Tarih:27.11.2022

php.testsparker.com
Sızma Testleri
Sonuç Raporu

İçindekiler

1. GİRİŞ iii
2. KAPSAM iv
3. YÖNETİCİ ÖZETİ v
4. GENEL SIZMA TESTİ METODOLOJİSİ vi
4.1 Bilgi Toplama vii
4.2 Ağ Haritalama viii
4.3 Zafiyet/Zayıflık Tarama Süreci viii
4.4 Penetrasyon (Sızma) Süreci viii
4.5 Erişim Elde Etme ve Hak Yükseltme viii
4.5.1 Hak Yükseltme ix
4.6 Detaylı Araştırma ix
4.7 Erişimlerin Korunması ix
4.8 İzlerin silinmesi ix
4.9 Raporlama ix
5. GERÇEKLEŞTİRİLEN GÜVENLİK TESTLERİ VE SONUÇLARI x
5.1 SQL Injection x
5.2 Local File Inclusion xv
5.3 Server Side Template Injection xv
5.4 Command Injection xvi
5.5 XSS xvi
5.6 HTML Injection xvii

1. GİRİŞ

Bu rapor, Tech Career tarafından php.testsparker.com web sitesi üzerindeki güvenlik açıklarını ortaya çıkarmak amacıyla gerçekleştirilen güvenlik ve sızma testlerinin (penetration test) detaylı sonuçlarını içermektedir.

Pentest çalışması kapsamında "php.testsparker.com" 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.

2. KAPSAM

Sızma testinde ana amaçlardan biri tüm zafiyetlerin değerlendirilerek sisteme sızılmaya çalışılmasıdır. Bu amaç doğrultusunda gerçekleştirilecek sızma testlerinde kapsam pentest çalışmasının en önemli adımını oluşturmaktadır.

Gerçekleştirilen denetimlerde "php.testsparker.com" yetkilileri tarafından bildirilen sistemlere yönelik sızma testleri gerçekleştirilmiştir.

Test hesabı kullanılarak gerçekleştirilen sistemlere ait bilgiler:

Sızma testi gerçekleştirilmesi istenen web uygulamaları ve hangi haklarla testlerin gerçekleştirildiği listesine aşağıda yer verilmiştir.

Uygulama Adı	Hesap Bilgisi	Yetki Seviyesi
php.testsparker.com	test	Kullanıcı

3. YÖNETİCİ ÖZETİ

Bu rapor, Tech Career tarafından php.testsparker.com web sitesi üzerindeki güvenlik açıklarını ortaya çıkarmak amacıyla gerçekleştirilen güvenlik ve sızma testlerinin (penetration test) detaylı sonuçlarını içermektedir.

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, 3 kritik, 2 yüksek olmak üzere toplamda 6 farklı güvenlik açığı tespit edilmiştir. Bir açıklığın birden fazla sistemde bulunması açıklık sayısını etkilememektedir.

Kategori/Risk Seviyesi Özet Dağılım Tablosu

Risk Seviyesi / Kapsam	Acil	Kritik	Yüksek	Orta	Düşük	Toplam
SQL Injection	1	-	-	-	-	1
LFI	-	1	-	-	-	1
SSTI	-	1	-	-	-	1
Command Injection	-	1	-	-	-	1
XSS	-	-	1	-	-	1
HTML Injection	-	-	1	-	-	1
TOPLAM	1	3	2			6

4. 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.

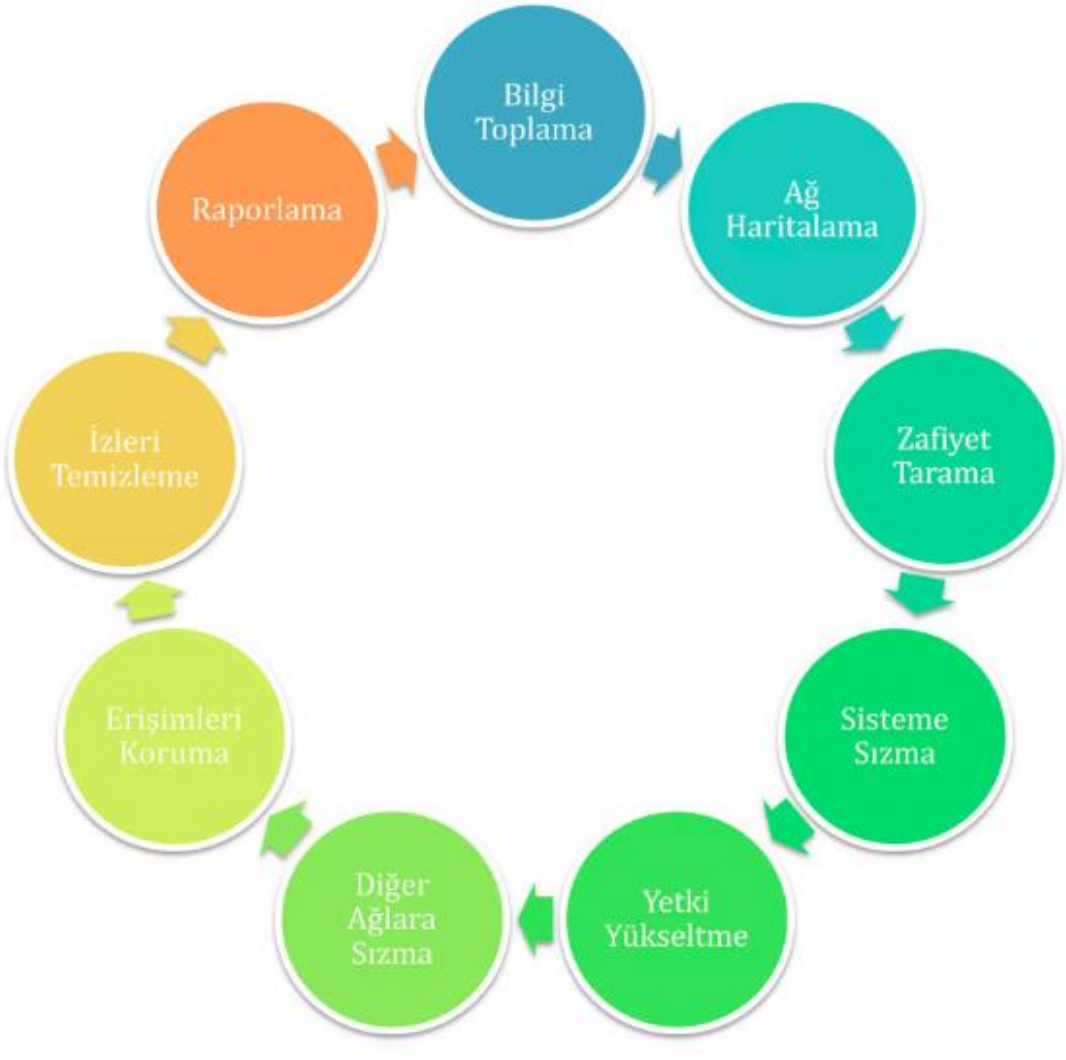
Pentest (sızma testleri) ve Vulnerability assessment(zayıflık tarama) birbirine benzeyen fakat farklı kavramlardır. Zayıflık tarama, hedef sistemdeki güvenlik açıklıklarının çeşitli yazılımlar kullanarak bulunması ve raporlanması işlemidir. Pentest çalışmalarında amaç sadece güvenlik açıklıklarını belirlemek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

Konu hakkındaki 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 Industry (PCI), ISO 27001) tam uyumludur.

Sızma testlerinde ISSAF tarafından geliştirilen metodoloji temel alınmıştır. Metodolojimiz üç ana bölümde dokuz alt bölümlerden oluşmaktadır.



4.1 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.

4.2 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 bu bileşenler belirlendikten sonra hedef sisteme ait ağ haritasının çıkarılması 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.

4.3 Zafiyet/Zayıflık Tarama Süreci

Bu sürecin amacı belirlenen hedef sistemlerdeki açıklıkların ortaya çıkarılmasıdır. Bunun için sunucu servislerdeki bannerler ilk aşamada kullanılabilir. Ek olarak birden fazla zayıflık tarama aracı ile bu sistemler ayrı ayrı taranarak oluşabilecek false positive oranı düşürülmeye çalışılır.

Bu aşamada hedef sisteme zarar vermeyecek taramalar gerçekleştirilir. Zayıflık tarama sonuçları mutlaka uzman gözler tarafından tekrar tekrar incelenmeli, olduğu gibi rapora yazılmamalıdır. Otomatize zafiyet tarama araçlar öntanımlı ayarlarıyla farklı portlarda çalışan servisleri tam olarak belirleyememektedir.

4.4 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.

4.5 Erişim Elde Etme ve Hak Yükseltme

Sızma sürecinde amaç sisteme bir şekilde giriş hakkı elde etmektir. Bu süreçten sonra sistemdeki kullanıcının haklarının arttırılması 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.

4.5.1 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 ulaşılabiliyor olabilir. Bunun için rhost, ssh dosyaları ve mümkünse history den eski komutlara bakılarak nerelere ulaşılabiliyor detaylı belirlemek gerekir.

4.6 Detaylı Araştırma

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

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

4.7 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.

4.8 İzlerin silinmesi

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

4.9 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.

5. 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 açıklığı farklı sistemlerde bulunması) açıklıklar tek bir başlık altında yazılarak bulgu içerisinde ayrım yapılmaktadır.

Aşağıda gerçekleştirilen testler ve testlere ait çıktılara yer verilmiştir.

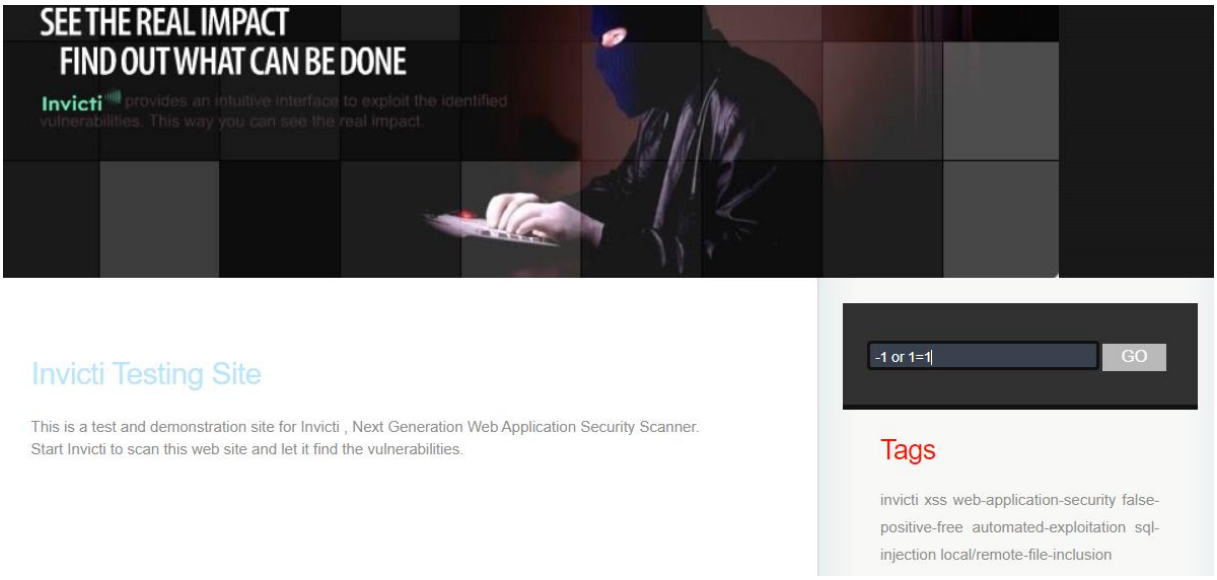
5.1 SQL Injection

Önem derecesi: Acil

SQL Injection web uygulamasının yaptığı SQL sorgusuna müdahale edilerek veri tabanında bulunan verilere yetkisiz erişme yöntemi cevabı uygun olacaktır. Bu güvenlik açığı, normalde görülmesi imkânsız verilerin görüntülenmesine izin verir.

Bir müşteri sisteme girerken kendi kullanıcı adı ve şifresini vererek, giriş izni alır. Bu izin sadece kendi verilerini görmeye yetki verir. SQL injection yönteminde ise bir saldırgan bununla birlikte diğer kullanıcıların ve web uygulamasının diğer verilerine erişebilir. Buradaki SQL injection açığı ile saldırgan verileri transfer edebilir, değiştirebilir, silebilir. Yani eriştiği tüm verileri manipüle edebilir hale gelir.

Aşağıdaki ekran görüntüsünde arama kısmına -1 or 1=1 payload'u girilmiştir.

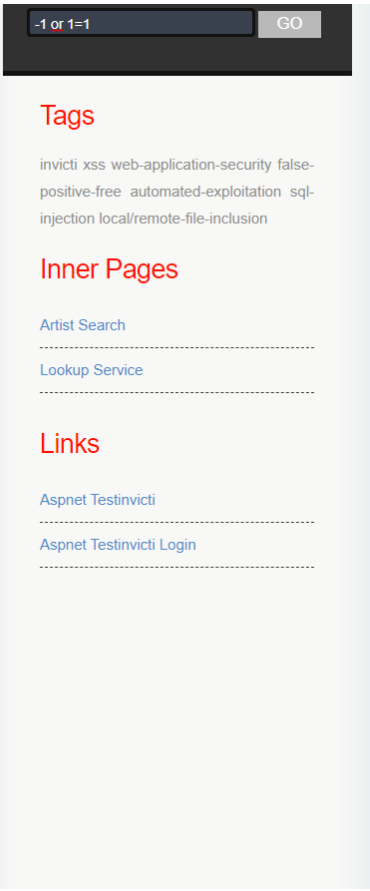


GO butonuna basıldığında ise aşağıdaki veriler elde edilmiştir.

Artist Service

Results: -1 OR 1=1

ID	Name	SURNAME	CREATION DATE
2	NICK	WAHLBERG	2006-02-15 04:34:33
3	ED	CHASE	2006-02-15 04:34:33
4	JENNIFER	DAVIS	2006-02-15 04:34:33
5	JOHNNY	LOLLOBRIGIDA	2006-02-15 04:34:33
6	BETTE	NICHOLSON	2006-02-15 04:34:33
7	GRACE	MOSTEL	2006-02-15 04:34:33
8	MATTHEW	JOHANSSON	2006-02-15 04:34:33
9	JOE	SWANK	2006-02-15 04:34:33
10	CHRISTIAN	GABLE	2006-02-15 04:34:33
11	ZERO	CAGE	2006-02-15 04:34:33
12	KARL	BERRY	2006-02-15 04:34:33
13	UMA	WOOD	2006-02-15 04:34:33
14	VIVIEN	BERGEN	2006-02-15 04:34:33
15	CUBA	OLIVIER	2006-02-15 04:34:33
16	FRED	COSTNER	2012-03-13 12:14:54 22
17	HELEN	VOIGHT	2012-03-13 12:14:54 22
18	DAN	TORN	2012-03-13 12:14:54 22
19	BOB	FAWCETT	2012-03-13 12:14:54 22
20	LUCILLE	TRACY	2012-03-13 12:14:54 22
21	KIRSTEN	PALTROW	2012-03-13 12:14:54 22
22	ELVIS	MARX	2012-03-13 12:14:54 22
23	SANDRA	KILMER	2012-03-13 12:14:54 22
24	CAMERON	STREEP	2012-03-13 12:14:54 22
25	KEVIN	BLOOM	2012-03-13 12:14:54 22
26	RIP	CRAWFORD	2012-03-13 12:14:54 22
27	JULIA	MCQUEEN	2012-03-13 12:14:54 22
28	WOODY	HOFFMAN	2012-03-13 12:14:54 22
29	ALEC	WAYNE	2012-03-13 12:14:54 22
30	SANDRA	PECK	2012-03-13 12:14:54 22
31	SISSY	SOBIESKI	2012-03-13 12:14:54 22
32	TIM	HACKMAN	2012-03-13 12:14:54 22
33	MILLA	PECK	2012-03-13 12:14:54 22
34	AUDREY	OLIVIER	2012-03-13 12:14:54 22



35	JUDY	DEAN	2012-03-13 12:14:54 22
36	BURT	DUKAKIS	2012-03-13 12:14:54 22
37	VAL	BOLGER	2012-03-13 12:14:54 22
38	TOM	MCKELLEN	2012-03-13 12:14:54 22
39	GOLDIE	BRODY	2012-03-13 12:14:54 22
40	JOHNNY	CAGE	2012-03-13 12:14:54 22
41	JODIE	DEGENERES	2012-03-13 12:14:54 22
42	TOM	MIRANDA	2012-03-13 12:14:54 22
43	KIRK	JOVOVICH	2012-03-13 12:14:54 22
44	NICK	STALLONE	2012-03-13 12:14:54 22
45	REESE	KILMER	2012-03-13 12:14:54 22
46	PARKER	GOLDBERG	2012-03-13 12:14:54 22
47	JULIA	BARRYMORE	2012-03-13 12:14:54 22
48	FRANCES	DAY-LEWIS	2012-03-13 12:14:54 22
49	ANNE	CRONYN	2012-03-13 12:14:54 22
50	NATALIE	HOPKINS	2012-03-13 12:14:54 22
51	GARY	PHOENIX	2012-03-13 12:14:54 22
52	CARMEN	HUNT	2012-03-13 12:14:54 22
53	MENA	TEMPLE	2012-03-13 12:14:54 22
54	PENELOPE	PINKETT	2012-03-13 12:14:54 22
55	FAY	KILMER	2012-03-13 12:14:54 22
56	DAN	HARRIS	2012-03-13 12:14:54 22
57	JUDE	CRUISE	2012-03-13 12:14:54 22
58	CHRISTIAN	AKROYD	2012-03-13 12:14:54 22
59	DUSTIN	TAUTOU	2012-03-13 12:14:54 22
60	HENRY	BERRY	2012-03-13 12:14:54 22
61	CHRISTIAN	NEESON	2012-03-13 12:14:54 22
62	JAYNE	NEESON	2012-03-13 12:14:54 22
63	CAMERON	WRAY	2012-03-13 12:14:54 22
64	RAY	JOHANSSON	2012-03-13 12:14:54 22
65	ANGELA	HUDSON	2012-03-13 12:14:54 22
66	MARY	TANDY	2012-03-13 12:14:54 22
67	JESSICA	BAILEY	2012-03-13 12:14:54 22
68	RIP	WINSLET	2012-03-13 12:14:54 22
69	KENNETH	PALTROW	2012-03-13 12:14:54 22
70	MICHELLE	MCCONAUGHEY	2012-03-13 12:14:54 22
71	ADAM	GRANT	2012-03-13 12:14:54 22
72	SEAN	WILLIAMS	2012-03-13 12:14:54 22
73	GARY	PENN	2012-03-13 12:14:54 22
74	MILLA	KEITEL	2012-03-13 12:14:54 22
75	BURT	POSEY	2012-03-13 12:14:54 22
76	ANGELINA	ASTAIRE	2012-03-13 12:14:54 22
77	CARY	MCCONAUGHEY	2012-03-13 12:14:54 22
78	GROUCHO	SINATRA	2012-03-13 12:14:54 22
79	MAE	HOFFMAN	2012-03-13 12:14:54 22
80	RALPH	CRUZ	2012-03-13 12:14:54 22
81	SCARLETT	DAMON	2012-03-13 12:14:54 22
82	WOODY	JOLIE	2012-03-13 12:14:54 22
83	BEN	WILLIS	2012-03-13 12:14:54 22
84	JAMES	PITT	2012-03-13 12:14:54 22
85	MINNIE	ZELLWEGER	2012-03-13 12:14:54 22
86	GREG	CHAPLIN	2012-03-13 12:14:54 22
87	SPENCER	PECK	2012-03-13 12:14:54 22
88	KENNETH	PESCI	2012-03-13 12:14:54 22
89	CHARLIZE	DENCH	2012-03-13 12:14:54 22
90	SEAN	GUINESS	2012-03-13 12:14:54 22
91	CHRISTOPHER	BERRY	2012-03-13 12:14:54 22
92	KIRSTEN	AKROYD	2012-03-13 12:14:54 22
93	ELLEN	PRESLEY	2012-03-13 12:14:54 22
94	KENNETH	TORN	2012-03-13 12:14:54 22
95	DARYL	WAHLBERG	2012-03-13 12:14:54 22

95	DARYL	WAHLBERG	2012-03-13 12:14:54 22
96	GENE	WILLIS	2012-03-13 12:14:54 22
97	MEG	HAWKE	2012-03-13 12:14:54 22
98	CHRIS	BRIDGES	2012-03-13 12:14:54 22
99	JIM	MOSTEL	2012-03-13 12:14:54 22
100	SPENCER	DEPP	2012-03-13 12:14:54 22
101	SUSAN	DAVIS	2012-03-13 12:14:54 22
102	WALTER	TORN	2012-03-13 12:14:54 22
103	MATTHEW	LEIGH	2012-03-13 12:14:54 22
104	PENELOPE	CRONYN	2012-03-13 12:14:54 22
105	SIDNEY	CROWE	2012-03-13 12:14:54 22
106	GROUCHO	DUNST	2012-03-13 12:14:54 22
107	GINA	DEGENERES	2012-03-13 12:14:54 22
108	WARREN	NOLTE	2012-03-13 12:14:54 22
109	SYLVESTER	DERN	2012-03-13 12:14:54 22
110	SUSAN	DAVIS	2012-03-13 12:14:54 22
111	CAMERON	ZELLWEGER	2012-03-13 12:14:54 22
112	RUSSELL	BACALL	2012-03-13 12:14:54 22
113	MORGAN	HOPKINS	2012-03-13 12:14:54 22
114	MORGAN	MCDORMAND	2012-03-13 12:14:54 22
115	HARRISON	BALE	2012-03-13 12:14:54 22
116	DAN	STREEP	2012-03-13 12:14:54 22
117	RENEE	TRACY	2012-03-13 12:14:54 22
118	CUBA	ALLEN	2012-03-13 12:14:54 22
119	WARREN	JACKMAN	2012-03-13 12:14:54 22
120	PENELOPE	MONROE	2012-03-13 12:14:54 22
121	LIZA	BERGMAN	2012-03-13 12:14:54 22
122	SALMA	NOLTE	2012-03-13 12:14:54 22
123	JULIANNE	DENCH	2012-03-13 12:14:54 22
124	SCARLETT	BENING	2012-03-13 12:14:54 22
125	ALBERT	NOLTE	2012-03-13 12:14:54 22
126	FRANCES	TOMEI	2012-03-13 12:14:54 22
127	KEVIN	GARLAND	2012-03-13 12:14:54 22
128	CATE	MCQUEEN	2012-03-13 12:14:54 22
129	DARYL	CRAWFORD	2012-03-13 12:14:54 22
130	GRETA	KEITEL	2012-03-13 12:14:54 22
131	JANE	JACKMAN	2012-03-13 12:14:54 22
132	ADAM	HOPPER	2012-03-13 12:14:54 22
133	RICHARD	PENN	2012-03-13 12:14:54 22
134	GENE	HOPKINS	2012-03-13 12:14:54 22
135	RITA	REYNOLDS	2012-03-13 12:14:54 22
136	ED	MANSFIELD	2012-03-13 12:14:54 22
137	MORGAN	WILLIAMS	2012-03-13 12:14:54 22
138	LUCILLE	DEE	2012-03-13 12:14:54 22
139	EWAN	GOODING	2012-03-13 12:14:54 22
140	WHOOPI	HURT	2012-03-13 12:14:54 22
141	CATE	HARRIS	2012-03-13 12:14:54 22
142	JADA	RYDER	2012-03-13 12:14:54 22
143	RIVER	DEAN	2012-03-13 12:14:54 22
144	ANGELA	WITHERSPOON	2012-03-13 12:14:54 22
145	KIM	ALLEN	2012-03-13 12:14:54 22
146	ALBERT	JOHANSSON	2012-03-13 12:14:54 22
147	FAY	WINSLET	2012-03-13 12:14:54 22
148	EMILY	DEE	2012-03-13 12:14:54 22
149	RUSSELL	TEMPLE	2012-03-13 12:14:54 22
150	JAYNE	NOLTE	2012-03-13 12:14:54 22
151	GEOFFREY	HESTON	2012-03-13 12:14:54 22
152	BEN	HARRIS	2012-03-13 12:14:54 22
153	MINNIE	KILMER	2012-03-13 12:14:54 22
154	MERYL	GIBSON	2012-03-13 12:14:54 22
155	IAN	TANDY	2012-03-13 12:14:54 22
156	FAY	WOOD	2012-03-13 12:14:54 22
157	GRETA	MALDEN	2012-03-13 12:14:54 22
158	VIVIEN	BASINGER	2012-03-13 12:14:54 22
159	LAURA	BRODY	2012-03-13 12:14:54 22
160	CHRIS	DEPP	2012-03-13 12:14:54 22
161	HARVEY	HOPE	2012-03-13 12:14:54 22

162 OPRAH	KILMER	2012-03-13 12:14:54 22
163 CHRISTOPHER	WEST	2012-03-13 12:14:54 22
164 HUMPHREY	WILLIS	2012-03-13 12:14:54 22
165 AL	GARLAND	2012-03-13 12:14:54 22
166 NICK	DEGENERES	2012-03-13 12:14:54 22
167 LAURENCE	BULLOCK	2012-03-13 12:14:54 22
168 WILL	WILSON	2012-03-13 12:14:54 22
169 KENNETH	HOFFMAN	2012-03-13 12:14:54 22
170 MENA	HOPPER	2012-03-13 12:14:54 22
171 OLYMPIA	PFEIFFER	2012-03-13 12:14:54 22
172 GROUCHO	WILLIAMS	2012-03-13 12:14:54 22
173 ALAN	DREYFUSS	2012-03-13 12:14:54 22
174 MICHAEL	BENING	2012-03-13 12:14:54 22
175 WILLIAM	HACKMAN	2012-03-13 12:14:54 22
176 JON	CHASE	2012-03-13 12:14:54 22
177 GENE	MCKELLEN	2012-03-13 12:14:54 22
178 LISA	MONROE	2012-03-13 12:14:54 22
179 ED	GUINESS	2012-03-13 12:14:54 22
180 JEFF	SILVERSTONE	2012-03-13 12:14:54 22
181 MATTHEW	CARREY	2012-03-13 12:14:54 22
182 DEBBIE	AKROYD	2012-03-13 12:14:54 22
183 RUSSELL	CLOSE	2012-03-13 12:14:54 22
184 HUMPHREY	GARLAND	2012-03-13 12:14:54 22
185 MICHAEL	BOLGER	2012-03-13 12:14:54 22
186 JULIA	ZELLWEGER	2012-03-13 12:14:54 22
187 RENEE	BALL	2012-03-13 12:14:54 22
188 ROCK	DUKAKIS	2012-03-13 12:14:54 22
189 CUBA	BIRCH	2012-03-13 12:14:54 22
190 AUDREY	BAILEY	2012-03-13 12:14:54 22
191 GREGORY	GOODING	2012-03-13 12:14:54 22
192 JOHN	SUVARI	2012-03-13 12:14:54 22
193 BURT	TEMPLE	2012-03-13 12:14:54 22
194 MERYL	ALLEN	2012-03-13 12:14:54 22
195 JAYNE	SILVERSTONE	2012-03-13 12:14:54 22
196 BELA	WALKEN	2012-03-13 12:14:54 22
197 REESE	WEST	2012-03-13 12:14:54 22
198 MARY	KEITEL	2012-03-13 12:14:54 22
199 JULIA	FAWCETT	2012-03-13 12:14:54 22
200 THORA	TEMPLE	2012-03-13 12:14:54 22
412 -1 OR 1=1	test	2012-03-13 12:14:54 22
413 -1 OR 1=1	test	2012-03-13 12:14:54 22
414 NS1NO	test	2012-03-13 12:14:54 22
415 1 AND 'NS='ss	test	2012-03-13 12:14:54 22
416 ' OR 'ns'='ns	test	2012-03-13 12:14:54 22
417 -1 OR 17-7=10	test	2012-03-13 12:14:54 22
418 1 OR X='ss	test	2012-03-13 12:14:54 22
419 ' OR '1'='1	test	2012-03-13 12:14:54 22
420 ' OR '1'='1	test	2012-03-13 12:14:54 22

Açıklığı barındıran sistemler:

- http://php.testsparker.com/artist.php

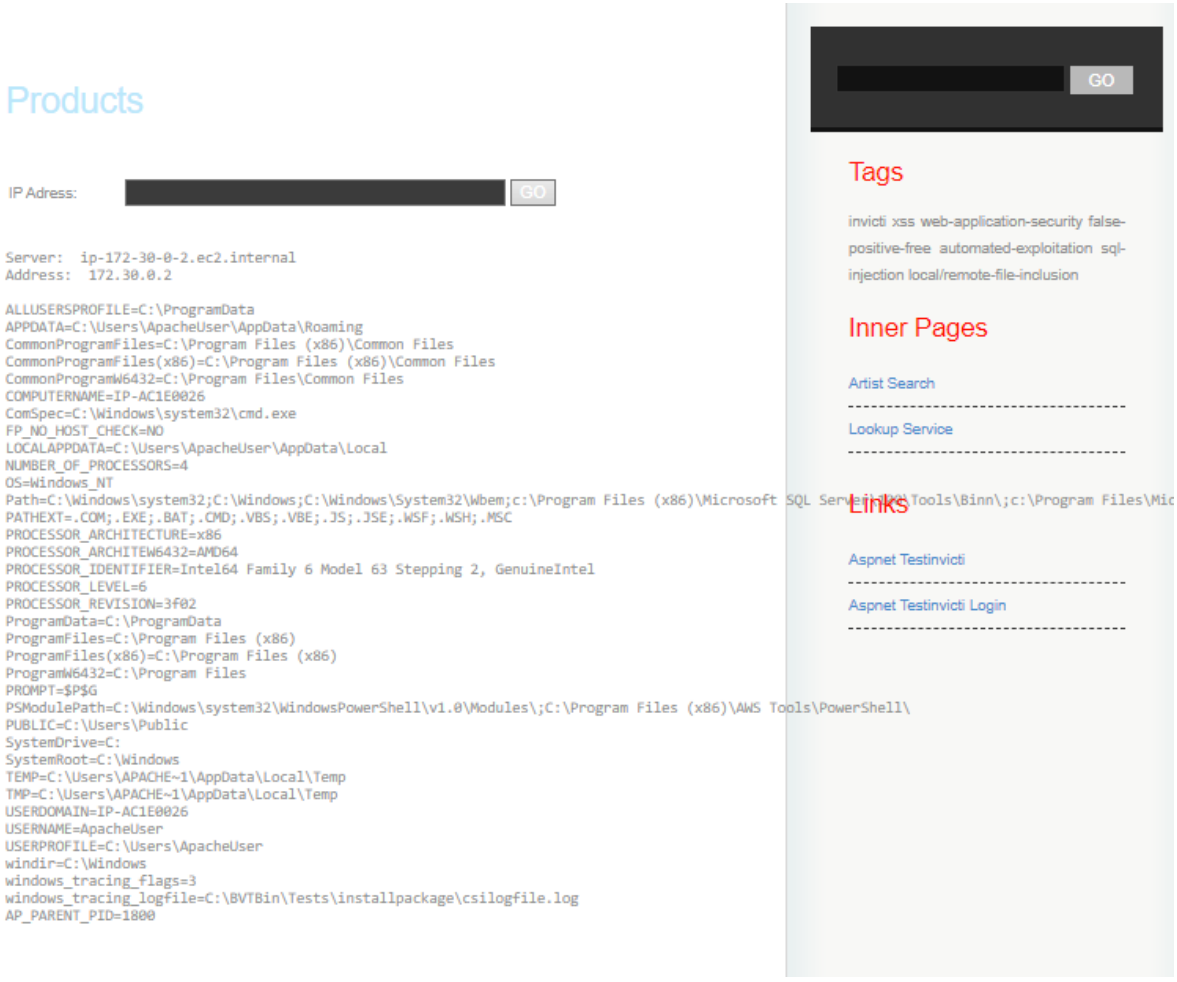
5.2 Local File Inclusion

Önem derecesi: Kritik

Local File Inclusion sayfaya dahil edilen dosyaların kullanıcıdan alınması ya da bir yere data olarak yollanırken filtreleme işlemine tabii tutulmaması sonucunda kullanıcının yetkisi dışında dosyaları okuyabilmesine yol açan bir zafiyet türüdür.

Açıklığı barındıran sistemler

- http://php.testsparker.com/nslookup.php



5.3 Server Side Template Injection

Önem derecesi: Kritik

Server Side Template Injection (SSTI) zafiyeti, template'ın bulunduğu sayfa render işlemine uğramadan önce, template data'ya gelen güvenli olmayan user input ile yapılan manipülasyon işleminden kaynaklanmaktadır. SSTI'ın kritik bir web güvenlik zafiyeti olmasının sebebi, hedef sistemde tespit edilmesinden sonra XSS gibi güvenlik zafiyetlerine de sebep verip, hedef sistemde Remote Code Execution'a (RCE) kadar gidebilmesidir.

Açıklığı barındıran sistemler

- http://php.testsparker.com/artist.php

5.4 Command Injection

Önem derecesi: Kritik

Command injection, web sayfası üzerinde bulunan bir parametreye girilen girdilerin işletim sistemi tarafından komut olarak algılanmasıyla meydana gelir.

Saldırganlar bu zafiyetten yararlanarak sunucu üzerindeki herhangi bir bilgiyi görüntüleyebilir ve sunucu üzerinde komut satırı elde edebilirler. Böylece sunucunun kontrolünü ele geçirmiş olurlar.

Açıklığı barındıran sistemler

- http://php.testsparker.com/nslookup.php

5.5 XSS

Önem derecesi: Yüksek

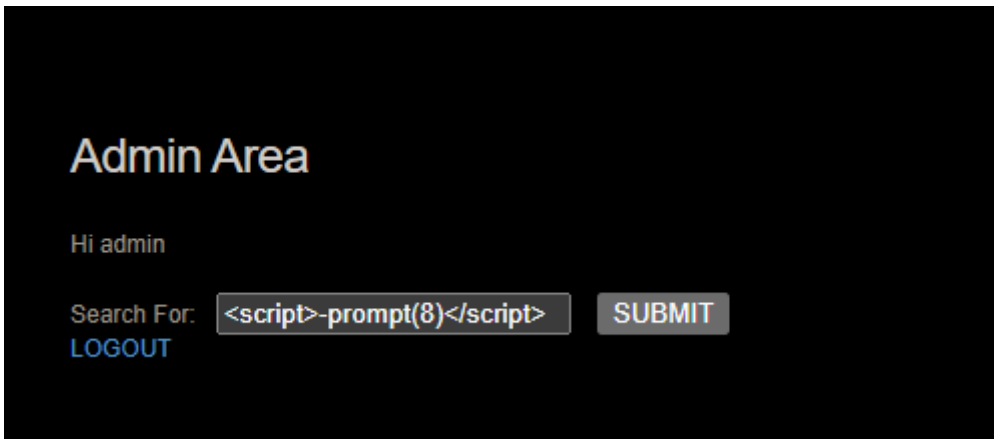
Cross-site scripting attack (XSS) yani siteler arası komut dosyası çalıştırma saldırısı, bir bilgisayar korsanının, iyi huylu ve güvenilir olarak görülen bir web sayfasının içeriğine, genellikle istemci tarafı komut dosyası biçiminde kötü amaçlı kod enjekte etmesiyle oluşur. Kötü amaçlı komut dosyası genellikle, JavaScript ve HTML olan istemci tarafı programlama dillerinde yazılır.

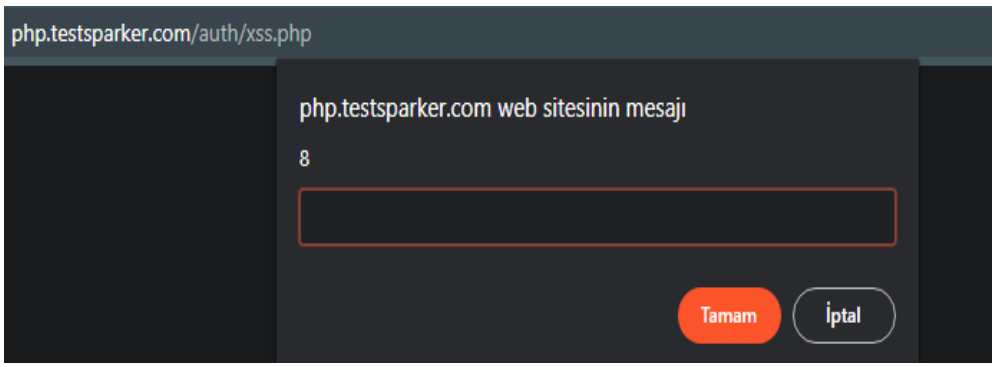
Genel olarak, XSS saldırılarına yatkın web uygulamaları, kullanıcıların girdilerini doğrulamaz veya kodlamaz. Bir siber suçlu, bu kusurdan yararlanabilir ve şüphelenmeyen bir son

kullanıcıya tehlikeli bir komut dosyası gönderebilir. Ne yazık ki, kullanıcının tarayıcısı, komut dosyasına güvenilir bir kaynaktan geliyormuş gibi davranır ve onu yürütür; bu, potansiyel olarak şüphelenmeyen kullanıcıya zarar verir.

Açıklığı barındıran sistemler

- http://php.testsparker.com/auth/internal.php





5.6 HTML Injection

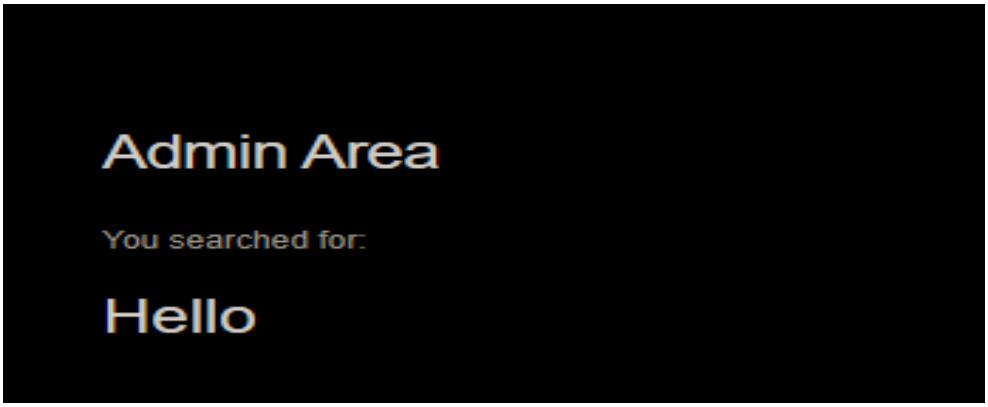
Önem derecesi: Yüksek

Uygulamaların kodları üzerinde bulunan bazı eksiklikler sonucu ortaya çıkan bir güvenlik açığı türüdür. HTML Injection ile web sitelerinin veya uygulamaların misyonlarının dışına çıkmasına sebep olunabilir. Bu yöntemler ile birlikte uygulamayı kullanan kullanıcıların veyahut yeni gelen kullanıcıların oturum bilgileri, parola, kullanıcı adı ve eğer kullanılan uygulama E-Ticaret gibi gerçek anlamda özel bilgileri barındıran bir site/uygulama ise; kredi kartı bilgileri, kimlik numarası gibi maddi ve manevi değer taşıyan birçok bilgiye erişim açılabilir, çalınabilir.

Açıklığı barındıran sistemler

- http://php.testsparker.com/auth/internal.php
- http://php.testsparker.com/artist.php


Admin Area
Hi admin
Search For:
<h1>Hello</h1>
SUBMIT
LOGOUT


Admin Area
You searched for:
Hello


Artist Service
Results:
hello
no rows returned
<h1>hello</h1>
GO
Tags
invicti xss web-application-security false-positive-free automated-exploitation sql-injection local/remote-file-inclusion