

Web Application Penetration Test Report

Sızma testleri (Pentest) ve zayıflık tarama (Vulnerability Assessment) birbirine benzeyen iki aşamadan oluşur. Zayıflık tarama hedef sistemdeki güvenlik açıklıklarının çeşitli yazılımlar kullanarak bulunması ve raporlanması işlemidir.

Pentest ise amaç sadece güvenlik açıklıklarını belirlemek değil, bu açıklıklar kullanılarak hedef sistemler üzerinde gerçekleştirilebilecek ek işlemlerin (sisteme sızma, veritabanı bilgilerine erişme gibi) belirlenmesidir.

Amacımız Belirlenen bilişim sistemlerine mümkün olabilecek her yolun denenerek sistemlerde güvenlik zafiyetine sebep olabilecek açıklıkların araştırılması tespit edilmesi ve ayrıntılı bir şekilde raporlanmasıdır.

Önemli Bilgilendirme:

- Bu testler uluslararası ISO 27001 Bilgi Güvenliği Yönetim Sertifikası standartlarına uygun olarak yapılmaktadır.

ISO	Adı	TSNO
ISO/IEC 27001:2005	Information technology Security techniques Information security management systems	TS ISO/IEC 27001:2006

Adım	Yapılan İşlemler	Sonuç
A	Web Güvenlik Testleri Rapor	
1	Site Dizinleri Taranması(Dirbuster)	
2	Hedef Sistemin İşletim Sistemi Tespiti	
3	Kimlik Doğrulama Atlatma Testleri	
4	SQL Enjeksiyonu Testleri	
5	Local / Remote File İnclusion Testleri	
6	Xpath Enjeksiyon Testleri	
7	Cross-site scripting Testleri	
8	Domainin Statik Güvenlik Açıklarının Tespiti	
9	EBYS'nin bulunduğu sunucunun tespit edilmesi ve Zafiyet Taraması	

Talep Eden Onay

İmza

Üst Yönetim Onay

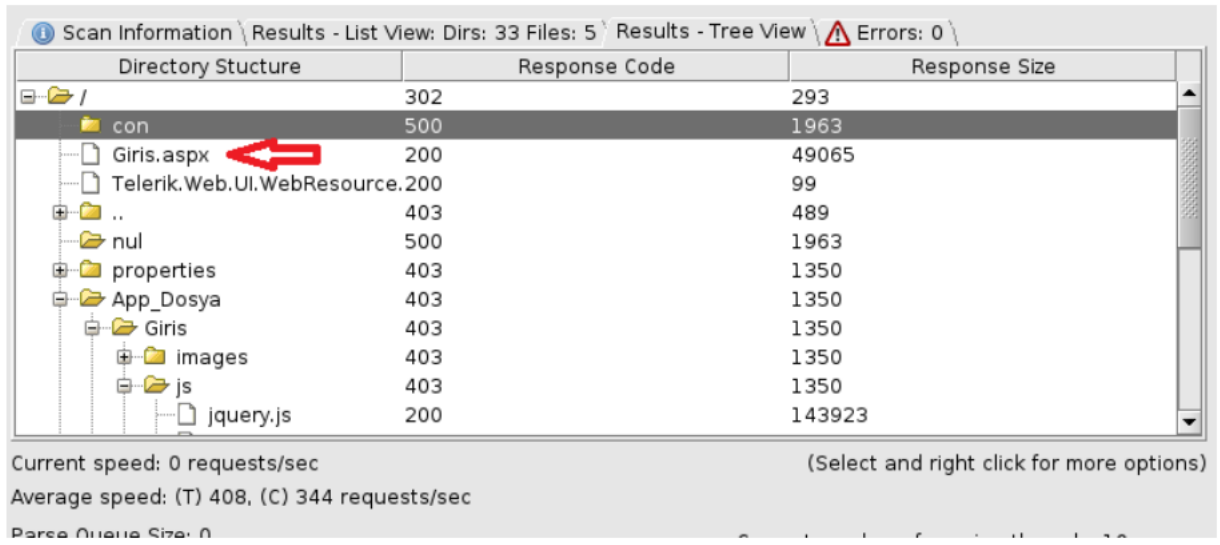
İmza

A. Web Güvenlik Testleri Sonuç Listesi

1.Site Dizinleri Taranması(Dirbuster)

Amaç: Kurumun Web sitesinin hassas bilgiler içeren dizinleri taranarak admin girişi ve config dosyalarının bulunduğu dizinlere erişim hedeflenmektedir. Buradaki diğer bir amaç ise kurumun web sitesinin haritasının çıkarılmasıdır.

Sonuç: Site dizinleri taranarak kullanıcı login sayfası tespit edilmiştir Başka önemli bir dizine erişim sağlanamamıştır.



Directory Structure	Response Code	Response Size
/	302	293
con	500	1963
Giris.aspx	200	49065
Telerik.Web.UI.WebResource.200	99	
..	403	489
nul	500	1963
properties	403	1350
App_Dosya	403	1350
Giris	403	1350
images	403	1350
js	403	1350
jquery.js	200	143923

Current speed: 0 requests/sec (Select and right click for more options)
Average speed: (T) 408, (C) 344 requests/sec
Parse Queue Size: 0

2. Hedef Sistemin İşletim Sistemi Tespiti

Amaç: Kurumun web sitesinin bulunduğu sunucunun işletim sistemini tespit etmek ve bu doğrultuda hedef sistem üzerinden güvenlik açıkları arayarak sisteme sızmak hedeflenmektedir.

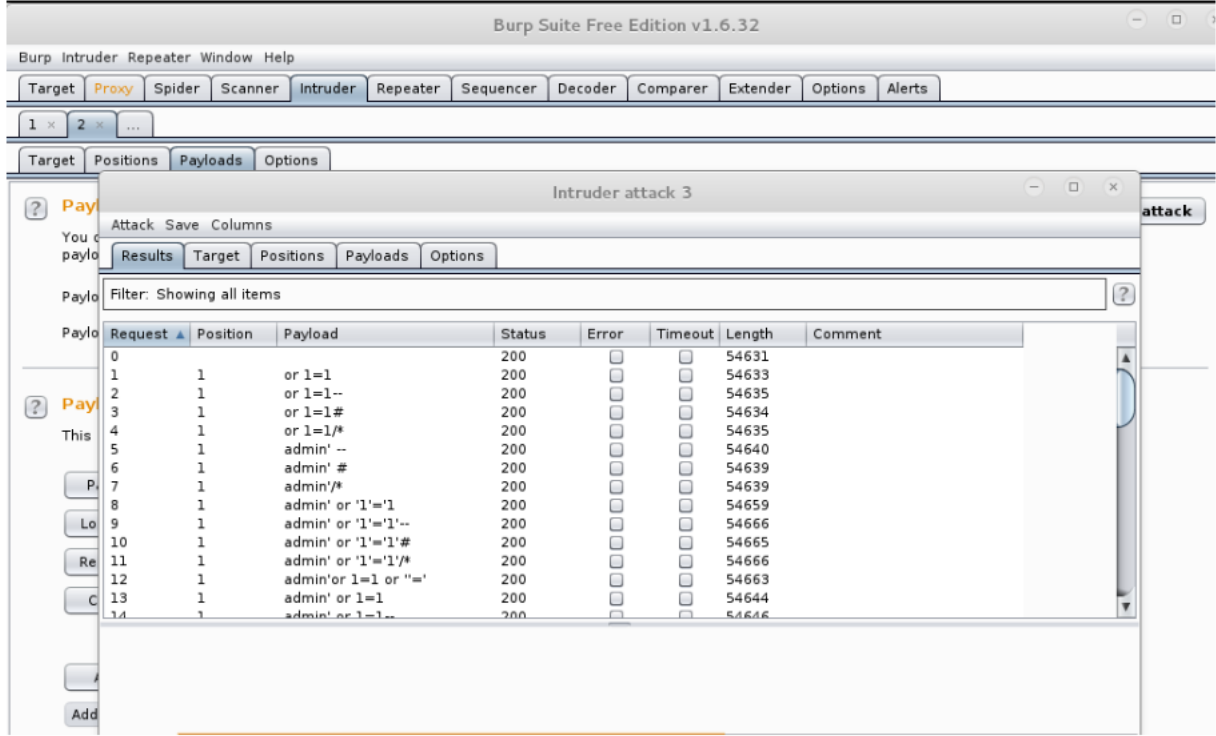
Sonuç: Hedef sistemin işletim sistemi Windows server 2012 olarak tespit edilmiştir.

```
1077/Adp7
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-04-07 00:39 EEST
Nmap scan report for ebyssorgu.aski.gov.tr (172.16.30.240)
Host is up (0.13s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_._. http-methods: _._. _._. 200 53172
_._. Potentially risky methods: TRACE 403 489
_._. http-server-header: Microsoft-HTTPAPI/2.0 200 99
_._. http-title: Belge Sorgulama Ekran\xC4\xB1 302 331
443/tcp    open  ssl/http  Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
_._. http-methods: _._. _._. 302 339
_._. Potentially risky methods: TRACE 403 1370
_._. http-server-header: Microsoft-HTTPAPI/2.0 302 337
_._. http-title: Belge Sorgulama Ekran\xC4\xB1 302 321
_._. ssl-cert: Subject: commonName=*.aski.gov.tr/organizationName=Aski Genel Mudurlugu/stateOrProvinceName=Ankara/countryName=TR 500 1951
Not valid before: 2015-05-13T13:07:05
Not valid after: 2018-08-13T13:07:05
ssl-date: 2017-04-07T13:43:14+00:00; +16h02m45s from scanner time.
614/tcp    filtered shell
Device type: general purpose
Running: Microsoft Windows 7|2012|XP.
OS CPE: cpe:/o:microsoft:windows 7 cpe:/o:microsoft:windows server 2012 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows 7 -> Windows Server 2012, Microsoft Windows XP SP3
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.15 ms 192.168.38.2
2 0.15 ms ebyssorgu.aski.gov.tr (172.16.30.240)
```

3. Kimlik Doğrulama Atlatma Testleri

Amaç: Kuruma ait web sitesinde tespit edilen kullanıcı adı şifre alanlarını çeşitli SQL sorguları deneyerek kimlik doğrulama yapmadan sisteme giriş yapmak hedeflenmektedir.

Sonuç: Kimlik Doğrulama atlatma testi başarısız. EBYS login paneline yapılan bypass saldırısı başarılı olmamıştır. Sistem Güvenlidir.



5. SQL Enjeksiyonu Testleri

Amaç: Kuruma ait web sitesinde SQL sorgularına dışardan müdahalede bulunarak veri tabanına kayıt ekleyerek sisteme girmek veya veri tabanından kayıt listeleme yaparak yetkili kişilerin kullanıcı hesabı bilgilerine erişmek hedeflenmektedir.

Sonuç: Yapılan testler Sonucunda ebys üzerinde herhangi bir SQL injection zafiyetine rastlanmadı.

6. Local / Remote File Inclusion Testleri

Amaç: Bu testin amacı kuruma ait web sitesi üzerinde local ve remote inclusion zafiyetlerinin tespit edilmesidir. Local file inclusion ile /etc/passwd/ dosyalarının okunarak kullanıcı adı ve şifrelerin tespit edilmesi hedeflenmektedir. Remote file inclusion ile hedef siteye uzaktan kod dahil ederek sisteme bir backdoor oluşturup sisteme sızmak hedeflenmektedir.

Sonuç: Sistem üzerinde local file include güvenlik zafiyeti tespit edilmiştir. Fakat güvenlik zafiyetinin doğrudan sisteme sızmaya yol açabilecek bir zafiyet değildir.

6.1 Possible Local File Include

Açıklama(Description): Saldırgan yetkisi olmadığı yerel dosyaları çalıştırarak yerel dosyalar içerisinde varsa hassas bilgilere ulaşabilir.

Rate: Medium

Çözüm(Solution): AspNet uygulamalarda GetFullPath() kullanarak lfi açığı önlenabilir.

Page Fingerprint Differential Detected - Possible Local File Include

► AT A GLANCE

Classification	Error Message
Resource	/Telerik.Web.UI.WebResource.axd
Parameter	guid
Method	GET

► REQUEST

GET /Telerik.Web.UI.WebResource.axd?type=rca&isc=true&guid=../

7. Xpath Enjeksiyon Testleri

Amaç: Bu testin genel amacı kuruma ait web sitesi üzerindeki xml dosyalarına ulaşarak içinde bulunan verilere erişmek ve bu xml dosyaları içinde saklanan kullanıcı bilgilerine ulaşmaktır.

Sonuç: EBYS üzerinde yapılan testler sonucunda Xpath injection zafiyetine rastlanmamıştır.

8. Cross-site scripting Testleri

Amaç: Kuruma ait web sitesi üzerinde javascript kodları arasına zararlı kod yerleştirerek kullanıcı cookieilerini elde etmek ve siteye redirect kodu yerleştirerek daha önceden hazırlanmış zararlı kodlar içeren başka bir siteye yönlendirme hedeflenmektedir.

Sonuç: EBYS üzerinde yapılan testler sonucunda cross site scripting zafiyetine rastlanmamıştır.

9. Domainin Statik Güvenlik Açıklarının Tespiti2

Amaç: Kuruma ait web sitesini vega ya da nikto gibi open source web Vulnerability scanner yazılımları ile güvenlik taraması yapmak ve elde edilen sonuçlar doğrultusunda sisteme sızmak hedeflenmektedir.

10. EBYS'nin bulunduğu sunucunun tespit edilmesi ve Zafiyet Taraması

Amaç: EBYS 'nin tutulduğu serverin tespit edilmesi ve bu server üzerindeki güvenlik zafiyetlerinin tespit edilmesi hedeflenmektedir.

Sonuç: EBYS 'nin bulunduğu server tespit edilmiş, işletim sistemi belirlenmiş ve zafiyet taraması gerçekleştirilmiştir. Herhangi bir güvenlik zafiyeti tespit edilmemiştir.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Output

A web server is running on this port.

Port ▼	Hosts
80 / tcp / www	172.16.30.240 

A TLSv1 server answered on this port.

Port ▼	Hosts
443 / tcp / www	172.16.30.240 

A web server is running on this port through TLSv1.

Port ▼	Hosts
443 / tcp / www	172.16.30.240 

Önemli Bilgilendirme: EBYS üzerinde yapılan web application penetrasyon testleri sonucunda sistemde bazı zafiyetler tespit edilmiştir. Bunların içerisinde kritik öneme sahip yani doğrudan EBYS'yi hedef alacak sistemin çalışmasını engelleyecek bir zafiyet tespit edilmemiştir.