International Journal of Scientific and Technological Research
ISSN 2422-8702 (Online)
Vol 1, No.10, 2015

Software Development for Blocking File Change Attacks on Web Servers

Mustafa Ali Akca
Depertmant of Computer Education & Instructional Technology, Faculty of Education,
Suleyman Demirel University, Isparta, Turkey
E-mail: mustafaakca@sdu.edu.tr

Abstract

Today web servers, websites, web based applications, cloud applications, e-government applications etc are used actively in many areas. With the increase in the usage of Web servers some of the security needs are emerged. Especially disrupting services made to the web server, to access information and change the information as a result of attacks on sites and applications can be quite seriously damaged. In our study a software has been developed as a measure to the attacks by estimating or stealing the FTP password to the web server. This software is installed to the serving server and sites are observed. The software always follows the desired files. If a change is wanted to be done in the file or the file is wanted to be deleted completely optionally Access is completely blocked or it lets to delete the file after that closes FTP, brings it back into the previous item. In this way, the file which belongs to this attack attempt has been obtained. Optionally, notifications via email or sms are sent to the server administrator or site owner.

Key words: Blocking FTP attacks, webserver attacks

Web Sunucularındaki Dosya Değişikliği Saldırılarının Engellenmesine Yönelik Yazılım Geliştirilmesi

Özet

Günümüzde web sunucuları, internet siteleri, web tabanlı uygulamalar, bulut uygulamaları, e-devlet uygulamaları vb gibi birçok alanda aktif olarak kullanılmaktadırlar. Web sunucularının kullanımlarının artmasıyla beraber bazı güvenlik ihtiyaçları da ortaya çıkmıştır. Özellikle web sunucularına yapılan hizmet aksatma, bilgilere erişme ve değiştirme gibi saldırılar sonucunda sitelere ve uygulamalara oldukça ciddi zararlar verilebilmektedir. Çalışmamızda web sunucularına FTP şifresi tahmin edilerek ya da çalınarak yapılan saldırılara önlem olarak bir yazılım geliştirilmiştir. Bu yazılım hizmet veren sunucuya kurulur ve siteler izlemeye alınır. Yazılım sitedeki istenen dosyaları sürekli takip eder, dosya üzerinde bir değişiklik yapılmak istenildiğinde ya da dosya tamamen silinmek istediğinde opsiyonel olarak istenirse erişimi tamamen engeller ya da dosyanın silinmesine izin verip hemen sonra FTP'yi kapatıp dosyayı önceki haline tekrar geri getirir. Bu sayede bu saldırı girişimini yapan kişinin dosyası da elde edilmiş olur. Opsiyonel olarak sunucu yöneticisine ya da site sahibine email yada sms yoluyla bildirim yollanır.

Anahtar Kelimeler: FTP saldırılarını önleme, web sunucusu saldırıları

1. Giriş

Web sunucuları günümüzde internet siteleri, web uygulamaları, e-devlet uygulamaları, bulut uygulamaları vb. bir çok alanda kullanılmaktadır. Web sunucularının kullanımlarının artmasıyla birlikte sunucuların ve sunucuda bulunan dosyaların güvenliklerinin sağlanması için bazı güvenlik ihtiyaçları da ortaya çıkmıştır. Özellikle kurumsal ağların web sunucularına yapılan saldırıları saptayacak ve engelleyecek bir güvenlik sistemi her zaman ihtiyaç olmuştur [1]. Web sunucularına hizmet aksatma saldırıları, dağıtık hizmet aksatma saldırıları, ticari bilgi ve teknoloji hırsızlıkları, web sayfası içeriği değiştirme saldırıları gibi bir çok farklı türde saldırılar yapılmaktadır [2]. Web saldırıları, hedef gözeten saldırılar olarak bilinmektedir. Bu konuda da bir değişim yaşanmaktadır. Günümüzde, arama motorları ile yayılan ve hedef gözetmeyen web uygulaması solucanları tehdidi de bulunmaktadır[3]. Saldırgan, bu saldırılar sonucunda sisteme ilişkin bilgi edinebilmekte ve uygulamanın kapsamı dışındaki veri ve kaynaklara erişim kazanabilmektedir[1]. Bu saldırıların gerçekleştiği ilk anda tespit edilebilmesi ya da önceden bir önlem alınabilmesi siber güvenliğin sağlanması için zorunlu hale gelmiştir [4]. Siber güvenlikte yapılan "Durumsal Farkındalık" çalışmaları bu ihtiyaçlara hitap etmektedir [5]. Web sunucularına kurulacak güvenlik yazılımlarının sunucu ve sunucu içerisindeki bilgiler hakkında detaylı bilgi sahibi olması gerekmektedir [6]. Güvenlik için gerekli işlemler tanımlanırken çok katmanlı yapılardan söz edilmektedir. Çok katmanlı güvenlik modellerinde Engelleme, Saptama ve Kurtarma olmak üzere üç farklı katman yer almaktadır[7-8]. Saldırı Saptama Sistemleri (SSS), saldırıların saptaması ve olağan dışı etkinliklerin saptanması için kurulan sistemlerdir. Bir veya daha fazla ağ tabanlı SSS, kritik ağ kesimlerinde konuşlandırılabilir. Saldırganların sistemde yapabilecekleri değişikliklerin takibi açısından, Tripwire (http://sourceforge.net/projects/tripwire/) ve benzeri programlarla kritik sistem dosyalarında yaşanan değişimler izlenmelidir[9]. Web sunucularına yapılan sayfa içeriği değiştirme saldırılar genel olarak FSO (File System Object) üzerinden dosya yükleyip içerik değiştirme veya FTP (File Transfer Protocol) şifresi ele geçirilerek dosyalara erişip/değiştirme şeklinde olmaktadır. FSO sunucu üzerindeki dosya sistemine erişip, dosya oluşturma, dosya silme, klasör oluşturma, klasör silme, bilgisayardan dosya yükleme gibi işlemler yapabilen bir nesnedir [10]. Birçok sitenin kullanıcılara açık olan dosya yükleme sayfasında bu sınıf kullanılır. Gerekli tedbirler alınmadıysa kullanıcılar buradan sitelere "asp","aspx","php" vb uzantılı Shell dosyaları yükleyerek diğer dosyalara erişebilirler. Shell dosyaları, siteye yüklendiğinde, yükleyen kişiye okuma, yazma, silme, yükleme yetkileri veren bir dosyadır. FSO üzerinden dosya yükleme işlemi ile sisteme yüklenen bir Shell dosyası ile artık tüm dosyalar üzerinde işlem yapma yetkisine sahip olunur [11].

2. Saptama, Engelleme ve Kurtarma Yazılımı Geliştirilmesi

FTP üzerinden yapılan dosya değişikliği saldırılarında, saldırganlar genel olarak sitenin en çok kullanılan dosyalarını hedef almaktadır. Bu sayede tüm siteyi durdurabilir yada yazmak istedikleri mesajı tüm kullanıcılara gösterebilmektedirler. Bu tür dosyalar genelde config dosyaları ile index veya default dosyalarıdır. Bu dosya isimleri hemen hemen tüm yazılım dillerinde sitelerde en sık kullanılan ve sitenin ilk açılışında çalışan dosyalardır. Saldırganlarda bu dosyaları hedef alarak içeriğinin bir kısmını yada tamamını değiştirmeye çalışmaktadırlar.

Geliştirilen yazılım sunucudaki tüm sitelerde kullanılabilecek iki farklı şekilde çalışabilmektedir. Birinci seçenekte kullanıcılar koruma altında almak istedikleri dosyaları belirler ve ikinci bir düzenlemeye kadar bu dosyalar yazılım tarafından readonly olarak işaretlenir değiştirilmesine / düzenlenmesine izin verilmez. İkinci seçenekte ise kullanıcılar saldırganı ve saldırganın amacını tespit edebilmek amacıyla dosyalarını değiştirme ve düzenlemeye açık bırakır. Ancak belirledikleri dosyalar ise yazılım tarafından ilk olarak belirli aralıklarla yedeklenir. Biri dosyaları değiştirmek istediğinde dosya boyutlarını, oluşturma tarihini karşılaştırarak dosya değişimine anlık olarak izin verir, daha sonra saldırganın dosyasını kopyalar, FTP'yi kapatır ve önceden yedeklenmiş olan dosyayı sisteme geri yükler. İsteğe bağlı olarak site sahibine sms yada email yoluyla haber verir.

Yazılımın, site sahipleri için geliştirilen kontrol paneli kısmı ASP tabanlı olarak MSSQL veri tabanı kullanılarak tasarlanmıştır. Site sahipleri bu kontrol paneline girerek, koruma altına almak istedikleri dosyaları ve koruma yöntemlerini seçerek sistemi aktif hale getirmiş olurlar. Yazılımın diğer bir kısmı ise Windows sunucu üzerinde çalışan dosyaları yedekleyen, kurtaran, silinmesine engel olan, FTP'yi kapatan, email ya da sms yoluyla site sahibine haber verebilen uygulamadır. Bu uygulama C# ile geliştirilmiş olup kullanıcı kontrol paneli ile aynı MSSQL veri tabanını kullanmaktadır. Sistem temelde üç kısımdan oluşmaktadır.

2.1. İzlenecek dosyaların seçilmesi

Site sahipleri için mevcut hosting yönetim panellerine ek olarak, güvenlik ayarlarını yapabilecekleri ayrı bir kontrol paneli geliştirilmiştir. Bu kontrol paneli alt yapısı XML ile haberleşmeye açık olup istenirse, plesk, cpanel gibi panellere entegresyon yapılıp mevcut özelliklerin bu panellerden kontrolü sağlanabilir. Site sahipleri Şekil 1'de görülen kontrol paneline kullanıcı adı ve şifreleriyle giriş yapıp gerekli seçenekleri kaydederler.

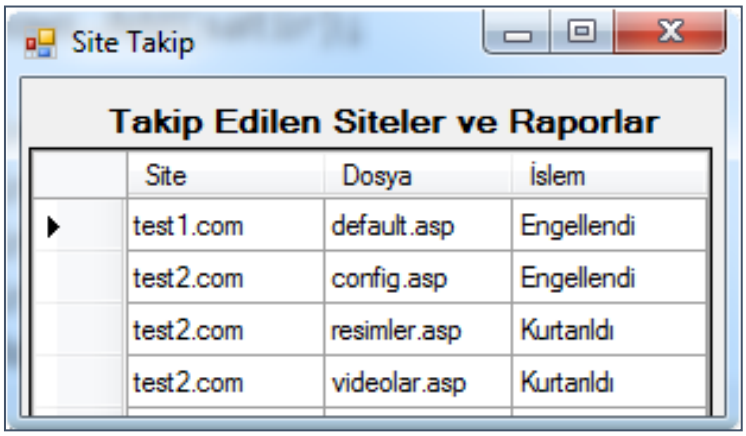
Şekil 1. Kontrol paneli seçenekleri

Kullanıcılar bu seçenekleri belirlerken site için hayati öneme sahip default, config ve admin vb dosyaları için engelle modunu seçebilirler. Bu seçimi kaydettikten sonra saldırganlar FTP şifrelerini ele geçirseler bile bu dosyaları kesinlikle silemez/değiştiremezler.

Bir diğer seçenek ise izleme seçeneğidir. Bu seçenek genel olarak kurtarma seçeneği ile birlikte kullanılır. İzleme seçeneği işaretlendiğinde sunucu içerisindeki yazılım seçilen dosyaları takip etmeye başlar. Eğer bu dosyalardan biri FTP üzerinden silinirse sms veya email bildirimi yoluyla site sahibine haber verilir. "İZLE" seçeneğine ek olarak "KURTAR" seçeneği de önceden seçildiyse, FTP üzerinden dosya silinir silinmez, sunucudaki yazılımın daha önceden almış olduğu yedek dosya aynı dizine tekrar kopyalanarak sitenin hizmetine devam etmesi sağlanır.

2.2. Engelleme veya Kurtarma

Sunucu içerisinde site sahiplerinin kontrol panellerinden belirledikleri dosyaları takip eden C# tabanlı bir yazılım bulunmaktadır. Bu program kullanıcının yaptığı konfigürasyonlara göre izleme/engelleme/kurtarma ve haber verme işlemlerini yürütür.



Şekil 2. Sunucudaki siteleri takip eden yazılım

Şekil 2'de görüldüğü gibi yazılım kontrol panelinden eklenen "test1.com" sitesine ait "default.asp" dosyasını ve "test2.com" sitesine ait "config.asp", "resimler.asp", "videolar.asp" dosyalarını takip etmektedir.
Sunucudaki yazılım aktif hale getirildiği ilk anda takipteki sitelerde silinmesi/değiştirilmesi engellenen dosyalar var ise ilk olarak bu dosyaların bayraklarını "readonly" olarak değiştirir ve sadece okunmasına izin verir. Bu yazılım kapanana kadar mevcut dosyalar üzerindeki "readonly" özelliği sabit kalır. Yazılım bunu C# taki Filestream sınıfını kullanarak aşağıdaki gibi sağlar;

```
string yol = "D:\\site.com\\default.asp";
FileStream s2 = new FileStream(yol, FileMode.Open, FileAccess.Read,
FileShare.Read);
```

Site kontrol panelinden kullanıcının belirleyip sunucudaki MSSQL veri tabanına kaydedilen ve engellenmesi istenen tüm dosyalar için yukarıdaki kodlarda görünen read modu uygulanır. Bu sayede dosyanın silinmesi/değiştirilmesi tamamen engellenmiş olur.

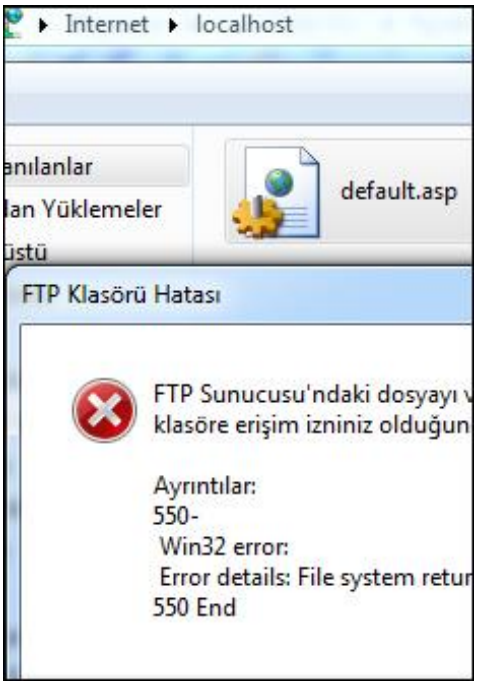
2.3. Site Sahibine Haber Verme ve FTP Hesabını Kapatma
Dosyalara yapılan müdahaleleri sürekli kontrol eden yazılım, isteğe bağlı olarak site sahiplerine sms ya da email yoluyla haber verebilir, siteye ait FTP hesabını kapatabilir. Yazılımın email kısmında C#'a ait System.Net.Mail kütüphanesi kullanılmıştır. Kullanıcılara SMS yoluyla haber vermek için Turkcell çözüm ortağı olan Mobilparkın C# ve ASP için geliştirmiş olduğu kütüphaneler kullanılmıştır. Bu siteden deneme hesabı açılarak saldırı anında site sahibine sms gönderilmesi sağlanmıştır.

3. Saldırı Denemeleri

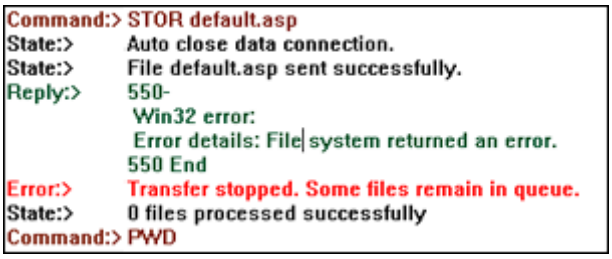
3.1. FSO Üzerinden Yapılan Saldırı Denemeleri
Sunuculara yapılan dosya değişikliği saldırılarının bir kısmı da FSO üzerinden yapılmaktadır. Web sitelerinin kullanıcılara açık olan kısımlarındaki resim ve video yükleme sayfalarında eğer dosya türü filtreleri uygulanmadıysa kullanıcılar bu sayfalardan sunucu içerisinde dosya değişikliği yapabilecek FSO kodlarından oluşan Shell dosyaları yükleyebilmektedirler. Saldırgan daha sonra bu Shell dosyalarını kullanarak sunucudaki tüm dosyalar üzerinde değişiklikler yapabilirler. Çalışmamızda kullandığımız programı aktif ettikten sonra Shell dosyalarından "Scripting.Dictionary" ile yapılmak istenen dosya değişikliği saldırıları başarılı bir şekilde engellenmiştir.

3.2 IE Tarayıcından FTP'ye Girilerek Yapılan Saldırılar
Web sunucularına FTP ile dosya yükleme metodlarından biride tarayıcılar üzerinden yapılan yüklemelerdir. Tarayıcı üzerinden FTP'ye giriş yapıldıktan sonra kişisel bilgisayarlardaki gibi dosya silme isimlendirme düzenleme işlemleri yapılabilmektedir. FTP şifresini çalan saldırganlar genel olarak sitelerin ana sayfalarını ya da çok kullanılan bazı sayfalarını buradan da değiştirebilmektedirler.
Şekil 3'te görülen FTP sunucusunda daha önceden yüklenmiş sitenin ana sayfası olan "default.asp" dosyası yer almaktadır. Yapılan saldırı denemesinde Şekil 3'te görüldüğü gibi sunucu üzerindeki default.asp silinmek istendiğinde yada üzerine yeni bir default.asp yazılmak istendiğinde erişim izni hatası oluşturularak dosya korunmuş olmaktadır.

3.3. FTP Programı İle Yapılan Saldırılar
FTP şifresini ele geçiren saldırganların site dosyalarına erişmek için kullandıkları diğer bir yol FTP programlarından sunuculara bağlanarak dosya üzerinde değişiklik yapma işlemidir. Bu denemede geliştirilen program aktif edildikten sonra "Blaze FTP" programı üzerinden sunucunun FTP hesabına girilmiş ve "default.asp" üzerinde değişiklik yapılmak istenmiştir. Şekil 4'te görüldüğü gibi sistem tarafından bu değişiklik engellenmiş ve siteye zarar verilmesinin önüne geçilmiştir.



Şekil 3. Tarayıcı üzerinden dosya değiştirmeye çalışma



Şekil 4. FTP Programı üzerinden dosya değiştirmeye çalışma

4. SONUÇLAR ve TARTIŞMA

Günümüzde web sunucularındaki siteleri hedef alan birçok saldırı metodu bulunmaktadır. Bunlardan bazıları hedef sitelerin hizmetlerini aksatma, bazıları site hedef siteyi ele geçirerek üzerinde değişiklik yapma, siteye giren kullanıcılara sitenin ele geçirildiğine dair bilgi verme şeklinde olmaktadır.

FTP ve hosting yönetim paneli şifreleri, sitelerin güvenliği açısından hayati öneme sahip olsada bazen dikkatsiz kullanımlar sonucunda başkalarının eline geçebilmektedir. Bu çalışmada hem şifre çalınma durumlarına karşı hem de Shell dosyaları kullanılarak yapılan saldırılara karşı bir çözüm önerisi sunulmuştur. Çalışmada kullanılan yazılım ve metodlar kolayca tüm sistemlere ve tüm dillere uyarlanabilir. Bu sayede web sitelerine yapılan saldırılar engellenip site sahiplerinin veri kayıplarının önüne geçilmiş olur. Ayrıca sistem saldırı kayıtlarını da tuttuğu için olası güvenlik açıklarını telafi etmek amacıyla site sahipleri tarafından önlem alınmasına olanak tanımaktadır.

5. KAYNAKLAR

[1] Karaarslan Enis, Tuglular T, Sengonca, H, 2004. “Enterprise Wide Web Application Security: An Introduction”, EICAR 2004.

[2] Özavcı, F., http://seminer.linux.org.tr/wp-content/uploads/guvenlikrisklerivesaldiriyontemleri.ppt Son Erişim : 12.05.2015

[3] Sima, C., 2005, Web Application Worms- the next Internet infestation, (In)secure, Sayı 2, Syf 17-21

[4] Seymour E. Goodman, "Critical Information Infrastructure Protection", Terrorism (Ed.), Responses to Cyber Terrorism NATO Science for Piece and Security, IOS Press (Cilt 34), Ankara, 2008, p. 25.

[5] Sushil Jajodia and Peng Liu, et all. (Ed.), Cyber Situational Awareness. New York, Springer, 2010, p. V.

[6] Karaarslan E, Tuglular T, Sengonca, H, 2006. Does NetworkAwareness Make Difference In Intrusion Detection of Web Attacks, ICHIT 2006.

[7] Karaarslan E., Doktora Tezi, 2008

[8] Magiera J., Pawlak A., Security Frameworks for Virtual Organizations, In Virtual Organizations: Systems and Practices, Springer, 2005

[9] Riden J., McGeehan R., Engert B., Mueter M., Know your Enemy: Web Application Threats, Using Honeypots to learn about HTTP-based attacks, http://honeynet.org/papers/webapp/

[10] http://www.w3schools.com/asp/asp_ref_filesystem.asp Son Erişim: 14.05.2015

[11] http://www.furkanemre.com.tr/shell-nedir-nasil-atilir-neye-yarar/ Son Erişim: 14.05.2015