WGT Capture the Flag

Onur Yılmaz, Aralık 2010, WGT E-Dergi 7. Sayı

'Etik Saldır, Kitap Kazan' ana başlığı altında üçüncüsünü düzenlediğimiz CTF yarışmasını bu akşam itibariyle sonlandırmış bulunuyoruz. Yarışmaya gösterilen ilgi için teşekkür ediyor, Web Güvenliği Topluluğu adına yarışmada ilk ikiye girerek bizden kitap hediyesi kazanan Serkan Özkan ve A. Kadir Altan arkadaşlarımızı tebrik ediyorum.

Senaryo

CTF yarışmasını, yaptığım gerçek bir güvenlik testinden esinlenerek hazırlamaya çalıştım. Testini yaptığım sistemde, uygulama, firmanın çeşitli lokasyonlardaki kullanıcılarının özel bir URL ile eriştiği public bir uygulama iken, sisteme erişilen sayfa uygulamanın herhangi bir yerinde bulunmuyordu. İlgili firma dışarıdan gelebilecek bir saldırıyı gerçeğe en yakın şekilde simule etmemiz için bize uygulamaya giriş yapacağımız URL'i vermemişti.

Bu bilgiler ışığında da; public bir uygulamaya farklı lokasyonlardan erişildiğini biliyor, erişimin sağlandığı URL'i, erişimi sağlayan kişilerle kontak kurmadan nasıl öğrenirim? noktasından hareket ile CTF yarışmasının senaryosunu hazırladım.

Çözüm

CTF yarışması için tek verilen bilgi, yarışmanın yapılacağı URL oldu.
http://ctf.webguvenligi.org/

CTF'de bizi karşılayan mesaj; 'Sisteme Giriş Sayfasını bulmanız gerekmekte !' şeklinde.

- Aslında bu mesaj bir ipucu idi. Çünkü sisteme giriş yapmak için kullanacağınız sayfanın adı; 'SistemeGirisSayfasi.aspx' olarak belirlenmişti. Güvenlik testi yapan kişilerin, teknik bilgilerinin yanında doğal bir yeteneklerinin, sezgi ve tahmin güçlerinin kuvvetli olmasının saygıyla karşılanması gerektiği düşündüğümden böyle bir isimle giriş sayfasını uygulamaya yerleştirmiştim. Yarışmada ilk ikiye giren arkadaşlar da bu şekilde tahmin ettikleri için kendilerini tebrik ediyorum.
- Giriş sayfasını tahmin edemeyenler için ikinci bir yöntem fuzzing olacaktı.
- Bunlar haricinde benim kurguladığım ise uygulamanın analizi ile hareket ederek giriş sayfasına ve oradan diğer adımlara geçmekti.

Uygulamaya yapılan bir GET isteğine dönen cevaba baktığımızda;

X-Powered-By: PleskWin

şeklinde bir başlık bilgisine ulaşılacaktı.

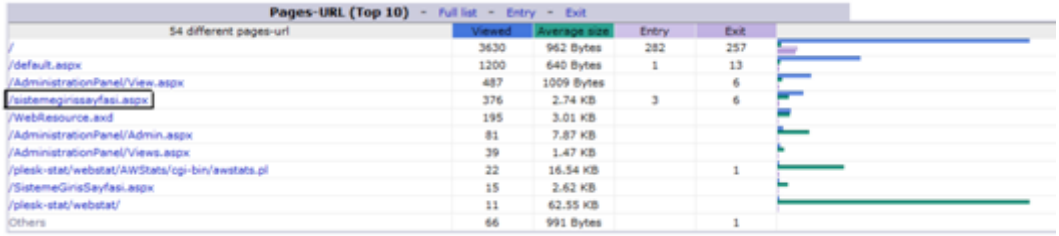
Daha önceden Plesk uygulamasını kullananlarınızın bileceği üzere, sunucuda koşan Plesk üzerinden yeni bir web sitesi oluşturduğunuzda, 'hosting management' alanından, Plesk ile gelen 'log / analiz' uygulamalarını aktif edebiliyor ve uygulamanıza gelen trafik ve benzeri bilgileri periyodik güncellemeler sonucunda görebiliyordunuz.

Ben Plesk'in 'unlimited' template`i ile ctf.webguvenligi.org alan adı için bir web sitesi oluşturduğumdan, 'Awstats' isimli log / analiz uygulaması da otomatik olarak devreye girdi.

Bu başlık bilgisinden, sunucu üzerinde Plesk'in olduğunu sızdırmış olduk. CTF`e katılan arkadaşların, 'uygulamada bir giriş sayfası var ama ben bu sayfanın neresi olduğunu bilmiyorsam nasıl ulaşırım?' sorusunu kendilerine sormalarını amaçlayarak, bu log / analiz sayfasını bulmalarını istemiştim. (Bu noktada yine fuzzing devreye girebileceği gibi, benim gibi daha önce Plesk kullanan arkadaşlar bu uygulamanın path'ini biliyor olabilir.)

http://ctf.webguvenligi.org/plesk-stat/webstat/

Awstats uygulamasına girildiğinde ise, nasılsa bu uygulamayı kullanan kullanıcılar daha önce sisteme giriş yaptıkları sayfaya erişim sağlamışlar diye düşünerek loglar analiz edilmeliydi.



Bu şekilde sisteme girişin yapılabileceği sayfa tespit edilmiş olacaktı.

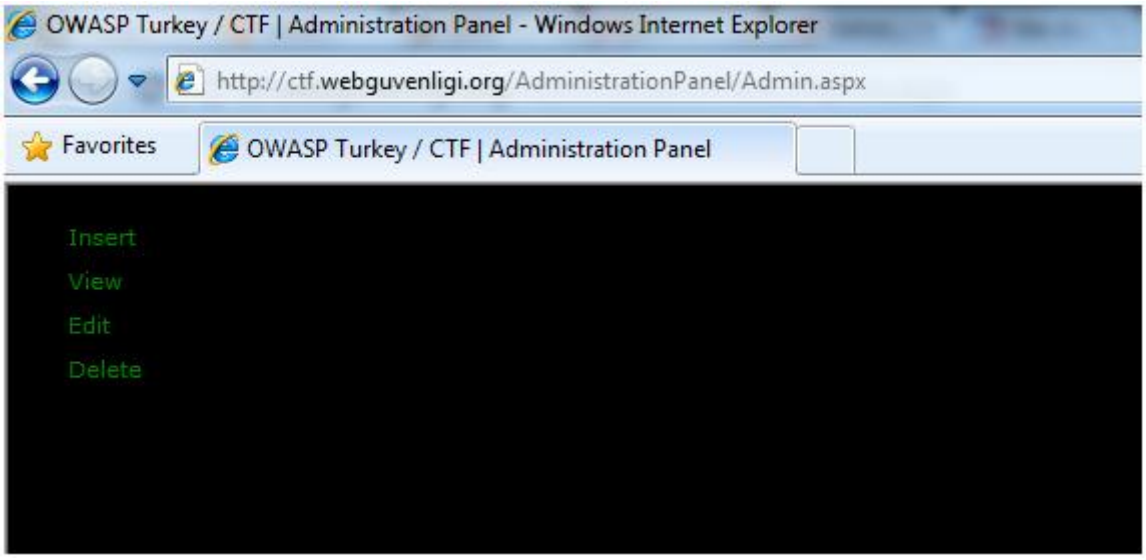
http://ctf.webguvenligi.org/SistemeGirisSayfasi.aspx

Sisteme girişin yapılacağı sayfayı bir önceki CTF'lerden hatırlayabilirsiniz. Bu sefer diğerlerinden farklı olarak giriş alanında herhangi bir veritabanı ya da veri kaynağı bağlantısı yoktu ve bu nedenle SQL Injection denemeleri sonuçsuz kalacaktı.

Güvenlik testlerinde giriş arayüzlerine yapılacak testlerden olan 'Öntanımlı / Zayıf Kimlik Doğrulama Bilgisi Kullanımı'nın önemini ve kullanıcı ya da yazılımcıların öntanımlı ya da varsayılan kullanıcı adı ve şifrelerini kullanmamalarını hatırlatmak amacıyla, kullanıcı adı ve şifre kombinasyonunu 'admin/admin' olarak belirledim.

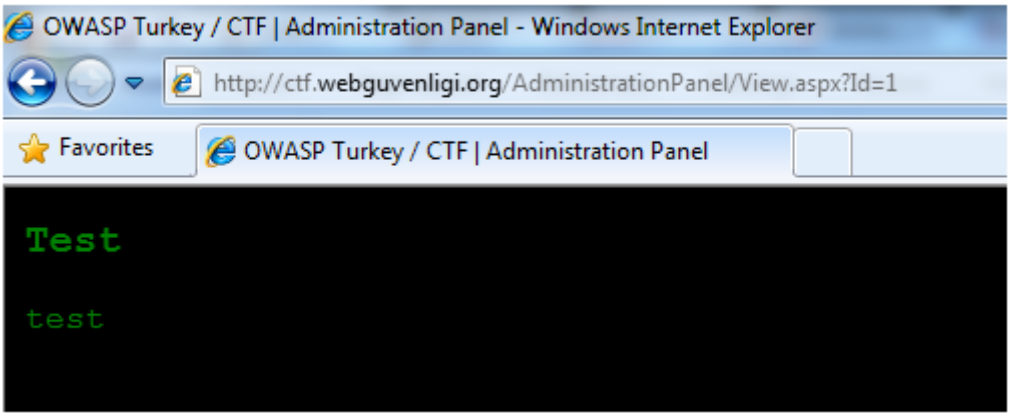
Bu aşamayı da brute-force (kaba kuvvet) ya da tahmin yoluyla geçenler için son aşama geliyor olacaktı. (Bu aşamayı çabuk geçmeniz gerekiyordu. Kombinasyonu doğru da bilseniz session süresini kısıtlı tutmuş idim)

http://ctf.webguvenligi.org/AdministrationPanel/Admin.aspx



Yönetici arayüzüne erişim sağladıktan sonra, 'Insert, View, Edit, Delete' şeklinde CRUD işlemlerinin temelini oluşturan dört fonksiyonun yerleştiğini görecektiniz. Buradaki amacım 'acaba bir veriyi sisteme ekleyerek, daha sonra onu düzenleyeceğimiz alandan mı saldırı gerçekleştireceğiz' düşüncesini oluşturarak zaman kaybettirmekti :) View alanına girdiğinizde, uygulamaya eklenmiş bir veriyi görecektiniz.

http://ctf.webguvenligi.org/AdministrationPanel/View.aspx?Id=1



Ve tahmin edeceğiniz üzere, Id parametresine ilk olarak SQL Injection deneyecek ve veritabanı ismini elde etmiş olacaktınız.

Herkese ‘mutluyillar’ dileriz :)