افزایش امنیت در نرم افزار های تحت وب

پژمان رودخانه ئی
دانشگاه آزاد اسلامی واحد لاهیجان
P. Roudkhaneei@Gmail.com

چکیده : با توجه به گسترش روز افزون نرم افزارهای تحت وب و انجام انواع تبادلات ملی و تجاری بروی بستر وب ، نیاز به امنیت بالا در این نوع از نرم افزار امری ضروری است . در حل حاضر بسیاری از سازمانها و موسسات دولتی و خصوصی در داخل و خارج از کشور، بسیاری از خدمات خود را بر بستر وب ارائه می دهند . از جمله این خدمات می توان به انواع ثبت نام های اینترنتی ، دوره های آموزش مجازی ، ارائه انواع خدمات بانکی ، خرید و فروش آنلاین کالا و صدها خدمت دیگر که امروزه با استفاده از نرم افزار های تحت وب چه در سطح اینترنت و چه در سطح شبکه های خصوصی مورد استفاده وسیع می باشد . در این مقاله روش های مرسومی که هکر ها برای هک کردن نرم افزارهای تحت وب استفاده می کنند معرفی می گردد و همچنن راه کارهای مقابله با این حملات در لایه برنامه نویسی نیز بیان می شود . در پایان چند نرم افزار هایی معرفی می گردد که نرم ازار های تحت وب را از نظر انواع آسیب پذیری ها مورد تست و آزمون قرار می دهد.

واژه های کلیدی : SQl injection - - Encryption – Hacker - CRLF injection - نرم افزار تحت وب

۱ - مقدمه

امروزه با حضور انواع دیواره های آتش ، آنتی ویروسهای قوی و همچنین افزایش امنیت در نرم افزار های شبکه و استفاده از تکنولوژیهای جدید در قطعات سخت افزاری شبکه ، باعث کاهش آمار هک شدن سرور های وب شده است و از این رو هکر ها کم کارتر از گذشته شده اند ! ولی هچ چیزی نمی تواند جلودار هکر های سمج شود و آنها را از کار بیکار کند . اکنون هکر ها توجه خود را به هک کردن سایت ها و نرم افزار های تحت وب دوخته اند تا از نقاط ضعف طراحان نرم افزار های تحت وب استفاده کنند سایت مورد نظر را نابود سازند . در ادامه این مقاله به مرسوم ترین شیوه های هک سایت های اینترنی اشاره می شود و راه کار های مقابله با اینگونه حملات نیز بیان می شود.

۲ - نرم افزار تحت وب (Web Based) چیست ؟

نرم افزار تحت وب ، برنامه کاربردی است که بروی وب سرور سازمان یا شرکت نصب است و کاربران مجاز اینترنت یا اینترانت می توانند از آن استفاده کنند و از خدمات آن بهره مند شوند . یک نرم افزار تحت وب در سه لایه قابل تعریف می شود ، لایه اول مرورگرهای وب هستند ، لایه دوم تولید کننده محتوا می باشد که با استفاده از تکنو لوژیهای سمت مشتری مانند Java Script ، VB Script و یا سمت سرور مانند ASP ، CGI و PHP پیاده سازی می شود . لایه سوم نیز سیستمهای بانک اطلاعاتی می باشد که از جمله پرکاربردترین آنها می توان به My SQL ، MS SQL ، Oracle و DB2 اشاره کرد .

۲ – طرز کار نفوذگران نرم افزار های تحت وب

هکرها گنجینه ای از انواع مکانیزمهای نفوذ به نرم افزارهای تحت وب برای خود دارند که با توجه به شرایط بهترین شیوه را برای آسیب رسانی استفاده می کنند . از جمله ویژگیهایی که هکر برای شناسایی راه های نفوذ به سیستم مورد ارزیابی قرار می دهد به قرار زیر است :

۲-۱ بررسی زیرساختار سرور و سیستم عامل سرور

هکر در ابتدا سعی می کند با استفاده از یک سری ابزار هایی که به Sniffer Scanner معروفند به شناسایی ساختار سرور می پردازد تا بتواند به ماهیت سیستم عامل که وب سرور بروی آن در حال جراست پی ببرد ، از جمله معروفترین این سیستم عامل ها سرور می توانند به Windows, unix , Redhat linux , Sun Solaris , FreeBSD اشاره کرد . در فاز بعدی نفوذگر به شناسایی نوع وب سرور مورد استفاده می پردازد تا بتواند از حفره های امنیتی آنها برای نفوذ به سرور استفاده کند ، از معروفترین وب سرور های می توان به Apache ، IIS ,Lighttpd Oversee, GWS(Google Web Server) و Ngnix اشاره کرد که به ترتیب موارد کاربرد ذکر شده .

۲-۲ نقشه برداری از عملکرد سایت

یک هکر با حوصله کل سایت را پویش می کند تا بتواند حفره های امنیتی و اشتباهاتی که از چشم برنامه نویس پنهان مانده را بیابد و از آن برای نفوذ و آسیب رساندن به نرم افزار تحت وب استفاده کند . هکر برای این منظور از انواع مکانیزم هایی از قبیل تزریق اسکریپ های آلوده به سایت و همچنین جهل هویت برای نفوذ به نرم افزار تحت وب استفاده می کند. هکر ها با استفاده از اسکریپ های آلوده (جهت رخ دادن استثنا پیش بینی نشده و برگرداندن یک سری داده بعنوان خطا که برای هکر بسیار ارزشمند است) به سیستم تحت وب و بازخورد دریافتی سعی در یافتن راهی برای نفوذ یا آسیب رسانی دارند ، در اینجا این موضوع اهمیت پیدا می کند که برنامه نویس یک نرم افزار تحت وب باید با انواع روش های نفوذ آشنا باشد تا با استفاده از راه کارهای مناسب تا حد امکان آسیب پذیری سیستم را کاهش دهد .

۲-۳ اعتبار سنجی ورودی ها در سایت

از جمله روشهای دیگری که هکر ها برای نفوذ به سایت مورد استفاده قرار می دهند اعتبار سنجی در مقابل انواع داه هاست ، اگر برنامه نویس نرم افزار تحت وب در این مورد کوتاهی کند به احتمال فروان باید منتظر تبعات زیانبار باشد ! چه بسا در برخی موارد هکر ها می توانند با استفاده از این نقطه ضعف دستورات بسیار خطرناک را بروی سرور اجرا کنند که به قیمت از دست رفتن اطلاعات نرم افزار و آسیب دیدن سایر سایت ها و نرم افزار های تحت وبی که سرور میزبان آنهاست تمام شود.

۲ - ۴ ضربه آخر

اکنون هکر با توجه به اطلاعاتی که از ماهیت سرور و نقاط ضعف نرم افزار تحت وب بدست آورده و پس از ایزوله کردن آنها ضربه آخر را خواهد ضد و می تواند آسیب هایی جدی به صاحبان وب سایت ، وب سرور و کاربرانی که از این سایت ها و نرم افزار های تحت وب استفاده می کنند وارد کند، از قبیل تغییر home page گرفته ، پاک کردن داده ها در بانک اطلاعاتی و یا فایل های مهم و همچنین استفاده از وب سرور قربانی بعنوان پایگاهی برای انتشار ویروس و کرم های اینترنتی جهت آلوده ساختن کامپیوتر های کاربران و بازدید کنندگانی که جهت استفاده از نرم افزار تحت وب به آن مراجعه کرده اند و نا خواسته در دام ویروس افتاده اند !

۳ – شیوه های محبوب هکر ها برای نفوذ

در این قسمت از این مقاله به مرسوم ترین شیو ه های هک کردن وب سایت ها و نرم افزارهای تحت وب در لایه application و همچنین راه کارهای مقابله با اینگونه حملات نیز بیان می شود.

۱-۳ تزریق دستورات SQL آلوده به سایت (Sql injection)

این شیوه نفوذ یکی از پرکاربردترین راه نفوذ به وب سایت ها و نرم افزار های تحت وب می باشد که هکر ها برای آسیب رساندن و دزدیدن اطلاعات از آن استفاده می کنند ، این شیوه از پرکاربردترین روش هایی حمله در لایه کاربردی (application) است که امروزه به کررات مورد استفاده قرار می گیرد و با این وجود هنوز بسیاری از سایت ها هستند که در مقابل اینگونه حملات کاملاً آسیب پذیرند . بعنوان مثال یک هکر می تواند به فورمی که برای ورود به نرم افزار نیاز به نام کاربری و رمز عبور دارد بگوید که بدن نیاز به نام کاربری و رمز عبور اجازه دسترسی بدهد !

وب سایت ها و نرم افزار های تحت وب به کاربران مشروع خود اجاره می دهند تا اطلاعاتی را ارسال کنند و همچنین داده هایی را از پایگاه وب بازیابی کنند . بانک اطلاعات هسته مرکزی وب سایت است که داده های مورد نیاز کاربران و سایر موارد از جمله اطلاعات محصولات ، اخبار ، مقالات آموزشی را در آن ذخیره می شود و می توان این اطلاعات را پس ار بازیابی در اختیار کاربران قرار داد . هکر ها با استفاده از دستورات غیر اصولی زبان SQL در پس زمینه به وب سایت ها حمله می کنند که در صورت موفقیت می توانند به اطلاعاتی ارزشمندی از نرم فزار تحت وب دست یابند . برخی از قسمت های سایت در معرض خطر نفوذ حملاتی از نوع Sql injection قرار دارندکه از جمله آنها می توان به فورم ورود به سیستم ، جستجو در سایت ، فورم ارسال پیشنهاد و انتقاد ، بخش خرید آنلاین اشاره کرد.

لازم می بینم برای درک بهتر مثالی را مطرح کنم ، فرض کنید که ما فورمی در وب سایت خود داریم که قرار است کاربران سایت بعد از اینکه نام کاربری و رمز عبور خود را وارد کردند بتواند وارد سیستم شوند و سوالات خود را در بخش سوال و جواب (Faq) درج کنند . بعد از اینکه کاربر نام کاربری و رمز عبور خود را وارد کرد منتظر تایید نرم افزار می ماند تا بعد از اینکه صحت نام کاربری و رز عبور بررسی شد اجاره کار با نرم افزار تحت وب به وی داده شود. برای گرفتن این تائیدیه تعاملی بین نرم افزار و بانک اطلاعاتی انجام می گیرد . این مکانیزم نفوذ می تواند به تمامی تکنولوژی های برنامه نیسی که جهت تولید سایت های داینامیک و پویا استفاده می شود آسیب برساند ، تلنولوژیهایی نظیر : ASP , ASP.Net , PHP , JSP and CGI . برای تمامی این تکنولوژی فقط به یک ابزار جهت هک کردن نیاز است و آن چیزی جز یک مرورگر وب سایت نیست !

سوال : شاید برایتان سوال پیش آمده باشد گه چرا ارسال مستقیم دستورات SQL بروی بانک اطلاعاتی که در پشت دیوارهای ها آتش (Firewall) و مکانیزم های امنیتی دیگر قرار دارد ممکن است ؟

جواب : از زمانیکه وب سایت بر بستر وب انتشار می یابد سیاست های امنیتی برای حفاضت از آن در نظر گرفته می شود و با استفاده از

فایروال ها و سایر ابزار های امنیتی از پورت ها ی آن در مقابل نفوذ حفاظت می شود ، ولی همیشه اجازه بروز آوری و ایجاد داده های جدید در بانک اطلاعاتی فراهم است زیرا برای تغییر داده ها و افزودن داده های جدید باید به بانک طلاعاتی دسترسی داشت .

زبان SQL به شما امکان می دهد که داده ها را تغییر دهید و یا داده های جدید را به بانک اطلاعاتی بیفزایید و در نهایت اطلاعات را بازیابی کنید . در واقع زبان SQL تنها راهی است که این امکان را فراهم می سازد که وب سایت ها و نرم افزار های تحت وب بتوانند با بانکهای اطلاعاتی رابطه ای ارتباط داشته باشد . از جمله بانک های اطلاعاتی رابطه ای می توان به Oracle , Microsoft Access , My SQL , Microsoft SQL server اشاره کرد .

در اینجا قطعه کدی را می بینیم که اکثر برنامه نویسان نرم افزار های تحت وب از این مکانیزم برای نوشتن سیستم Login استفاده می کنند ، به کد زیر توجه کنید :

```
<form method="post"
action="http://testasp.acunetix.com/login.a
sp">
<input name="txtUserName" type="text"
id="tfUName">
<input name="TxtPassword" type="password"
id="tfUPass">
</form>
```

کد Html بالا دو فیلد در فورم ظاهر می کند که برای گرفتن نام کاربری و رمز عبور از کاربر در نظر گرفته شده است حالا کد SQL که بصورت معمول در لایه برنامه نویسی از سوی برنامه نویسان مورد استفاده قرار می گیرد را بررسی می کنیم :

```
SELECT id,UName,Pwd
FROM tbl_users
WHERE username = '@username'
AND password = '@password'
```

اگر برنامه نویس مقادیر متغیر های @username و @password بصورت مستقیم و بدون فیلتر کردن از فورم کاربری دریافت کند کار هکر ها را برای هک کردن سایت بسیار آسان کرده است . به کد زیر توجه کنید :

```
SELECT id,UName,Pwd
FROM tbl_users
WHERE username = 'reza'
AND password = 'anything' OR 'x'='x'
```

هکر فرض می کند که کاربری با نام Reza در این سایت یا سیستم تحت وب عضویت دارد ولی به رمز عبور آن دسترسی ندارد ، اگر سیاست های صحیح امنیتی از سوی برنامه نویس در نظر گرفته نشده باشد هکر با استفاده از تجربه و خلاقیت خود به سایت حمله خواهد کرد ، همان گونه که در کد دیدید هکر برای رمز عبور رشته OR 'x'='x' را وارد می کند ، حال خود قضاوت کنید . این ترفند به هکر اجاره می دهد که از قسمت اول شرط WHERE صرف نظر شود و هکر موفق می شود بدون اینکه واقعاً رمزعبور و نام کاربری را بداند وارد سیستم می شود .

راه حل : بنده در اینجا الگوریتمی را بیان می کنم که بر اساس تجربیات شخصی خود در طراحی نرم افزار های تحت وب طراحی شده . من از این الگوریتم در سایت یکی از سازمان های کشور استفاده کرده ام و تا کنون پس از گذشت ک سال و با بیش از یک میلیون و سیصد هزار بازدید هیچ نفوذی به سایت با استفاده از SQL injection گزارش نشده . این الگوریتم به زبان Vb.Net است و با اندکی تغییر می توانید در سایر زبان ها از آن استفاده کنید :

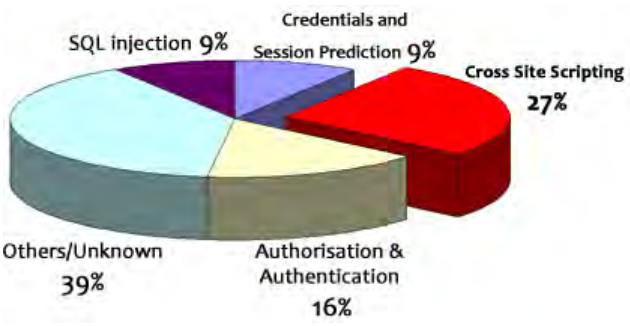
```
Public Function ClearIllegalString(ByVal sInput
As String) As String

   Dim sBadChars() As String = {"select", "drop",
"--",
   "insert", "delete", "xp_", "#", "%", "'", "(",
")", "/", "\",
   ":", "@", ";", "<", ">", "[", "]", "`", "|"}

   Dim iCounter As Integer
   Dim output As String

   sInput = Trim(LCase(sInput))

  For iCounter = 0 To UBound(sBadChars)
       If InStr(sInput, sBadChars(iCounter)) > 0
Then
          sInput = Replace(sInput,
BadChars(iCounter), "")
      End If
   Next

     output = sInput
     Return output

 End Function
```

این تابع در صورتی که کاراکتر های آلوده در ورودی رشته باشد آنها را از رشته حذف می کند . این تابع را می توان به گونه ای دیگر نیز تغییر داد که بصورت تشخیص دهنده عمل کند و با برگشت مقدار true یا false بیان کند که رشته ورودی آلوده است یا نه .

۲-۳ حملاتی از نوع Cross Site Scripting(CSS or XSS)

هکر ها دائماً در حال کشف روش های جدید نفوذ هستند تا با استفاده از آن به داده های بسیار مهم مانند رمز عبور حساب های اینترنتی و اطلاعات مهم دولتی دسترسی داشته باشند . همانگونه که در شکل ۱ مشاهده می کنید مشخص است که بیشترین تعداد حمله به سایت ها از بین روش های شناخته شده حمله هایی از نوع Cross site Scripting است . در حالت کلی در این روش هکر بعنوان کاربر نهایی نرم افزار کد های خطرناک برای سایت ارسال می کند که با استفاده از آنها اطلاعات مهمی را نیز به دست می آورد .

شکل ۱



آمار میزان استفده از روش های مختلف در نفوذ به سایت ها

هکر با استفاده از روش XSS کد های خطرناکی از نوع , JavaScript VB Script , Html , Active و Flash به صفحات پویا و دینامیک سایت ها تزریق می کند و با استفاده از نقاط ضعف و حفره های امنیتی که در تکنولوژیهای مورد استفاده در سایت وجود دارد کار خود راانجام می دهد . هکر ها با استفاده از این روش می توانند به اهدافی مثل سرقت هویت ، دستیابی به اطلاعات مهم و حساس ، بدست آوردن دستیابی رایگان به حساب های اینتر نتی ، اینکه اطلاعات کوکی ها و Session های کاربران ، جاسوسی کردن اطلاعات کاربران سیستم های تحت وب و حملاتی از نوع (Denial of Service) برسند . فرض کنید می خواهیم برای سایت خود سیستم ورود به سایت طراحی کنیم به کد زیر توجه کنید :

```
<form action="destination.aspx">
<table><tr><td>
Login:</td><td>
<input type=text length=20 name=login>
</td></tr><tr><td>
Password:</td><td>
<input type=text length=20 name=password>
</td></tr></table>
<input type=submit value=LOGIN></form>
```

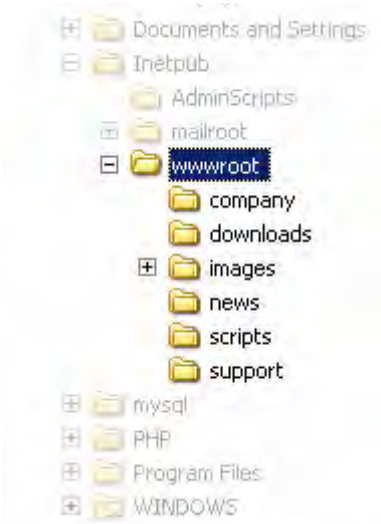
یک هکر با استفاده از یک صفحه login جهلی و تزریق آن به صفحه destination.aspx سعی در نفوذ به سیستم دارد . هکر برای نفوذ به آدرس زیر URL زیر redirect می کند .

http://www.mysite.ir/Search.aspx?tfSearch=%3Cbr%3E%3Cbr%3EPlease+login+with+the+form+below+before+proceeding%3A%3Cform+action%3D%22test.asp%22%3E%3Ctable%3E%3Ctr%3E%3Ctd%3ELogin%3A%3C%2Ftd%3E%3Ctd%3E%3Cinput+type%3Dtext+length%3D20+name%3Dlogin%3E%3C%2Ftd%3E%3C%2Ftr%3E%3Ctr%3E%3Ctd%3EPassword%3A%3C%2Ftd%3E%3Ctd%3E%3Cinput+type%3Dtext+length%3D20+name%3Dpassword%3E%3C%2Ftd%3E%3C%2Ftr%3E%3C%2Ftable%3E%3Cinput+type%3Dsubmit+value%3DLOGIN%3E%3C%2Fform%3E

راه کار : برنامه نویس نرم افزار باید قبل از اینکه سایت را بروی اینترنت انتشار دهد نرم افزار خود را با استفاده از نرم افزار های "جستجوگر نقاط آسیب پذیری" مورد تست و بررسی قرار دهد تا نرم افزار از نظر آسیب پذیری در مقابل حملات XSS مورد آزمون قرار گیرد. این حملات با استفاده از دستکاری در URL سایت و از طریق مرورگر وب صورت می پذیرد . برنامه نویس باید قالب صحیح آدرس دهی و انتقال اطلاعات در صفحات مختلف و استفاده صحیح از session ها و Catch را بداند تا از این حیث سایت از حملات هکر ها مصون بماند .

۳-۳ حمله با استفاده از پیمایش دایرکتوری ها

روش که به Directory Teraversal Attack معروف است که هکر با استفاده از این روش می تواند به پوشه هایی که دسترسی به آنها محدود شده دسترسی داشته باشد و همچنین در برخی موارد حتی می تواند به پوشه هایی بیرون از پوشه ریشه (Root directory) دسترسی یابد . وب سرور ها دو مکانیزم برای امنیت دایرکتوری ها دارند که عبارتند از لیست کنترل دسترسی (Access control lists) که منظور میزان سطح دسترسی به آن پوشه است و مورد دیگر دایرکتوری ریشه است . در وب سرور IIS به همراه ویندوز سرور ارائه شده مسیر پیش فرض دایرکتوری ریشه C:\Inetpub\wwwroot می باشد . یک کاربر فقط به دایرکتوری wwwroot دسترسی دارد و نمی تواند به پوشه windows و یا پوشه download دسترسی داشته باشد . به شکل زیر توجه کنید .



شکل ۲

دایرکتوری ریشه از دسترسی کاربران به فایل های مهم و حساس ممانعت می کند فایل هایی مانند cmd.exe در سرور های ویندوز و یا فایل passwd در سرور های linux و Unix . همچنین نرم افزار هایی که بروی سرور نصب می شود و نیز کد هایی که توسط برنامه نویس نوشته می شود می تواند مشکلاتی را بوجود آورد که باعث بروز چنین حملاتی از سوی هکر ها گردد. یک هکر برای انجام اینگونه حملات به یک مرورگر وب نیاز دارد بعلاوه آگاهی از مسیر های پیش

فرض دایرکتوریهای مهم . برای درک بهتر موضوع در ادامه مثالی از اینگونه حملات مطرح می شود.

در نرم افزار های تحت وب که از صفحات پویا و دینامیک بهره می برند برای دریافت اطلاعات از ورودی بطور متداول از دو نوع متد استفاده می شود ، GET و Post . به URL زیر توجه کنید :

http://wwww.iau-lahijan.ac.ir/article.aspx?view=a789.html

مرورگر ، صفحه دینامیک article.aspx را از سرور تقاضا می کند و همچنین مقدار a789.html برای پارامتر view ارسال می کند . هنگامیکه این تقاضا بروی سرور اجرا می شود صفحه دینامیک article.aspx فایل a789.html را از سیستم فایل سرور تقاضا می کند . یک هکر می تواند با استفاده از کدی مشابه مثال زیر به فایل هایی خارج از دایرکتوری ریشه دسترسی داشته باشد .

http://wwww.iau-lahijan.ac.ir/article.aspx? view=
../../../../../Windows/system.ini

هکر با استفاده از این کد می تواند محتویات فایل system.ini را بازیابی کند و همچنین می تواند سایر پوشه های واقع در پوشه windows را پیمایش کند .

مثال دیگری را با هم بررسی می کنیم که چطور یک هکر می تواند دستوری را بروی سرور اجرا کند و اطلاعات ارزشمندی را از سرور بدست آورد . به URL زیر توجه کنید که چگونه بروی سرور فایل cmd.exe اجرا می شود :

http://ww.domain.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\

این تقاضا یک لیست کامل از تمام دایرکتری هایی که در درایو C سرور قرار دارد بر می گرداند . واژه %5c رمز شده کاراکتر "\" می باشد. این نوع تبدیل کاراکتر به کد معروف به escape code معروف است .

راه کار : برای جلوگیری از این نوع حملات برنامه نویس باید تابعی را در برنامه طراحی کند تا بتواند انواع escape code را تشخیص دهد و از تزریق آن به سایت جلوگیری کند ، در ادامه این مقاله Scanner هایی را معرفی می کنیم که نرم افزار تحت وب را در مقابل انواع حملات پیمایش دایرکتوری تست می کند . همچنین مدیر سایت باید توجه داشته باشد که همیشه از آخرین نسخه نرم افزار های سرور استفاده شود و مدام بروزآوری گردد و همیشه patch های امنیتی سیستم عامل مورد استفاده را بروی سرور نصب کند .

۳-۴ حمله از نوع CRLF Injection

منظور از CRLF مقداری است که در پایان خط ها در فایل ها تعریف می شود (CR, ASCII 13, \r) و (LF, ASCII 10, \n) . این کاراکترهای اسکی در حالت نمایش ظاهر نمی شوند ولی در سیستم فایل به معنی پایان خط می باشد . ترکیب CR و LF هنگامی استفاده می شود که مثلاً شما کلید Enter را از روی کیبرد بفشارید. بسته به نوع نرم افزاری که استفاده می کنید کلید Enter به معنای اجرای فرمان و یا رفتن به خط جدید می باشد . این نوع از حملات جز مشکلات امنیتی سرور و یا سیستم عامل نیست بلکه بسته به نوع کدنویسی برنامه نویس دارد و بسیاری از توسعه دهندگان وب از این نوع حملات بی خبرند و این خبر خوبی برای هکر هاست . هکر ها با استفاده از این نوع حملات می توانند به اطلاعات ارزشمندی از عملکرد های سیستم تحت وب و سرور و همچنین Log File های سرور و کوکی ها بدست آورد . هکر می تواند با جستجوی این کاراکتر ها ی اسکی به مقاصد خود برسد .

راه کار : برای جلوگیری از چنین حملاتی برنامه نویس سایت باید ورودی ها را فیلتر کند و تابع تشخیص دهنده بنویسد . نوشتن چنین تابعی بسیار آسان است و می تواند کمک شایانی برای مصون ماندن سایت از چنین حملاتی باشد . همچنین برای تشخیص این نوع از حملات نیز می توان از scanner ها استفاده کرد .

۴ – رمزنگاری داده های حساس

اطلاعات مهم و حساس مانند رمز عبور و نام کاربری حساب های اینترنتی بهتر است بصورت رمز شده در بانک اطلاعاتی ذخیره شود تا اگر نفوذگرها به سیستم هم نفوذ کنند نتوانند و از اطلاعات بدست امده استفاده کنند . الگوریتم های رمز نگاری به سه دسته کلی الگوریتم های متقارن، الگوریتم های نامتقارن و الگوریتم های هشینگ تقسیم می شوند . از مهمترین الگوریتم های رمز نگاری متقارن می توان به الگوریتم های DES , RC2 , Rijndael , TripleDEC اشاره کرد ، همچنین الگوریتم های DSA و RSA از معروفترین الگوریتم های رمزنگاری نامتقارن هستند . معروف ترین الگوریتم های رمزنگاری هشینگ عبارتند از : MD5 , SHA1 , SHA256 , SHA384 , SHA512 . بنا به کاربرد می توان یکی از الگوریتم ها را استفاده کرد .

به کد زیر توجه کنید، این تابع به زبان VB.Net نوشته شده :

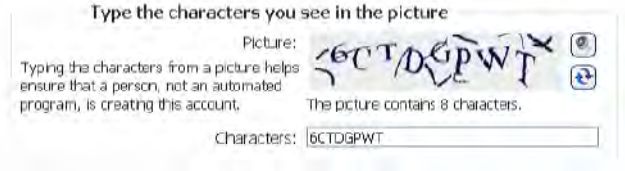
```
Public Function ComputeMD5Hash(ByVal StrPlainText As
String) As Byte()
        Dim hashedDataBytes As Byte()
        Dim Enconder As New UTF8Encoding
        Dim MD5Hasher As New MD5CryptoServiceProvider
        hashedDataBytes =
MD5Hasher.ComputeHash(Enconder.GetBytes(StrPlainText))
   Return hashedDataBytes
End Function
```

بنده برای سیستم Login یکی از نرم افزار های تحت وبی که اخیراً طراحی کرده ام از الگوریتم MD5 جهت ذخیره سازی رمزعبور در بانک اطلاعاتی استفاده کرده ام . تابعی که ذکر شده رشته ورودی را

Encrypt می کند فریم ورک Net. کتابخانه کاملی از انواع الگوریتم های رمزنگاری دارد که می توان به آسانی از آنها در طراحی نرم افزار های امن استفاده کرد.

۵ – استفاده از تصاویر امنیتی

با افزایش روزافزون تبادلات جهانی و ارسال انواع اطلاعات از سوی کاربران برای سایت ها و پایگاه های اینترنتی مختلف هکر ها را برآن داشت که حملاتی را برای آسیب رساندن به این پایگاه های اینترنی ترتیب دهند . همین امر باعث شد که توسعه دهندگان به فکر استفاده از تصاویر امنیتی باشند تا رباتهای خزنده (Crawler) نتوانند به سایت ها حمله کنند و با ارسال تقاضا های زیاد بار ترافیکی به سرور را افزایش دهند و مقدمات حملاتی از نوع Dos را ترتیب دهند . البته هکر ها بیکار ننشستند و رباتهایی طراحی کردند که می تواند تصاویر امنیتی را اسکن کند و مقادیر آنر بخواند .



شکل ۳

توسعه دهندگان وب نیز با خلاقیت زیاد هر روز روش جدیدی را برای تولید تصاویر امنیتی بکار می برند و امروزه علاوه بر تصاویر از سوالات مفهومی نیز استفاده می کنند تا رباتها را از تشخیص صحیح عاجز سازند . به شکل شماره ۳ توجه کنید .

۶ – معرفی نرم افزار های جستجو گر نقاط آسیب پذیری

با افزایش روز افزون اخبار هک شدن سایت ها و نرم افزار های تحت وب برخی از شرکت هایی که در زمینه راه کارهای امنیتی فعالیت دارند به آن داشت تا نرم افزار هایی را طراحی کنند که بتواند بصورت آفلاین سایت ها و نرم افزارهای تحت وب را از نظر امنیت و میزان آسیب پذیری مورد تست و آزمون قرار دهد . برخی نرم افزار های آنلاین هم وجود دارد که سایت ها را بصورت آنلاین نیز مورد تست و بررسی قرار می دهد . به جدول شماره ۱ توجه کنید که چند نرم افزار معرفی شده و ویژگیهای آن نیز بیان شده.

جدول ۱

Product name	Features
Web Vulnerability Scanner	Provides protection from the following attacks : • CRLF injection attacks • Code execution attacks • Directory traversal attacks • File inclusion attacks • Input validation attacks
	• Authentication attacks Creates professional security audit reports
AppDetective	A network-based vulnerability assessment tool that rates the security strength of applications within your network.
SecureSphere Dynamic Profiling Firewall	Provides total protection for Web application and Web service attacks, database breaches and worm infections. Incorporates a Web firewall, a database firewall, database auditing, Web services firewall, Intrusion Prevention System (IPS) and a network firewall. Includes one gigabit performance sub-millisecond latency.
Scando Web application scanner	Detects and eliminates Web application vulnerabilities before exploitation by hackers and thieves. Compatible with all Web technologies like Flash, ASP, JavaScript, XML and Web Services. Follows a structured three-stage scanning process: 1. Studies the structure and content of the Web application. 2. Executes dummy hacking instances to detect vulnerabilities. 3. Displays scan results in systematic reports along with suggestions for remedial solutions.
AppScan DE	Integrated seamlessly into VS.NET, AppScan DE is a powerful automated unit-testing tool that enables rapid development of secure Web applications.
WebInspect	Efficiently detects vulnerabilities in Web applications. Ensures that there's no chance of an attack at any point in the Web application development and implementation of the lifecycle.

معرفی نرم افزار های یابنده نقاط آسیب پذیری و ویژگی های آنها

۷ – نتیجه گیری

با توجه به مباحثی که در ایم مقاله مطرح شد می توان به این مهم رسید که اکثر دلایلی که باعث هک شدن سایت می شود در لایه Application قابل بررسی و رفع است و برنامه نویس باید تمامی مقادیری را که از فیلدهای ورودی و Query String ها می خواند را برای یافتن کد های آلوده آنالیز کند و این مهم در سایه آگاهی برنامه نویس از جدیدترین مکانیزم های نفوذ میسر می شود. اگر برنامه نویس

های سیستم های تحت وب با انواع روش های امنیتی آشنایی داشته باشند و یا با متخصصان امنیتی مشاوره کنند می توانند نرم افزار امنی را طراحی کنند که در مقابل نفوذ هکر ها تا حدد امکان ایمن باشد . امیدوارم مباحث مطرح شده در این مقاله بتواند دید جدیدی در برنامه نویسی این دسته از نرم افزار ها به شما بدهد .

مراجع

[1] Fiach Reid , *Network programming in dot.NET C.Sharp and Visual.Basict.NET*, Digital.Press , May.2004

[2] Thiru Thangarathinam, *Professional ASP.NET2.0 Databases* , Wrox Press, Feb 2007

[3] Matthew MacDonald , Mario Szpuszta, *"Pro ASP.NET 2.0 in CSharp 2005"*, Apress , 2005.