İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc330026386)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc330026387)

[ÖRNEK PARSING 4](#_Toc330026388)

[TEMEL PARSING YAPISI 5](#_Toc330026389)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 27.03.2013 |  | Mcaffee Webwasher Access.log yapısı değişikliği sonucu tekrar recorder geliştirmesi gerekmektedir. | Kaan Emre KOŞAR |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | - |
| Ürün Adı | Mcaffee Webwasher Access |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | WebWasherAccessV6\_9\_3\_2Recorder.dll |
| İstek yapan Adı Soyadı | Kaan Emre KOŞAR |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi |  |
| İstek yapılan kurum adı | CFCU |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | /opt/mwg/log/user-defined-logs/access.log/access1303271058.log |
| İlişkili form adı |  |
| Servis Yetkilisi Notları | Log yapısı Mcaffee Reporter aracı için tekrar değiştirilmiş, kurum tarafından yapılan istek sonucu son yapıya göre tekrar recorder geliştirilmesi gerekmiştir. Log dosyası isimlerinin yanına oluştuğu tarih ve saati alarak çıkmaktadır. Parse yapısı tamamen ayrıntılandırılmıştır. |
| Geliştirici Notları |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| 192.168.10.159 23.52.49.224 "gscebe" [26/Mar/2013:17:30:45 +0200] "GET http://platform.twitter.com/widgets.js?v=717858584&\_=1364312037656 HTTP/1.1" 200 1087 83299 "http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetayV3&ArticleID=1126751&CategoryID=41" "Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.17 (KHTML, like Gecko) Chrome/24.0.1312.57 Safari/537.17" "Blogs/Wiki, Social Networking" 0 "application/javascript" 6 "Buraya Karakter Değer Gelebilir" "Minimal Risk" TCP\_MISS\_RELOAD | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 26/Mar/2013:17:30:45 +0200 (formatı uyarlanmalı) |
| SOURCENAME |  |
| EVENTCATEGORY | Blogs/Wiki, Social Networking |
| EVENTTYPE | GET |
| USERSID | gscebe |
| LOGNAME | Recorder İsmi |
| COMPUTERNAME |  |
| CUSTOMSTR1 | http://platform.twitter.com/widgets.js?v=717858584&\_=1364312037656 |
| CUSTOMSTR2 | Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.17 (KHTML, like Gecko) Chrome/24.0.1312.57 Safari/537.17 |
| CUSTOMSTR3 | HTTP/1.1 |
| CUSTOMSTR4 | application/javascript |
| CUSTOMSTR5 | Minimal Risk |
| CUSTOMSTR6 | TCP\_MISS\_RELOAD |
| CUSTOMSTR7 | Buraya Karakter Değer Gelebilir |
| CUSTOMSTR8 | 192.168.10.159 |
| CUSTOMSTR9 | 23.52.49.224 |
| CUSTOMSTR10 | http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetayV3&ArticleID=1126751&CategoryID=41 |
| CUSTOMINT1 | 200 |
| CUSTOMINT2 | 1087 |
| CUSTOMINT3 | 83299 |
| CUSTOMINT4 | 0 |
| CUSTOMINT5 | 6 |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Tam Log |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME | time\_stamp |
| SOURCENAME |  |
| EVENTCATEGORY | attribute |
| EVENTTYPE | req\_line(1) |
| USERSID | auth\_user |
| LOGNAME | Recorder İsmi |
| COMPUTERNAME |  |
| CUSTOMSTR1 | req\_line(2) |
| CUSTOMSTR2 | user\_agent |
| CUSTOMSTR3 | req\_line(3) |
| CUSTOMSTR4 | media\_type |
| CUSTOMSTR5 | rep\_level |
| CUSTOMSTR6 | cache\_status |
| CUSTOMSTR7 | virus\_name |
| CUSTOMSTR8 | src\_ip |
| CUSTOMSTR9 | server\_ip |
| CUSTOMSTR10 | referer |
| CUSTOMINT1 | status\_code |
| CUSTOMINT2 | bytes\_from\_client |
| CUSTOMINT3 | bytes\_to\_client |
| CUSTOMINT4 | block\_res |
| CUSTOMINT5 | elapsed\_time |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | Tam Log |