İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc329872435)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc329872436)

[ÖRNEK PARSING 4](#_Toc329872437)

[TEMEL PARSING YAPISI 6](#_Toc329872438)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | Websense |
| Versiyonu | 7.7.0 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | WSenseSyslogV\_1\_0\_0Recorder1 |
| İstek yapan Adı Soyadı | Emir AY |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 01.03.2013 |
| İstek yapılan kurum adı | IMKB |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi |  |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları | WebSenseRecorder v\_1\_0\_0 ile çıkartılmış ve düzgün olarak çalışmaktadır. Ancak IMKB için log conf. Yapılmadığı için bu form ile yeniden parsing’i düzenlenip v\_1\_0\_1 versiyonlu olarak çıkarılmıştır. Ayrıca formdaki örnek ham log doğru değildir. Doğru loğlar WSenseSyslogV\_1\_0\_1HamLog dosyasındadır. |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| SIEMLOG|Feb 28 17:27:54|10.66.10.126|7.7.0|117|Transaction blocked|reason=-|act=blocked|7|app=http|dvc=10.66.10.126|dst=95.100.143.139|dhost=connect.facebook.net|dpt=80|src=10.40.19.22|spt=57158|suser=LDAP://10.8.2.101 OU\=GIP,OU\=MUDURLUKLER,OU\=IMKB,DC\=LOKAL,DC\=IMKB/Filiz Seyman|destinationTranslatedPort=0|rt=1362065274000|in=322|out=0|requestMethod=GET|requestClientApplication=Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)|Policy=role-8\*\*IMKB Policy|DynCat=0|ContentType=-|DispositionCode=1025|ScanDuration=2|request=http://connect.facebook.net/tr\_TR/all.js | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | Feb 28 17:27:54 |
| SOURCENAME | 10.66.10.126 |
| EVENTCATEGORY | GET |
| EVENTTYPE | blocked |
| USERSID | Filiz Seyman |
| LOGNAME |  |
| COMPUTERNAME | SIEMLOG |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | 10.40.19.22 |
| CUSTOMSTR4 | 95.100.143.139 |
| CUSTOMSTR5 | suser=LDAP://10.8.2.101 OU\=GIP,OU\=MUDURLUKLER,OU\=IMKB,DC\=LOKAL,DC\=IMKB/Filiz Seyman |
| CUSTOMSTR6 | request=http://connect.facebook.net/tr\_TR/all.js |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 | connect.facebook.net |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | 1025 |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 57158 |
| CUSTOMINT4 | 80 |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| SIEMLOG|Feb 28 17:27:54|10.66.10.126|7.7.0|117|Transaction blocked|reason=-|act=blocked|7|app=http|dvc=10.66.10.126|dst=95.100.143.139|dhost=connect.facebook.net|dpt=80|src=10.40.19.22|spt=57158|suser=LDAP://10.8.2.101 OU\=GIP,OU\=MUDURLUKLER,OU\=IMKB,DC\=LOKAL,DC\=IMKB/Filiz Seyman|destinationTranslatedPort=0|rt=1362065274000|in=322|out=0|requestMethod=GET|requestClientApplication=Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)|Policy=role-8\*\*IMKB Policy|DynCat=0|ContentType=-|DispositionCode=1025|ScanDuration=2|request=http://connect.facebook.net/tr\_TR/all.js | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | Feb 28 17:27:54 |
| SOURCENAME | 10.66.10.126 |
| EVENTCATEGORY | GET |
| EVENTTYPE | blocked |
| USERSID | suser=LDAP://10.8.2.101 OU\=GIP,OU\=MUDURLUKLER,OU\=IMKB,DC\=LOKAL,DC\=IMKB/Filiz Seyman |
| LOGNAME |  |
| COMPUTERNAME | SIEMLOG |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | 10.40.19.22 |
| CUSTOMSTR4 | 95.100.143.139 |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 | connect.facebook.net |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | 1025 |
| CUSTOMINT2 |  |
| CUSTOMINT3 | 57158 |
| CUSTOMINT4 | 80 |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |