

"In The Name Of God"

<http://Hackerz.ir>
<http://simorgh-ev.com>

(Learning Perl For Writing Exploits)

موضوع : آموزش برنامه نویسی پرل برای نوشتن اکسپلویت

نویسنده : شاهین رضانی (vampire_chiristof@yahoo.com)

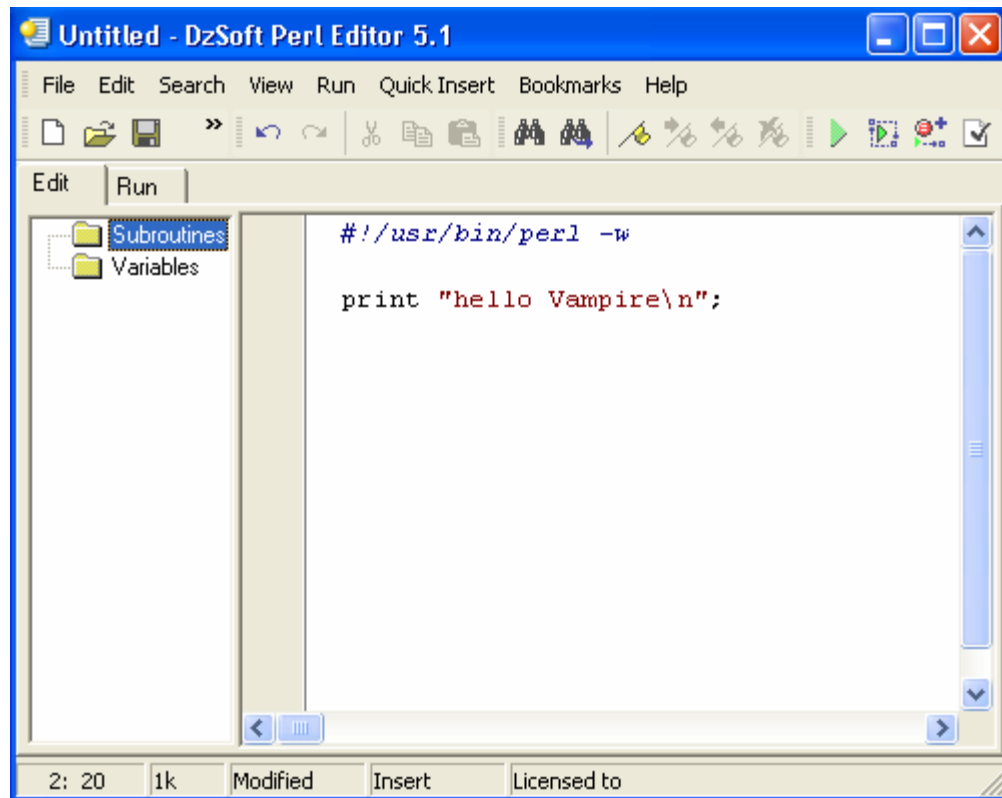
وبلاگ : <http://c0d3r.blogfa.com>

مقدمه :

خوب با نام و یاد خدا به مقاله ی دیگر رو شروع میکنیم ! خوب برنامه نویسی با پرل کار خیلی خیلی ساده ای است خوب پرل یک زبان مفسر است که کارایی فوق العاده زیادی در سیستم عامل های خانواده ی Unix دارد ! این زبان در عین سادگی شباهت زیادی به زبان C دارد و قدرت مانور فوق العاده ی دارد ! (به خاطر همین است که اکثر Exploit های امروزی مخصوصا Exploit های مبتنی بر Web Application ها اکثرا با این Perl نوشته می شوند !) دیگر دلیل محبوبیت پرل این است که با کمی تغییر قابل اجرا بر روی هر سیستم عاملی میباشد ! البته بنده شخصا برای Exploiting از C استفاده میکنم D: جدیدا حتی Python اما نمیتوان از قدرت

و توانایی بالای Perl در این امر را نادیده گرفت !
شروع کار با پرل :

خوب قبل از شروع کار برنامه نویسی با پرل شما حتما باید Active Perl رو داشته باشید شما میتونید این رو از سایتش یعنی www.activestate.us دانلود کنید ! بعد از دانلود Active Perl شما به یک ویرایش گر متنی احتیاج دارید من از DzSoft Perl Editor ماله www.dzsoft.com استفاده میکنم ! اما شما میتونید از همون NotePad استفاده کنید ! (اگه مجانی میخواید ☺) در ضمن تمامی برنامه هایی که مینویسد باید با پسوند .pl ذخیره کنید ! و در واقع این (.pl) شناسه ی اصلی برنامه های نوشته شده به زبان Perl است !



(DzSoft Perl Editor)

خوب مثل بقیه ی زبان های برنامه نویسی با برنامه ی معروف و ساده ی
Hello Word که جدیداً به Hello Vampire تغییر کرده کار رو شروع میکنیم!

```
#usr/bin/perl  
Print "hello Vampire\n";
```

خوب نکته ی اول اینکه #usr/bin/perl شناسه ی perl است پس باید

همیشه در خط اول وجود داشته باشد!

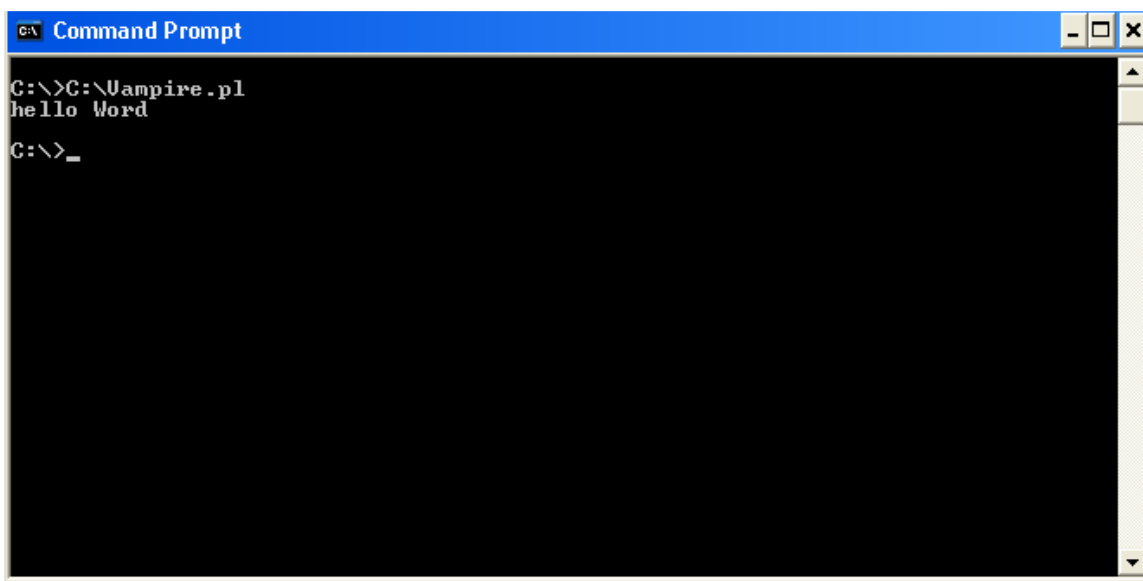
دستور Print هم که برای چاپ در خروجی است که دقیقاً مانند Printf در C

میباشد و اینجا عمل کردی مانند MsgBox در Visual Basic یا Print در

Python و دارد!

خوب اجرا کافیه فایلی که Save کردید در Command Prompt خودتون

Drop کنید و Enter بزنید!



```
Command Prompt  
C:\>C:\Uampire.pl  
hello Word  
C:\>_
```

(فایل Vampire.pl در درایو C)

البته برای اجرای فایل در سیستم عامل های خانواده Unix کافیه از دستور
Perl yourfilename.pl استفاده کنید و قبل از آن `#!/usr/local/bin/perl` و
(اگه عمری موند در مورد برنامه نویسی پیشرفته پرل در لینوکس بعدا
صحبت میکنیم !)
خوب در پرل یک سری کاراکتر مخصوص وجود دارد که من براتون لیست
کاملشو میارم ! (فرمتهای مختفم نمایش رشته)

`\n` بعدی خط

`\t` یک اندازه به جلو به پرش Tab

`\b` رود می عقب به کاراکتر یک اندازه به

`\\` نمایش

`\` خروجی در " نمایش برای

`\l` بصورت بعدی کاراکتر نمایش lower case

بین کاراکترهای کلیه `\L` تا `\E` بصورت lower case شوند می داده نمایش `\L`

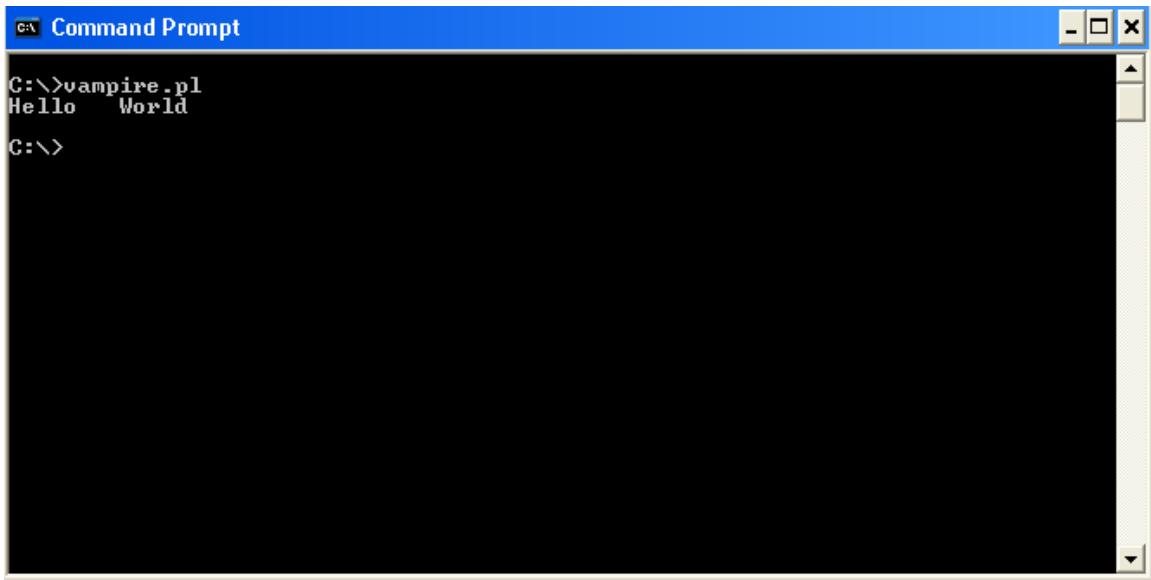
`\u` بصورت بعدی کاراکتر نمایش upper case

بین کاراکترهای کلیه `\L` تا `\E` بصورت upper case شوند می داده نمایش `\U`

`\a` Alert (دادن یک صدا)

برای درک این مطلب به این مثال توجه کنید !

```
#!/usr/bin/perl -w  
print "Hello\tWorld\n\a;"
```



```
CA\ Command Prompt
C:\>vampire.pl
Hello World
C:\>
```

(نتیجه به این صورت است)

در ضمن (-W) که در خط اول استفاده کردم یک بررسی کننده ساده ی
اشتباه متغییر است (!
و نکته ی دیگر اینکه گذاشتن سمی کالون را در آخر پایان حر دستور فراموش
نکنید !
در پرل شاخصهایی یا زمینه هایی برای دستور Print وجود دارند که من چند
تاشونو بهتو معرفی میکنم !

زمینه	عملکرد آن
s	نمایش دادن به صورت کاراکتری
S	نمایش دادن به صورت رشته ای
f	عدد با نقطه ی شناور
d	بخش صحیح اعشار (گرد شده)

متغیرها در پرل : Perl Variables

مثل تمام زبان های برنامه نویسی دیگه پرل هم باید دارای متغیر باشد !

متغیرها در پرل به 4 دسته تقسیم میشوند :

1-متغیرهای عددی

2-متغیرهای کاراکتری

3-آرایه های اسکالر

4-آرایه های شرکت پذیر

خوب متغیرها در Perl توانایی نگه داری اطلاعات را به صورت همیشگی و

موقت را دارند ! و میتوانند اعداد و رشته ها رو در بر بگیرند ! متغیرها در

Perl با علامت \$ تعریف میشوند !

خوب بهتره روی یک برنامه ی خیلی ساده به طور عملی نحوه ی عملکرد

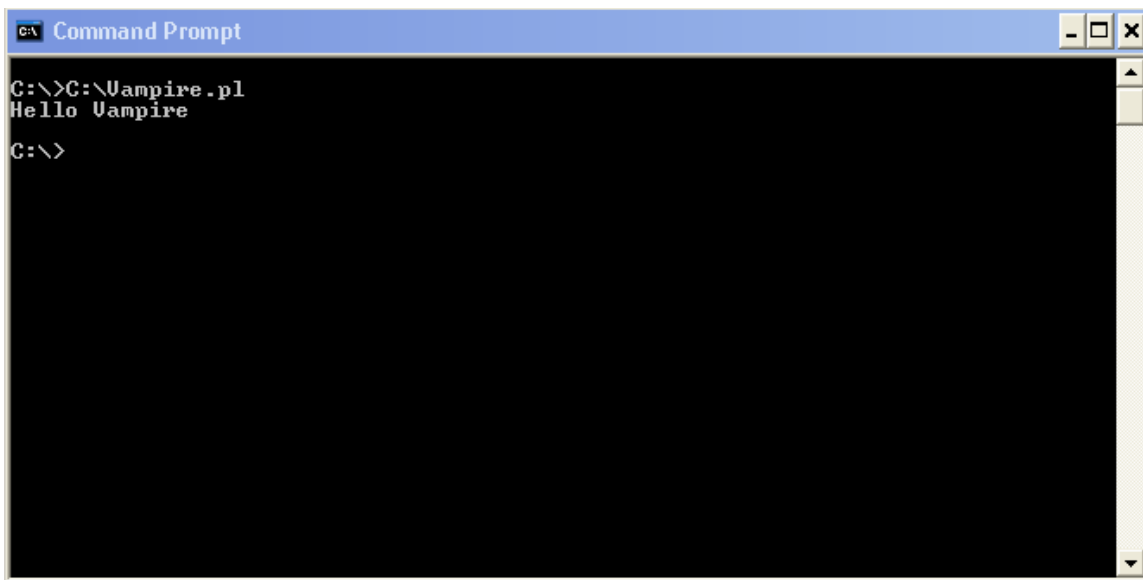
متغیرها رو نشون بدیم و بعد بیشتر دربارش توضیح بدیم !

```
#!/usr/bin/perl -w
$Hello = "Hello Vampire\n";
print $Hello;
```

خوب متغیر در این برنامه "\$hello" میباشد ! و ارزش "hello Vampire\n"

بهش داده شده است و در آخر هم محتویات متغیر چاپ شده که نتایجش به

این صورت میباشد !



```
C:\>C:\Uampire.pl
Hello Uampire
C:\>
```

(نتیجه ی برنامه ی بالا)

خوب یکم بیشتر در این مورد توضیح میدم :

در Perl لازم نیست حتما Type برای متغیرتون تعیین کنید و در زمان مقدار دهی به متغیرها در طول برنامه تعریف میشوند که به چه صورت بوده اند برای مثال متغیر عددی یا

نکته ی دیگر این است که در پرل Type مغیرها قابل تبدیل هستند برای مثال به راحتی میتونید یک متغیر عددی را به کاراکتری یا کاراکتری را به عددی تبدیل کنید !

نکته :

فاصله ی بعد یا قبل = هیچ مشکلی در برنامه به وجود نمیآورد یعنی بین `$vampire="shahin"` و `$vampire = "shahin"` هیچ تفاوتی وجود نخواهد داشت !

در ادامه :

آرایه ها رو بررسی میکنیم!

روی جملات شرطی و نحوه ی بکار گیری آن در پرل کار میکنیم!

گرفتن مقدار از ورودی بررسی میکنیم!

حلقه ها یا Loops را بررسی میکنیم!

LibWWW را کامل بررسی میکنیم!

Socket و برنامه نویسی تحت شبه در پرل را بررسی میکنیم!

نوشتن یک اکسپلویت مبتنی بر وب به وسیله ی پرل و نتیجه ی کار!

و

خوب تا بعد خدا نگه دار

"خدا نصیب هیچ کس نارقیق نکند"

"هر که بشناسد نمک کافیت انگشتی زند"

"کی شناسد گر خورد نامرد انباری نمک"

Special TNX TO : My Beautiful Girl Friend , Hossein asgary , P4th0n , Jack karti , Kaper , Alijsb , WarpBoy , L!Nux and All Real Hacker



(Vampire)

"I'am a hacker, knowledge is what I seek. I exist only to fulfill a lumbering quota of curiosity. To test my skills challenge me, but question my skills, fall before me. The lawprohibits my actions, but my actions are unknown and unpredictable as everything in nature.This fear of the unknown promotes flagitious crimes against the birth rights that everyhuman is given: freedom, curiosity, the right to question. I am a hacker, my actions areflawless, and that way they shall stay. This curiosity completes us all, and drives us all.Hacking is no solo trip, we ride together as notorious bandits, but you cannot stop us, afterall, we are just cyber ghosts, but its not who we are, it's what we do... that defines us."

The End