

WEB SUNUCU GÜVENLİĞİ:

Web Siteleri Neden Hacklenir?

Gereksiz yedek dosyaları

Default ayarlarla gelen konfigürasyon dosyaları

Yetkisi tam olarak verilmiş dosyalar ya da dosya izni kontrolü yapılmadan sunucuda barındırılan dosyalar

Örn:777 dosya izni

Default Kullanıcı ve Default şifreleri değiştirilmeyen kullanıcı hesapları

Örnek:Açık bırakılmış guest hesabı şifresi de guest'dir.

Yetkili bir ssl sağlayıcısından alınmamış self-sign sertifikalar!

Yeni çıkan açıklıklara karşı güncellenmeyen ya da güncellemeye kapalı web sunucuları

Web Sunucu Güvenliğindeki Atak Vektörleri:

Kullanıcı hesaplarının ele geçirilmesi.

Web Sitelerinin İçeriklerinin Değiştirilmesi(Web Site Defacement)

Data Tampering

Data Theft:Veri Hırsızlığı

Root Access:Web sitesi tahrif edildikten sonra web sunucu kök dizinine erişme aynı ağda yer alıyorsa diğer sunuculara erişme ve zarar verme.

Yanlış Konfigüre Edilmiş Web Sunucusu:

- Web sunucusundaki debug ve hata mesajlarının açık bırakılması
- Sunucuda yer alan web uygulama script dosyaları ve konfigürasyon dosyaları
- Anonymous yani herkesin erişebileceği hesapların açık bırakılması,default kullanıcı ve şifrelerinin açık unutulması
- Kullanılmadığı halde açık bırakılan servisler
- Sunucunun uzaktan yönetilmesine imkan veren ayarların açık bırakılması, aktif hale getirilmesi

Web Sunucu Konfigürasyon hatası örnekleri:

Example

httpd.conf file on an Apache server

```
<Location /server-status>
SetHandler server-status
</Location>
```

This configuration allows anyone to view the server status page which contains detailed information about the current use of the web server, including information about the current hosts and requests being processed

php.ini file

```
display_error = On
log_errors = On
error_log = syslog
ignore_repeated_errors = Off
```

This configuration gives verbose error messages

CEH
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Şekil 1:httpd.conf dosyasında yapılan ayarda sunucu durumu ve ayrıntıları görüntülenebilir.

Php.ini dosyasındaki söz konusu konfigürasyon doğru bir ayarlama biçimi değildir. display_error off yapılırsa php ile ilgili oluşan hatalar ekrana basılmaz.

Directory Traversal Saldırıları:

Directory traversal atağı saldırganın hassas dizinlere kadar girebilmesini sağlayan, web kök dizini dışından da komut çalıştırmasına imkan veren HTTP zaafiyetidir.

Web Sunucu Saldırı Metodolojisi:

Bilgi Toplama:

Örnek:netcraft.com üzerinden bilgi toplama.

Telnet ile banner grabbing yaparak bilgi toplama.

Website Mirroring:

Web sitesinin klasörlerini listelemek,dosya yapısını çıkarmak,harici linklerini listelemek için websitesinin offline bir kopyası oluşturulur.

Örnek:Teleport Pro, HTTrack

Web Sunucu açıklık taramaları:

Örnek:Nessus aracı ile tarama
Nikto aracı ile tarama

Oturum Çalma:

BurpSuite,Hamster,WebScarab,ParosProxy gibi araçlar kullanılarak oturum bilgileri elde edilebilir.



Şekil 2:Wfetch programı

Web sitesine gönderilen ham istek ve dönen cevabı görmek için Wfetch gibi araçlardan faydalanılır.

Protokol Bazlı Önlemler:

Gereksiz bütün portlar filtrelenmelidir.ICMP portu, netbios vb. kullanım gerekliliği olmayan protokoller kapatılmalıdır.

Uzaktan erişim yapılması şart ise vpn vb. Şifreli tünelleme yoluyla erişim gerçekleştirilmelidir.

POP3,telnet,ftp,smtp protokolleri vb. Şifresiz protokoller kullanılıyorsa IPsec vb. Yetkilendirme ve şifreleme servisleri aktif hale getirilmelidir.

Dosya ve Klasör Bazlı Önlemler:

Arşiv dosyaları,yedek dosyaları,web script dosyaları vb. hassas bilgi içeren dosyaları internete açık klasörlerde unutmamak önemlidir!

Web sitesine yapılan giriş kayıtları, sql sunucu kayıtları gözlemlenmeli ve anomalilere karşı önlem alınmalıdır.

How to Defend Against Web Server Attacks?

- Ports**
 - Audit the **ports on server** regularly to ensure that an insecure or unnecessary service is not active on your Web server
 - Limit inbound traffic to **port 80 for HTTP** and **port 443 for HTTPS (SSL)**
 - Encrypt or restrict **intranet traffic**
- Server Certificates**
 - Ensure that **certificate data ranges** are valid and certificates are used for their intended purpose
 - Ensure that the certificate has not been revoked and **certificate's public key** is valid, all the way to a trusted root authority
- Machine.config**
 - Ensure that protected resources are mapped to **HttpForbiddenHandler** and **unused HttpModules** are removed
 - Ensure that **tracing is disabled** <trace enable="false"/> and **debug compiles** are turned off
- Code Access Security**
 - Implement **secure coding** practices to avoid source code disclosure and input validation attack
 - Restrict **code access security policy** settings to ensure that code downloaded from the Internet or Intranet have no permissions to execute
 - Configure IIS** to reject URLs with **"../"** to prevent path traversal, lock down **system commands** and utilities with **restrictive access control lists (ACLs)**, and install new patches and updates

CEH Certified Ethical Hacker

48

Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Patch Yönetim Aracı:MBSA(Microsoft Baseline Security Analyzer) programı ile güvenlik taraması gerçekleştirilmeli ve zayıflıklar tespit edilerek kapatılabilmektedir.

Zaafiyet Tespit Programları:Wiko windows için kullanılabilen web sunucu açıklık tarama programı.

Nikto linux için kullanılabilecek zaafiyet tarama programı.

Patch Management Tools



Altiris Client Management Suite
<http://www.symantec.com>



Novell ZENworks Patch Management
<http://www.novell.com>



ProManage Remote Infrastructure Monitoring
<http://www.silverbacktech.com>



Security Manager Plus
<http://www.manageengine.com>



GFI LANguard
<http://www.gfi.com>



Prism Patch Manager
<http://www.newboundary.com>



Kaseya Security Patch Management
<http://www.kaseya.com>



MaaS360's Patch Management
<http://www.maas360.com>

CEH
Certified Ethical Hacker

60

Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Web sunucu yama takibi ve yönetimi için diğer programlar