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 |
| 12.09.2012 | V1.0 | Mevcut dll çalışmakta, ancak dosya isim formatı değiştiği için yeniden düzenlenmesi gerekecektir. | Erson Özdemir |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası | - |
| Ürün Adı | WebwasherAccess |
| Versiyonu | 6.9.3 |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi | WebWasherAccessV6\_9\_3\_1Recorder.dll |
| İstek yapan Adı Soyadı | Erson Özdemir |
| Geliştirici Adı Soyadı | Onur Sarıkaya |
| İstek tarihi | 12.09.2012 |
| İstek yapılan kurum adı | CFCU |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi | webwasher\_access.txt |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| 192.168.10.199 83.66.160.20 "ahektas" [22/Aug/2012:11:47:55 +0300] "GET http://ad.e-kolay.net/bt.js?v=2.0 HTTP/1.1" 403 533 3111 "http://www.eksisozluk.com/show.asp?t=g%C3%B6khan+g%C3%B6n%C3%BCl&a=td" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" "Malicious Sites" 10 "" 292 "" "High Risk" TCP\_MISS | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | 2012-08-22 11:47:55.000 |
| SOURCENAME | 192.168.10.199 |
| EVENTCATEGORY |  |
| EVENTTYPE | GET |
| USERSID | ahektas |
| LOGNAME | WebwasherAccessDeniedRecorder |
| COMPUTERNAME | 83.66.160.20 |
| CUSTOMSTR1 | http://ad.e-kolay.net/bt.js?v=2.0 |
| CUSTOMSTR2 | Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0) |
| CUSTOMSTR3 | HTTP/1.1 |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 | http://www.eksisozluk.com/show.asp?t=g%C3%B6khan+g%C3%B6n%C3%BCl&a=td |
| CUSTOMINT1 | 403 |
| CUSTOMINT2 | 533 |
| CUSTOMINT3 | 3111 |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION | 192.168.10.199 83.66.160.20 "ahektas" [22/Aug/2012:11:47:55 +0300] "GET http://ad.e-kolay.net/bt.js?v=2.0 HTTP/1.1" 403 533 3111 "http://www.eksisozluk.com/show.asp?t=g%C3%B6khan+g%C3%B6n%C3%BCl&a=td" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)" "Malicious Sites" 10 "" 292 "" "High Risk" TCP\_MISS |

# 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 |  |