SQUİD PROXY İLE GERÇEK ZAMANLI WEB TRAFİK KONTROLÜ

Erhan YELİ
Fırat Üniversitesi
Bilgisayar Müh. Bölümü
erhanyeli@hotmail.com

Gürkan KARABATAK
Fırat Üniversitesi
Enformatik Bölümü
gkarabatak@firat.edu.tr

Yrd.Doç.Dr Hasan H.BALIK
balik@firat.edu.tr

ÖZET

Üniversite içerisindeki ağdan internete giren kullanıcıların web trafiğinin geçek zamanlı olarak kontrol edilip, izlenmesi. İzleme işlemi trace.firat.edu.tr adresindeki web arayüzü ile dinamik olarak yapılabilmektedir. İzleme işlemi site admini tarafından açılan kullanıcılar tarafından yapılabilmektedir. Her kullanıcıya belirli sınırlamalar verilir. Yani her kullanıcı istediği her şeyi izleyemez. Adminin verdiği haklar çerçevesinde izleme işlemini yapabilir.

Ayrıca üniversite içerisindeki öğrenci laboratuarlarının daha etkin ve faydalı olarak kullanılması. Bu işlem laboratuar sorumlularına açılan kullanıcılar ile laboratuarların gerçek zamanlı izlenmesiyle sağlanır.

Üniversite laboratuarları genel kullanımda olduğu için internet üzerinden yapılan suçlara açık yerlerdir. Gerçek zamanlı izleme sistemi caydırıcı bir önlem olabilir bu bu suşların önüne geçilebililir.

1. GİRİŞ

Üniversite içerisindeki ağdan internete giren kullanıcıların web trafiğinin geçek zamanlı olarak kontrol edilip izleme işlemi http://trace.firat.edu.tr adresindeki web arayüzü ile dinamik olarak hızlı ve güvenli bir şekilde yapılabilmektedir. Site kullanıcıları internete bağlı herhangi bir bilgisayardan kendilerine tanınan haklar çerçevesinde gerçek zamanlı web trafik kontrolü işlemini yapabilirler.

Gerçek zamanlı web trafik kontrolünde Linux Redhat 9.0 üzerinde çalışan Squid Proxy Server önemli bir iş yapmaktadır. Proje Squid Proxy ile entegre çalışmaktadır. Squid Proxy'den alınan verilerin anında işlenmekte ve trace.firat.edu.tr adresinde site kullanıcılarına anında gösterilmektedir.

Projede web programlama dili olarak PHP; Veritabanı olarak MySQL kullanılmıştır. PHP kullanılmasının nedeni Linux altında çok verimli, performanslı ve hızlı olmasıdır ayrıca veritabanıyla

çok uyumlu çalışabilmesidir. Veritabanının MySQL seçilmesinin nedeni PHP ile en uyumlu çalışabilen veritabanı olması, bu çok karmaşık olmayan verilerin tasnif edilmesinde en ferformanlı veritabanı olmasıdır. Hız ve performans için MySQL seçilmiştir.

Squid Proxy Server'dan alınan veriler PHP ile parse edilerek MySQL' e aktarılır. Sonra PHP ile MySQL sorgulanır ve sonuçlar web adresine aktarılır. Bu işlemlerin hepsi gerçek zamanlı olarak yapılmaktadır.

2. YÖNETİCİ ARABİRİMİ

Site yöneticisi kullanıcıları siteye ekler ve kullanıcı haklarını düzenler. Aşağıdaki işlemleri admin modülü ile yapabilir.

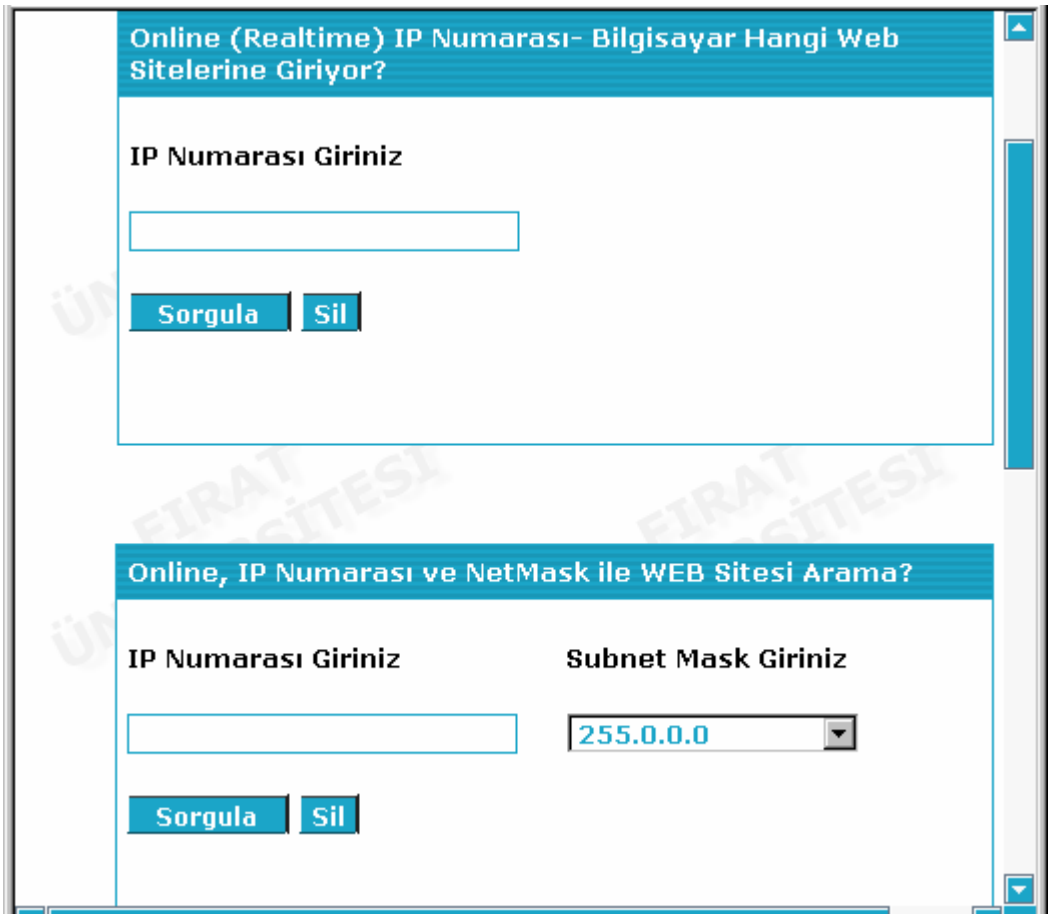
- Gerçek zamanlı web trafik kontrolü.(Adminin izleme işlemi sınırsızdır)
- Kullanıcı ekleme ve kullanıcı hakları verme.
- Kullanıcı bilgilerinin güncellenmesi.
- Kullanıcı silme.
- Duyuru modülü.(Sadece site kullanıcılarının okuyabilecekleri duyuru sistemi)

2.1. Gerçek zamanlı web trafik kontrolü

Adminin hakları sınırsız olduğu için, hak sınırlaması olmadan web trafik kontrolünü istediği gibi yapabilir.

- İp numarasına göre gerçek zamanlı web trafik kontrolü
- Alt ağ maskesine göre gerçek zamanlı web trafik kontrolü.
- Web adresine göre gerçek zamanlı web trafik kontrolü.
- Girilen kelimeye göre gerçek zamanlı web trafik kontrolü.

Bu modülün genel görüntüleri.

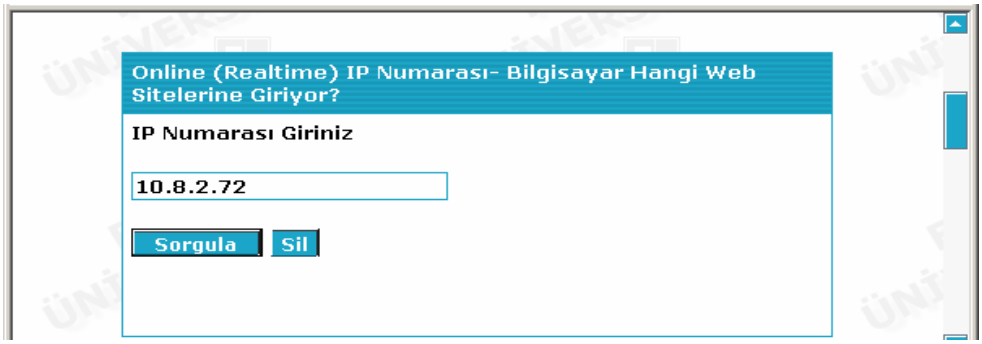


Şekil 1 Web trafik tontrolü yapan modülün genel görüntüsü 1

Şekil 2 Web trafik tontrolü yapan modülün genel görüntüsü 2

2.1.1. İp numarasına göre gerçek zamanlı web trafik kontrolü

Admin yazdığı ip numarasının şu an hangi sitelere girdiğini bu form sayesinde görebilir. Örneğin 10.8.2.72 numaralı ip'nin girdiği siteler aşağıdaki şekilde sorgulanır.



Şekil 3 İp numarasına göre gerçek zamanlı web trafik kontrolü

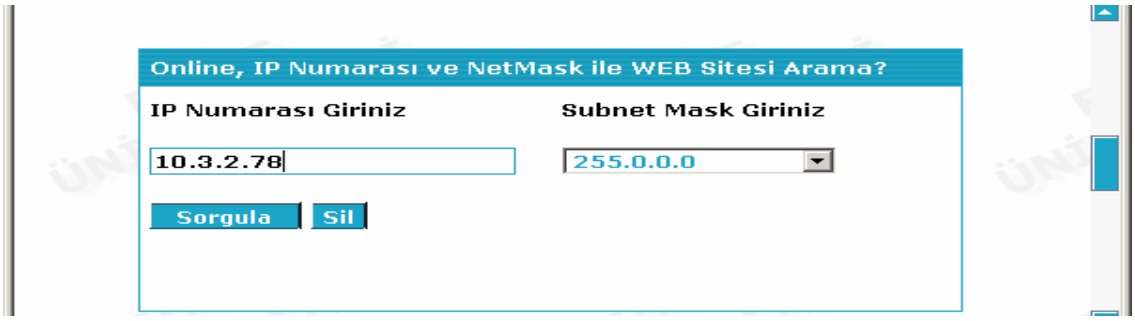
Bu sorgulama sonucu aşağıdaki gibi olur.

Şekil 4 İp numarasına göre gerçek zamanlı web trafik kontrolü sonucu

2.1.2. Alt ağ maskesine göre gerçek zamanlı web trafik kontrolü

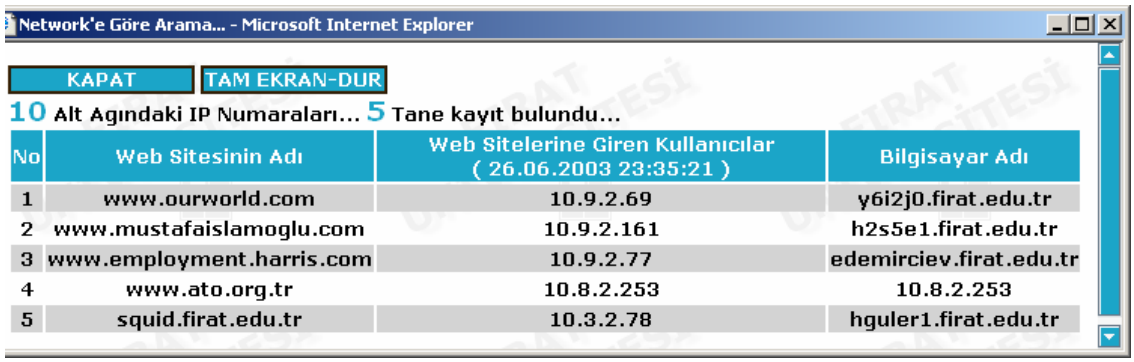
Girilen ip numarasının bulunduğu alt altdaki bütün bilgisayarları ve bu bilgisayarların girdiği internet adreslerini gerçek zamanlı olarak listeler. Önce ip numarası yazıp alt ağı seçiyoruz(Seçilebilen alt ağ adresleri : 255.0.0.0 – 255.255.0.0 – 255.255.255.0 – 255.255.255.255). Daha sonra gerçek zamanlı olarak webde sorgu sonuçları oluşur.

Aşağıda 10.3.2.78 ip numarasının bulunduğu alt ağla ilgili sorgulama yapıyoruz. Alt ağ maskesi 255.0.0.0 ‘dır.



Şekil 5 Alt ağ maskesine göre gerçek zamanlı web trafik kontrolü

Bu sorgulama sonucu aşağıdaki gibi olur.



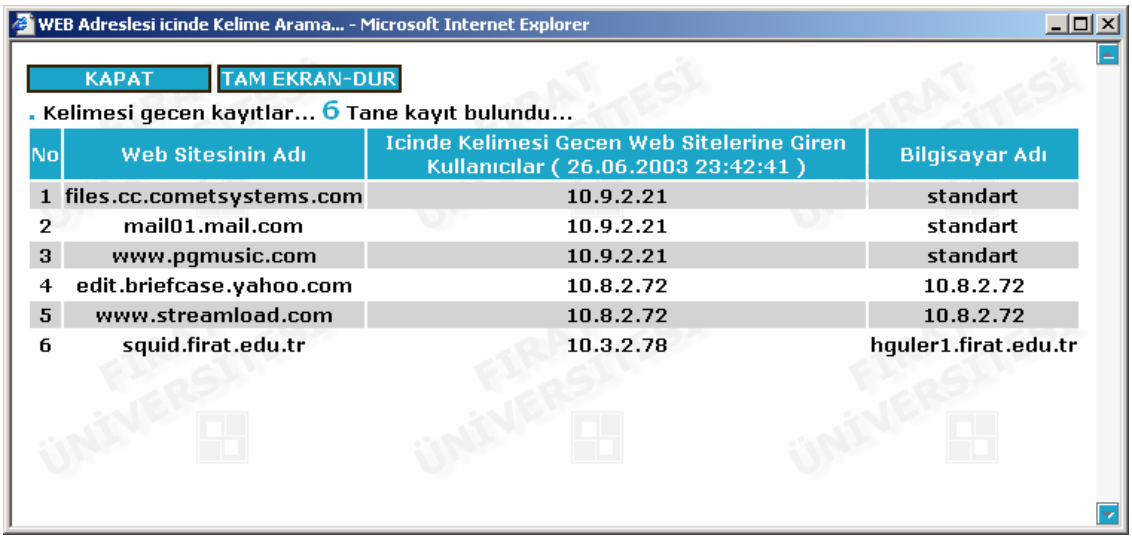
Şekil 6 Alt ağ maskesine göre gerçek zamanlı web trafik kontrolü sonucu

2.1.3 Girilen kelimeye göre gerçek zamanlı web trafik kontrolü

Formda girilen kelimenin geçtiği web adreslerini ve bu web adreslerine giren kullanıcıların ip numarası-bilgisayar adlarını gösterir. Örneğin " . " nın geçtiği web adreslerini arayalım.

Şekil 7 Girilen kelimeye göre gerçek zamanlı web trafik kontrolü

Bu sorgulama sonucu aşağıdaki gibi olur.



Şekil 8 Girilen kelimeye göre gerçek zamanlı web trafik kontrolü sonucu

2.2 Kullanıcı ekleme ve kullanıcı haklarını belirleme

Bu modülde kullanıcı bilgileri alınır. Kullanıcının siteden ne ölçüde yararlanacağını belirten kullanıcı hakları admin tarafından belirlenir.

Bu haklar aşağıdaki formların tamamını kullanıcıya gösterme veya belirli bir kısmını gösterme şeklindedir.

- İp numarasına göre gerçek zamanlı web trafik kontrolü
- Alt ağ maskesine göre gerçek zamanlı web trafik kontrolü.
- Web adresine göre gerçek zamanlı web trafik kontrolü.
- Girilen kelimeye göre gerçek zamanlı web trafik kontrolü.

İp numarasına göre gerçek zamanlı web trafik kontrolü formunu site üyesine kullanma hakkını vermişseniz site üyesine ya sınırsız ip kontrol hakkı vermelisiniz veya sadece belirli bir ip aralığı vermeniz gerekir.

Alt ağ maskesine göre gerçek zamanlı web trafik kontrolü formunu site üyesine kullanma hakkını vermişseniz site üyesine ya sınırsız sınırsız sorgulama hakkı vermelisiniz veya sadece belirli bir ip ve alt ağ maskesi ile sorgulama yapmasına izin vermeniz gerekir.

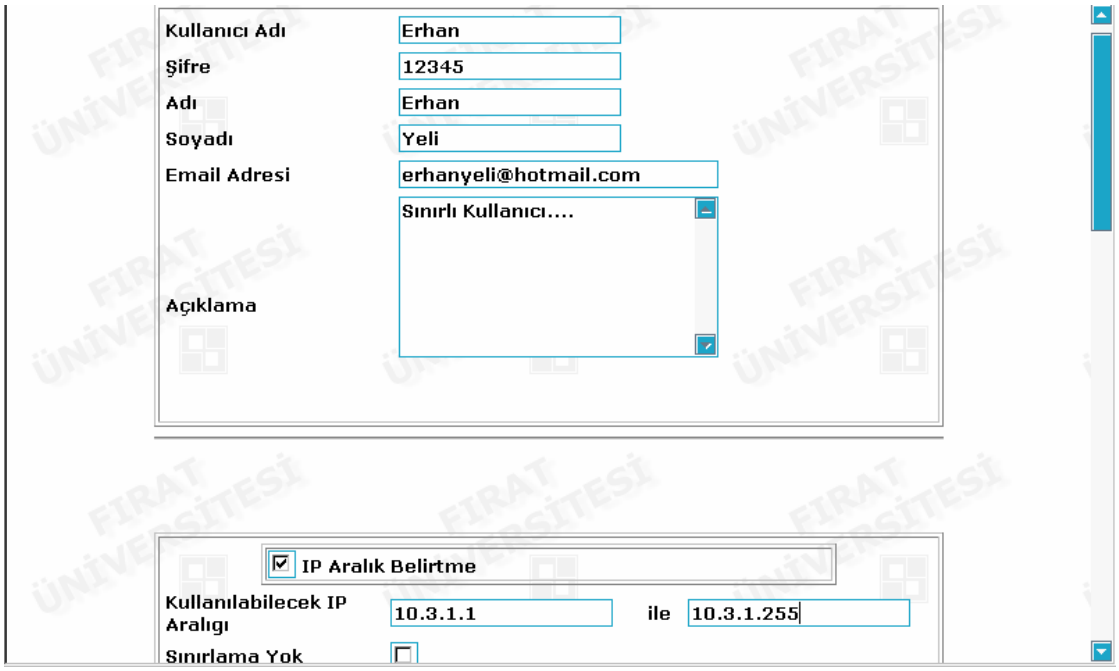
Web adresine göre gerçek zamanlı web trafik kontrolü formunu site üyesine kullanma hakkını vermişseniz site üyesine ya sınırsız sınırsız sorgulama hakkı vermelisiniz veya sadece belirli web sitelerinin adlarını aratma hakkını vermeniz gerekir. Web sitelerinin adları admin tarafından kullanıcı ekleme modülünden girilebilir.

Girilen kelimeye göre gerçek zamanlı web trafik kontrolü formunu site üyesine kullanma hakkını vermişseniz site üyesine ya sınırsız sınırsız sorgulama hakkı vermelisiniz veya sadece belirli

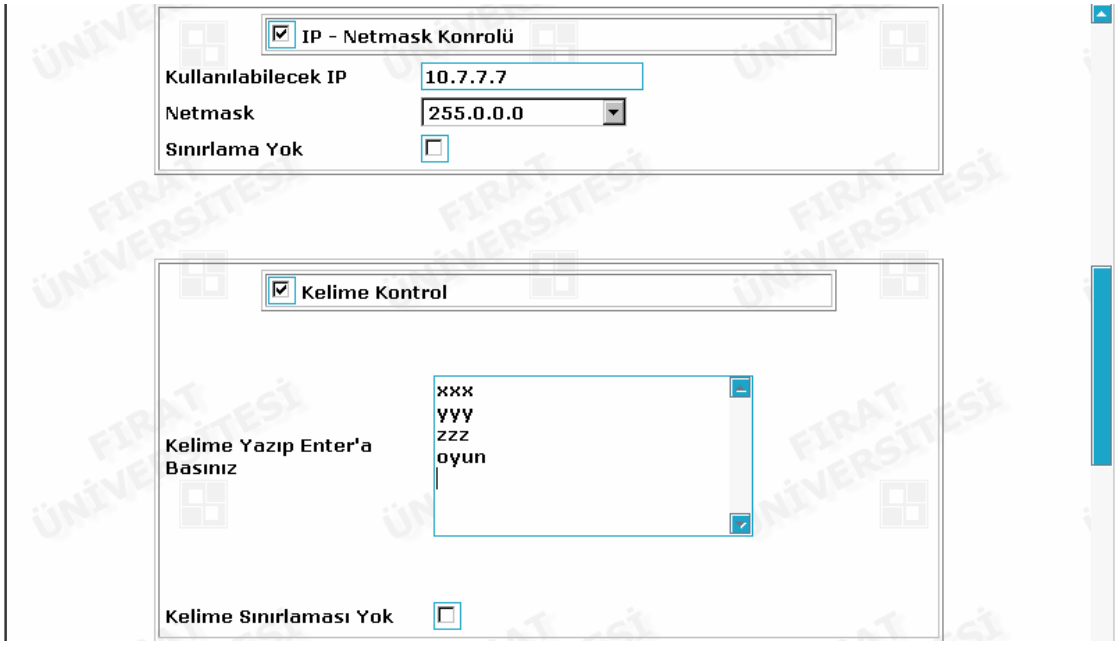
kelimeleri aratma hakkını vermelniz gerekir. Kelimeler admin tarafından kullanıcı ekleme modülünden girilebilir.

IP sınırlama kontrolleri server üzerinde çalışan javascript ile yapılmıştır.

Kullanıcı ekleme modülünün ekran görüntüleri



Şekil 9 Kullanıcı ekleme 1



Şekil 10 Kullanıcı ekleme 2

Şekil 11 Kullanıcı ekleme 3

3. KULLANICI ARABİRİMİ

Kullanıcı, admin tarafından verilen haklara göre aşağıdaki sorgulamaları gerçek zamanlı olarak yapabilmektedir.

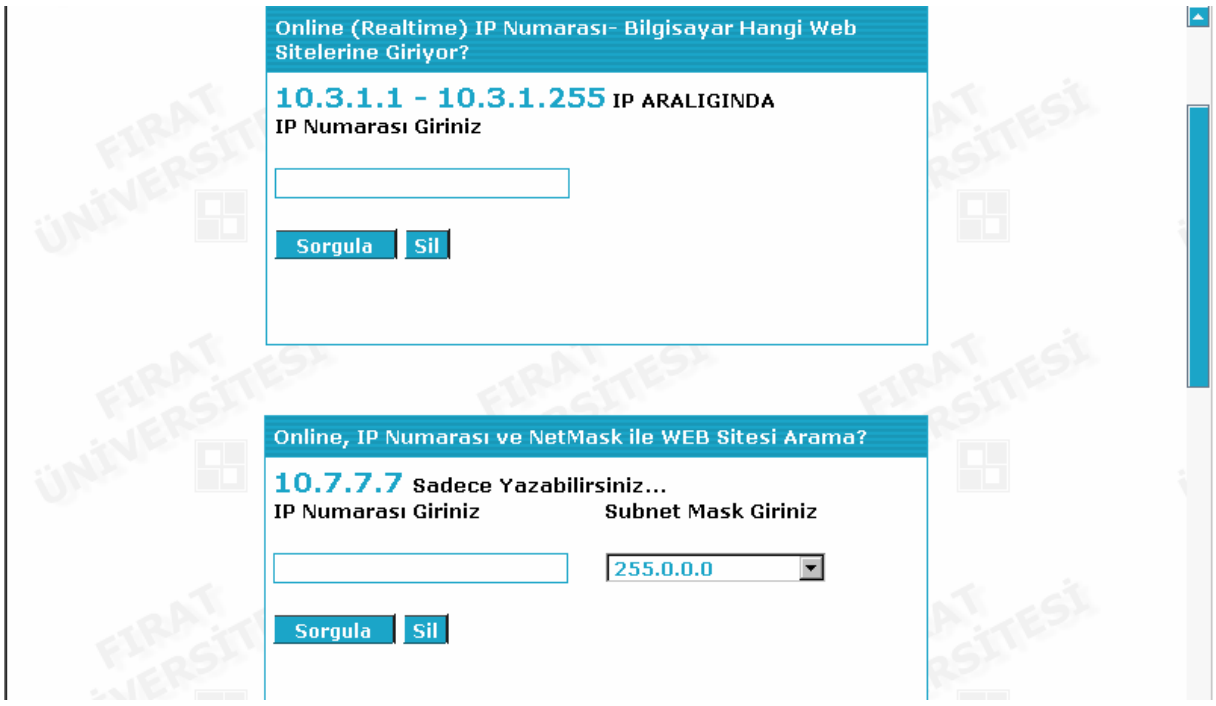
- İp numarasına göre gerçek zamanlı sorgulama.
- Alt ağ maskesine göre gerçek zamanlı sorgulama.
- Web adresine göre gerçek zamanlı sorgulama.
- Girilen kelimeye göre gerçek zamanlı sorgulama.

Örneğin Erhan kullanıcısının hakları yukarıda kullanıcı ekleme modülünde girilmiştir. Bu kulanıcı login olduktan sonra hakları ve bununla ilgili ekran görüntüleri aşağıdaki gibidir. Admin formlardan herhangi birini işaretlemeseydi o form kullanıcı arabiriminde gözükmeyecekti.

Bu formlardan herhangi birinde gerçek zamanlı sorgulama yaptığı zaman oluşan sonuçların ekran görüntüleri bölüm **2.1**'de gösterilmiştir.

Şekil 12 Kullanıcı girişi

Şekil 13 'te kullanıcıya ayrılmış ip sınırları dışında ip sorgulaması yapamaz. Bu serverda çalışan javascript koduyla yapılmıştır. Ayrıca kensine verilmiş olan ip ve alt ağ maskesi dışına çıkıp sorgulama da yapamamaktadır.



Şekil 13 Hakları sınırlandırılmış kullanıcı ekranı 1

Şekil 14 'te kullanıcıya adminin vermiş olduğu web adresleri dışında sorgulama hakkı tanınmamıştır.

Şekil 14 Hakları sınırlandırılmış kullanıcı ekranı 2

Şekil 15'te kullanıcıya adminin vermiş olduğu kelimeler dışında sorgulama hakkı tanınmamıştır.

Şekil 15 Hakları sınırlandırılmış kullanıcı ekranı 3

KAYNAKLAR

1. www.linux.org.tr
2. www.php.org.tr
3. www.php.net
4. www.linux-sevenler.de
5. www.belgeler.org
6. www.turk-php.com
7. www.gelecek.com.tr
8. www.zend.com
9. www.mysql.com
10. www.enderunix.org
11. www.w3.com
12. www.squid-cache.org
13. www.fazlamesai.net
14. www.programlama.com
15. www.sorucevap.com
16. www.wrox.com

KİTAPLAR

1. Özgür ÇAYCI, PHP ve MySQL
2. Kayra OTANER, PHP ve MySQL ile Web Yazılımı Geliştirme
3. Görkem ÇETİN, Bilgisayar Ağları ve Linux Ağ Yönetimi
4. T. H. CORMEN, Instruction To Algorithms