي شوند كه Application اين نوع از خطاها را برگرداند .
براي جلوگيري از سوء استفاده از اين نوع از Error ها ما مي توانيم از عمليات هايي مانند Redirect به HomePage و يا نمايش يك متن از پيش ساخته به جاي پيغام خطاي اصلي استفاده نماييم .
دومين نوع Error , خطايي است كه به وسيله Application Code ها ايجاد مي شوند . اين نوع از خطا ها به دليل اشتباهات برنامه نويسي Application ها توليد مي شوند .
به عنوان مثال اگر يك Application داشته باشيم كه داراي يك صفحه به نام News.Asp باشد , اين صفحه وظيفه دارد كه يك Id به عنوان ورودي دريافت نمايد و بعد از دريافت مقدار Id , اطلاعات مربوط به Id را از Database دريافت نموده و سپس جزئيات خبر را در صفحه نمايش مي دهد .
حالا اگر Application فقط مقدار Id ورودي را چك كند كه مقداري معتبر و Valid باشد و هيچ بررسي ديگري انجام ندهد , هكر مي تواند از اين اشتباه برنامه نويسي استفاده كند و يك Id را به عنوان ورودي اعلام نمايد كه هيچ رديفي در جدول News براي آن وجود نداشته باشد و در نتيجه يك Record خالي برگشت داده مي شود و هنگاهي كه Application تلاش مي كند كه اطلاعات Record بازگشتي را بررسي نمايد , يك Error توليد مي شود .
يك هكر در ابتدا چندين Invalid Request به سمت Application ارسال مي نمايد تا متوجه شود كه Application چطور با Error ها برخورد مي كند .

مشخص نمودن Error در Page ها
در مرحله بعدي SQL Injection , مي بايست Page ها يي كه در نتيجه دستكاري داده هاي ورودي دچار خطا مي شوند را مشخص نماييم . براي اين منظور ما مي توانيم از كلماتي مانند AND , OR و . . . و همچنين كاراكتر هايي مانند ; و ' استفاده نماييم .
پارامتر هايي آسيب پذير در برابر SQL Injection
SQL داراي چندين نوع داده مي باشد كه به طور كلي به سه دسته تقسيم مي شوند :

۱- Number
۲- String
۳- Date

هر پارامتر ارسال شده از سمت Web Application به سمت SQL يكي از انواع داده مطرح شده مي باشد .مثلا 'Ali' يك داده String و ۵ يك داده Number مي باشد .
تمام پارامتر هاي عددي دقيقا به همان صورتي كه هستند به سمت SQL ارسال مي شوند ولي پارامتر هاي String و Data به در داخل كاراكتر ' به سمت SQL ارسال مي شوند .

```
SELECT * FROM News WHERE NewsId=5

SELECT * FRPM News WHERE NewsTitle='News'
```

پارامتر هايي كه داراي مقدار Number و يا عددي هستند بهترين روش براي تشخيص آسيب پذير بودن يك پارامتر در برابر SQL Injection مي باشند .

```
www.site.com/news.asp?NewsId=10
```

براي تست كردن اين Url مي توانيم از دو راه جهت تشخيص پارامتر هاي آسيب پذير در برابر SQL Injection استفاده كنيم . راه اول استفاده از كاراكتر ' بعد از Id مي باشد و راه دوم نيز استفاده از كاراكتر + مي باشد .

```
SELECT * FROM News WHERE NewsId=10'
SELECT * FROM News WHERE NewsId=9+1
```

اجراي اولين SQL Query يك خطا مبني بر اينكه ساختار دستور SQL دچار مشكل است را نمايش مي دهد , ولي دستور دوم بدون Error اجرا مي شود . و اين مورد نشان مي دهد اين پارامتر داراي آسيب SQL Injection مي باشد و ما توانسته ايم به وسيله دستورات خود SQL را مديريت نماييم .
دقيقا از همين دستورات مي توانيم جهت تست پارامتر هاي String نيز استفاده نماييم .

```
www.site.com/news.asp?NewsTitle='News'

SELECT * FROM News WHERE NewsTitle='News''
SELECT * FROM News WHERE NewsTitle='New'+'s'
```

اجراي اولين SQL Query يك خطا مبني بر اينكه ساختار دستور SQL دچار مشكل است را نمايش مي دهد , ولي دستور دوم بدون Error اجرا مي شود . و اين مورد نشان مي دهد اين پارامتر داراي آسيب SQL Injection مي باشد و ما توانسته ايم به وسيله دستورات خود SQL را مديريت نماييم .
بنابراين تشخيص اين كه پارامتر داراي آسيب SQL Injection مي باشد و يا خير ساده مي باشد حتي اگر پيغام خطايي نمايش داده نشود .

(ادامه مقاله در شماره بعد)

امنیت ایمیل (قسمت اول)

۹۷ روش برای امنیت بیشتر و نگارش بهتر ایمیل :

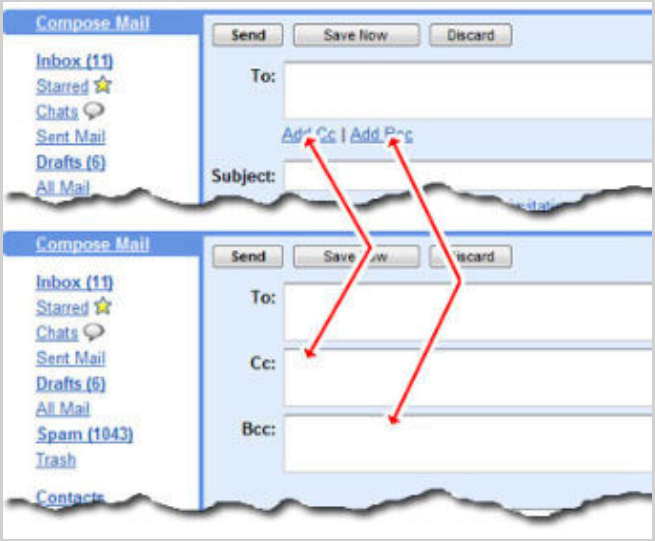
اینترنت در واقع دنیایی مجازی است و مانند هر جای دیگر اصول و قوانین خاص خود را دارد. تقریبا همه می‌دانیم رعایت مجموعه‌ای از نکات هنگام سیروسفر در این دنیای مجازی ضروری است. حدود ۶ میلیارد ایمیل در طول روز در کل جهان رد و بدل می‌شود که تقریبا اکثرشان بر اساس آئین معاشرت اینترنتی تهیه نشده‌اند .
فراگرفتن این اصول که نتیکت نام دارند، برقراری ارتباط با سایر افراد در اینترنت را برای کاربران آسان‌تر و امنیت‌شان را تضمین می‌کند.
کلمه «نتیکت (netiquette) «از ترکیب دو واژه شبکه (network) و آداب معاشرت (etiquette)به دست آمده است. آن را در واقع میتوان مجموعه‌ای از قراردادهای اجتماعی دانست که تعاملات صورت گرفته میان کاربران را در شبکه‌های مختلف اینترنت از جمله سرویس‌های بحث و گفت‌وگو، ایمیل، وبلاگ و فروم ساده‌تر می‌کند. برای آگاهی بیشتر، برخی از این روش‌ها در ادامه آورده شده‌اند. رعایت آنها برای شما امنیت بالاتر، برخورد حرفه ای تر و روابط مثبت تر به همراه خواهد شد.

هرگز از ایمیل کاری، استفاده شخصی نکنید :

اگر می‌خواهید از محل کار ایمیل شخصی بفرستید، بهتر است از حساب‌های کاربری شخصی خود در یاهو، جیمیل یا هاتمیل استفاده کنید، البته اگر قوانین شرکت تان این اجازه را به شما می‌دهد. در این صورت، کارفرما به محتویات ایمیل و پیغام‌های خصوصی شما دسترسی ندارد و آنها محرمانه باقی می‌مانند.

در صورت نیاز از Blind Carbon Copy استفاده کنید :

اگر در نظر دارید ایمیلی را برای افراد مختلف بفرستید که یکدیگر را نمی‌شناسند، بهتر است از BCC استفاده کنید . BCCمخفف واژه انگلیسی Blind Carbon Copy به معنای رونوشت مخفیانه است. با این کار دست اسپمرهای فرصت‌طلب را از آدرس ایمیل دوستان‌تان کوتاه می‌کنید. همچنین باعث می شوید که افرادی که یکدیگر را نمی شناسند و یا قرار نیست با هم در ارتباط باشند، ایمیل همدیگر را نداشته باشند.



نامه های زنجیره ای را Forward نکنید:

لطفا خرافه پرستی را کنار بگذارید و ایمیل های زنجیره ای را که به طور مثال در آنها نوشته شده است اگر این نامه را برای ۱۰ نفر ارسال کنید حتما تا آخر امروز خبری خوش خواهید شنید، یا آرزویتان برآورده خواهد شد را برای دیگران فوروارد نکنید. کاملا واضح است که این ایمیل‌ها ارزش فکر کردن هم ندارند چه برسد به ارسال. پس امنیت خود را به خطر نیندازید. و ایمیل های خود و دوستان تان را به این لیست خوشمزه مورد نظر اسپمرها اضافه نکنید.

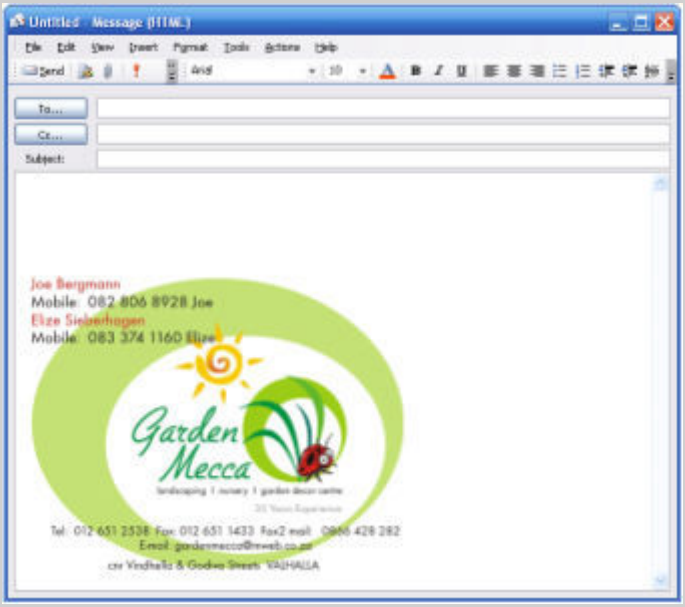
هنگام نگارش نامه بهتر است قبل از هر چیز به نوع رابطه خود و گیرنده ایمیل و اینکه چقدر با هم دوست و صمیمی هستید، توجه داشته باشید. این کار به شما در انتخاب موضوع و عنوان مناسب کمک شایانی می‌کند .

نام کاربری ایمیل ها در مسایل کاری اهمیت به سزایی دارند. بهتر است نام مناسبی برای ایمیل کاری خود انتخاب کنید. به طور مثال از انتخاب اسم یا واژه‌های کودکانه، کارتونی یا غیر رسمی اجتناب کنید .

ایمیل، یک حرف شفاهی ساده و یا نامه کاغذی نیست. ممکن است به راحتی به گیرنده‌های مختلف ارسال شود. شاید تا مدت‌های طولانی در inbox گیرنده باقی بماند و به عنوان نقل قول برای فرستند دوباره ارسال شود. پس حتما قبل از ارسال هر نامه ای خوب فکر کنید تا بعدها از ارسالش پشیمان نشوید. ممکن است متن ایمیل تان در آینده علیه خودتان استفاده شود .

امضای انتهای نامه کوتاه باشد :

امضای انتهای نامه ها و ایمیل های رسمی و اداری اصولا به صورت چند خطی نوشته میشوند. این خطوط شامل اسم، سِمت، شماره تلفن و ... هستند. این فرمت کلی آنها است. اما ایمیل های شخصی فرق دارند. نحوه صحیح امضا در انتهای این گونه نامه ها این است که تا حد امکان کوتاه باشد. زیرا چندان جالب نیست که بر فرض مثال نامه دو خطی را با امضای ۵ خطی تمام کنیم !



نقل قول از فرستنده :

حتما متوجه شده اید که هنگام پاسخگویی یا به اصطلاح reply کردن نامه، متن فرستنده نیز در پایین آن آورده میشود. اصول نتیکت میگوید فقط قسمت هایی را که قرار است به آنها پاسخ دهید را از ایمیل اصلی Cut و همراه با علامت '>' در نامه خود paste و بقیه متن را پاک کنید .

شفاف سازی کنید :

بیشتر اوقات نامه های الکترونیک بیانگر احساس واقعی نویسنده (مخصوصا در مورد شوخی و مزاح) نیستند. شاید شما جمله‌ای را به شوخی برای دوست تان می نویسید، اما او تصور میکند عصبانی یا ناراحت هستید. پس با دقت بیشتری واژه هایتان را انتخاب کنید .

برای دوستان تان اسپمر نشوید :

گاهی پیش می آید که مِیل سرور درست کار نمیکند و به اشتباه یک ایمیل را مثلا ۱۰ بار برای گیرنده می فرستد. این تقصیر شما نیست و گاهی این اتفاق ها می افتند. اما مودبانه تر این است که از دوست، همکلاس، همکار یا فامیلتان صمیمانه برای این اتفاق عذرخواهی کنید .

انواع مختلف سیستمهای ایمیل را بشناسید :

هر کاربری باید حداقل مطالعه‌ای سطحی در مورد نحوه عملکرد سرویس های مختلف ایمیل همچون یاهو، جیمیل و هاتمیل داشته باشد. البته شاید این کار کمی مشکل به نظر برسد، اما امکان بروز مشکلات احتمالی را به طور چشمگیری کاهش میدهد. به طور مثال شما کاربر هاتمیل هستید و میخواهید فهرستی از لینکهای مختلف را برای دوستتان بفرستید، اگر ندانید که Hotmail در این زمینه - یعنی کپی - URL عملکرد ضعیفی دارد، حتما با مشکل روبهرو خواهید شد .

به همه ایمیل های گروهی پاسخ ندهید :

شرکت نکردن در بحث های گروهی و دور ماندن از خطرات احتمالی، یکی از راههای حفظ امنیت است. البته بهتر است ایمیل دریافتی را به دقت مطالعه کنید و مطمئن شوید که به طور مستقیم مورد خطاب قرار نگرفته اید و نیازی به پاسخ گویی نیست .

به قوانین و ضوابط احترام بگذارید :

هر کشوری و سایتی قوانین خاصی برای ارسال نامه های الکترونیک به خصوص در حجم بالا دارد. اگر کاربری به منظور ترویج و تبلیغ کار و تجارت خود اقدام به ارسال ایمیل به تعداد زیاد میکند، نه تنها باید قوانین کشور خود، بلکه هر جایی که مقصد نامه است را رعایت کند و به آنها احترام بگذارد. این کار شاید به نظر کمی مشکل باشد اما اهمیت بسیاری دارد و باید به آن توجه داشت .

عنوان ایمیل باید معنی دار باشد :

بعضی از ایمیل ها عنوان و موضوع فریبنده ای دارند. پس حتما در نظر داشته باشید که موضوعی که برای ایمیل انتخاب میکنید نمایانگر محتویات آن باشد .این کار در واقع کلید راهنمایی برای مخاطب است که بداند نامه در مورد چیست و بتواند آن را از اسپمها یا بدافزارها تشخیص دهد .

در صورت نیاز از گزینه « Reply to All » استفاده کنید :

اصولا همه معتقدیم که نیازی نیست ایمیلهایمان را برای همه آدرسهای موجود در لیست مخاطبین ارسال کنیم. این نوع تفکر کاملا صحیح است. اما گاهی لازم است بیشتر مخاطبین از پیغام شما آگاه شوند که در این صورت بهترین راه، استفاده از گزینه «ارسال برای همه» است زیرا علاوه بر صرفهجویی در وقت، احتمال از قلم افتادن آدرسهای مورد نظر نیز کم خواهد شد .

(ادامه مقاله در شماره بعد)

آموزش PHP (قسمت اول)

مقدمه :

شبکه گسترده جهانی یا به عبارتی Word Wide Web دنیاي عجیبی است که تکنولوژیهاي مربوط به آن، اغلب بدون پشتیبانی کافی عرضه می شوند و کاربران این تکنولوژي ها، همه روزه با واژگان جدیدي برخورد می کنند،که باعث سردرگمی آنها می شوند.
براي نمونه می توان به رشد نرم افزارهاي open source اشاره کرد (برنامه هایی که می توان آنها را گسترش داد و یا تغییراتی در ساختار آنها ایجاد کرد.) متداولترین این برنامه ها، سیستم عامل Unix و به طور خاص Linux می باشد. این برنامه ها، با وجود ثبات و پایداري، داراي مشکل بزرگ می باشند و آن دشوار بودن آموختن این برنامه ها می باشد .کمبود راهنماهایی که به زبان ساده، این برنامه ها را به مبتدیان آموزش دهد، باعث شده است که این دسته از نرم افزارها از جایگاه واقعی خود دور نگه داشته شوند.
در ادامه این مقاله با زبان PHP آشنا خواهیم شد .با استفاده از این مقاله شما دانش کافی براي آغاز به کارایجاد سایت هاي پویا توسط PHP را کسب خواهید نمود .

تاریخچه مختصري از PHP :

فکر اولیه PHP در پاییز سال ۱۹۹٤ توسط Rasmus Lerdorf شکل گرفت . در ابتدا نگارشی از PHP در صفحه شخصی وي به کار گرفته شد تا اطلاعاتی از کسانی که روزمره او را می بینند نگاه داشته شود . اولین نگارش عمومی آن در اوایل سال ۹۵ ارائه شد و با نام " **P**ersonal **H**ome **P**age Tools " روانه بازار شد که البته شامل پارسري بسیار ساده بود که ماکروهاي خاصی را می شناخت و نیز برخی کاربردهاي مشترك در صفحات شخصی از قبیل شمارنده ، دفتر میهمانان و برخی از ابزارهاي دیگر را به همراه داشت.
پارسر در نیمه سال 95 بازنویسی شد و با نام PHP/FI "نگارش ۲" ارائه گردید. FI نام بسته نرم افزاري دیگري از Rasmus بود که فرم هاي داده HTML را تفسیر می کرد . پس از آن وب مسترهاي بسیاري از PHP در صفحات خود استفاده کردند . در میانه سال 96 میزان استفاده کنندگان به حدود 15 هزار سایت رسید . این میزان در نیمه سال 97به 50 هزار سایت مختلف افزایش پیدا کرد . در این زمان PHP از حالت یک پروژه شخصی درآمد و نیمه سال 97 به 50 هزار سایت مختلف افزایش پیدا کرد . در این زمان PHP از حالت یک پروژه شخصی درآمد و توسط تیمی توسعه یافت . این گروه نگارش جدیدي از PHP را ارائه دادند و پارسر آن را بازنویسی نمودند و بسیاري از مشکلات اساسی آن را برطرف کردند. PHP3 به سرعت مورد استفاده قرار گرفت . هم اکنون نیز PHP4 آخرین نگارش این محصول است که در آن از موتور اسکریپت Zend براي بدست آوردن قابلیت هاي بیشتر استفاده شده است .
امروزه PHP3 و PHP4 بر روي بسیاري از محصولات تجاري مانند RedHat's Stronghold WEB SERVER ارائه می گردد .هم اکنون برآورد می شود بیش از 6 میلیون سایت از PHP استفاده کرده اند که این میزان کمی بیشتر از تمامی سایت هایی است که از سرور IIS مایکروسافت استفاده می کنند .

چرا PHP ؟

گذشته از اینکه PHP یک زبان Open Source یا منبع باز است ، دلایل بسیار زیاد دیگري براي انتخاب PHP براي ایجاد محتواي محاوره اي بر روي سایت هاي وب وجود دارد.
یکی از این دلایل این است که این زبان ساختار و ترکیبی بسیار شبیه زبان C دارد.

نوع داده ها و ساختار هايPHP به آسانی آموخته و به کار گرفته می شوند . در واقع می توان گفت PHP ميداند منظور شما چيست و نوع داده هاي خود را بر اساس اطلاعات شما تغيير می دهد.
نيازي به دانستن دستور خاصی براي کامپايل برنامه نداريد . برنامه شما در مرورگر اجرا می شود ولازم نيست براي شروع برنامه و نوشتن برنامه هاي کاربردي درباره PHP اطلاعات زيادي داشته باشيد.
PHP سرويسی از مجموعه فايلهاي کتابخانه اي C را ارائه می دهد که به آسانی درون زبان قرار گرفته و با انعطاف بسيار به آن قابليت پاسخ دهی سريع براي تغييرات در وب را می دهد.
آنچه می توانيد شما با PHP انجام دهيد ، با ديگر زبانها نيز قابل انجام است . اما PHP براي کار کردن در زمينه وب طراحی شده است . بنابراين کارهاي مشکل و خسته کننده اي که برنامه نويسان با Perl انجام می دادند ، به آسانی با PHP قابل انجام است.
اين زبان پويا وب سايت ها را قادر می سازد تا با سرعت مبهوت کننده اي گسترش يابند و اين عامل يکی ازدلايل عمده اي است که براي صفحات پويا و پشتيبانی پايگاه داده ها در نظر گرفته شده است . همانطور که گفته شد در حدود 6 ميليون سايت در سراسر وب از PHP استفاده می کنند.
کدهاي کوچک توکار در يک صفحه وب بسيار کارآمدند . به عنوان مثال در يک صفحه ايستا ، ممکن استشما مقدار يک متغير را بدست آوريد و سپس آن را براي ايجاد تغييرات در محتواي صفحه ، تغيير بدهيد . اما در PHP مقادير متغير ها مستقيما در سورس صفحه يافت نمی شود . به اين مثال توجه کنيد :

```
<?php
$browser = getenn("HTTP_USER_AGENT");
?>
<p>You are using the <?php echo($browser);?> web browser .
</p>
```

در اين مثال به جاي عبارت متغير ، نام مرورگر وب کاربر در صفحه نمايش داده خواهد شد .

PHP زبانی براي همه سيستم عامل ها :

يکی از برترين مزاياي زبان PHP سازگاري آن با اکثر سيستم عامل ها و نرم افزارهاي وب سرور (مانند IIS و Apache) است .برخی از ديگر زبان ها و تکنولوژي ها مانند ASP محدود به سيستم عامل windows است و پشتيبانی از آن در ديگر سيستم عامل ها بسيار پرهزينه و محدود است، و برخی نيز مانند JSP مشکلاتی با برخی نرم افزارهاي وب سرور دارد.
ساختار و امکانات پی اچ پی به شکل مستقل از سيستم عامل شکل گرفته است و اين بدان معنا است که بهطور مثال برنامه هنويس می تواند اسکريپت خود را تحت سيستم عامل ويندوز نوشته و تست کند و سپس آنرا بدون تغيير به سيستم عامل يونيکس يا لينوکس انتقال دهد.
در PHP امکان استفاده از برخی از امکانات خاص سيستم عامل هاي مشهور نيز در نظر گرفته است که براي نمونه می توان از پشتيبانی از تکنولوژي DCOM و يا Windows API نام برد.
نسخه هاي جديد مفسر PHP سازگار با ديگر تکنولوژي هاي خاص وبسرورها مانند ISAPI نيز می باشد.

PHP رايگان و Open Source :

تهيه برنامه مفسر PHP براي همه سيستم عامل ها رايگان است و علاقه مندان می توانند آخرين نسخه مفسر اين زبان را از سايت رسمی PHP بارگذاري کند.
همچنين امکان تهيه رايگان سورس مفسر پی اچ پی نيز فراهم است ، و اين مسئله علاوه بر اين که در گسترش امکانات اين زبان بسيار موثر بوده است، مزيتی براي شرک تها و توسع هدهندگان براي انتخاب اين زبان است چرا که پشتيبانی و اعتماد به آن را راحت تر کرده است.
بسياري از ويرايشگرهاي حرفه اي اين زبان نيز يا رايگان هستند و يا با هزينه بسيار کم می توان آنها را تهيه کرد، در حالی که ديگر تکنولوژي ها ، مثلا پلاتفورمهاي جاوا هزينه هنگفتی دارد و همچنين کار حرفه اي با تکنولوژي .NET نيز نياز به تهيه Visual Studio.NET و پرداخت هزينه چند صد دلاري است.

سرعت بالاي تفسير و اجراي PHP :

پی اچ پی یکی از سریع ترین زبان ها در نوع خود است .تفسیر و اجراي یک اسکریپت php به طور متوسط تا سه و چهار برابر یک اسکریپ ASP است (البته باید در نظر داشته باشیم که IIS با Cach اسکریپت های ASP سرعت اجراي آنها را در دفعات بعد بالا می برد)
همچنین در ASP استفاده زیادی از اشیا COM می شود که باعث کاهش سرعت و مصرف منابع سیستم می شود در حالی که در PHP بسیاري از امکانات و حتی برقراري ارتباط با یکی محبوب ترین نرم افزار مدیریت بانک هاي اطلاعاتی mySql به صورت توکار نهاده شده است.
شرکت Zend که تهیه کننده فعلی موتور مفسر و پشتیبانی کننده آن است، محصولات دیگري را نیز در جهت بهینه کردن سرعت اجراي PHP ارائه کرده است این محصولات با افزایش سرعت تفسیر و همچنین ذخیره کردن نتیجه تفسیر (Cash) باعث افزایش چندین برابر اجراي آن می شوند.

آموزش MySQL (قسمت اول)

مروری بر پایگاه داده MySQL :

- سیستم مدیریت پایگاه داده MySQL :

Mysql پرکاربردترین سیستم مدیریت پایگاه داده sql متن باز است که توسط شرکت mysql ab پشتیبانی می شود.
Mysql ab شرکتی تجاری است که توسط توسعه دهندگان mysql تاسیس شده است، و دومین شرکت تولید محصولات متن باز با یک مدل تجاری موفق است. آخرین اطلاعات در مورد mysql و mysql ab را می توان از وب گاه http://www.mysql.com بدست آورد.
MYSQL یک سیستم مدیریت پایگاه داده است.
پایگاه داده مجموعه ای از داده های ساخت یافته است. برای اضافه کردن ، دسترسی و پردازش داده های ذخیره شده در پایگاه داده، رایانه نیاز به یک سیستم مدیریت پایگاه داده کارساز mysql دارد. در رایتنه هایی که روی حجم زیادی از دهده ها کار می کنند، سیستم مدیریت پایگاه داده نقشی مرکزی را در محاسبات ایفا می کند.
Mysql یک سیستم مدیریت پایگاه داده رابطه ای است.
پایگاه داده رابطه ای ، داده را به جای ذخیره در یک مکان بزرگ ، در جداول جداگانه ذخیره میکند که باعث افزایش سرعت و انعطاف پذیری می شود. Sql بخشی از mysql و زبان استاندارد mysql است که توسط ansi/iso sql تعریف شده است.
Mysql نرم افزاری متن باز است.
منظور از متن باز این است که هرکسی می تواند آن را توسعه و تغییر دهد. هرکسی می تواند آن را از اینترنت بدون پرداخت هیچ وجهی دریافت نماید. هر فردی می تواند متن آن را مطابق با نیاز خود تغییر دهد. Mysql دارای یک GPL است که مشخص می کند در چه جاهایی می توان و در چه جاهایی نمی توان ای این ابزار استفاده نمید.
کارساز پایگاه داده mysql بسیار سریع، انعطاف پذیر و استفاده از آن آسان است.
Mysql بصورت کارساز/کارخواه استفاده میشود.
زبانها برنمه های کاربری بسیاری امکان استفاده از پایگاه داده mysql را فراهم می کنند.

- ویژگی های اصلی پایگاه داده mysql :

از جمله ویژگیهای مهم پاایگاه داده mysql می توان به موارد زیر اشاره کرد:
با زبانهای برنامه نویسی c و c++ نوشته شده است.
با کامپایلرهای مختلف زیادی تست شده است.
در بسترهای مختلف امکان استفاده از آن وجود دارد
از GNU Automake, Autoconf و Libtool برای قابلیت حمل استفاده می کند.
دارای تعدادی API برای Tcl, C, C++ , Eiffel, Java, Perl, PHP, Python, Ruby است.
با استفاده از پردازش های kernel ، به طور کامل چند پردازه شده است و می تواند در صورت وجود چندین CPU استفاده کند.
از جدوال درخت باینری خیلی سریع، با ایندکس فشرده شده استفاده میکند.
به آسانی امکان استفاده از موتور ذخیره اضافی را میدهد.
دارای یک سیستم تخصیص حافظه خیلی سریع است.
در حافظه از جداول هش به عنوان جداول موقتی استفاده میکند.

توابع SQL بکار برده شده از کتابخانه ای سریع ، استفاده می کنند.
کد Mysql به خوبی تست شده است.
کارساز آن به صورت یک برنامه جداگانه برای استفاده در محیطهای شبکه کارساز/کارخواه موجود است.
انواع فیلدها را پشتیبانی می کند.
انواع رکورد با طول ثابت و طول متغیر را پشتیبانی می کند.
مملو از تابع و عملگر برای استفاده در پرس و جوها است.
GROUP BY و ORDER BY را بطور کامل پشتیباین میکند
LEFT OUTER JOIN و RIGHT OUTER JOIN را هم برای SQL استاندارد و هم برای ساختار ODBC پشتیبانی می کند.
آلیاس برای جدول و ستون، مورد نیاز SQL استاندارد را پشتیبانی می کند.
در هنگام استفاده از عبارات ELITE,INSERT,REPLACE و UPDATE تعداد ردیفهایی را که تغییر کرده اند را بر می گرداند.
دستور SHOW مخصوص Mysql بوده و امکان کسب اطلاعات در مورد پایگاه داده، جداول و ایندکس ها را می دهد.
توابع، جداول و ستونها در نام با هم تداخل ندارد.
در یک پرس و جو می توان جدئوال پایگاه داده های مختلف را با هم ترکیب کرد.
دارای یک سیستم کلمه عبور اانعطاف پذیر و امن است.
امکان بکارگیری پایگاه های داده بزرگ را می دهد. هر پایگاه داده می تواند ۵۰ میلیون رکورد داشته باشد، و کارساز Mysql می تواند ٦۰ هزار جدول به همراه ۵ میلیارد ردیف را پشتیبانی کند.
بالای ٦٤ ایندکس در جدول می توان ایجاد کرد . هر ایندکس می تواند شامل ۱ تا ۱٦ ستون و یا بخشی از یک ستون باشد. حداکثر عرض ایندکس ۱۰۰۰ بایت می تواند باشد.
کارخواه می تواند با استفاده از سوکتهای TCP/IP تحت هر بستری با کارساز ارتباط برقرار کند.
در ویرایش های بالاتر از ٤,۱ کارسازهای ویندوزی نیز امکان ارتباط های shared-memory را فراهم می کنند.
برنامه های کارخواه که از ODBC استفاده می کنند می توانند از Connector/ODBC (MYODBC) برای پشتیبانی از MYSQL استفاده کنند. برای مثال شما می توانید از Ms ACCESS برای اتصال به کارساز mysql استفاده کنید.
برنامهای کارخواه جاوا که از JDBC استفاده می کنند برای مپشتیبانی از MYSQL می توانند از Connector/J استفاده کنند.
کارساز می تواند پیغامهای خطا را با زبانهای مختلف برای کارخواهان نمایش دهد.
مجموعه نویسه های مختلف را پشتیبانی می کند.
همه داده ها با همان مجموعه نویسه انتخاب شده انجام می شود.
مجموعه نویسه های مختلف را پشتیبانی می کند
همه داده ها با همان مجموعه نویسه انتخاب شده ذخیره می شوند.
مرتب سازی بر اساس همان مجموعه نویسه انتخال شده انجام می شود.
کارساز mysql امکان چک کردن بهینه سازی و تعمیر جدوال را میدهد، برای این کار می توان از دستور mysqlcheck استفاده کرد.
رهنمای همه برنامه های mysql را میتوان با استفاده از help– و ؟- بدست آورد.
هر جدول در mysql ۳,۲۲ حداکثر ٤ گیگا بایت می توانست باشد. توسط موتور ذخیره myasm این فضا در ۳,۲۳ mysql ۸ میلیون ترابایت افزایش یافت. موتور ذخیره InnoDB امکان ذخیره جداول InnoDB را درون یک فضای جدولی تشکیل شده از چندین فایل مختلف را میدهد. حداکثر اندازه این فضای جدولی 64TB می تواند باشد.
جداول زیر محدودیت اندازه جدول در هر سیستم عامل را مشخص می کند :

حداکثر اندازه فایل	سیتم عامل
2GB (LFS:4GB)	Linux 2.2-intel 32-bit
(using ext3 filesystem)4TB	Linux 2.4
16TB	Solaris 9/10
8TB	NetWare w/NSS filesystem
2GB/4GB	Win32 w / fat/fat32
2TB (possibly larger)	Win32 w / NTFS
2TB	MacOS X w/ HFS+

جدول ۱-۱ محدودیت اندازه جدول در هر سیستم عامل

- **طرح توسعه MySQL :**

جدول زیر حاوی طرح توسعه MySQL در ویرایش های مختلف است :

ویژگی	
Unions	4.0
Subqueries	4.1
R-trees	4.1(for myisam tables)
Stored produres	5.0
Views	5.0
Cursors	5.0
Foreign key	5.1 (already implemented in 3.23 for InnoDB)
Triggers	5.0 and 5.1
Full outer join	5.1
Constraints	5.1

آموزش C# (قسمت اول)

درس اول آغاز کار با C# :

در این در س با ارائه چند برنامه و مثال ساده به طرز کار C# می پردازیم.اهداف این درس عبارتند از:

۱. فهم ساختار پایه ای یک برنامه C#
۲. آشنایی با Namespace
۳. آشنایی با مفهوم کلاس (Class)
۴. آشنایی با عملکرد متد Main()
۵. آشنایی با ورودی /خروجی یا IO

لیست ۱-۱، یک برنامه ساده با عنوان Welcome در زبان C# :

```
//namespace اعلان
Using system;
//کلاس آغازین برنامه
Class WElcomeCSS
{
Public static void Main()
{
// نوشتن متن در خروجی
Console.writeline("Welcome to C#");
}
```

برنامه لیست ۱-۱ دارای چهار پارامتر اصلی است.اعلان Namespace ،کلاس ، متد Main() و یک دستور زبان C# .
در همین جا باید به یک نکته اشاره کنم،برای زبان C# همانند بیشتر زبان های برنامه سازی دو نوع کامپایلر وجود دارد.یک نوع کامپایلر که به کامپایلر Command line معروف است و نوع دیگر کامپایلر Visual است.کامپایلر های Command Line محیطی شبیه به محیط DOS دارندو با دادن یک سری دستورات به اجرا در می آیند.کامپایلر های Visual محیطی همانند ویندوز دارند که با دارا بودن محیط گرافیکی و ابزار های خاص ، برنامه نویسی را در امر برنامه سازی کمک می کند.از نمونه های هر یک از کامپایلر ها می توان ،Microsoft C# Command line Compiler که یک کامپایلر Command Line و Microsoft Visual C# که که یک کامپایلر Visual است ، اشاره کرد.
البته در حال حاضر بیشتر از کامپایلر های Visual استفاده می شود.
من در آینده سعی می کنم به توضیح محیط Visual C# و Visual studio.Net بپردازم.
اما فعلا برای اجرای برنامه ها می توانید از Visual Studio.Net استفاده کنید.پس از نصب آن وارد محیط C# شده و در قسمت انتخاب برنامه جدید گزینه Console را جهت اجرای برنامه ها انتخاب نمایید.

در این درس ، فعلا برای توضیح بیشتر درباره محیط ویژوال نمی پردازم اما در آینده به توضیح کامل محیط Visual Studio.NET خواهم پرداخت.
برای اجرای کد بالا در صورتی که از محیط ویژوال استفاده می کنید باید بر روی دکمه RUN کلیک کنید و در صورتی که کامپایلر Command Line دارید با دستور زیر می توانید برنامه را اجرا کنید .

```
Csc welcome.cs
```

پس از اجرای برنامه ،کامپایلر برای شما یک فایل قابل اجرا (Executable) تحت نام welcome.exe تولید می کند.
نکته:در صورتی که از Visual Studio.Net(VS.Net) استفاده کنید، پس از اجرای برنامه ، یک صفحه برای نمایش خروجی به سرعت باز شده و بسته می شود و شما قادر به دیدن خروجی نخواهید بود . برای این که بتوانید خروجی برنامه را ببینید در انتهای برنامه دستور زیر را وارد نمایید .

```
Console.ReadLine();
```

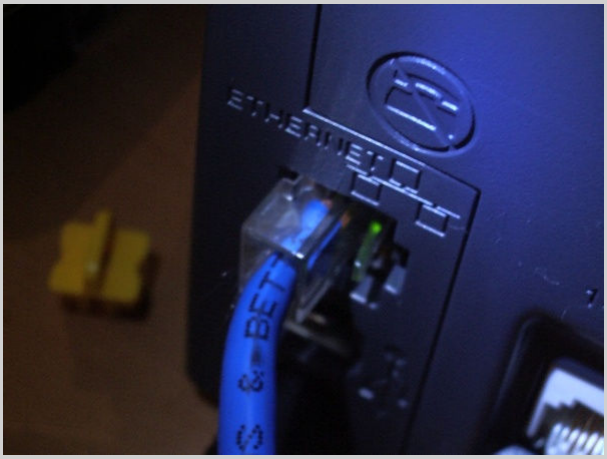
استفاده از این دستور باعث می شود تا برنامه منتظر دریافت یک ورودی از کاربر بماند ، که در این حالت شما می توانید خروجی برنامه خود را دیده و سپس با زدن کلید Enter برنامه خاتمه بدهید.
نکته دیگری که در مورد زبان برنامه نویسی C# باید مورد توجه قرار بدهید این است که این زبان Case Sensitive است.بدین معنا که به حروف کوچک و بزرگ حساس است یعنی برای مثال ReadLine با readline متفاوت است به طوری که اولی جزو دستورات زبان C# و دومی به عنوان یک نام برای متغیر یا یک تابع که از طرف کاربر تعریف شده است در نظر گرفته می شود.
اعلان namespace به سیستم اعلان می نماید که شما از توابع کتابخانه ای System جهت اجرای برنامه های خود استفاده می نمایید.دستوراتی مانند ReadLine و WriteLine جزو توابع کتابخانه ای System می باشند.اغلب دستورات و توابع مهم و کلیدی استفاده از کنسول ورودی/خروجی در این کتابخانه می باشد.در صورتی که در ابتدای برنامه از using System استفاده نکنید ، باید در ابتدای هر یک از دستورات برنامه که مربوط به این کتابخانه است از کلمه System استفاده نمایید.
به عنوان مثال در صورت عدم استفاده از using System باید از دستور System.Console.WriteLine() به جای Console.WriteLine() استفاده نمایید.
تعریف کلاس ، Class Welcome CSS شامل تعریف داده ها(متغیر ها) و متد ها جهت اجرای برنامه است.یک کلاس جوز معدود عناصر زبان C# است که به وسیله آن می توان به ایجاد یک شی (object) از قبیل واسط ها (interfaces) و ساختار ها(Structures) پرداخت.توضیحات بیشتر در این زمینه در درس های آینده ذکر می شود.در این برنامه کلاس هیچ داده یا متغیری ندارد و تنها شامل یک متد است.این متد رفتار(Behavior) کلاس را مشخص می کند.
متد درون این کلاس بیان می کند که چه کاری را پس از اجرا شدن انجام خواهد داد.کلمه کلیدی Main() که نام متد این کلاس نیز می باشد جزو کلمات رزرو شده زبان C# است که مشخص می کند برنامه باید از کجا آغاز به کار نماید.وجود متد Main() در تمام برنامه های اجرایی ضروری است در صورتی که یک برنامه حاوی متد Main() نباشد به عنوان توابع سیستمی همانند dll های ویندوز در نظر گرفته می شود.
قبل از کلمه Main() کلمه دیگری با عنوان static آورده شده است.این کلمه را در اصطلاح Modifier می گویند.استفاده از static برای متد Main() بیان می دارد که این متد تنها در همین کلاس قابل اجراست و هیچ نمونه (Instance) دیگری از روی آن قابل اجرا نمی باشد.
استفاده از static برای متد Main() الزامی است زیرا در ابتدای آغاز برنامه هیچ نمونه ای از هیچ کلاس و شی ای موجود نمی باشد و تنها متد Main() است که اجرا می شود.(در صورتی که با برخی اصطلاحات این متن از قبیل کلاس ، شی ، متد و نمونه آشنایی ندارید ،این به دلیل آن است که این مفاهیم جزو مفاهیم اولیه برنامه نویسی شی گرا (OOP) هستند .سعی می کنم در درس های آینده به توضیح این مفاهیم نیز بپردازم ، ولی فعلا در همین حد کافی می باشد).
هر متد باید دارای یک مقدار بازگشتی باشد یعنی باید مقداری را به سیستم بازگرداند.در این مثال نوع بازگشتی void تعریف شده است که نشان دهنده آن است که این متد هیچ مقداری را باز نمی گرداند یا به عبارت بهتر خروجی ندارد.همچنین هر متد می تواند دارای پارامتر هایی نیز باشد که لیست پارامتر های آن در داخل پرانتز های جلوی آن قرار می گیرد.برای سادگی کار در این برنامه متد ما دارای هیچ پارامتری نیست ولی در ادامه همین درس به معرفی پارامتر ها نیز می پردازم.
متد Main() رفتار و عمل خود را به وسیله Console.WriteLine(...) مشخص می نماید.Console کلاسی در System است و WriteLine متدی در کلاس Console .در زبان C# از اپراتور "." (نقطه dot) جهت جداسازی زیرروتین ها و

زیرقسمت ها استفاده می کنیم. همان طور که ملاحظه می کنید چون WriteLine یک متد درون کلاس Console است به همین جهت از "." جهت جداسازی آن استفاده کرده ایم.
در زبان #C جهت قرار دادن توضیحات در کد برنامه از // استفاده می کنیم . بدین معنا که کامپایلر در هنگام اجرای برنامه توجهی به این توضیحات نمی کند و این توضیحات تنها به منظور بالا بردن خوانایی متن و جهت کمک به فهم بهتر برنامه قرار می گیرند.استفاده از // تنها در مواردی کاربرد دارد که توضیحات شما بیش از یک خط نباشد در صورت تمایل برای استفاده از توضیحات چند خطی باید در ابتدای شروع توضیحات از /* و در انتهای آن از */ استفاده نمایید.در این حالت تمامی مطالبی که بین /* */ قرار می گیرند به عنوان توضیحات (Comment) در نظر گرفته می شوند.
تمامی دستورات (Statements) با ";" پایان می یابند.کلاس ها و متد ها با { آغاز شده . با } پایان می یابند.تمامی دستورات بین { } یک بلوک را می سازند.بسیاری از برنامه ه از کاربر ورودی دریافت می کنند.انواع گوناگونی از این ورودی ها می توانند به عنوان پارامتری برای متد Main() در نظر گرفته شوند .لیست 2-1 برنامه ای را نشان می دهد که نام کاربر را از ورودی دریافت کرده و آن را بر روی صفحه نمایش می دهد .این ورودی به صورت پارامتری برای متد Main() در نظر گرفته می شود.
لیست 2-1 :برنامه ای ورودی را از کاربر به عنوان پارامتر Main() دریافت می کند .

```
//Namespac اعلان
using System;
//کلاس آغازین برنامه
class namedWelcome
{
   //آغاز اجرای برنامه
   public static void Main(string args[])
   {
//       نمایش بر روی خروجی
      Console.WriteLine ("hello,{0}!",args[0]);
      Console.WriteLine ("Welcome to the C#");

   }
}
```

دریافت می کند و در هنگام اجرای برنامه باید Command Lineتوجه داشته باشید که این برنامه ورودی را به صورت وارد نمایید.در صورتی که ورودی را وارد ننمایید برنامه دچار مشکل شده و اجرای برنامه Command Lineورودی را در متوقف خواهد شد .
همان طور که در لیست ۲-۱ مشاهده می نمایید پارامتر متد Main() با عنوان args مشخص شده است.با استفاده از این نام در داخل متد می توان از آن استفاده نمود.نوع این پارامتر از نوع رشته ای در نظر گرفته شده است.انواع (types) و آرایه ها را در درس های بعدی بررسی می کنیم.
فعلا بدانید که رشته برای نگهداری چندین کاراکتر مورد استفاده قرار می گیرد.[] مشخص کننده آرایه هستند که مانند یک لیست عمل می کنند.
همان طور که ملاحظه می کنید در این برنامه دو دستور Console.WriteLine(...) وجود دارد که اولین دستور مقداری با دستور دوم متفاوت است.همان طور که مشاهده می کنید در داخل دستور Console.WriteLine(...) عبارتی به شکل {۰} وجود دارد .این آرگومان نشان می دهد که به جای آن چه مقداری باید نمایش داده شود که در اینجا args[0] نشان داده می شود.عبارتی که در داخل " " قرار دارد عینا در خروجی نمایش داده می شود،به جای آرگومان {0} مقداری که پس از " قرار دارد،قرار می گیرد.حال به آرگومان بعدی یعنی args [0] توجه کنید.مقدار صفر داخل [] نشان می دهد که کدام عنصر از آرایه مورد استفاده است.در #C اندیس آرایه از صفر شروع می شود به همین جهت برای دسترسی به اولین عنصر آرایه باید از اندیس صفر استفاده کنیم .



آموزش +Network (قسمت اول)

مقدمه :

در این مقاله مبحث Network+ که امروزه یکی از پیش نیازهای حیاتی برای درک مفاهیم شبکه و در ابعاد بالاتر امنیت شبکه و ضدامنیت شبکه است را مورده بررسی نکته به نکته قرار می دهیم. امیدواریم که بتوانیم سهمی هرچند اندک در ارتقای دانش و سواد کامپیوتری و در راس آن مسایل مرتبط به شبکه هم میهنان عزیزمون داشته باشیم .
بسیاری از افراد علی الخصوص افراد عجول به هنگام تصمیم گیری برای فراگیری شبکه مدام دو کلمه ((کار عملی)) را ورد زبان خود قرار داده و بدون توجه به مسایل تئوریک راه خود را به سمت کار شبکه می گشایند ، هرچند این مساله در تمامی صنعت های مهم از قبیل کامپیوتری و اقتصادی و ... شیوع دارد وآن هم در کشورهایی به مانند ایران که اشخاص از درک اهمیت یادگیری مسایل پایه ای و بنیادین عاجز یا فراری ! هستند ، در حالیکه با یادگیری مسایل پایه ، خواهند توانست راه عملی موفقیت در شاخه مدنظرشان را که واردش شده اند هموارتر از زمانیکه بدون سواد تئوری وارد کار عملی شده اند بنمایند.
این مقاله در چندین قسمت مسایل مرتبط با شبکه براساس نتورک پلاس و تمام تعاریف مرتبط را که در کتب و منابع گوناگون به صورت ناقص یا با اسامی مختلف بیان شده است را یکجا ارایه میدهد، امروزه خوده نتورک پلاس به دلیل گستردگی روز افزون مسایل شبکه و انواع و اقسام اصطلاحات به کار برده شده در آن به صورت یک منبع و مرجع حتی الامکان کامل درآمده است تا افرادی که بدون آشنایی قبلی یا کم با شبکه وارد محیط کار شده اند یا خواهند شد از تعدد اصطلاحات و مفاهیم سرگیجه نگیرند و نیز بتوانند راه خود را در شبکه بسازند و بروند. به همین خاطر به همه دوستان توصیه میشه این سلسله مقالات رو با دقت تمام مطالعه نمایند که یقینا چراغ راه آینده آنان در زمینه شبکه و ... خواهد بود.

شبکه چیست ؟

اولین پرسش متداول که ذهن بسیاری از شنوندگان را به خود مشغول میکند کلمه شبکه است ، در ساده ترین تعریف آن، وصل کردن دو سیستم را به همدیگر شبکه کردن می نامند ، اگر دقت کنید اکثر کارهایی که ما در زندگی روزمره انجام می دهیم همان مفهوم شبکه را تداعی میکند ، ما تا تشنه نشویم احتیاج به آب پیدا نخواهیم کرد و وقتی نیاز به آب پیدا کردیم نیاز به منبع آب و احیانا وسایل مورده نیاز برای خوردن آن پیدا میکنیم ، این موضوع خود به نوعی شبکه است ، شبکه یا زنجیره ای که انسان عطش خود را رفع میکند ، ولی در مبحث نتورک پلاس منظور ما از شبکه شبکه های کامپیوتری و اجزا و وسایل مرتبط به آن است.
به همین خاطر تعریف کاملی از شبکه های کامپیوتری ارایه خواهیم داد:
به مجموعه ای از کامپیوترها (شامل serverها, clinetها) ، پردازشگرها و دیگر وسایل جانبی(مانند چاپگر) که توسط خطوط ارتباطی (media) به یکدیگر متصل (connection) گشته تا از منابع (Resources) و امکانات(Shared Peripherals and Hardware resources) و اطلاعات(Share Data) یکدیگر به صورت مشترک استفاده نمایند ، شبکه می گویند .

حال که تعریف تخصصی شبکه را فهمیدیم بهتر است با برخی کلمات که در آینده به مرور به صورت دقیق تر بیان میکنیم اشنا گردیم.
Server : به کامپیوتر سرویس دهنده که خدمات گوناگون را در شبکه ارایه می دهد سرور می گویند.
client : به کامپیوتر سرویس گیرنده که از خدمات موجود در شبکه استفاده میکنند کلاینت می گویند.

شبکه

media : به تمامی وسایل ارتباط دهنده کامپیوترها، پردازشگرها و ...، شامل کابل ها و مسیریاب ها و تجهیزات ارتباطی مدیا می گویند
Share Data : تمامی منابع موجود در شبکه که اطلاعات را به اشتراک می گذارند.
Shared Peripherals and Hardware resources : به منابع سخت افزاری و... به اشتراک گذاشته شده اطلاق می گردد.
Resources : به تمام منابع موجود در شبکه گفته می شود.
Connection : به چگونگی برقرای ارتباط کامپیوترها که می تواند به صورت با سیم یا بی سیم باشد گفته می شود.

چرا ما به شبکه نیازمند هستیم ؟

همانطور که انسان به وسیله ای برای پخت و پز و دوری از سرما و فراری دادن حیوانات و ساخت سلاح و... نیاز داشت و برای رفع نیازش آتش را ابداع نمود و به مرور آنرا گسترش داد در مبحث شبکه های کامپیوتری نیز انسان امروزی به وسایلی جهت برقراری ارتباط با افراد در اقصی نقاط جهان، انتقال اطلاعات و مدیریت بر اطلاعات و کاهش هزینه نیاز داشت و این خود سرآغازی بر گسترش شبکه بود. زمانی را تصور کنید که دو ابرقدرت در اوج جنگی سرد قرار دارند که هر لحظه احتمال تبدیل به جنگ گرم برای آن وجود دارد و تمامی منابع غذایی ، نظامی ، الکترونیکی و کامپیوتری در خطر حمله قرار دارند و از طرفی باید در حین این جنگ اطلاعات حیاتی در مسافت های طولانی منتقل گردد و امنیت این اطلاعات و منابع حفظ شود ، راهکار چه بود ؟ آیا باید کماکان از فلاپی هایی که زمانی نیاز انسان را برای انتقال اطلاعات برطرف میکرد استفاده می نمودند ؟ فلاپی ها و دیگر حافظه هایی که با هزینه گران قیمت (دهه ۶۰ و ۷۰) ساخته میشد و با سرعت پایین اطلاعات انتقال می یافت و از طرف دیگر حجم کمی را هربار روی یک حافظه انتقال میتوانست داده شود؟ تایید میکنید که وقت بسیاری علاوه بر هزینه ها تلف میشد و سرانجام نیز نه امنیت نه سرعت انتقال مورده نظر حداقل برای نیازهای آن زمان جنگ سرد و کشور آمریکا برآورده نمیشد، در نتیجه به مرور نیاز به ابزاری مناسب تر از هر نظر سبب ساز سرمایه گزاری گسترده وزارت دفاع آمریکا با همکاری دانشگاه های علاقه مند در زمینه شبکه شدند و شبکه های امروزی معنا پیدا کردند. می توان نیاز انسان به شبکه را دلایل و اهداف شبکه نیز دانست :

۱.بکارگیری منابع اشتراکی ، شامل سخت افزاری و نرم افزاری
۲.مدیریت در منابع به صورت دقیق و مطمئن و آسان
۳.کاهش هزینه ها چه مالی چه زمانی
۴.سرعت و امنیت مناسب در انتقال اطلاعات
۵.انجام کارهای گروهی منجر به سریعتر شدن پروژه ها وغیره

و دیگر دلایل و نیازها که با توجه به کمتر مطرح بودن از بیان شان خودداری میگردد.
حال که مفهوم شبکه و دلایل ایجاد آنرا فهمیدیم سوالاتی همچون :
نحوه اتصال سیستم ها چگونه است ؟ قوانین انتقال و اشتراک گذاری اطلاعات چطور است ؟ آیا می توان با اقصی نقاط جهان اطلاعات را اشتراک گذاری نمود ؟ چگونه ؟ در ذهن متبادر می شود و از این جهت توضیح انواع خطوط ارتباطی وانواع ساختارها و تئوری های چگونگی برقراری اتصال بین حداقل دو سیستم (و بیشتر) الزامی می گردد.

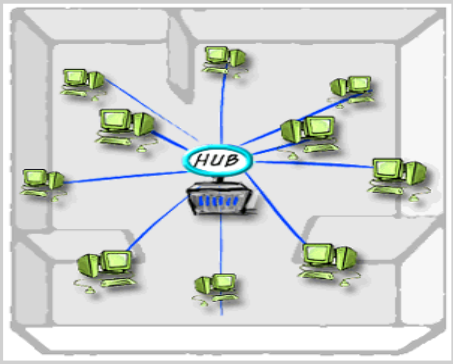
انواع کانال های ارتباطی:

۱. wired (با سیم) ، ۲.wireless (بی سیم) ، می باشند که امروزه از هر دو نوع به وفور استفاده می گردد.

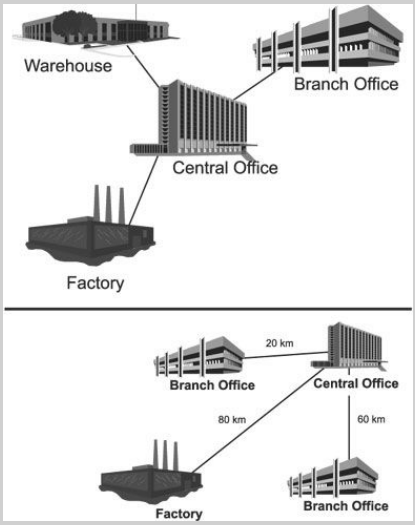
انواع مختلف شبکه

از منظر جغرافیایی:

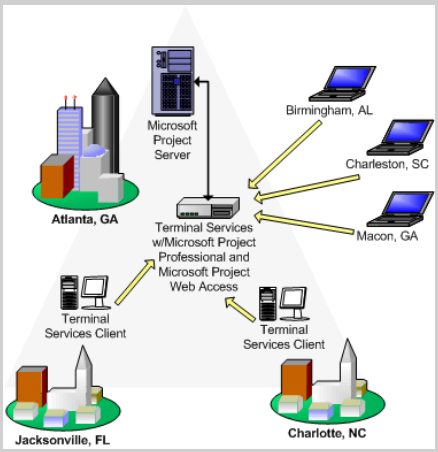
۱. LAN (Local Area Network)
۲. MAN (Metropolitan Area Network)
۳. WAN (Wide Area Network)



LAN به معنی شبکه های محلی به کار برده می شود که یک محدوده کوچک را پوشش می دهد و در آن فاصله نودها از یکدیگر کم و در نتیجه سرعت انتقال بالاتر است (10Gbps، ده گیگابیت در ثانیه) و نیز دقت انتقال بالا و خطاپذیری در شبکه کم است.



MAN به معنی شبکه شهری به کار برده می شود که از شبکه های LAN بزرگتر می باشند و همانطور که از نامش پیداست دارای فواصلی در ابعاد شهری می باشند. این شبکه ها معمولا از ترکیب چندین و چند شبکه LAN به وجود می آیند.



WAN به معنی شبکه گسترده به کار برده می شود که عملا این شبکه محدودیت جغرافیایی ندارد و می توان ارتباط بین چند شهر یا چند استان یا چند کشور و ... به یکدیگر را از این نوع دانست. معمولا این نوع شبکه توسط بسترهای مخابراتی فراهم می شود بدون استفاده از شبکه اینترنت که خود نیز یک شبکه گسترده محسوب می گردد. از سویی دیگر از ترکیب چندین و چند شبکه LAN و MAN شبکه ی گسترده حاصل می گردد.

انواع شبکه از نظر ساختار منطقی :

Workgroup (Peer to Peer) :

در این نوع شبکه جایگاه مشخصی برای سرویس دهنده و سرویس گیرنده مشخص نیست و به عبارتی ایستگاه کاری مشخصی برای آن تعریف نشده است و سیستم میتواند هم client (سرویس گیرنده) باشد هم server (سرویس دهنده) .

هرایستگاه می تواند به منابع سایر ایستگاه های کاری داخل شبکه دسترسی داشته باشند. در این ساختار حفاظت و مدیریت اطلاعات پایین می باشد و هر کاربر خود مسئول ارتقا دادن نرم افزارهای ایستگاه کاری

(سیستم) می باشد. این ساختار بیشتر برای شبکه هایی که نیاز به حداکثر ۱۰ ایستگاه کاری دارند به کار برده می شود.
این ساختار می تواند بیشتر از ۱۰ سیستم نیز باشد ولی به دلیل مشکلاتی که برای شبکه از نظر ترافیک و نیز امنیت ایجاد میکند از آن برای شبکه کردن نهایتا ۱۰ سیستم استفاده می گردد. در Peer to Peer برای اینکه کاربر بتواند با دیگر سیستم های داخل شبکه ارتباط برقرار کند نیاز دارد که روی تک تک آنها اکانت (Account) داشته باشد که به این امر Authentication اطلاق می شود.
به طور خلاصه می توان گفت که کاربر برای ورود به سیستمی دیگر در شبکه باید یوزر و رمز ورود برای تعیین هویت و میزان دسترسی ها داخل سیستم میزبان داشته باشد که به فرآیند انجام این کار Authentication گفته می شود. در حقیقت سیستم با بررسی مشخصات متقاضی عمل Authentication را انجام می دهد که همان معنی Login کردن در شبکه را دارد.
حال که فهمیدیم Authentication یعنی وارد کردن یوزر و رمز ورود به سیستم میزبان باید بدانیم که سیستم میزبان چگونه از صحت هویت متقاضی اطمینان حاصل میکند ؟ هر سیستم دارای قسمتی با نام LSD که مخفف Local Security Database میباشد که هرگاه سیستم تقاضای لوگین کردن کاربر را دریافت نماید با مراجعه به LSD صحت Login را تشخیص می دهد. حال همین موضوع را تصور کنید برای ده سیستم در شبکه workgroup (peer to Peer) تکرار می شود تا اجازه ورود به شبکه و استفاده از سیستم ها داده شود و باید روی تمامی آنها اکانت معتبر داشته باشیم و همین موضوع از دلایل اصلی می باشد که تا ده سیستم بیشتر در workgroup (peer to Peer) وارد شبکه نمی شود (هرچند در ویندوزv قابلیت شبکه شدن ۲۰ سیستم فراهم گشته است)
قسمتی مربوط به امنیت پایین در روش می باشد زیرا ممکن است یک ایستگاه کاری مامن نفوذگران به شبکه (hacker) باشد و امنیت اطلاعات و... به خطر بیافتد و از طرفی سرعت و پهنای باند و ترافیک شبکه نیز به مشکل برمیخورد.
این مساله برای ویندوزهایی به غیر از ویندوز سرورها (که محدودیتی ندارند) میباشد.
به طور خلاصه معایب و فواید workgroup (peer to Peer) را این چنین برآورد می نمایند.
الف.محدودیت در تعداد سیستم هایی که شبکه می شوند.
ب.مدیریت در این نوع شبکه ثابت و متمرکز نیست.
پ.هر سیستم می تواند کلاینت یا سرور باشد که دلیل غیرمتمرکز بودن مدیریت در peer to peer میباشد.
ت.راه اندازی workgroup (peer to Peer) آسان و سریع می باشد.
ث. داشتن اکانت روی سیستمی که تقاضای login کردن به آن وجود دارد الزامی است .

: (Domain) Server Base

اولین نکته ای که در این ساختار به چشم میخورد متمرکز بودن و وجود یک سرور مرکزی در آن است که به همین خاطر آنرا مطمئن ترین ساختار منطقی شبکه نموده است. با ایجاد سرور مرکزی روی تمامی منابع شبکه و کامپیوترها و کاربران میشود مدیریت متمرکز داشت. به همین خاطر امنیت در این ساختار بسیار بیشتر از Workgroup میباشد.
نکته قابل تامل اینکه عمل Authentication به مانند شبکه های Workgroup در این ساختار انجام می گردد با این تفاوت که توسط سرور مرکزی اطلاعات و صحت آنها کنترل می شود. به سرور مرکزی که مسئولیت کنترل صحت اطلاعات و دسترسی ها و محدودیت ها را دارد اصطلاحا Domain Controller یا به صورت مخفف C.D نیز گفته میشود.
این شبکه ها نیازمند حداقل یک Server میباشند که اطلاعات مرتبط با یوزرهای کاربری (User Account) تمام شبکه در آن تعریف می گردد. تقاضای ورود به شبکه و برقراری ارتباط به سرور مرکزی فرستاده می شود و در صورت تایید اجازه ورود به شبکه با میزان محدودیت های تعریف شده کاربر Login می نماید.
به طور خلاصه می توان خواص Server base را این چنین بیان نمود :
الف. در این شبکه حداقل یک C.D یا کنترل کننده مرکزی که همان سرور میباشد وجود دارد که همه قوانین و اکانت ها و دسترسی های تعریف شده در شبکه مورده نظر داخل آن تعریف می شود.
ب.امنیت این شبکه به دلیل متمرکز بودن روی یک سرور بالاست و می شود گفت حداقل از Workgroup بیشتر است.
پ.محدودیت تعداد کامپیوتر روی این ساختار وجود ندارد.
ت.برای استفاده از این ساختار مسلما نیازمند به یک سیستم عامل سرور هستید.

برای انتخاب یکی از این دو ساختار Sever Base یا Workgroup شما نیازمند دانستن نوع کاربری محلی که قرار است شبکه نمایید هستید ، یعنی باید میزان بودجه تامینی و میزان امنیت مورده تقاضا و تعداد کاربران و ... تماما مورده تجزیه تحلیل قرار گیرد تا یک نتیجه گیری منتج به انتخاب ساختار منطقی شبکه شما گردد.

آشنایی با شبکه های هدف

آشـنایی بـا عملیـات حملـه بـه شـبکه و آگـاهی از تکنیکهـای نفـوذگری,صـرفا بـه منظـور مقابلـه و دفـاع اسـت. بعنوان یک فرد متعهد و متخصص , از آموزش عملی این روش ها به افراد کم ظرفیت و غیر عملی احتراز کنید و هرگز آنهارا بر علیه دیگران به کار نگیرید .
در صورت داشتن پیشینه ای خوب در ۳ مبحث زیر این تاپیک را دنبال کنید :

TCP/IP
مروری کلی بر سیستم عامل Windows 2000 , NT
مروری کلی بر سیستم عامل Linux و Unix

مباحث کلی این مقاله آموزشی :

۱- شناسایی مقدماتی شبکه هدف بدون نیاز به ابزار
۲- شناسایی به روش روان شناختی و تعاملات اجتماعی
۳- جستجو در وب به دنبال اطلاعات و اخبار شبکه هدف
۴- بانک اطلاعاتی Whois
۵- استفاده از سایت ARIN جهت تحقیق در مورد آدرس IP
۶- مقابله با جستجوی مخرب از طریق Whois
۷- سیستم دی ان اس کسب اطلاعات از سرویس دی ان اس در راستای حمله
۸- ابزارهای همه منظوره برای شناسائی مقدماتی شبکه هدف
۹- ابزارهای شناسایی شبکه مبتنی بر وب

مقدمه :

یک نفوذگر حرفه ای هیچ گاه و بدون مقدمه و کوردست به حمله علیه یک شبکه نخواهد زد زیرا نه تنها احتمال موفقیت در آن ناچیز است بلکه منجر به گرفتاری او نیز خواهد شد.در اولین مرحله از یک حمله خطرناک و موفق نفوذگر سعی می کند مجموعه ای از اطلاعات در خصوص شبکه هدف را جمع آوری و دسته بندی کرده و از آنها برای شناسائی مشخصات فنی و عمومی شبکه هدف استفاده نماید.اگرچه نوجوانان کم سن و سالی هستند که بدون هیچ تجربه و به اقتضای سن و سالشان دست به ماجراجوئیهای کور و بی هدف بر علیه شبکه می زنند و غالبا یا ناموفقند ویاگرفتار چنگ قانون می شوند.در حالیکه نفوذگران حرفه ای برای شناسایی مقدماتی هدف وقت بسیار زیادی صرف می کنند چون موفقیت آنها منوط به داشتن اطلاعات کافی وبه کارگیری روشهای متناسبی است که از همین اطلاعات اولیه نتیجه گیری می شود .

هدف از این فصل آنست که بدانیم یک نفوذگر حرفهای چه روشهائی را برای شناسایی شبکه هدف به کار می گیرد,منظور او از شناسایی شبکه چیست و در پی چه نوع اطلاعاتی است و نهایتا چگونه باید تلاشهای اورا به صورت دقیق خنثی کرد .

هرگاه خواستید بدانید که شناسایی مقدماتی هدف به چه معناست یک جنگ واقعی در میدان نبرد را در ذهن خود مجسم کنید.نه می توان بدون آگاهی از موقعیت جغرافیائی محل استقرار نیروهای دشمن,آگاهی از حجم نیرو و مهمات,آگاهی از نوع مهمات,محدودیتهای فیزیکی و جغرافیائی میدان نبرد و حتی میزان روحیه سربازان دست به حمله زد؟

شما تا کنون دهها فیلم در تلویزیون در رابطه با سرقت بانک دیده اید.یک سارق بانک چگونه می تواند بدون اطلاعات مقدماتی در مورد راه های نفوذ به بانک,موقعیت دوربینها,موقعیت زنگهای خطر,راه های فرار و موقعیت خیابانهای اطراف به سرقت کند .

حمله به یک شبکه نیز چنین وضعیتی را دارد.نفوذگر در مقدماتی ترین مرحله,به جمع آوری عمومی و غیر محرمانه ای که در مورد شبکه منتشر شده است,اقدام می کند.بدست آوردن اطلاعات عمومی برای شناسایی مقدماتی شبکه هدف,کار چندان مشکلی نیست ولیکن اصول راه کارهای ویژه دارد در این فصل پس از آشنایی با "اصول شناسایی مقدماتی شبکه هدف حمله" راهکارهای پیشگیری از دسترسی نفوذگر به اطلاعات حساس را معرفی خواهیم کرد . اصولی که به عنوان روشهای شناخته شده برای شناسایی مقدماتی هدف مطرح هستند و آنهارا به تفصیل معرف می کنیم .

عبارتند از :

۱- شناسایی مقدماتی شبکه با اتکا به روشهای روانشناختی و مهندسی اجتماعی ، بدون نیاز هیچگونه ابزار فنی
۲- روش جستجو در وب به دنبال اطلاعات و اخبار راجع به شبکه هدف
۳- جستجو از طریق سرویس دهنده DNS (Domain Name System)

موضوعات مطرح شده در مباحث بعد :

۱- شناسایی مقدماتی شبکه هدف بدون نیاز به ابزار
۲- شناسایی به روش روان شناختی و تعاملات اجتماعی

شناسائی مقدماتی شبکه هدف بدون نیاز به ابزار:

یک نفوذگر حتی بدون کامپیوتر هم می تواند اطلاعات با ارزشی از شبکه هدف گردآوری کند.بدین روش یک نفوذگر زیرک ضمن شناسائی شبکه شماحتی برخی از کلمات عبور کاربران یا ساختار شبکه,نوع سخت افزار و ابزار مورد استفاده,سیستم های عامل و نوع سرویس دهنده ها,شماره های تلفن متصل به مودم و گزارش ها فنی شبکه را براحتی به چنگ بیاورد.روشهایی که نفوذگر در اولین اقدام به آن متوصل می شود نیاز به ابزار و تخصص فنی ندارد بلکه مبتنی بر اصول روان شناسی و نوع برخورد او با شبکه شماست.شاید شما با مطالعه این بخش لبخندی زده وتصور کنید این روشها مسخره و غیر عملی هستند درحالی که گزارش های بسیار فراوانی در مورد حملات مختلف به شبکه ها منتشر شده که نقطه آغاز همین اطلاعات جزئی ولی ارزشمند بوده است.به عنوان مثال فرض کنید نفوذگر در یک مهمانی خانوادگی از یکی از کارمندان شبکه شما می شنود که در شبکه شما از DNS از سرویس دهنده قدیمی BIND بعنوان سیستم استفاده شده و سیستم عامل آن سولاریس است.شبکه شما با همین جمله خانه خراب و ویران خواهد شد!!((در فصول بعدی با سیستم BIND آشنا خواهید شد و خواهید دانست که در این سیستم یک شکاف امنیتی بسیار وحشتناک وجود دارد))

شناسائی به روش روان شناختی و تعاملات اجتماعی:

مسخره ترین نوع شناسائی آنست که نفوذگر از تلفن همگانی با روابط عمومی شبکه شما تماس گرفته و سوال کند که مثلا از چه نوع مسیر یاب,سیستم عامل,توپولوژی و ساختاری در شبکه استفاده شده است.برخی از مسئولین روابط عمومی یا منشی به اقتضای شغلشان آنچه را که در مورد اینگونه سوالات به خاطر دارند,دودستی تقدیم می کنند.شاید تصور می کنند با بیان آنکه از کدام مسیر یاب یا سیستم عامل در شبکه استفاده کرده اند به اعتبار موسسه آنها اضافه شود.اگر نفوذگر به لحن خود اندکی تواضع,التماس و کمی هم ابلهی بیفزاید احتمال موفقیت او بیشتر خواهد بود.ارتباط نفوذگر با کارمندان ناراضی یا کم ضرفیت شبکهبه او خدمت فراوانی خواهد کرد.

روشی دیگر برای شناسایی مقدماتی شبکه,تماسهای مکرری است که گاه و بی گاه با گروه "پشتیبانی فنی" شبکه برقرار می شود.وظیفه شبانه روزی این گروه رسیدگی به مشکلات احتمالیکاربران بی اطلاعی است که در مورد شبکه با مشکل مواجه می شوند.حال فرضکنید که در زمان اوج مشغله کاری,یک نفر با گروه پشتیبانی تماس می گیرد و ادعا می کند که او دیشب نتوانسته با کلمه عبور ۱۲۳٤٥٦ به شبکه شما وارد شود و از این موضوع ناراحت است و تصمیم دارد از شما شکایت کند!گروه پشتیبانی فنی کلمه کاربری(User ID) و را می گیرند و بعد از بررسی کلمات عبور با ملاطفت به او پاسخ می دهند که او کلمه عبورش را فراموش کرده و کلمه عبورش wxyz است!گروه پشتیبانی چگونه به او اعتماد کرده اند!!!!

کسی نیمه شب با گرئه پشتیبانی تماس می گیرد و خودش را مسئول سبکه و یا مسئول یک سرویس دهنده معرفی می کند.لحن و لهجه او دقیقا مشابه فرد مذکور احساس می شود لذا محترمانه به حرفهای او گوش می دهند.او از گروه پشتیبانی می خواهد تا سرویس دهنده Telnet را روی فلان ماشین اجرا کنند و پورت ۲۳ از دیوار آتش را نیز باز بگذارند!آیا می توان به صدای کسی اعتماد کرد؟

یک نامه از یک مقام محترم یا یک هنرپیشه معروف دریافت شده و خواهش کرده بصورت افتخاری برای او حساب کاربری (User Account) با سطح دسترسی کامل و کلمه عبور موردنظر او ایجاد شود.آیا این کار به صلاح است؟کسی به یکی از کارکنان شبکه زنگ می زند و خودش را یکی از بستگان مسئولین سیستم معرفی می کند و ار او آدرس e-mail یا شماره تلفن او را می خواهند!!
فردی عصبانی با گرئه پشتیبانی فنی تماس گرفته و با حالت ظلبکارانه می گوید که نتوانسته یرای ارتباط با شبکه از Telnet استفاده کند.آنها مهربانانه به اوپاسخ می دهند که بواسطه دیوار آتش (Fire Wall) تمام پرتهای TCP به غیر از 53,21,20,25 و ۸۰ مسدود است.آیا این جواب لازم است؟

کسی با گروه پستیبانی تماس گرفته و همه آهارا متهم به بی سوادی کرده است چراکه توپولوژی شبکه و نوع مسیر یاب شبکه را نمی دانند!همچنین بلد نیستند قواعد دیوار آتش را به درستی تنظیم کنند!گروه پشتیبانی با ناراحتی در پاسخ می گویند اولا هیچ دیوار آتشی درکار نیست که بخواهند قواعد آن را تنظیم کنند ثانیا بهترین مسیریاب cisco را تهیه کرده اند و ثالثا توپولوژی شبکه با بهترین سوئیچ های ۳ comشکل گرفته است!سپس تلفن را با عصبانیت می کوبند درحالیکه ترف مقابل خودکار به دست درحال لبخند زدن است.

نکات امنیتی:

۱. ایرانی ها در مهربانی و ملاطفت افراط (و گاهی تفریط!!!) می کنند لذا برخی اوقات در مواجهه با اینگونه شرارت ها اطلاعات حساس خود را بروز می دهند,مواظب باشید.

۲. یکی از بدترین محیطهایی که افراد اطلاهات خود را فاش می کنند,گپ اینترنتی (chat)است چرا که همه فکر می کنند کسی آنهارا نمی شناسد.

۳. اگر قانونی و درست عمل می کنید از هیچ کس نترسید و به هیچ کس اعتماد نکنید,حتی اگر رئیس شما باشد و تقاضای کوچکی بر روی ماشین شما داشته باشد.

۴. موضوعات اشاره شده در قالب مثال را شوخی نگیرید!اینها مطالبی حدی هستند و حملاتی که به این طریق انجام شده اند بسیار زیادند.

امنیت در سیستم مدیریت محتوای جوملا

بگذارید بحث را با یک سوال شروع کنیم
جوملا چیست؟
جوملا !یک سیستم مدیریت تحت وب است که در ساختن وب سایت و دیگر برنامه های تحت اینترنت به شما کمک می کند. مهم تر اینکه جوملا یک برنامه open source میباشد که به طور رایگان دراختیار همه قرار دارد.
جوملا در سراسر دنیا برای قدرت بخشی به کلیه برنامه ها، از یک صفحه شخصی ساده تا برنامه های تحت وب شرکت های عظیم استفاده می شود. چند مورد از موارد استفاده نرم افرار جوملا به شرح زیر است:

۱. پرتال ها و یا وب سایت های شرکت های عظیم
۲. تجارت آنلاین
۳. وب سایت های تجاری در مقیاس کوچک
۴. وب سایت های سازمانی و رایگان
۵. کاربرد های دولتی
۶. اینترنت و اینترانت های شرکت های عظیم
۷. سایت های مذهبی و مرتبط با آموزش
۸. صفحات شخصی و خانوادگی
۹. پورتال های مبتنی بر گروه ها و اصناف
۱۰. مجلات و روزنامه ها

قابلیت های جوملا نامحدود هستند ...

خب نا محدود بودن قابلیت ها در وب در ظاهر نکته مثبتی می باشد اما آن روی سکه را هم در نظر بگیرید که این انعطاف فوق العاده و نا محدود بودن ممکن است حفره های امنیتی را دور از چشم طراحان و مدیران امنیتی سیستم به وجود آورد . البته جوملا به جرات قوی ترین تیم توسعه دهنده را در سراسر دنیا دارد تا در سریعترین زمان ممکن وصله های امنیتی را ایجاد و در اختیار چندین میلیون مصرف کننده این سیستم مدیریت محتوا در سراسر جهان قرار دهد . در ایران نیز چند تیم به طور فعال و مستمر در زمینه ترجمه و ارائه بسته های به روز رسانی سازگار با زبان پارسی نیز فعالیت دارند.
اگر بخواهیم از نظر امنیتی سیستم را بررسی کنیم میبینیم که هسته اصلی سیستم تا حد قابل قبول و بالایی امن میباشد اما سوالی که اینجا مطرح میشود این است که اگر این سیستم تا حد قابل قبولی امن است چرا در برخی مواقع میبینیم که یک سایت جوملایی به سادگی هک میشود
پاسخ ساده است :بسیاری ار کامپونت ها و ماژولی هایی که بر روی سیستم نصب میشود از نظر امنیتی تست نشده و بعضا همین الحاقات هستند که راه را برای هکر باز میکنند و خب نتیجه این میشود که سیستم امن جوملا تبدیل به یک سیستم نا امن و ناپایدار میشود و این خطا تنها از مدیر سیستم می باشد که سیستم خود را کاملا بررسی نکرده و بدون توجه به نکات امنیتی الحاقات خود را به سیستم افزوده .

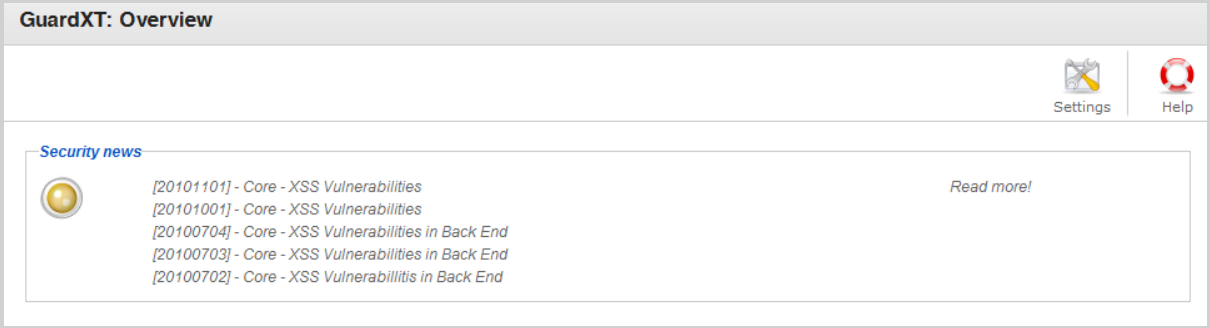
هدف از این سری مقالات ارئه افزونه ها و راه حل های مناسب برای بالا بردن امنیت سیستم های مدیریت محتواست ، در این شماره قصد داریم تا شما را با یک افزونه سیستم مدیریت محتوای جوملا آشنا کنیم که مزایای بسیاری در بر دارد و به شما کمک میکند تا امنیت سرور جوملا و خود سیستم را تا حد زیادی بالا ببرید با ما همراه باشید .

افزونه GuardXT :

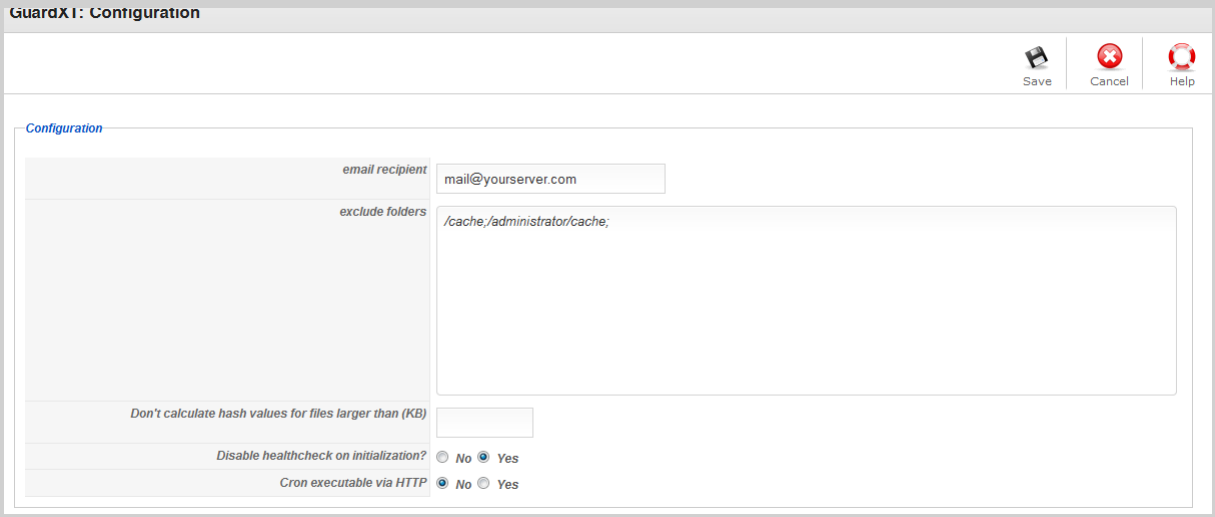
این افزونه وظیفه تست و بررسی سرور و نکات امنیتی مختص جوملا و همچنین بررسی فایلهای هسته جوملا را دارد تا در هنگام تغییر و دستکاری فایلها به شما اطلاع دهد . قابلیت آخر زمانی به شما کمک میکند که یک شل درون سرور بارگذاری شود و یا یکی از فایلهای شما محتوایش توسط یک نفوذ گر با محتویات یک شل عوض شود ، در حالت عادی فهمیدن این موضوع که آیا چنین کاری صورت گرفته یا نه امری سخت و بعضا غیر ممکن میباشد اما این افزونه به شما در این امر کمک میکند
حال ببینیم این افزونه چگونه کار میکند
ابتدا افزونه را از یکی از ادرسهای زیر دانلود و در سیستم جوملا خود نصب نمایید .

http://www.joomlaxt.com/download-topmenu-31?func=fileinfo&id=45
http://ashiyane.org/forums/showthread.php?t=32500

خب پس از نصب افزونه از منوی کامپوننت افزونه Guardxt را انتخاب کنید تا صفحه مربوط به آن باز شود
شرح توضیحات کامپوننت با عکس در زیر آمده:

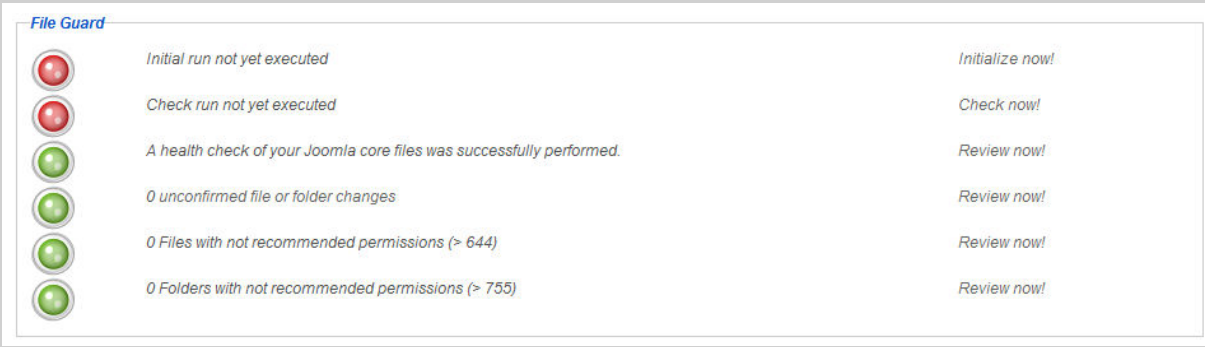


اولین بخش کامپوننت اختصاص به اخبار امنیتی سیستم جوملا دارد که با کلیک بر روی read more میتوانید اخبار مربوطه را به طور کامل مشاهده کنید،
اگر بر روی دکمه Settings کلیک نمایید به صفحه ای مانند شکل زیر خواهد رفت که تنظیمات کامپوننت در آنجا تعریف میشود .

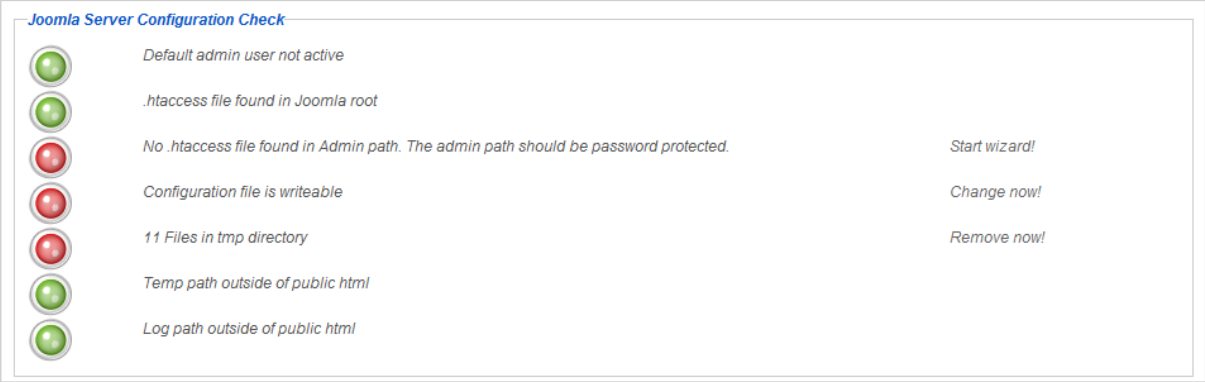


email recipient : در این قسمت ای میل خود را وارد کنید تا برنامه اطلاعات مربوطه را برای شما ارسال کند.
exclude folders : در این قسمت پوشه هایی که میخواهید اسکن در آنها صورت نگیرد تعریف کنید . پوشه ها را با ; از هم جدا کنید.
Don't calculate hash values for files larger than (KB) : در این قسمت میتوانید مشخص کنید که اگر حجم فایلی بیشتر از مقدار مورد نظر شما بود هش فایل تولید و بررسی نگردد.مقدار را به کیلو بایت وارد کنید.
Disable healthcheck on initialization? : در صورت yes بودن بررسی سالم بودن فایلها در هنگام اجرای کامپوننت صورت نمیگیرد ، به طور پیشفرض همین تنظیم صحیح است.
Cron executable via HTTP : این گزینه را هم به صورت پیش فرض باقی بگذارید.

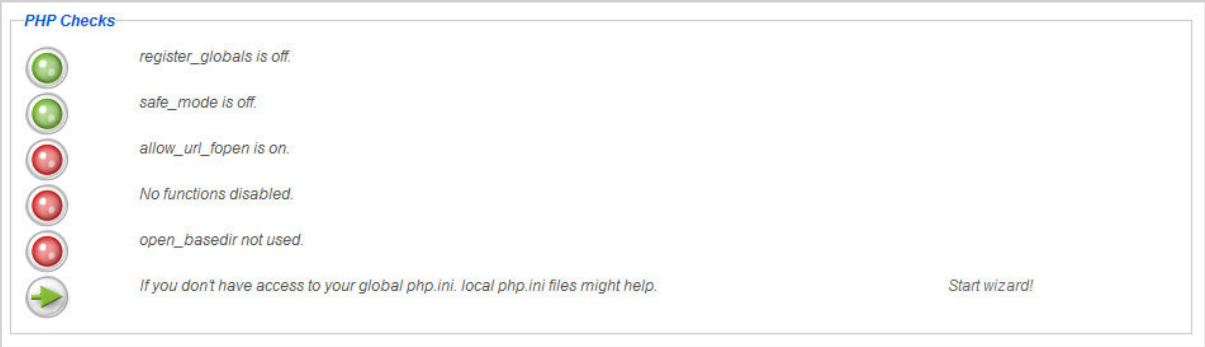
در صفحه اصلی قسمت دوم کامپوننت اختصاص به نسخه نصب شده خود کامپوننت و جوملای شما دارد که در صورتیکه نسخه شما قدیمی تر از نسخه های موجود در اینترنت باشد سیستم به شما پیغامی مبنی بر این امر خواهد داد. به عکس توجه کنید : هم نسخه جوملا و هم خود کامپوننت قدیمی می باشد پس مدیر سایت باید هر چه زودتر سیستم خود را ارتقا دهد.سومین گزینه هم به روز بودن سایر کامپوننت های نصب شده در سیستم را در صفحه ای دیگر بررسی میکند .



بخش File guard بخش مهم محافظت کننده فایلهاست بدین شکل که از تمامی فایلهای شما لیستی تهیه کرده و در بانک اطلاعاتی نگه میدارد و هر بار که میخواهد سلامت این فایلهارا تست کند هش این فایلها را با هش موجود در بانک اطلاعاتی خودش بررسی میکند ، این قسمت به شما کمک میکند تا همیشه از سالم بودن فایل سیستم جوملای خود مطمئن باشید . به جرات این قسمت از مهمترین بخش های امنیتی این کامپوننت با ارزش می باشد.
گزینه Initial run not yet executed که در اینجا قرمز می باشد را تنها یک بار باید initialize کنید تا لیست مورد بحث تهیه شود و دفعات بعد کافی است که گزینه check now را برای بررسی فایل سیستم اجرا کنید .
سیستم شما را در مورد تغییرات دسترسی پوشه ها ، فایلها و هسته سیستم آگاه می سازد.



در این قسمت تنظیمات سرور جوملا مورد بحث قرار خواهد گرفت و هر جا که قرمز بود کامپوننت به شما در حل مشکل کمک خواهد کرد
اولین گزینه فعال بودن نام کاربری admin را بررسی میکند که البته برای امنیت سیستم شما باید این نام را تغییر دهید که در اینجا میبینیم انجام شده.
دومین گزینه وجود htaccess. را در پوشه اصلی جوملا بررسی میکند ، این قسمت را در Global Configuration جوملا میتوانید فعال کنید.
سومین گزینه وجود htaccess. را در پوشه administrator بررسی میکند که در اینجا قرمز می باشد پس با استفاده از Wizard میتوانید تنظیمات مناسب را اعمال کنم.(این قسمت به شما در رمزگذاری پوشه مدیریت کمک میکند)
چهارمین گزینه بررسی میکند که آیا فایل configuration.php قابل نوشتن می باشد یا نه که اگر قابل نوشتن باشد میتوانید با استفاده از Change now سطح دسترسی فایل را تغییر دهید.
پنجمین گزینه به بررسی خالی بودن پوشه tmp جوملا میپردازد که با استفاده از گزینه Remove now میتوانید در صورت خالی نبودن این پوشه آنرا خالی کنید
دو گزینه بعد هم بررسی میکند که آیا پوشه های tmp و log در مسیری خارج از public_html قرار گرفته اند یا نه که در صورت قرمز بودن این گزینه ها به شما راهنمایی های لازم برای تغییر مسیر خواهد شد .



و در نهایت کامپوننت به بررسی تنظیمات php شما میپردازد
برای اینکه جوملا به طور صحیح کار کند و مشکل امنیتی نداشته باشد نیاز است تا بعضی از تنظیمات PHP خاموش باشند که در اینجا به شما نشان میدهد که وضعیت php سرور شما به چه شکل است .
اگر شما به تنظیمات سرور دسترسی نداشته باشید برنامه با ساخت یک فایل php.ini به شما کمک میکند تا تنظیمات مورد نظر را در سرور اشتراکی خود اعمال کنید (البته از ادمین سرور سوال کنید که ایا php.ini برای هر سرویس قابل تعریف است یا نه، در بعضی از سرور ها میتوانید از htaccess. برای تغییر تنظیمات PHPاستفاده کنید).

در زیر تنظیمات مورد نیاز php برای یک سرور جوملا شرح داده شده:

register_globals = off.
safe_mode = off.
allow_url_fopen = off.
open_basedir هم باید فعال باشد و متناسب با تنظیمات سرور تعریف شود

در ضن توابع زیر نیز در php باید غیر فعال شوند :

Show_source
System
Shell_exec
Passthru
Exec
Phpinfo
Popen
Proc_open

و در نهایت دو نکته مهم : همیشه نسخه جوملا خود را به روز نمایید ، همیشه کامپوننت Guardxt را به روز نگه دارید .

در انتها باید اول به خاطر تاخیر در انتشار مجله از همه خوانندگان عزیز طلب پوزش کنیم .
بعد تشکر فراوان از دوستانی که زحمت کشیدند و مقالاتشان را برای ما ارسال نمودند .

elvator
Alexander
Ruinder_blackhat
A.S.P.I.R.I.N
DarkC0d3r
Pr0grammer
ADNST
iEnemy
Ernesto Rommel
Sil3nt Di3

و تشکر از بقیه دوستان برای کمک در ساخت این شماره از مجله

خوانندگان عزیز می توانند مقالات خودشان را برای ما ایمیل کنند تا با نام خودشان در مجله قرار گیرد .

Magazine@Ashiyane.ir

و تشکر فراوان از دو مسئول عزیز سایت به خاطر زحمات فراوانشان در کمک به بهبود سطح کیفی مجله

بهروز کمالیان (Behrooz_ICE)
مهدی چینی چی (Virangar)

نویسنده و طراح مجله : پوریا محمدرضایی (Hijacker)

موفق باشید

www.Ashiyane.ir
www.Ashiyane.org