UTM DASHBOARD

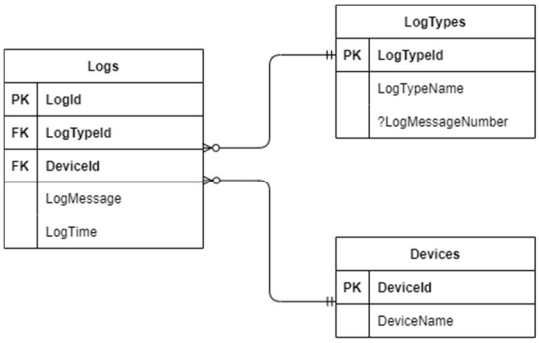
Projede son düzenlemelerin üzerine sahadan alınmış Syslog verileri (.txt) projeye import edilerek tablo üzerinde gösterimi gerçekleştirilmiştir. Bir log dosyasında cihazlara ait sistem logları bulunmakta olup, ötekinde ise bir cihaza ait durum logları bulunmaktadır. İkinci dosyada hangi cihaza ait olunduğu bilinmediğinden dolayı databasede bulunan ilk makineye atamaları yapılmıştır. Sistem logları görünümü aşağıdaki şekilde metin belgesinde bulunmaktadır.

```
Feb 24 18:04:58 Port J[Mainboard]: Siemens-Grid-Security - '7UT85': A user has initiated a remote session from '10.154.13.10'.
```

Durum logları ise şu şekilde bulunmaktadır.

```
╞" 17.11.2020 09:01:41.190"     =" 827" =" Pil arızası: Pili değiştirin."
```

Dosyalardan loglar çekilerek database'e aktarılmış ve tabloya aktarılmıştır. ERD diyagramı aşağıdaki şekildedir.



LogTypes Table		
LogTypeId	**LogTypeName**	**LogMessageNumber**
1	Sistem	NULL
2	Pil Arızası	827
3	Cihaz Başlatıldı	2112
4	Zaman Eşzamanlama Hatası	4739
5	Güç Kaynağı Arızası	4738

Devices Table	
DeviceId	**DeviceName**
1	7UT85
2	6MD85

Tablo görünümleri ise aşağıdaki şekilde olup, sıralama yapılabilmekte, arama sayesinde bir log tipine ait logların adedi veya spesifik bir tarih araması ile ince görüntülemeler yapılabilmektedir.

Tarih	Cihaz	Log Tipi	Mesaj	Durum
2023-03-15 02:33:20	6MD85	Sistem	A user-interactive session has been terminated due to timeout ('1' minutes).	Sistem
2023-03-09 17:21:31	6MD85	Sistem	A user has ended an interactive session.	Sistem
2023-03-09 17:06:17	6MD85	Sistem	A user has initiated a remote session from '10.10.41.60'.	Sistem
2023-03-09 16:36:10	6MD85	Sistem	User caused a control operation from '10.154.13.10': 'F01_Q0 close'. Additional information: ' -'.	Sistem
2023-03-09 16:36:05	6MD85	Sistem	User caused a control operation from '10.154.13.10': 'F01_Q0 open'. Additional information: ' -'.	Sistem
2023-03-09 16:35:57	6MD85	Sistem	User caused a control operation from '10.154.13.10': 'F01_Q0 close'. Additional information: ' -'.	Sistem
2023-03-09 16:33:00	6MD85	Sistem	User caused a control operation from '10.154.13.10': 'F02_Q0 open'. Additional information: ' -'.	Sistem
2023-03-09 16:32:54	6MD85	Sistem	User caused a control operation from '10.154.13.10': 'F01_Q0 open'. Additional information: ' -'.	Sistem
2023-03-09 16:32:52	6MD85	Sistem	User caused a control operation from '10.154.13.10': 'F01_Q0 close'. Additional information: ' -'.	Sistem
2023-03-09 16:32:47	6MD85	Sistem	User caused a control operation from '10.154.13.10': 'F01_Q0 open'. Additional information: ' -'.	Sistem

296 kayıttan 1 ile 10 arası gösteriliyor

Tarih	Cihaz	Log Tipi	Mesaj	Durum
2011-01-01 03:00:03	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2011-01-01 03:00:03	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2011-01-01 03:00:03	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2011-01-01 03:00:03	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2011-01-01 03:00:03	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2011-01-01 03:00:03	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2011-01-01 03:00:03	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2011-01-01 03:00:13	7UT85	Cihaz Başlatıldı	Cihaz başarıyla başlatıldı.	Başarılı
2011-01-01 03:00:13	7UT85	Cihaz Başlatıldı	Cihaz başarıyla başlatıldı.	Başarılı
2011-01-01 03:00:13	7UT85	Cihaz Başlatıldı	Cihaz başarıyla başlatıldı.	Başarılı

296 kayıttan 1 ile 10 arası gösteriliyor

Tarih	Cihaz	Log Tipi	Mesaj	Durum
2021-10-20 18:51:04	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2021-10-19 12:14:13	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2021-10-12 17:21:39	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2021-10-05 17:21:37	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2021-09-28 17:21:36	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2021-09-21 17:21:34	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2021-09-14 17:21:33	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2021-09-07 17:21:31	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2021-08-31 17:21:29	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza
2021-08-24 17:21:27	7UT85	Pil Arızası	Pil arızası: Pili değiştirin.	Arıza

89 kayıttan 1 ile 10 arası gösteriliyor

Bunlara ek olarak tasarımda hazırlamış olduğumuz güvenli yazılım geliştirme ilkelerine ait hazırladığımız checklistte şu ana kadar gelmiş olduğumuz durum aşağıdadır.

✓ Her bir prosedür, modül kendi işini bitirmesi için gerekli en az haklarla çalıştırılmalı ve bu süreç esnasında bu haklara gereken en az süre boyunca sahip olmalı

✓ Her bir nesneye yapılan erişimlerde yetki kontrolü yapılmalı ve bu kontrol normal durumların dışında başlatma, kapatma veya istek, yanıt aşamalarında da yapılmalı

✓ Gereksiz özellikler eklenmemelidir

✓ Kullanıcılar işini en kolay şekilde ancak en az yetkiyle yapabilmeli

✓ Uygulama veritabanında kişisel veri içeren birincil anahtar (kimlik no, e-posta adresi vb.) kullanılmamalıdır.

✓ Sistem mimarisi zayıf yönleri veya zayıf noktaları bulmak için saldırganın bakış açısı ile incelenmeli.

✓ Güvenli diller, güvenli ve onaylanmış kütüphaneler kullanılmalıdır. Eski ve güvensiz kütüphaneler kullanılmamalıdır.

✓ Kasıtlı veya kasıtsız uygulamada güvenlik açığı yatacak kodu kimin yarattığının kontrolü için sürüm kontrolü yapılmalıdır.

✓ Mimarideki tüm yazılım bileşenleri tanımlı olmalı ve ihtiyaç duyulmayan bileşenler kaldırılmalıdır.

✓ Gereksinimler açık, tutarlı, tam, uygulanabilir, takip edilebilir ve doğrulanabilir olmalıdırlar.

✓ Tüm parola alanlarında kullanıcı giriş yaparken kullanıcının parolası maskelenmeli ve açık olarak görünmemelidir.

✓ Kimlik doğrulama başarısız olduğu takdirde güvenli bir duruma geçilmeli ve saldırganların yetkisiz oturum açmaları engellenmelidir.

✓ Hesaba yeniden erişebilecek tüm hesap kimlik doğrulama işlevleri (profil güncelleme, parolamı unuttum vb.) en az ana kimlik doğrulama mekanizması kadar saldırılara dayanıklı olmalıdır.

✓ Kaynak kodunda veya kaynak kodu depolarında gizli bilgiler, API anahtarları ve parolalar mevcut olmamalıdır.

✓ Uygulamanın yönetim arayüzlerine güvenilmeyen taraflarca erişilmesi engellenmelidir.

✓ Güvenilmeyen kaynaklardan alınan dosyaların türü doğrulanmalı ve zararlı bir içeriğe sahip olup olmadığı kontrol edilmelidir.

✓ Oturumlar belirli bir süre etkinlik olmadığında kendiliğinden sonlanmalıdır.

✓ Kimlik doğrulamayla erişilen tüm sayfalardan oturum kapatma işlevine erişilebilmelidir.

✓ Oturum kimliğinin URL, hata mesajları ve iz kayıtları içerisinde yer almaması sağlanmalıdır. URL içerisinde oturum kimliğinin yeniden yazılması engellenmelidir.

✓ Tüm kimlik doğrulama ve yeniden kimlik doğrulama işlemleri sonucunda yeni bir oturum ve yeni bir oturum kimliği üretilmelidir.

✓ Kullanıcı sadece yetkilendirildiği uygulama bileşenlerine ve kaynaklara erişebilmeli ve bunları kullanabilmelidir.

✓ Bellekte tutulan önemli veriler gereksinimi sona erdiğinde güvenlik ihlali oluşturamayacak şekilde silinmelidir.

✓ Uygulama, hassas veri ve kişisel verileri içeren hata mesajı veya iz kaydı üretmemelidir.

✓ Uygulama tarafından, istemci ve sunucu tarafında, kabul edilen her bir veri tipi için girdi doğrulama denetimi yapılmalıdır.

✓ HTML form alanlarının veri girdileri, REST çağrıları, HTTP üst başlıkları, çerezler, toplu işlem dosyaları, RSS beslemeleri gibi veri girdileri için doğrulama denetimi yapılmalıdır.

✓ Uygulamanın istemci tarafında çalışan kodları, kişisel verileri başka ortamlara aktarmamalı (konsola yazma, başka dosya olarak kaydetme, yerel veya uzak uygulamalara transfer etme vb.), güvensiz ortamlarda (ortak dizin, USB disk vb.) güvensiz yöntemlerle (açık metin olarak, zayıf şifreleme algoritma kullanarak şifreleme vb.) saklamamalıdır.

✓ Değişen parola fonsiyonu eski parolayı, yeni parolayı ve bir parola onayını kapsamalıdır.

✓ Kaba kuvvet saldırıları ya da servis dışı bırakma saldırıları gibi otomatik yapılan yaygın kimlik doğrulama saldırılarını önlemek için istekler azaltılmalıdır. Aşırı kimlik doğrulama denemelerini engellenmeli.

✓ Desteklenmeyen, güvensiz veya teknolojisi zaman aşımına uğramış istemci teknolojileri kullanılmamalıdır.

✓ Uygulama, ayar ve denetim dosyaları kullanıcı verisiyle aynı konumda depolamamalıdır.

✓ Web uygulamalarında oturum çerezlerinde HTTPOnly bayrağı etkin olmalıdır.

✓ Tüm rastgele üretilen sayılar, dosya isimleri, global eşsiz değerler (GUID) ve karakter dizilerinin saldırgan için tahmin edilemez olması sağlanmalıdır. Rastgele sayıların yüksek entropiye sahip olarak üretilmelidir.

✓ Tüm anahtar ve şifreler kullanımları tamamlandığında, tamamen sıfırlanarak yok edilmelidir.

✓ Tüm formlarda istemci tarafında yapılan ön bellekleme işlevselliği önemli veriler için kapatılmalıdır.

✓ Uygulama, saklama gereksinimi sona erdikten sonra önemli verileri güvenlik sonunu yaratmayacak şekilde silinmelidir.

✓ İz kayıtlarında olayların zaman sıralamasına ilişkin araştırma yapılabilecek şekilde zaman bilgisi yer almalıdır.

✓ Uygulama tarafından üretilen iz kayıtları hassas bilgi içermemelidir.

✓ Uygulama hassas bilgileri formlarda bulunan gizli alanlarda saklamamalıdır.

✓ Uygulama, web servis kimlik doğrulama ve yetkilendirmesi için oturum temelli yapılar kullanacak şekilde tasarlanmalıdır.

✓ Uygulama, web servislerinden şifreli olarak paylaşılan verileri yine şifreli olarak saklayacak şekilde tasarlanmalıdır.

✓ Uygulama, kişisel veriler üzerinde işlem yapılması ana amaç olmayan durumlarda kişisel verileri maskeleyerek görüntülemeli, aktarmalı veya işlemelidir.