دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

گزارش کارآموزی

نام و نام خانوادگی کارآموز: علی اسماعیلی

شماره دانشجویی: 8718083

استاد کارآموزی: آقای دکتر خدیوی

سرپرست کارآموزی: آقای دکتر تدین

محل کارآموزی: مرکز تحقیقات مخابرات ایران

آدرس: تهران - امیرآباد شمالی - انتهای خیابان کارگر شمالی

تاریخ شروع : 90/4/11 **تاریخ پایان:** 90/6/3

تلفن: 8497629 – 021

فهرست مطالب

چکیده

قلب هر برنامه وب پایگاه داده است. پایگاه داده مکانیزم برای ذخیره سازی و بازیابی هم مشتری و هم هکر است. پایگاه داده جایی است که اطلاعات مشتری یا اطلاعات محرمانه در آن قرار دارد، در نتیجه امنیت پایگاه داده جزو مسائل کلیدی تلقی می شود. علاوه بر آن در نصب استاندارد پایگاه داده بسیاری حفره های امنیتی وجود دارد که لازم است برطرف شوند.

فصل اول

معرفی مرکز تحقیقات مخابرات ایران

1-1- مقدمه

مرکز تحقیقات مخابرات ایران به عنوان قدیمی ترین مرکز پژوهشی در حوزه فناوری اطلاعات (ICT)، با بیش از 39 سال سابقه تجربه علمی در امر تحقیق و مشاور مادر وزارت متبوع، اصلی ترین پایگاه تحقیقات در زمینه ارتباطات و فناوری اطلاعات در کشور است. این مجموعه هم اینک با برخورداری از کادری تخصصی و مجرب در حوزه های مختلف ICT و دیگر امکانات پژوهشی و آزمایشگاهی پیشرفته در قالب چهار پژوهشکده فعالیت های تحقیقاتی عمده ای را دنبال می کند.

این مرکز در سال 1349 با امضای تفاهم نامه ای بین دول تهای ایران و ژاپن تاسیس شد و به طور محدود فعالیت های تحقیقاتی بنیادی خود را که پیش از انقلاب اسلامی عمدتا ماهیتی دانشگاهی داشت ، آغاز کرد. با پیروزی انقلاب و تصویب شورای عالی انقلاب فرهنگی اداره امور مرکز تحقیقات مخابرات ایران به وزارت پست و تلگراف و تلفن(ارتباطات و فناوری اطلاعات) واگذار شد و به عنوان بازوی تحقیقاتی و مشاوره ای در این وزارتخانه فعالیت های گسترده ای را دنبال کرد. بازنگری در ساختار فعالیتهای مرکز با هدف خود کفایی ، استقلال فنی و تخصصی ،مسئولان را بر آن داشت تا نسبت به تحقیق و توسعه به ویژه تحقیقات کاربردی در زمینه فناوری مخابراتی اولویت خاصی قائل شود. در سال 1376 مرکز تحقیقات مخابرات ایران به پژوهشکده ارتقا یافت و در سال 1384 با تاسیس سه پژوهشکده به پژوهشگاه تبدیل شد. این

مرکز هم اینک با دارا بودن چهار پژوهشکده به عنوان پژوهشگاهی تحقیقاتی ، قطب پژوهشی فناوری ارتباطات و اطلاعات محسوب می شود و نقش مهمی را به عنوان مشاور مادر در بخش ICT دارا می باشد.

2-1- پژوهشکده امنیت اطلاعات و فناوری ارتباطات

در این پژوهشکده اهداف زیر دنبال می شوند.

- برنامه‌ریزی تحقیق و پژوهش در زمینه امنیت فضای تبادل اطلاعات (افتا)
- ارائه مشاوره‌های تخصصی و کلان به بخشهای اجرایی علی‌الخصوص وزارت ارتباطات و فناوری اطلاعات و زیر مجموعه‌های مرتبط جهت انتخاب و بکارگیری مناسب فناوری‌های افتا
- کمک به شکل‌گیری قوانین و مقررات و نیز نهادهای مؤثر در زمینه امنیت
- حمایت از صنعت بومی‌سازی افتا و کمک به توسعه نیروی انسانی متخصص و نیز ارتقاء جایگاه علمی کشور در زمینه تولید دانش و فناوری این حوزه.

هم اکنون در این پژوهشکده گروههای پژوهشی زیر مشغول به فعالیت هستند.

- گروه امنیت جامعه اطلاعاتی
- گروه فناوری امنیت شبکه
- گروه امنیت فناوری اطلاعات و سامانه ها
- اداره آزمایشگاه ها و استانداردهای امنیت

محورهای تحقیقاتی این پژوهشکده عبارتند از

- پژوهش در زمینه قوانین و مقررات و اخلاق مرتبط با امنیت فضای تبادل اطلاعات

- رشد و تقویت نهاد ها و سرمایه های اجتماعی موثر در تعالی امنیت جامعه اطلاعاتی
- امنیت پژوهش در نظام های مهم جامعه اطلاعاتی
- بررسی و تحقق در زمینه موضوعات بین المللی جهانی تاثیر گذار بر امنیت فضای تبادل اطلاعات ملی
- طرح و برنامه ریزی امنیت
- سامانه ی مدیریت امنیت اطلاعات ICT
- مدیریت امداد و هماهنگ آگاهی رسانی
- تامین امنیت محتوا در ICT
- ارزیابی مدیریت امنیت ICT
- ارزیابی و تحلیل امنیتی شبکه ها
- تامین امنیت شبکه ها
- نظارت و پشتیبانی امنیت شبکه ها
- پشتیبانی حوادث غیر مترقبه در شبکه ها
- کنترل دسترسی فناوری اطلاعات در سیستم ها
- تامین امنیت محتوا در ICT
- کنترل کاربردی در فناوری اطلاعات و سیستم ها
- تامین امنیت سیستم ها در فناوری اطلاعات
- تامین امنیت اطلاعات.

بطور خاص، در قسمت فناوری امنیت شبکه دو هدف اصلی زیر دنبال می شوند.

- هدایت و مدیریت پژوهش‌های راهبردی - کاربردی در زمینه‌های ارزیابی، ارتقاء و پشتیبانی امنیت در انواع شبکه‌های داده و مخابراتی کشور
- انجام فعالیت‌های علمی - پژوهشی بنیادی با هدف جذب و تولید دانش مفید جهت رفع نیازهای ICT کشور در حوزه امنیت شبکه

فصل دوم

پایگاه داده و امنیت آن

2-1- مقدمه

پایگاه داده ها (SQL) مدت طولاتی است که بخش جدا نشدنی از کسب و کار است. این پایگاه داده ممکن است یک فایل متن ساده تا یک پایگاه داده شی گرا باشد. لذا در هر شغل یا برنامه ای به ذخیره و بازیابی سریع اطلاعات نیاز است.

برنامه های وب امروزه با پایگاه داده ها خیلی در ارتباط هستند. آنها در همه چیز از جمله ذخیره سازی نام کاربر و رمز عبور تا آدرس پستی کاربران و اطلاعات مربوط به کارت اعتباری آنها مورد استفاده قرار می گیرد. در نتیجه لازم است که پایگاه داده را خوب بشناسیم و سپس چگونه هکرها محدودیت های درون پایگاه داده را دور می زنند و به اطلاعات آن دسترسی پیدا می کنند.

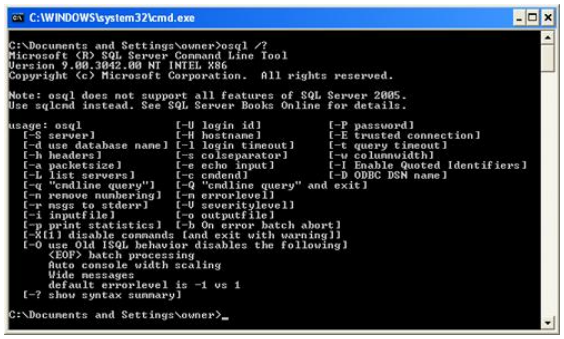
در بخش 2-2 انواع پایگاه داده ها را شناسایی کرده و در بخش 2-3 به حفره امنیتی آنها اشاره کرده و در بخش 2-4 بعضی از نرم افزارهای مورد استفاده جهت حمله به پایگاه داده را بررسی می کنیم. در بخش 2-5 نیز به راه های تشخیص نفوذ احنمالی و راه های مقابله با آن را معرفی می کنیم و در بخش 2-6 نتیجه نهایی تحقیق را بیان می کنیم.

2-2-انواع پایگاه داده

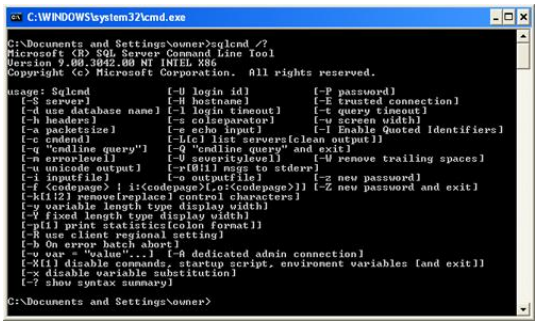
پایگاه داده های مورد استفاده در بازار Microsoft SQL Server و Oracle هستند. Microsoft SQL Server در حال حاضر به علت هزینه پایین مالکیت آن، مورد استفاده است. در نتیجه هزاران شرکت و افراد آن را به شکل هایی توسعه دادندو مسلط بر بانکداری اطلاعاتی آنلاین شدند. برای اتصال به پایگاه داده Microsoft SQL Server می توان از برنامه Management studio (شکل 2-1) یا Osql (شکل 2-2) یا sqlcmd (شکل 2-3) استفاده کرد.

سرویس گوش دهنده اوراکل نقطه ورود به پایگاه داده اوراکل است. این سرویس با گوش فرا خواندن درخواست ها از سوی منابع از راه دور یا محلی آنها را به پایگاه داده مورد نظر منتقل می کنند. سرویس از طریق پرت tcp 1521 به درخواست ها گوش می دهد اما مدیران می توانند به پرت های دیگر از جمله 1541 تغییر دهند. برای اتصال به پایگاه داده اوراکل می توان از برنامه های SQL Developer (شکل 2-4) یا SQL*PLUS (شکل 2-5) استفاده کرد[1].

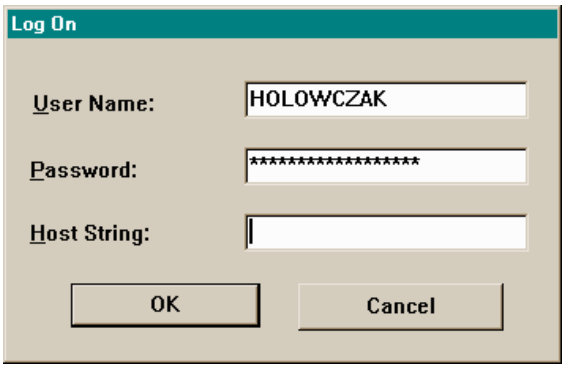
شکل 2 -1



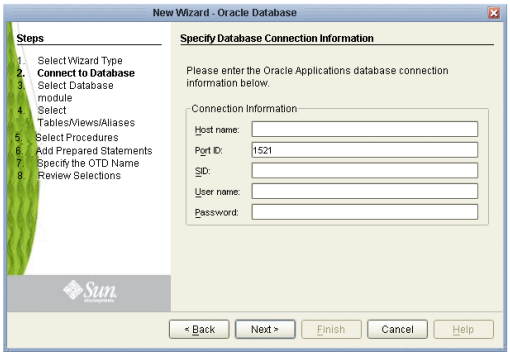
شکل 2- 2



شكل 2– 3



شكل2– 5



شكل 2 -4

2-3-حفره های امنیتی پایگاه داده ها

سرور های SQL دارای روال های ذخیره شده هستند که از طریق آن توسعه دهندگان بتوانند دستورات SQL را بر روی سرورهای وب اجرا کنند و راندمان برنامه را بالا ببرند. در نصب پیش فرض، SQL Server دارای یک سری حفره های امنیتی در روال های ذخیره شده دارد که حمله کننده می تواند از آن برای تخریب پایگاه داده استفاده کند. نمونه هایی از حفره های امنیتی در روالهای ذخیره شده را در جدول 2-1 می توان یافت[1].

جدول 2- 1

Procedure	**توضیحات**
sp_configure	تنظیمات پیکربندی کلی از جمله دسترسی از راه دور، اجازه به روز شدن، تماس ها و ... را می تواند تغییر یا نمایش دهد.
sp_helpdb	پایگاه داده های موجود را لیست می کند و با استفاده از نام پایگاه داده به عنوان پارامتر، اطلاعاتی در مورد آن را نمایش می دهد.
sp_helpprotect	اطلاعات در مورد اجازه دسترسی به اشیا را نمایش می دهد.
sp_OACreate	یک نمونه از شی OLE را ایجاد می کند.
sp_OADestroy	یک نمونه از شی OLE را تخریب می کند.
sp_OAGetProperty	اطلاعاتی در مورد شی OLE را نمایش می دهد.
sp_password	گذر واژه برای کاربری را ایجاد می کند یا آن را نغییر می دهد.
sp_tables	جداول درون پایگاه داده را نمایش می دهد.
sp_who	اطلاعاتی درباره اتصالات SQL SERVER از جمله وضعیت، کاربر، کامپیوتری که اتصال از آنجا برقرار می شود و نام پایگاه داده را نمایش می دهد.
xp_availablemedia	درایو های دستگاه را بازیابی می کند.
xp_cmdshell	دستوراتی را با اجازه administrator اجرا می کند.
xp_deletemail	یک پیغام را از Microsoft SQL Server inbox حذف می کند.

xp_dirtree	اجازه می دهد تا درخت یک directory بدست آید.
xp_enumgroups	یک لیست از گروه های سیستم را نشان می دهد.
xp_getnetname	اسم NetBIOS سیستم را نمایش می دهد.
xp_readmail	یک پیغام از SQL Server inbox را باز می کند.
xp_regdeletekey	کلید Registry را پاک می کند.
xp_regdeletevalue	مقدار درون کلید Registry را پاک می کند.
xp_regenumkeys	کلید Registry را می شمارد.
xp_regenumvalues	مقادیر درون کلید Registry را می شمارد.
xp_regread	کلید Registry را می خواند.
xp_regremovemultistring	کلید Registry چند رشته ای را پاک می کند.
xp_regwrite	مقداری درون کلید Registry می نویسد.
xp_sendmail	یک پست الکترونیکی به شخصی ارسال می کند.
xp_servicecontrol	اجازه می دهد یک کاربر سرویس ویندوز را شروع یا متوقف نماید.
xp_startmail	SQL Server mail را باز می کند.
xp_stopmail	SQL Server mail را می بندد.
xp_subdirs	زیر شاخه ها را لیست می کند.

پایگاه داده های موجود پیشفرض در نصب پیشفرض یکی دیگر از حفره های امنیتی SQL Server را تشکیل می دهد. بعضی از این پایگاه داده ها جهت تضمین کارایی پایگاه داده نصب می شوند که در جدول 2-2 خلاصه شدند.

جدول 2- 2

master	پایگاه داده master برای نگهداری تمام اطلاعات سیستم از جمله نام های کاربری، تنظیمات و روال های ذخیره شده سیستمی است. SQL SERVER بدون یک نسخه سالم از این پایگاه داده اجرا نمی شود.
msdb	پایگاه داده msdb اطلاعات SQL SERVER Agent از جمله وظایف تعریف شده، اپراتورها و alert های تعریف شده را نگهداری می کند.

model	پایگاه داده model به عنوان یک قالب برای تمام پایگاه داده های ساخته شده توسط کاربر است.
tempdb	پایگاه داده tempdb اشیا موقتی پایگاه داده از جمله جداول و روال های ذخیره شده موقتی را ذخیره می کند.

در درون هر کدام از پایگاه داده ها که توسط کاربر ساخته می شوند جداولی قرار دارند که اطلاعات درون آن می تواند برای حمله کننده مفید واقع شود[1]. در جدول 2-3 نمونه هایی از این جداول خلاصه شدند.

جدول 2- 3

Syscolumns	تمام ستون ها در درون تمامی جداول و view ها را نمایش می دهد. علاوه بر آن یک ردیف برای هر پارامتر درون روال ذخیره شده را نشان می دهد.
Sysfiles	تمام فایل های درون پایگاه داده را نمایش می دهد.
Sysobjects	تمام اشیا یک پایگاه داده خاص را نمایش می دهد.
Syspermissions	اجازه های گرفته شده و داده شده به کاربران، گروه ها و نقشها را نشان می دهد.
Sysprotects	اجازه های گرفته شده و داده شده به کاربران امنیتی را با بیانیه های grant ، deny نمایش می دهد.
Systypes	تمام نوع داده های سیستمی و تعریف شده کاربر درون پایگاه داده که برای شناسایی طراحی پایگاه داده مفید است را نمایش می دهد.
Sysusers	نام کاربران windows و SQL SERVER که دسترسی به پایگاه داده را دارند را نشان می دهد.

از طرفی دیگر Oracle همانند SQL SERVER دارای حفره های امنیتی است که به صورت زیر خلاصه شده اند.

جدول های سیستمی به طور پیشفرض برای حفظ اطلاعات نصب شده اند. آنها تمامی جداول (SYS.USER_TABLES) و نمایشهای کاربری (SYS.USER_VIEWS) را نگهداری می کنند. جدول 2-4 تمامی جداول موجود در Oracle که مورد هدف حمله کننده است را نشان می دهد.

جدول 2- 4

SYS.ALL_TABLES	SYS.USER_TAB_COLUMNS
SYS.TAB	SYS.USER_TABLES
SYS.USER_CATALOG	SYS.USER_TRIGGERS
SYS.USER_CONSTRAINTS	SYS.USER_VIEWS
SYS.USER_OBJECTS	

این جداول باید به خیلی امن باشند چرا که حمله کننده می تواند آن را مورد حمله قرار بگیرد و اطلاعات آن را سریع استخراج کند. Oracle و SQL SERVER هر دو دارای نقش ها و مجوزهای امنیتی هستند که باید در سریعترین زمان ممکن تغییر کنند تا امنیت داده ها بتواند تضمین شود.

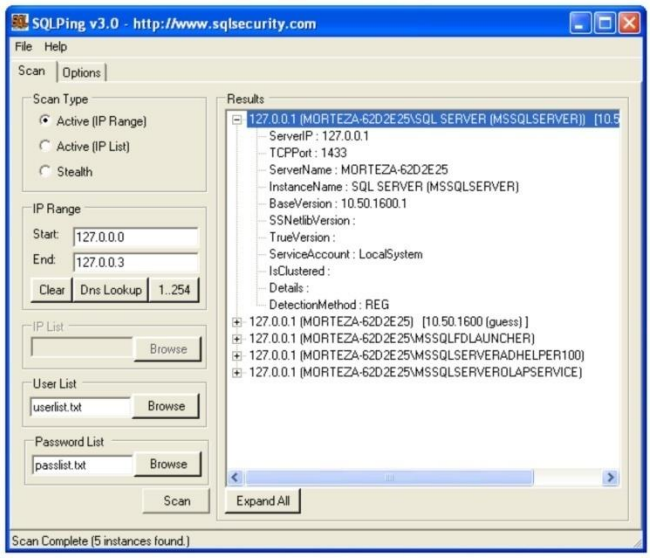
Oracle بیش از 100 نوع مجوز سیستمی از ساختن کاربر تا دسترسی به هر جدول دارد که می توان از درون پایگاه داده می توان آنها را کنترل کرد. مجوزهایی که مربوط به شی هستند به مدیر پایگاه داده اجازه می دهند که کاربرانی به اشیا خاص نظیر جدول دسترسی پیدا کنند. مجوزهایی که مربوط به شی هستند بر روی جداول و سایر اجزای پایگاه داده کنترل بیشتری دارند و اجازه دسترسی را به صورت جزئی امکانپذیر می سازند. اگر مجوزهای مرتبط با سیستم و اشیا با دقت تنظیم نشوند حمله کننده می تواند به اطلاعات دسترسی پیدا کند [1].

راه نفوذ به پایگاه داده Oracle از طریق سرویس گوش دهنده آن است. یک گزارش وضعیت از سرویس گوش دهنده اطلاعاتی در مورد پایگاه از جمله سیستم عامل سرور، سروسی های موجود، تاریخ شروع و زمان بالا آمدن، نسخه سرویس دهنده اوراکل و ... را می دهد[1].

تعداد حفره های امنیتی سرویس گوش دهنده اوراکل به نسخه پایگاه داده بر می گردد. بعضی از آنها می توانند حفره های دیگر از جمله شرایط انفجار بافرها، شرایط قطع دسترسی به سرویسها، نوشتن درون فایل ها و ... را نشان دهند.

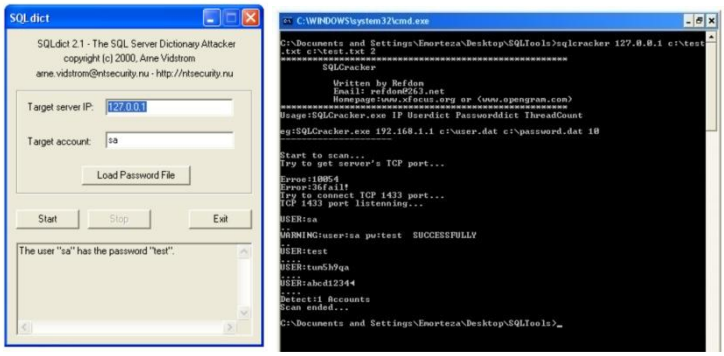
2-4-نفوذ به درون پایگاه داده ها

جهت حمله به پایگاه داده لازم است که بدانیم پایگاه داده درون کدام سرور قرار دارد، لذا لازم است جهت نفوذ به سرور، IP آن را داشته باشیم. برای این کار کافیست برنامه sqlping را اجرا کرده و محدوده IP سرور را به آن داده، تا IP سرور، نام سرور، پرت اتصال و نوع پایگاه داده مشخص شود[4] . شکل 2-6 نمونهای از اجرای این برنامه را نشان می دهد.



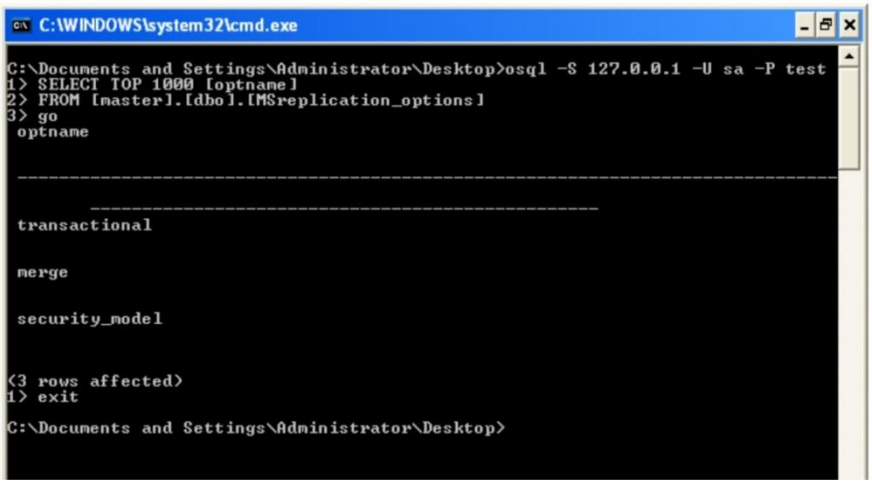
شکل 2 -6

برای قدم بعدی لازم است که یک نام کاربری و یک کلمه عبور داشته باشیم. برای این کار می توان از برنامه هایی نظیر sqlcracker و sqldict استفاده کرد که به صورت dictionary از دو لیست برای نام کاربری و کلمه عبور استفاده می کند. شکل 2-7 نمونه ای از این برنامه ها را نشان می دهد.



شکل 2- 7 سمت چپ برنامه sqldict و سمت راست برنامه sqlcracker را نشان می دهد

با توجه به اینکه نام کاربری و کلمه عبور را بدست آورده ایم می توان با برنامه osql یا sqlcmd وارد پایگاه داده شد و پایگاه داده را مورد حمله قرار داد. البته بهتر است از برنامه sqlcmd استفاده شود[5].شکل 2-8 نمونه ای از حمله را نشان می دهد.



شکل 2 - 8

توجه داشته باشید وقتی نام کاربری و کلمه عبور را به osql داده می شود osql به صورت زیر است

1)

معنی آن این است که باید دستورات خود را برای اجرا در محیط SQL SERVER را تایپ کنید و بعد از هر دستور اجرایی، دستور go را وارد کنید.

2-5-راه های شناسایی و دفاع در برابر حمله های احتمالی

هکر ها با استفاده از برنامه هایی که حمله های brute force را انجام می دهند. این برنامه ها با استفاده از دیکشنری و مجموعه قوائدی دست به حمله می زنند. موارد زیر می تواند نشانه هایی از یک حمله احتمالی باشد:

1. تعداد زیادی نام کاربری یا رمز عبور از طریق یک IP address خاص وارد شده باشد
2. استفاده زیاد از پهنای باند برای یک کار خاص
3. ورود به نام کاربری متعدد از طریق یک IP address خاص
4. نام کاربری با رمز عبور های مشکوک
5. لیستی از نام کاربری یا کلمه عبور وارد شده
6. ورود از طریق آدرس های اینترنتی که ارجاع به ایمیل افراد می کند

ساده ترین راه جهت جلوگیری از حمله احتمالی بستن نام کاربری پس از وارد کردن اشتباه نام کاربری یا کلمه عبور آن است.

برای باز کردن نام کاربری می توان با کمی صبر و امتحان مجدد یا رجوع به مدیر پایگاه داده کرد.

از جمله اشکالات این روش می توان به موارد زیر اشاره کرد:

1. ممانعت از سرویس دهی است که حمله کننده به واسطه امتحان نام کاربری زیاد، نام کاربری را می بندد.
2. چون نام کاربری باید در پایگاه داده وجود داشته باشد، لذا حمله کننده می تواند نام های کاربری موجود را شناسایی کند.
3. حمله کننده می تواند نام کابری را پس از فعالسازی توسط مدیر دوباره غیر فعال کند و به طور مفهومی نام کاربری برای همیشه غیر فعال باشد.

4. این روش در برابر یک کلمه عبور با یک لیست نام کاربری بی اثر است.

5. این روش می تواند منابع انسانی و کامپیوتر ها را درگیر کارهای بیهوده کند.

همانطور که اشاره شد، بستن نام کاربری راه حل مناسبی نیست. اما با افزودن چند ثانیه تاخیر در ورود به پایگاه داده می تواند سرعت بدست آوردن رمز را به طور قابل ملاحظه کاهش دهد.

راه حل دیگر بستن IP پس از وارد کردن اشتباه نام کاربری یا رمز عبور است. اشکال این روش، ممانعت دسترسی کاربرانی است که از یک ISP استفاده می کنند. اشکال دیگز آن استفاده حمله کننده از لیست proxy است که با آن می تواند نام کاربری یا رمز عبور متعددی را امتحان کند.

علاوه بر روش های گفته شده می توان پس از وارد کردن رمز عبور غلط یا نام کاربری غلط، یک سوال خصوصی از کاربر انجام داد. اگر جواب سوال خصوصی درست باشد، انگاه نام کاربری و رمز عبور تست می شود. با این روش می توان جلوی حملات بعدی را گرفت.

از جمله نمونه های دیگر کارهای قابل انجام عبارتند از :

1. ورود نام کاربری و رمز عبور برای هر کاربر فقط از طریق IP address خاص امکان پذیر باشد

2. از یک CAPTCHA جهت جلوگیری از حمله استفاده کنیم.

3. به جای بستن نام کاربری، بر ری آن محدودیت دسترسی به اشیا پایگاه داده ایجاد کنیم.

برای رمزهای عبور کاربران می توان موارد زیر را در نظر گرفت:

1. رمز عبور باید به گونه ای باشد که طول آن از تعدادی کاراکتر بیشتر باشد.

2. رمز عبور باید به گونه ای باشد که نتوان آن را با چند حدس بدست آورد.

3. پس از گذشت زمانی از کار نکردن با سیستم، از کاربر درخواست مجدد نام کاربری و کلمه عبور شود.

4. پس از گذشت چند هفته کاربر مجبور به تغییر رمز خود باشد.

5. از تغییر رمز عبور تکراری جلوگیری شود [2].

برای برنامه پایگاه داده نیز می توان موارد زیز را در نظر گرفت:

1. تا حد امکان اجازه دسترسی به اشیا پایگاه داده را کم کنیم.

2. تا حد امکان کدهای SQL خود را به صورت روال ذخیره شده ذخیره و استفاده کنیم.

3. تا حد امکان روال های ذخیره شده در نصب پیشفرض پایگاه داده را حذف کنیم.

4. داده های مربوط به ورودی و خروجی را به صورت کامل تست نمایید و از صحت داده ها اطمینان پیدا کنیم.

5. قوانین سنگین برای دیواره آتش اتخاذ نماییم، از جمله برای پرت های TCP و UDP پایگاه داده (برای SQL 1434 و برای Oracle 1530-1521).

6. نرم افزار پایگاه داده خود را مرتب به روز کنیم تا از احتمال نفوذ در پایگاه داده جلوگیری شود [1].

2-6-نتیجه گیری

پایگاه داده قلب یک برنامه وب را تشکیل می دهد. بدون توجه به امنیت پایگاه داده، تنظیمات پیشفرض آن حفره های زیادی را شامل می شود. پایگاه داده های مورد استفاده امروزی *SQL SERVER* و *Oracle* هستند.

پایگاه داده *SQL SERVER* در نصب پیشفرض خود دارای حفره های امنیتی از جمله روال های ذخیره شده پیشفرض می باشد. بیشتر این حفره ها را می توان با برداشتن گام های محکم پر کرد اما باید به این نکته توجه داشت که بدون حفظ برخی از روالها، پایگاه داده توانایی خود را از دست می دهد.

Oracle نیز دارای حفره های امنیتی است که بسته به نسخه برنامه این حفره ها متفاوت است. بیشتر این حفره ها شامل اجرای کد از راه دورو ممانعت از سرویس است[3]. بیشتر این حفره ها را می توان با به روز کردن نرم افزار پایگاه داده پر کرد.

اگر چه امنیت یک هدف نسیت و یک روند است اما می توان در حالت کلی امنیت پایگاه داده را به طور قابل چشمگیری افزایش داد

مراجع

[1] Stuart McClure, Saumil Shah and Shreeraj Shah, Web Hacking: Attacks and Defense, Addison Wesley, 2003
[2] http://www.cs.virginia.edu/~csadmin/gen_support/brute_force.php
[3] http://www.uscert.gov/cas/techalerts/TA09-015A.html
[4] http://www.sqlsecurity.com/Tools/FreeTools/tabid/65/Default.aspx
[5] http://blog.sqlauthority.com/2009/01/05/sql-server-sqlcmd-vs-osql-basic-comparison/