

S~SECURITY WEB GÜVENLİK DENETİM SONUÇ RAPORU

S~SECURITY BİLGİ GÜVENLİĞİ ANONİM ŞİRKETİ

YALANDAN DOLANDAN BİR ADRES SATIRI İLÇE/İL

T : 05TELEFON

F : 02FAX

bilgi@s-security.com.tr

19.08.2022 - 28.08.2022

S~Security Web Güvenlik Denetim Raporu

Bu belge “BGA BANK” kurumuna ait “GİZLİ” bilgiler içermektedir ve yetkili kişiler haricinde okunması yasaktır. Bu belge elinize yetkisiz bir şekilde ulaşırsa lütfen bilgi@s-security.com.tr adresine bildiriniz.

Rapor Detayları

RAPOR BAŞLIĞI	S~SECURITY WEB GÜVENLİK DENETİM SONUÇ RAPORU
VERSİYON	1.0
YAZAN	Sinan EĞİLMEZ
TEST EKİBİ	Sinan EĞİLMEZ
KONTROL EDEN	Sinan EĞİLMEZ
ONAYLAYAN	Sinan EĞİLMEZ
RAPOR SINIFI	GİZLİ

Müşteri Kurum Yetkilisi

Yetkili Adı ve Soyadı	Ünvanı	Kurum Adı
Sinan EĞİLMEZ	Genel Müdür	S~security

Rapor Denetimi

Versiyon	Tarih	Yazar	Tanım
1.0	25.08.2022	Sinan EĞİLMEZ	Final

S~Security Web Güvenlik Denetim Raporu

Yasal Sorumluluklar

Söz konusu raporun içeriği gizli olup, taraflar arasında yazılı mutabakat olmadan üçüncü kişilere basılı olarak (hardcopy) ya da elektronik ortamda (softcopy) paylaşılamaz, yayınlanamaz ve çoğaltılamaz.

....

....

....

....

1.GİRİŞ	5
2.KAPSAM	6
3.YÖNETİCİ ÖZETİ	6
4.WEB GÜVENLİĞİ TESTİ METODOLOJİSİ	9
5.TANIMLAR VE SEVİYELENDİRME	12
5.1. Testlerin Gerçekleştirildiği Erişim Noktaları	12
5.2. Testlerin Gerçekleştirildiği Kullanıcı Profilleri	12
5.3. Risk Seviyelendirme	12
6.GERÇEKLEŞTİRİLEN GÜVENLİK TESTLERİ VE SONUÇLARI	13
6.1.Web Uygulama Güvenlik Testleri	14
6.1.1 Gerçekleştirilen Güvenlik Testi İşlemleri	14
6.1.2 Tespit Edilen Açıklıklar	17
6.1.2.1 Yansıtılan Siteler Arası Script Çalıştırma/XSS (OWASP-DV-001)	17
6.1.2.2 Depolanan Siteler Arası Script Çalıştırma/XSS (OWASP-DV-001)	19
6.1.2.3 SQL Injection Zafiyeti (OWASP-DV-005)	21
6.1.2.4 Local File Inclusion Zafiyeti (OWASP-CM-006)	27

1.GİRİŞ

Bu rapor, BGA Bilgi Güvenliği Anonim Şirketi tarafından “TestPark” sistemleri üzerindeki güvenlik açıklarını ortaya çıkartmak amacı ile 15.02.2014 - 12.03.2014 tarihleri arasında gerçekleştirilen güvenlik ve sızma testlerinin (Web security test) detaylı sonuçlarını içermektedir.

Web güvenlik testi çalışması kapsamında “TestPark” altyapısı ve sunucularının çalışmasını olumsuz yönde etkileyecek araçlar ve yöntemler kullanılmamış, izinsiz ve yetkisiz bir şekilde hizmetin aksamasına neden olabilecek herhangi bir işlem gerçekleştirilmemiştir.

Rapor, kapsam, yönetici özeti, öneriler ve kategorik olarak tespit edilen güvenlik açıklıklarına ait detayları ve referansları içermektedir.

Web güvenlik testi raporunda kullanılan yabancı ve teknik terimlere ait sözlük rapor sonunda EK-1 olarak sunulmuştur.



Raporda sadece açıklık barındıran uygulamalar ve bu uygulamalardaki düşük, orta, yüksek, kritik ve acil seviye güvenlik zafiyetleri detaylı incelenmiş, yanlış alarm (false positive) olabilecek başlıklar elenerek, gerekli görülenler rapora eklenmiştir.

2.KAPSAM

Web güvenlik testinde ana amaçlardan biri tüm zafiyetlerin değerlendirilerek sisteme sızılmaya çalışılmasıdır. Bu amaç doğrultusunda gerçekleştirilecek web güvenlik testlerinde kapsam web güvenlik çalışmasının en önemli adımını oluşturmaktadır.

3.YÖNETİCİ ÖZETİ

Bu rapor, S~security Bilgi Güvenliği Anonim Şirketi tarafından Test Park bilişim sistemleri üzerindeki güvenlik açıklarını ortaya çıkartmak amacı ile 19.08.2022 - 28.08.2022 tarihleri arasında gerçekleştirilen web güvenlik testleri (web security test) çalışmalarının sonuçlarını içermektedir.

Testler, raporun devamında detayları verilen web uygulama, sosyal mühendislik, etki alanı/sunucu-istemci sistemler, anahtarlama/yönlendirici cihazları, e-posta servisi, DNS servisi, veritabanı sistemleri ve DoS/DDoS kapsamında gerçekleştirilmiştir.

Çalışmalar süresince dış/iç siber saldırgan gözüyle sistemler tüm detaylarıyla incelenmiş ve kurum yetkilisinin onayı dahilinde çıkan açıklıklar istismar edilerek sızma denemeleri gerçekleştirilmiştir.

Çalışmalar sonucunda 1 acil, 1 kritik, 2 yüksek olmak üzere toplamda 4 farklı güvenlik açıklığı tespit edilmiştir. Bir açıklığın birden fazla sistemde bulunması açıklık sayısını etkilememektedir.

SQL enjeksiyonu, siteler arası script çalıştırma açıklığı, güncelleştirme eksikliklerinden kaynaklanan kritik güvenlik açıklıkları, kontrolsüz dosya upload fonksiyonu ile işletim sistemi bazında erişim elde etme, öntanımlı kullanıcı hesapları ile erişilen sistemler ile elde edilen hassas bilgiler yapılan web güvenlik testlerindeki kritik bulgulardır.

Testler sonucu en büyük güvenlik eksikliği, çalışan sistemlerin güvenlik standartlarına ve prosedürlerine uygun olarak kurulmaması ve kurulumdan sonra gereken güvenlik sıkılaştırmalarının yapılmaması veya eksik yapılmasından kaynaklandığı belirlenmiştir.

Bu sebeple her bir işletim sistemi, ağ cihazı ve diğer cihazlar için bir kurulum prosedürünün hazırlanması, bütün kurulumların yazılı prosedürlere uygun olarak yapılması ve ürün ortamına alınmadan önce mutlaka güvenlik taramasından geçirilmesi önerilmektedir.

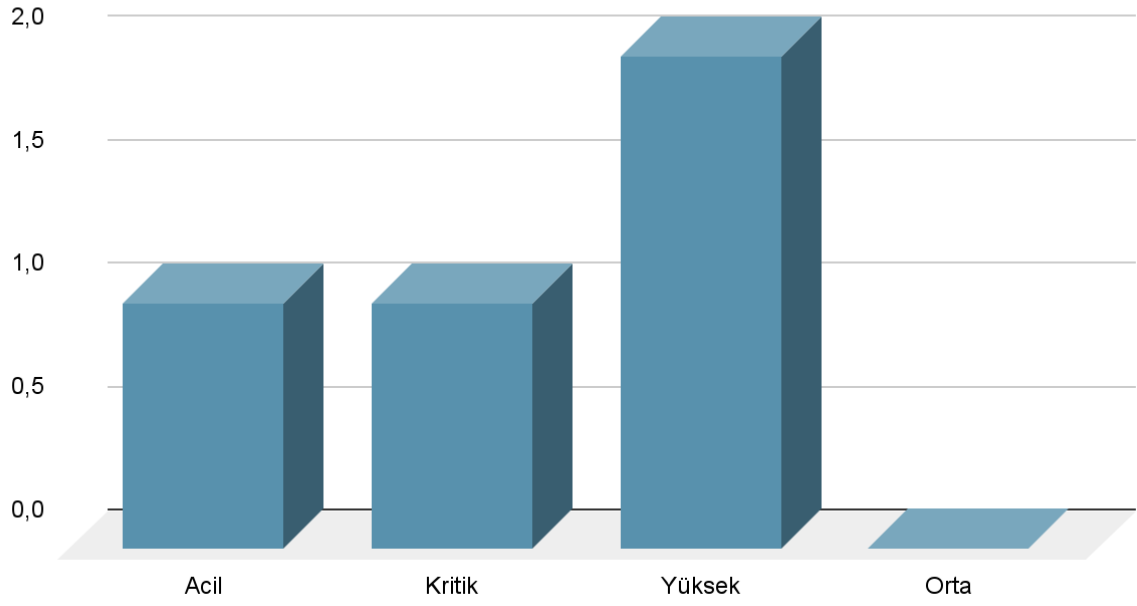
Raporda her bir açıklığın hangi sistemlerde bulunduğu, açıklıklar ile ilgili alınması gereken önlemler detaylı olarak açıklanmıştır. Kurum adına başarısız sonuçlanan testlerin sebebi olan güvenlik açıklıklarının kapatılması için gerekli çalışmalar yapılmalıdır. Açıklıkların kapatılmasında izlenecek sırayı belirlerken teknik raporda belirtilen açıklık önem dereceleri öncelikli rol oynamalıdır.

S~Security Web Güvenlik Denetim Raporu

Bulunan Güvenlik Açıklarına Ait Grafiksel Gösterimler

Müşteri kurum için yapılan sızma testine ait elde edilen bulguların kritiklik durumuna göre sayılarını gösteren grafik aşağıda verilmiştir :

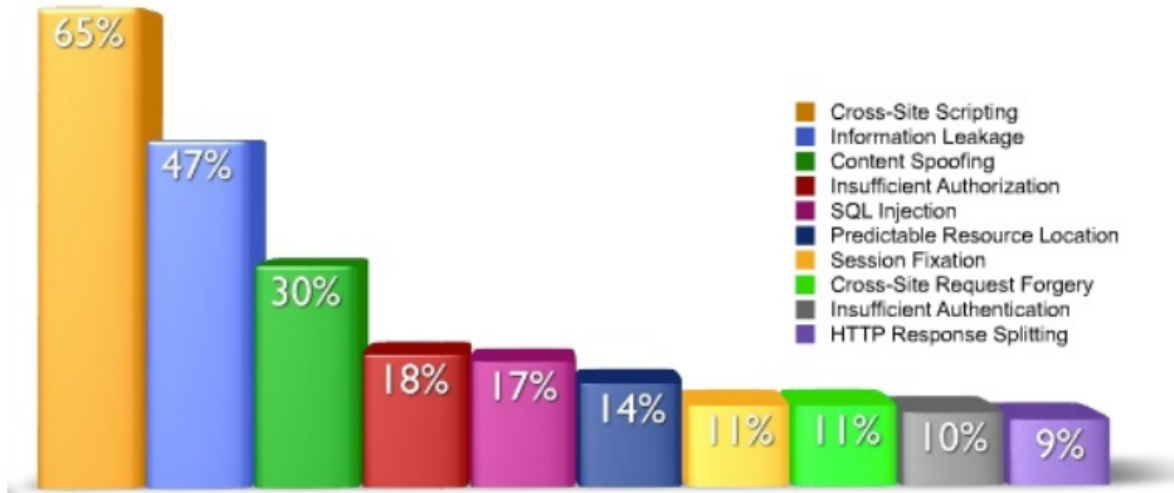
Bulunan Güvenlik Açıklarına Ait Grafik



Web Uygulama Güvenliği

Uygulama seviyesi açıklıklar genel olarak kullanılan programlama dilindeki kontrol eksikliği ve son kullanıcıdan alınan girdilerin yeterli kontrolden geçirilmemesinden kaynaklanmaktadır.

OWASP TOP 10 (2013 Yılı web uygulamalarında çıkan açıklıkların dağılımı) incelendiğinde XSS, SQLi ve session yönetimi konularının başı çektiği görülmektedir. Sızma testi sonuçları incelendiğinde OWASP TOP 10 listesi ile paralel sonuçların çıktığı gözükmemektedir.

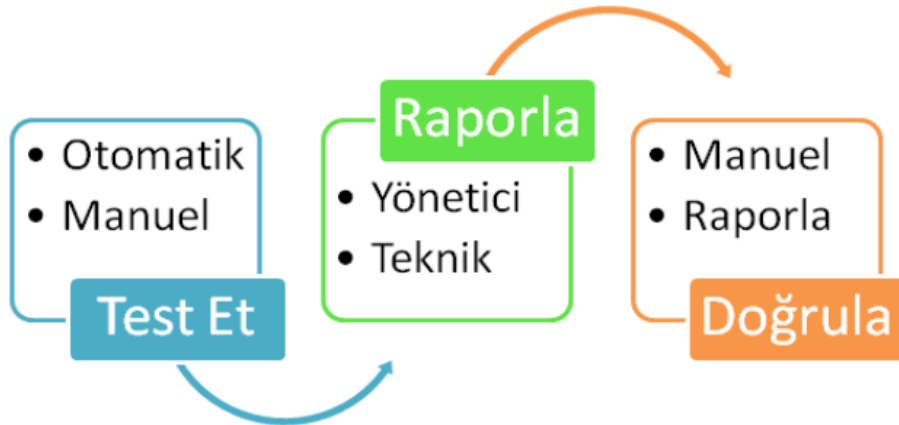


4.WEB GÜVENLİĞİ TESTİ METODOLOJİSİ

Günümüzde bilgi güvenliğini sağlamak için iki farklı yaklaşım sunulmaktadır. Bunlardan ilki savunmacı yaklaşım(defensive) diğeri de proaktif yaklaşım (offensive)olarak bilinir. Bunlardan daha yaygın olarak kabul göreni proaktif yaklaşımdır. Pentest –sızma testleri– ve vulnerability assessment –zayıflık tarama- konusu proaktif güvenliğin en önemli bileşenlerinden biridir.

Pentest(sızma testleri) ve Vulnerability assessment(zayıflık tarama) birbirine benzeyen fakat farklı kavramlardır. Zayıflık tarama, hedef sistemdeki güvenlik açıklıklarının çeşitli yazılımlar kullanarak bulunması ve raporlanması işlemidir. Pentest çalışmalarında amaç sadece güvenlik açıklıklarını belirlemek değil, bu açıklıklar kullanılarak hedef sistemler üzerinde gerçekleştirilebilecek ek işlemlerin (sisteme sızma, veritabanı bilgilerine erişme) belirlenmesidir.

Zayıflık tarama daha çok otomatize araçlar kullanılarak gerçekleştirilir ve kısa sürer. Pentest çalışmaları zayıflık tarama adımını da kapsayan ileri seviye tecrübe gerektiren bir süreçtir ve zayıflık tarama çalışmalarına göre çok daha uzun sürer.



Şekil 1 – Genel metodoloji

S~security “Security Assessment Framework” hazırlanırken konu hakkındaki uluslararası standartlar incelenmiş ve azami ölçüde faydalanılmıştır. Aşağıda bu belgenin hazırlanmasında kaynak olarak kullanılan dökümanların isimleri yer almaktadır.

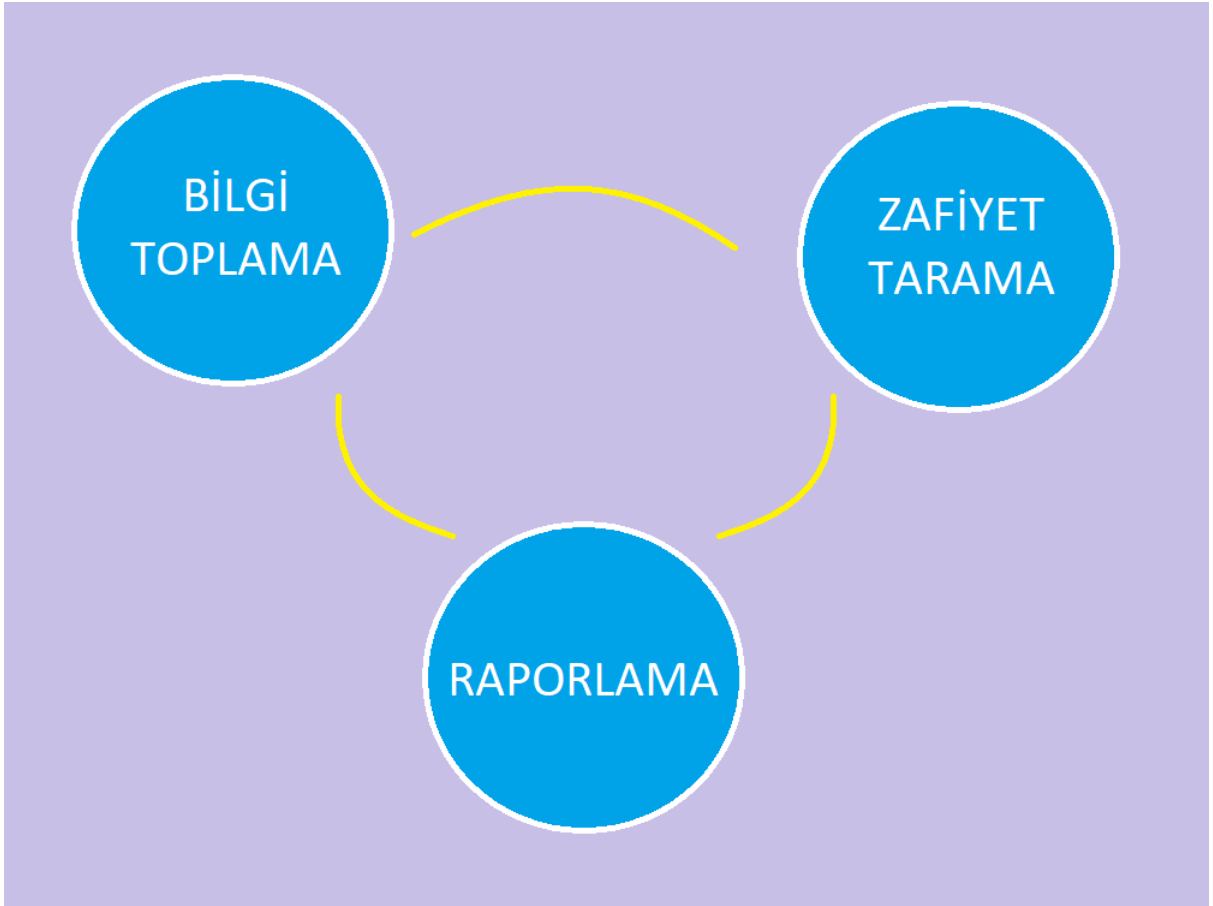
S~Security Web Güvenlik Denetim Raporu

- OWASP Testing Guide v3
- OSSTM
- ISSAF
- NIST

Gerçekleştirilen testler uluslararası standart ve yönetmeliklere(HIPPA, Sarbanes-Oxley, Payment Card Industry (PCI), ISO 27001) tam uyumludur.

S~security Web Güvenlik Testi Metodolojisi

S~security, web güvenlik testlerinde 3 aşamalı bir metodoloji kullanmaktadır.



Şekil 2 - Web Güvenlik Testi Metodolojisi

1.1[Bilgi Toplama]

Amaç, hedef sistem hakkında olabildiğince detaylı bilgi toplamaktır. Bu bilgiler firma hakkında olabileceği gibi firma çalışanları hakkında da olabilir. Bunun için internet siteleri haber grupları e-posta listeleri, gazete haberleri vb., hedef sisteme gönderilecek çeşitli paketlerin analizi yardımcı olacaktır.

Bilgi toplama ilk ve en önemli adımlardan biridir. Zira yapılacak test bir zaman işidir ve ne kadar sağlıklı bilgi olursa o kadar kısa sürede sistemle ilgili detay çalışmalara geçilebilir. Bilgi toplama da aktif ve pasif olmak üzere ikiye ayrılır. Google, Pipl, Shodan, LinkedIn, Facebook gibi genele açık kaynaklar taranabileceği gibi hedefe özel çeşitli yazılımlar kullanılarak DNS, WEB, MAIL sistemlerine yönelik detaylı araştırmalar gerçekleştirilir.

Bu konuda en iyi örneklerden biri hedef firmada çalışanlarından birine ait e-posta ve parolasının internete sızmış parola veritabanlarından birinden bulunması ve buradan VPN yapılarak tüm ağın ele geçirilmesi senaryosudur.

1.2[Zafiyet Tarama]

Amaç hedef sistemin ağ yapısının detaylı belirlenmesidir. Açık sistemler ve üzerindeki açık portlar, servisler ve servislerin hangi yazılımın hangi sürümü olduğu bilgileri, ağ girişlerinde bulunan VPN, Firewall, IPS cihazlarının belirlenmesi, sunucu sistemler çalışan işletim sistemlerinin ve versiyonlarının belirlenmesi ve tüm bu bileşenler belirlendikten sonra hedef sisteme ait ağ haritasının çıkartılması ağ haritalama adımlarında yapılmaktadır.

Ağ haritalama bir aktif bilgi toplama yöntemidir. Ağ haritalama esnasında hedef sistemde IPS, WAF ve benzeri savunma sistemlerinin olup olmadığı da belirlenmeli ve gerçekleştirilecek sızma testleri buna göre güncellenmelidir.

1.3[Raporlama]

Raporlar bir testin müşteri açısından en önemli kısmıdır. Raporlar ne kadar açık ve detaylı/bilgilendirici olursa müşterinin riski değerlendirmesi ve açıklıkları gidermesi de o kadar kolay olur.

Testler esnasında çıkan kritik güvenlik açıklıklarının belgelenecek sözlü olarak anında bildirilmesi test yapan takımın görevlerindendir. Bildirimin ardından açıklığın hızlıca giderilmesi için çözüm önerilerinin de birlikte sunulması gerekir.

S~Security Web Güvenlik Denetim Raporu

Ayrıca raporların teknik, yönetim ve özet olmak üzere üç farklı şekilde hazırlanmasında fayda vardır.

Teknik raporda hangi uygulama/araçların kullanıldığı, testin yapıldığı tarihler ve çalışma zamanı, bulunan açıklıkların detayları ve açıklıkların en hızlı ve kolay yoldan giderilmesini amaçlayan tavsiyeler bulunmalıdır.

5.TANIMLAR VE SEVİYELENDİRME

5.1. Testlerin Gerçekleştirildiği Erişim Noktaları

İnternet : Test park'ın internet üzerinden erişilebilen tüm sunucu ve servislerine internet üzerinden erişilerek web güvenlik testleri gerçekleştirilmiştir

5.2. Testlerin Gerçekleştirildiği Kullanıcı Profilleri






Anonim kullanıcı : İnternet üzerinden, testparkın web servislerine erişebilen ancak web uygulamalarına giriş yetkilerine sahip olmayan kullanıcıyı temsil eder. Bankaya ait web uygulamalarının üyesi olmayan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları gidermek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.

5.3. Risk Seviyelendirme

Penetrasyon ve denetim çalışmalarında bulunan açıklar 5 risk seviyesinde değerlendirilmişlerdir¹. Bu değerlendirmede, PCI-DSS güvenlik tarama prosedürleri dokümanında kullanılan beş seviye risk değerleri kullanılmıştır.

¹https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf

S~Security Web Güvenlik Denetim Raporu

Risk	Seviyesi	Risk Puanı	Detaylı Açıklama
	ACİL	5	Acil öneme sahip açıklıklar, niteliksiz saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Depolanmış XSS, SQL enjeksiyonu ve RFI/LFI, ayrıca müşteri bilgisi ifşasına yol açabilecek açıklık vektörleri bu kategoriye girerler.
	KRİTİK	4	Kritik öneme sahip açıklıklar, nitelikli saldırganlar tarafından uzaktan gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Ayrıca yansıtılan ve DOM tabanlı XSS açıklık vektörleri bu kategoriye girer.
	YÜKSEK	3	Yüksek öneme sahip açıklıklar, uzaktan gerçekleştirilen ve kısıtlı hak yükseltilmesi (mesela, yönetici hakları olmayan bir işletim sistemi kullanıcısı veya e-posta sahteciliği) veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan ataklara sebep olan açıklıkları içermektedir.
	ORTA	2	Orta öneme sahip açıklıklar, yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan ataklara sebep olan açıklıkları içermektedir.
	DÜŞÜK	1	Düşük öneme sahip açıklıklar ise etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin (best practices) izlenmemesinden kaynaklanan eksikliklerdir.

Şekil 3 - Risk Seviyeleri

6.GERÇEKLEŞTİRİLEN GÜVENLİK TESTLERİ VE SONUÇLARI

Sızma test sonuçlarının raporlanması temelde iki farklı şekilde yapılmaktadır. Bunlardan ilki bileşen bazlı raporlama, diğeri de hedef bazlı raporlama. Hedef bazlı raporlamada her bir zafiyet ayrı bir başlık olarak yazılmaktadır, bileşen bazlı raporlamada aynı kategorideki(kapatılması aynı aksiyona bağlı, aynı açıklığın farklı sistemlerde bulunması)açıklıklar tek bir başlık altında yazılarak bulgu içerisinde ayırım yapılmaktadır.

Raporun okunurluğu ve sadeliği açısından “TEST PARK” için gerçekleştirilen sızma testi çalışmasında bileşen bazlı raporlama tercih edilmiştir.

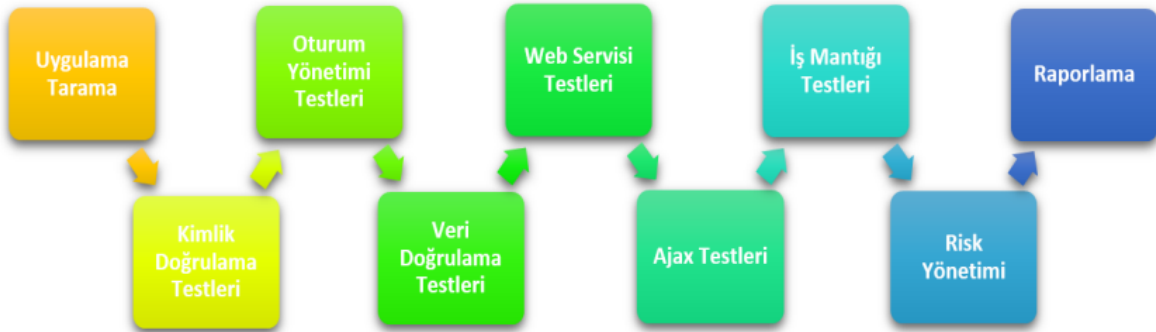
Aşağıda gerçekleştirilen testler ve testlere ait çıktılara yer verilmiştir.

6.1.Web Uygulama Güvenlik Testleri

6.1.1 Gerçekleştirilen Güvenlik Testi İşlemleri

Gerçekleştirilen güvenlik testi işlemleri Web uygulamalarına yapılan testler sisteme zarar vermeyecek şekilde, internet üzerinden gerçekleştirilmiştir. Sunucular üzerinde çalışan servislerin ve işletim sisteminin bilinen açıklıklarının araştırılmasının yanında, sistemdeki uygulamalara has güvenlik açıklıkları da araştırılmıştır.

Yapılan güvenlik testleri bileşen tabanlı ele alınmıştır. Bu testlerde ilk olarak S~security tarafından derlenen Test Prosedürleri adımları uygulanmıştır. Test prosedürleri ile tespit edilemeyen açıklıklar ise ticari tarama araçları yardımıyla bulunmaya çalışılmıştır. Bu araçların birçok yanlış alarmlar (false positives) verebileceği hususu göz önünde bulundurularak, tespit edilen açıklıklar detaylı olarak incelenmiştir.



Şekil 4 - Güvenlik Testi Adımları

Bu kapsamda aşağıda detaylandırılan test adımları gerçekleştirilmiştir:

- Uzaktan genel tarama araçları ile sunucuların açık olan servisleri, yama eksiklikleri ve yapılandırma hataları aranmıştır.
- Uygulama girdisi kontrol testleri (Siteler Ötesi Betik Çalıştırma, Parametre Enjeksiyonu ve Manipülasyonu) uygulanmıştır.
- Parametre bütünlüğü güvenlik kontrolleri denetlenmiştir.
- Sistem hakkında bilgi açığa çıkarmaya yönelik testler uygulanmıştır.
- Oturum yönetiminde bulunabilecek bazı zafiyetler araştırılmıştır.
- Yetkilendirme (URL tabanlı) süreçlerinde bulunabilecek bazı zafiyetler araştırılmıştır.
- Uygulamanın bulunduğu sunucu üzerinde konuşlanmış diğer servisler kullanılarak bilgi edinilmeye çalışılmıştır.
- İlgili veritabanlarına erişim sağlanmaya çalışarak, uygulamada yetkili kullanıcı hesapları edinilmeye çalışılmıştır.

S~Security Web Güvenlik Denetim Raporu

Ayrıca aşağıda verilen test başlıkları da manuel olarak; açık kaynak araçlar kullanılarak test edilmiştir.

Yapılandırma Yönetim Testleri

- ✓ SSL/TLS versiyon, algoritma ve sertifika geçerlilik testleri - OWASP-CM-001
- ✓ Hedef uygulamada kullanılan yönetim panelinin belirlenmesi - OWASP-CM-00
- ✓ Dosya uzantısı yönetimi testleri - OWASP-CM-005
- ✓ Yedek, kopya, test veya eski sürümlerden kalma sayfa ve uygulamaların belirlenmesi- OWASP-CM-00
- ✓ Sunucu tarafından desteklenen metodların ve XST belirlenmesi - OWASP-CM-008

Kimlik Doğrulama Testleri

- ✓ Hassas bilgilerin şifreli/şifresiz kanallardan aktarımı - OWASP-AT-001
- ✓ Hedef uygulama üzerinde kullanıcı adı belirleme/doğrulama çalışmaları - OWASP-AT-002
- ✓ Hedef uygulama üzerinde tanımlı kullanıcıların belirlenmesi - OWASP-AT-00
- ✓ Hedef uygulama üzerinde yetkili kullanıcılara yönelik brute force parola denemeleri - OWASP-AT-00
- ✓ Kimlik doğrulama aşamasını atlatma denemeleri - OWASP-AT-005
- ✓ Parola hatırlatma ve parola sıfırlama özelliklerinin testleri - OWASP-AT-006
- ✓ Browser ön bellek yönetimi ve "Log out" fonksiyonlarının testleri - OWASP-AT-007
- ✓ CAPTCHA güvenlik testleri - OWASP-AT-008

Oturum Yönetimi Testleri

- ✓ Oturum yönetimi zayıflıkları, oturum yönetimi bypass testleri - OWASP-SM-001
- ✓ Detaylı cookie güvenlik testleri - OWASP-SM-002
- ✓ Oturum sabitleme (session fixation) testleri - OWASP-SM-003
- ✓ Oturum değerleri tahmin saldırıları - OWASP-SM-004
- ✓ CSRF(Cross site request forgery) testleri - OWASP-SM-005

Yetkilendirme Testleri

- ✓ Dizin atlatma/gezme(Directory Treversal) testleri - OWASP-AZ-001
- ✓ Yetkilendirme atlatma, yetkilendirme geçiş testleri - OWASP-AZ-002
- ✓ Yetki yükseltimi testleri - OWASP-AZ-003

İş Mantığı Denetim Testleri

- ✓ Uygulamanın işleyişinin belirlenmesini takiben uygulamanın işleyişine yönelik teknik olmayan atakların denenmesi.

Veri Doğrulama Testleri

- ✓ Yansıtılan XSS testleri - OWASP-DV-001

S~Security Web Güvenlik Denetim Raporu

- ✓ Depolanmış XSS testleri - OWASP-DV-002
- ✓ DOM tabanlı XSS testleri - OWASP-DV-003
- ✓ XSF (Flash XSS) testleri -OWASP-DV-004
- ✓ SQL enjeksiyonu testleri - OWASP-DV-005
- ✓ LDAP enjeksiyonu testleri - OWASP-DV-006
- ✓ XNL testleri - OWASP-DV-008
- ✓ Xpath enjeksiyonu testleri - OWASP-DV-010
- ✓ Kod enjeksiyonu testleri - OWASP-DV-012
- ✓ İşletim sistemi komut enjeksiyonu testleri - OWASP-DV-013
- ✓ Bellek taşması (buffer overflow) testleri - OWASP-DV-014
- ✓ Http response splitting testleri - OWASP-DV-016

Hizmet Dışı Bırakma Testleri

- ✓ SQL wildcard üzerinden DoS testleri - OWASP-DS-001
- ✓ Hesap kitleme politikasının testi - OWASP-DS-002
- ✓ Buffer overflow DoS testleri - OWASP-DS-003
- ✓ Oturum boyutu arttırma DoS testleri - OWASP-DS-008
- ✓ http GET Flood DoS testleri
- ✓ SYN Flood DDoS testleri
- ✓ Uygulama sürümüne özel DoS testleri

Web Servisi ve Ajax Testleri

- ✓ Web servisi bilgi toplama çalışmaları - OWASP-WS-001
- ✓ WSDL testleri - OWASP-WS-002
- ✓ XML yapı testleri - OWASP-WS-003

Web Uygulama Güvenlik Sistemlerinin Testleri

- ✓ Web uygulama güvenlik duvarı keşif testleri
- ✓ Network IPS keşif testleri
- ✓ IPS/Web uygulama güvenlik duvarı atlatma testleri

6.1.2 Tespit Edilen Açıklıklar

6.1.2.1 Yansıtılan Siteler Arası Script Çalıştırma/XSS (OWASP-DV-001)

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu Açıklaması

Siteler arası script çalıştırma zafiyeti olarak bilinen XSS, kötü niyetli kişilerin bu site üzerinden diğer kullanıcılara istemci tarafında çalışmak üzere kod (genellikle JavaScript ve html) gönderip kötü amaçlarla çalıştırmalarına imkân tanımaktadır.

XSS zafiyetleri uygulamalarda dışarıdan alınan bilgiler için yeterli girdi ve çıktı denetimi yapılmadığı durumlarda ortaya çıkar ve art niyetli bir kullanıcı istediği gibi javascript kodu çalıştırarak hedef aldığı kişilere ait oturum bilgilerini çalabilir, hedef aldığı kişilerin browserini istediği gibi yönlendirebilir. Ele geçirdiği kurban browseri kullanılarak iç ağda port tarama, ortamda ses kaydı ve görüntü kaydı gerçekleştirilebilir.

Reflected(yansıtılmış) XSS açıklığı en sık karşılaşılan XSS açıklığı türüdür. İlgili açıklık türünde, hedef sisteme gönderilen kod parçaçığı(payload) kalıcı olarak veritabanında tutulmamaktadır. Bu sebeple ilgili açıklığın istismarı için, öncesinde kullanıcı tarafında bir bağlantı ziyaret ettirme şeklinde bir sosyal mühendislik saldırısı gerçekleştirilmelidir. Reflected XSS açıklığı HTTP GET ve POST taleplerinin her ikisinde iletilen parametrelerde de bulunabilir. Reflected XSS açıklığı, temelde hedef sisteme gönderilen payload'un, dönen sunucu cevabı içerisinde encode edilmeden döndürülmesi durumunda açığa çıkmaktadır. Bu durumda isteği yapan istemci tarafında enjekte edilen kod parçaçığı eylemini gerçekleştirecektir. Bu açıklık türü istismar edilerek client tarafında html, javascript, action script benzeri kod parçaçıkları sayfaya enjekte edilebilir. Kullanıcı kandırma veya cookie hırsızlığı gerçekleştirilebilir.

Uygulamanın URL kısmında Yansıtılan Siteler Arası Script çalıştırılabileceği görülmüştür. Aşağıdaki tablolarda hangi url adesinde ve hangi parametrelerde olduğu detaylı bir şekilde ifade edilmiştir.

S~Security Web Güvenlik Denetim Raporu

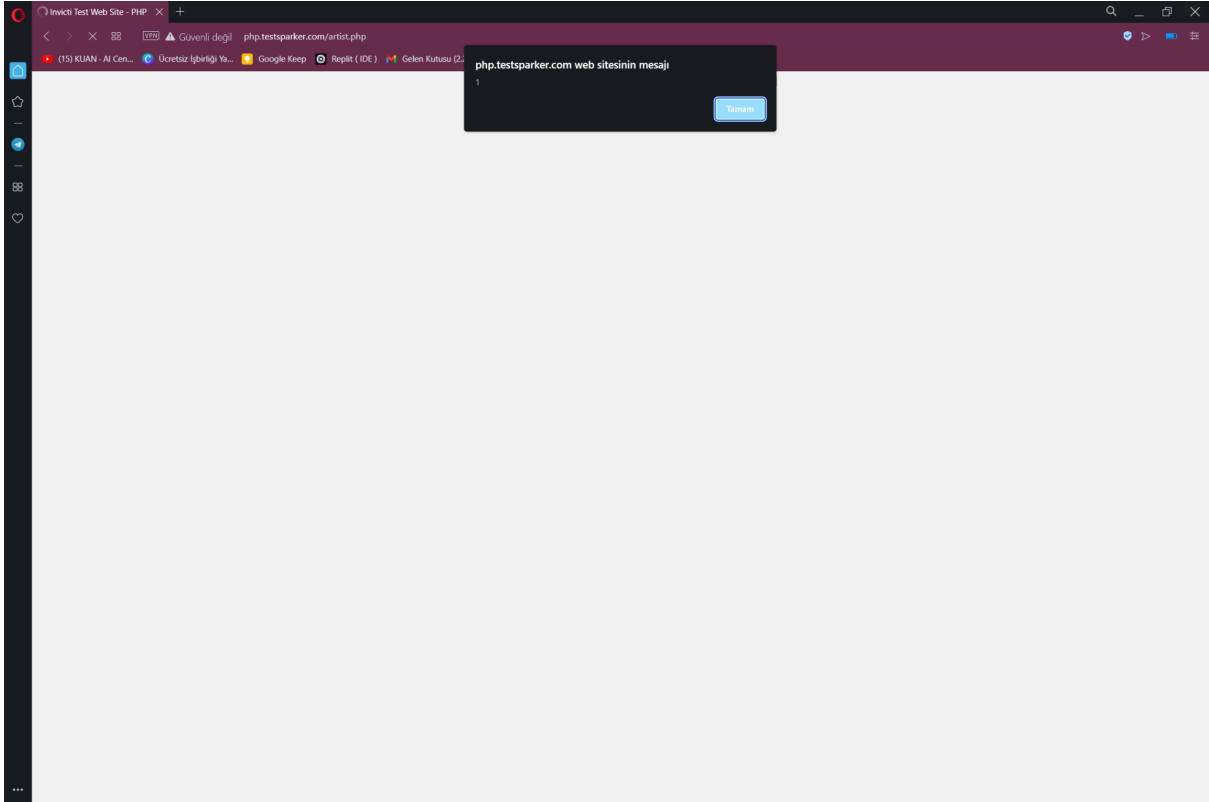
URL	<code>http://php.testsparker.com/artist.php?id=<script>alert(1);</script>&submit=</code>
HTTP Talep Türü	GET
Payload	<code><script>alert(1);</script></code>

Bu verilen bilgiler doğrultusunda uygulamanın URL kısmında belirtilen payload çalıştırıldığı zaman XSS çalışacaktır ve aşağıdaki gibi bir görüntü ile karşılaşılacaktır.

Zafiyeti barındıran sistemler

- <http://php.testsparker.com/process.php?file=Generics%2Findex.nsp>

İstismar Ekran Görüntüsü



Şekil 5: Sayfa üzerinde XSS ile komut çalıştırılabilir.

S~Security Web Güvenlik Denetim Raporu

Çözüm Önerileri

Uygulama kodlarının gözden geçirilerek parametreler ve http başlığındaki diğer alanlar vasıtası ile yollanan her türlü bilginin kullanılmadan önce zararlı karakterlerden filtrelenmesi önerilmektedir. Uygulamalardaki bütün girdi ve çıktı noktalarından gelen değişkenler kontrole tabi tutulmalı ve bu girdilerdeki bütün meta karakterler filtrelenmelidir. detaylı XSS önleme yöntemleri için aşağıda belirtilen referanslar incelenebilir.

Referanslar

- <http://www.owasp.org/index.php/XSS>
- <http://www.cgisecurity.com/articles/xss-faq.shtml>
- <http://ha.ckers.org/xss.html>

6.1.2.2 Depolanan Siteler Arası Script Çalıştırma/XSS (OWASP-DV-001)

Önem Derecesi	Kritik
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Web
Bulgu Sebebi	Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması

Siteler arası script çalıştırma zafiyeti olarak bilinen XSS, kötü niyetli kişilerin bu site üzerinden diğer kullanıcılara istemci tarafında çalışmak üzere kod (genellikle JavaScript ve html) gönderip kötü amaçlarla çalışmalarına imkân tanımaktadır.

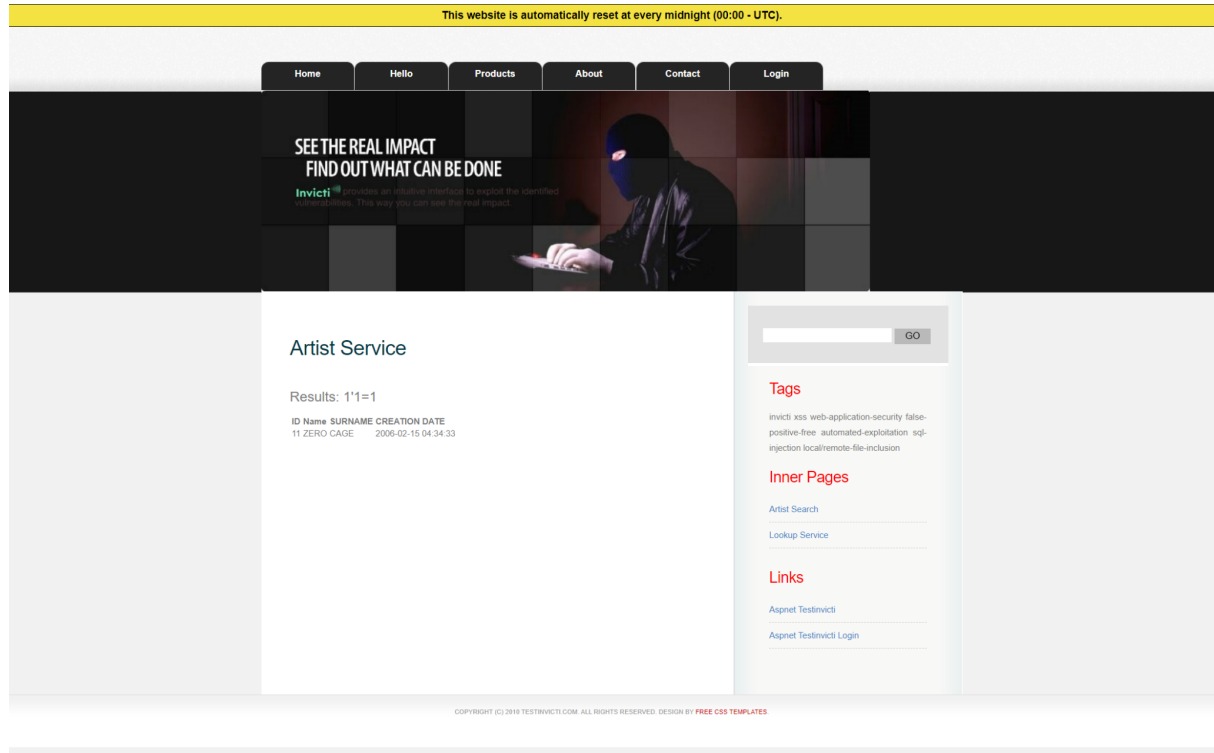
XSS zafiyetleri uygulamalarda dışarıdan alınan bilgiler için yeterli girdi ve çıktı denetimi yapılmadığı durumlarda ortaya çıkar ve art niyetli bir kullanıcı istediği gibi javascript kodu çalıştırarak hedef aldığı kişilere ait oturum bilgilerini çalabilir, hedef aldığı kişilerin browserini istediği gibi yönlendirebilir.

S~Security Web Güvenlik Denetim Raporu

Bulgu 1:

URL	php.testsparker.com/artist.php?id=1'1%3D1
HTTP Talep Türü	GET
Payload	1'1%3

Bu verilen bilgiler doğrultusunda uygulamanın URL kısmında belirtilen payload çalıştırıldığı zaman XSS çalışacaktır ve aşağıdaki gibi bir görüntü ile karşılaşılacaktır.



Şekil 6: Sayfa üzerinde XSS ile komut çalıştırılabilir.

Çözüm Önerileri

Uygulama kodlarının gözden geçirilerek parametreler ve http başlığındaki diğer alanlar vasıtası ile yollanan her türlü bilginin kullanılmadan önce zararlı karakterlerden filtrelenmesi önerilmektedir. Uygulamalardaki bütün girdi ve çıktı noktalarından gelen değişkenler kontrole tabi tutulmalı ve bu girdilerdeki bütün meta karakterler filtrelenmelidir. detaylı XSS önleme yöntemleri için aşağıda belirtilen referanslar incelenebilir.

Referanslar

- <http://www.owasp.org/index.php/XSS>
- <http://www.cgisecurity.com/articles/xss-faq.shtml>
- <http://ha.ckers.org/xss.html>

S~Security Web Güvenlik Denetim Raporu

6.1.2.3 SQL Injection Zafiyeti (OWASP-DV-005)

Önem Derecesi	Acil
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi İfşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu Açıklaması

SQL Injection zafiyeti, uygulama parametreleri aracılığı ile yollanan bilgilerin düzgün kontrol edilmemesi sebebi ile arka planda çalışan veritabanına yollanan sorgulara, saldırganın sorgularını eklemesine imkan tanıyan bir güvenlik açığıdır.

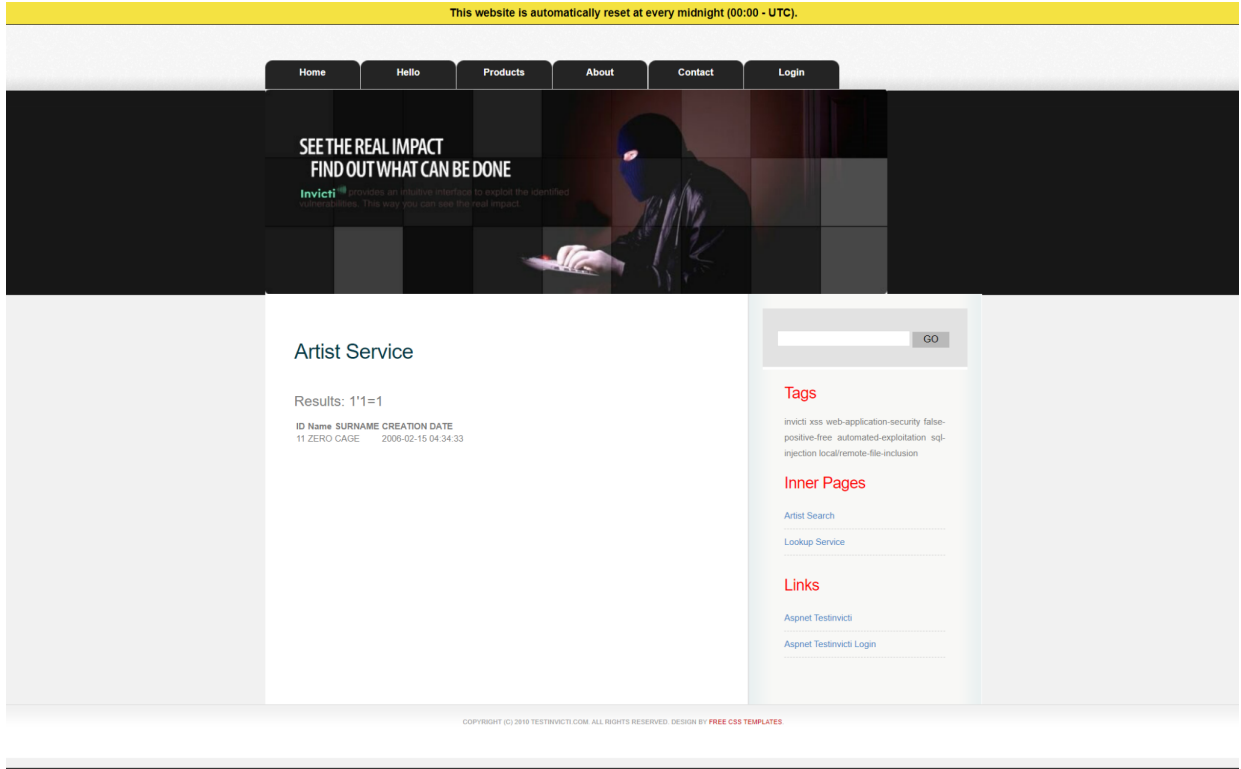
Hata tabanlı SQL Injetion saldırıları, uygulamanın veritabanına gönderdiği sorgularda herhangi bir yazım hatası syntax error olması durumunda veya sorgunun veri tabanında çalışması sonucu dönen verilerin, ekrana çıktı olarak verilmesi temeline dayanır.

Bulgu 1:

URL	http://php.testsparker.com/artist.php?id=1%271%3D1
HTTP Talep Türü	GET
Payload	id=1'1%3D1

Tabloda verilen bilgiler ile artist search sayfasında url kısmında uygulanan payload ile SQL Injection uygulanabilmektedir. Çıktı olarak id bilgisi eşleşen bir kullanıcının bilgilerine erişilebilmektedir. Sqlmap aracı kullanılarak hedef sistemin veritabanına erişilmiştir.

S~Security Web Güvenlik Denetim Raporu



Şekil 7 - SQL Injection tespit edilen URL

```
available databases [6]:
[*] `tes`}
[*] information_schema
[*] logs
[*] nysql
[*] phpmyadmin
[*] sqlbench
```

Şekil 8 - Hedef Sistem Veritabanıları

Tekrar sqlmap aracı ile hedef sistem veritabanlarından information_schema veritabanındaki 342 tabloya ulaşıldı.

S~Security Web Güvenlik Denetim Raporu

Database: information_ychema
[342 tables]

+	+
ACL_table	
ALL_USERS	
ANTIGUOS	
Anmeldung	
BOOK	
BlockInfo	
Booked_On	
CPG_users	
CUENTAS	
CUST_HIST	
Catogorie	
CheckType	
Chemicals	
Compagnie	
Component	
Continent	
CustomNav	
DOWNLOADS	
DWE_Roles	
DWE_Tasks	
D_Comment	
D_US_AREA_DE_TRABALHO	
Departure	
EMPLEADOS	
Equipment	
FACTSHEET	
FUNDGROUP	
FirstName	
INSTITUTE	
Joueur	
Kategorie	
Konten	
Konto	
Kontrolle	
LT_EVENTO	
LT_OBJETO	
M_FATURAS	
M_USUARIO	
Microsoft	
POINT_SET	
PREFIX_order_return_state_lang	
PRODUCTOS	
PUBLISHER	
Parametre	
Purchases	
R1Weights	
R2Weights	
ROLE_PERM	
SMS_TABLE	

Şekil 9 - Hedef Sistem Veritabanı Tabloları

SS_orders	
SYNALLAGI	
S_ORIGENS	
S_SESSOES	
SalesReps	
SchemaInfo	
Sitzungen	
Standorte	
StateList	
StateType	
Studenten	
THOT_DEEP	
THOT_TYPE	
THOT_YEAR	
Thumbnail	
UM_ROLE_PERMISSIONS	
UserAdmin	
VenuesNew	
catalog	
section	
session	
acc_trans	
addresses	
admin_passwords	
admin_psw	
admin_pwd	
adminname	
adminpass	
adminstbl	
adminuser	
aliastype	
archtypes	
argumento	
articulos	
atividade	
automated	
baza_site	
be_groups	
binn_articles	
binn_bann	
binn_docs	
binn_maillist_sent	
binn_menu	
binn_news	
binn_vote	
biosample	
blacklist	
blobs	
catalogue	
categoria	
categorie	
categorylinks	
cc_config	
cdb_crons	
cdb_itempool	
cdb_magics	
cdb_polls	
cdb_posts	
cell_line	
changeTva	
cmContent	
cms_admin	
cms_users	
commandes	
comp_group	
companies	
computers	
connexion	
copyright	
countries	
cron_send	
crops_tpl	

Şekil 10 - Hedef Sistem Veritabanı Tabloları

S~Security Web Güvenlik Denetim Raporu

customers
customurl
dbaccount
dbpersoon
dbstudent
defertest
dependent
depositor
derived_types
directeur
div_stock
div_trait
div_unit_of_measure
documento
dokumente
dpt_trans
dtb_class
dtb_deliv
dtb_order
dtb_order_detail
duyurular
dwp_popup
e107_user
egresadoxidiomaxhabilidad
emailinfo
employees
endpoints
etudiants
event_log
ew_gruppi
ew_moduli
f_options
form_data
forum_cat
fruit
functions
furniture
geo_River
guestbook
gws_admin
habilidad
icerikler
image
imageInfo
inclusion
injection
insertids
insurance
intGroups
interwiki
inventory
jiveGroup
jiveVCard
job_title
jos_polls
jos_users
keyboards
kontaklar
korisnici
kpro_user
kullanici
langlinks
languages
lc_fields
librarian
lieferant
locatedOn
locations
locus_data
lost_pass
macassocs
makemodel

Şekil 11 - Hedef Sistem Veritabanı Tabloları

map_event
mgbliuyan
mpassword
mucMember
municipio
musername
my_county
my_street
news_category
newsfeeds
nguoidung
nuke_banner_positions
nuke_downloads_modrequest
nuke_gallery_rate_check
nuke_main
oil_modules_menu
oil_polls
oil_users
operation
osvendors
pagelinks
paramtres
pass_hash
passwords
payload
perdorues
personnel
pg_ts_cfg
phonelist
php_users
phpshop_categories
physician
platforms
poll_data
poll_date
poll_menu
poll_user
preguntas
principal
profiling
promocoos
promotion
psw
pswd
pw_config
pw_favors
pw_forums
pw_smiles
pw_styles
pw_wordfb
questions
realttable
reg_users
reglement
reklamlar
relations
resources
sazog_urtiertoba_ge
sic
site_iwis
sitelogin
sizes
snipe_gallery_cat
softwares
specialty
spip_meta
spip_mots
spip_versions
sporti_ge
statename
stkWeight
subscribe

Şekil 12 - Hedef Sistem Veritabanı Tabloları

S~Security Web Güvenlik Denetim Raporu

```
| subscriber  
| superuser  
| sysadmins  
| tb_account  
| tb_admins  
| tb_logins  
| tb_member  
| tb_nguoidung  
| tb_useraccount  
| tbaccount  
| tbaccounts  
| tbadmins  
| tblOrders  
| tblStones  
| tbl_account  
| tbl_admin  
| tbl_event  
| tbl_login  
| tbl_logins  
| tbl_state  
| tbl_users  
| tbl_works  
| tblaccount  
| tblaccounts  
| tbladmin  
| tbladmins  
| tblclient  
| tbllogin  
| tbllogins  
| tblnguoidung  
| tblnguoidungs  
| tbllogins  
| tblproduct  
| tblproducts  
| tbluseraccount  
| tbluseraccounts  
| tbnguoidungs  
| tbuseraccounts  
| tbusers  
| telephone  
| templates  
| test_user  
| testusers  
| time_zone  
| topicinfo  
| transfers  
| transport  
| user_auth  
| user_data  
| user_info  
| user_list  
| user_name  
| user_pass  
| user_passwd  
| user_pwd  
| user_pwr  
| user_role  
| user_test  
| userfiles  
| usernames  
| users_tmp  
| vcd_Users  
| vcd_VcdToPornCategories  
| vendor_types  
| vendortax  
| vertreter  
| verwalten  
| verwaltet  
| vis_typen  
| warehouse  
| watchlist  
| way_nodes
```

Şekil 13 - Hedef Sistem Veritabanı Tabloları

```
| web  
| webadmins  
| webmaster  
| xar_roles  
| zuseserver  
+-----+
```

Şekil 14 - Hedef Sistem Veritabanı Tabloları

S~Security Web Güvenlik Denetim Raporu

Bu tabloların içerisindeki user_passwd tablosundaki verilere sqlmap aracı ile erişildi. Yine aynı biçimde yapılan bir saldırı ile hedef sistemin tüm veritabanına erişilebiliyor. Burdan sonrası hassas veriler içerdiği ve gizlilik arz ettiği için rapora eklenmemiştir.

Açığı barındıran sistemler

- php.testsparker.com/artist.php?id=1'1%3D1

Çözüm önerileri

Uygulama kodlarının gözden geçirilerek parametreler ve http başlığındaki diğer alanlar vasıtası ile yollanan her türlü bilginin kullanılmadan önce zararlı karakterlerden filtrelenmesi önerilmektedir.

Uygulamalardaki bütün girdi noktalarından gelen değişkenler girdi kontrolüne sokulmalı ve bu girdilerde bütün zararlı karakterlerin filtrelenmesi önerilmektedir. Detaylı SQL enjeksiyonu önleme yöntemleri için aşağıda belirtilen referanslar incelenebilir.

Referanslar

- http://www.owasp.org/index.php/Injection_Flaws
- <http://www.unixwiz.net/techtips/sql-injection.html>
- http://www.ngssoftware.com/papers/more_advanced_sql_injection.pdf
- http://www.nextgenss.com/papers/advanced_sql_injection.pdf

S~Security Web Güvenlik Denetim Raporu

6.1.2.4 Local File Inclusion Zafiyeti (OWASP-CM-006)

Önem Derecesi	Yüksek
Açıklığın Etkisi	Yetkisiz Erişim, Bilgi Ifşası
Erişim Noktası	İnternet
Kullanıcı Profili	Anonim Kullanıcı
Bulgu Kategorisi	Web
Bulgu Sebebi	Uygulama Geliştirmedeki Eksiklikler/Hatalar

Bulgu Açıklaması

File Inclusion, yani dosya dahil etme saldırısı saldırganın hedef web sitesine bir dosya dahil etmesine ya da hedef web sitesinin kendinde olan ama sunmadığı bir dosyayı görüntüleyebilmesine denir.

File Inclusion açıklığını kullanan iki tür saldırı vardır: Bunlardan birincisi Local File Inclusion diye adlandırılmaktadır, ikincisi ise Remote File Inclusion diye adlandırılmaktadır. Local File Inclusion saldırısı hedef sitenin barındığı sunucudaki ziyaretçilere sunulmamış dosyanın hedef site üzerinden görüntülenebilmesine denir. Remote File Inclusion saldırısı ise hedef siteye saldırganın kendi dosyasını görüntülemesine denir.

URL	http://php.testsparker.com/process.php?file=c%3A%5CWindows%5CSystem32%5Cdrivers%5Cetc%5Cservices%00.nsp
HTTP Talep Türü	GET
Payload	c%3A%5CWindows%5CSystem32%5Cdrivers%5Cetc%5Cservices%00.nsp

Bu bilgiler ışığında URL ile belirtilen payload denendiğinde zafiyet gözlemlenmektedir. Hedef sisteme ait hassas bilgilere erişilebilmektedir.

İstismar ekran görüntüsü



- ### Çözüm önerileri

Referanslar

- S~security Bilgi Güvenliği Anonim Şirketi | www.ssecurity.com.tr | bilgi@s-security.com.tr