

php.testsparker.com Sızma Testi-Zaafiyet
Taraması
Sonuç Raporu

22.08.2022 – 02.09.2022

Rapor Detayları

Rapor Başlığı	Php.testsparker.com Sızma Testi Sonuç Raporu
Versiyon	1.0
Yazan	Caner Özcanlı
Test Ekibi	Caner Özcanlı
Kontrol Eden	Caner Özcanlı
Onaylayan	Caner Özcanlı
Rapor Sınıfı	-

Rapor Yetkilisi

Yetkili Adı ve Soyadı	Ünvanı
Ammar Karabulut	Techkariyer Siber Güvenlik Bootcamp Eğitmeni

Rapor Denetimi

Versiyon	Tarih	Yazar	Tanım
V 1.0	29.08.2022	Caner Özcanlı	Final

İçindekiler

Giriş.....	4
Kapsam	5
Yönetici Özeti.....	6
Bulunan Güvenlik Zaafiyetleri Özet Tablosu	7
Zaafiyetler - Sistem Özelliklerinin Web Üzerinde Bulunması.....	8
Zaafiyetler – Composer Erişimi	10
Zaafiyetler – Açık Erişimli phpinfo Verileri	12
Zaafiyetler - Kullanıcı Kimlik Bilgisi İçeriği	15
Zaafiyetler – Captcha Eksikliği	16
Zaafiyetler – Clickjacking- X-Frame Option Eksikliği	18
Zaafiyetler – clientaccesspolicy Yapılandırması	22
Zaafiyetler – X-Content Type Option Eksikliği	23
Zaafiyetler – XSS (Cross Site Scripting)	25
Zaafiyetler – HTTPS Protokol Eksikliği	27
Zaafiyetler – HTTP Başlık Bilgisi İçerisinde Kull.Adı – Şifresi Bilgisi İçeriği	28
Zaafiyetler – SQL Injection	30
EK-1 : Raporda Geçen Teknik Terimler ve Kısaltmalar	33
EK-2 : Güvenlik Testleri Sırasında Kullanılan Araçlar	34

GİRİŞ

Bu rapor, “php.testsparker.com” web sitesi üzerindeki güvenlik açıklarını ortaya çıkartmak amacı ile 22.08.2022 - 02.09.2022 tarihleri arasında 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. Sızma testine ait çalışma takvimi ve projede yer alan uzmanların bilgisine aşağıda yer verilmiştir

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

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 yetkililer tarafından bildirilen ve aşağıda verilen sistemlere yönelik sızma testleri gerçekleştirilmiştir

Web Uygulamaları : php.testsparker.com

Dış Ağ Ip Adresi : 107.20.213.223

İç Ağ Ip Adresi: -

E-posta Sunucuları: -

Dns Sunucuları : -

Sosyal Mühendislik: -

Kablosuz Ağ Sistemleri: -

Dağıtık Servis Bırakma: -

Mobil Uygulama : -

YÖNETİCİ ÖZETİ

Bu rapor, php.testsparker.com web sitesi üzerindeki güvenlik açıklarını ortaya çıkartmak amacı ile 22.08.2022 - 02.09.2022 tarihleri arasında gerçekleştirilen sızma testleri (penetration test) ve güvenlik testleri çalışmalarının sonuçlarını içermektedir.

Testler, raporun devamında detayları verilen etki alanı/sunucu-istemci sistemler, veritabanı sistemleri kapsamında gerçekleştirilmiştir. Çalışmalar süresince dış/iç siber saldırgan gözüyle sistemler tüm detaylarıyla incelenmiştir.

Çalışmalar sonucunda 1 acil, 2 kritik, 5 yüksek, 4 orta olmak üzere toplamda 12 farklı güvenlik açıklığı tespit edilmiştir. Bir açıklığın birden fazla sistemde bulunması açıklık sayısını etkilememektedir.

SQL enjeksiyonu,XSS(siteler arası script çalıştırma) açıklığı, güncelleştirme eksikliklerinden kaynaklanan kritik güvenlik açıklıkları sızma 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. Web sitesi 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.

Bulunan Güvenlik Zaafiyetleri Özet Tablosu

Bulgu Adı	Önem Derecesi	Bulgu Kategorisi
Sistem Özelliklerinin Web Sitesi Üzerinde Bulunması	Orta	Web
Kullanıcı Kimlik Bilgileri İçeriği	Acil	Web
Captcha Eksikliği	Yüksek	Web
X Frame Option Eksikliği	Yüksek	Web
X Content Type Option Eksikliği	Orta	Web
XSS Zaafiyeti	Kritik	Web
Https Protokolü Eksikliği	Yüksek	Web
http Başlık Bilgisi İçerisinde Kullanıcı Adı ve Parola İletimi	Yüksek	Web
SQL Injection	Kritik	Web
Açık Erişimli phpinfo	Yüksek	Web
Composer Herkese Açık Erişimi	Orta	Web
Clientaccesspolicy Yetkilendirmesi	Orta	Web

Sistem Özelliklerinin Web Sitesi Üzerinde Bulunması

Önem Derecesi : Orta

Açıklığın Etkisi: Yetkisiz Erişim,Bilgi İfşası

Erişim Noktası: İnternet

Kullanıcı Profili : Anonim Kullanıcı

Bulgu Kategorisi : Web

Bulgu Sebebi : Uygulama Geliştirmedeki Eksiklik

Bulgu Açıklaması:

Web siteleri çeşitli uygulamalar ve yazılımsal teknolojiler ile kodlanmakta ve/veya inşa edilmektedir. Her gün geçtikçe , web siteleri yapılırken kullanılan programlarda zafiyet bulunması ihtimali vardır. Bu yüzden sistemler son sürümlerine güncellenmeli ve olası zafiyetler minimuma indirgenmelidir. Sistemler bu şekilde korunurken, web sitesinin hangi teknoloji ile yapıldığı ve sürüm bilgisi olabildiğince gizli tutulmalıdır.

Bu bilgiler çeşitli hata bildirim mesajlarında görülebileceği gibi, web sitesini kuran kişiler tarafından gözden kaçmış veya unutulmuş olabilir.

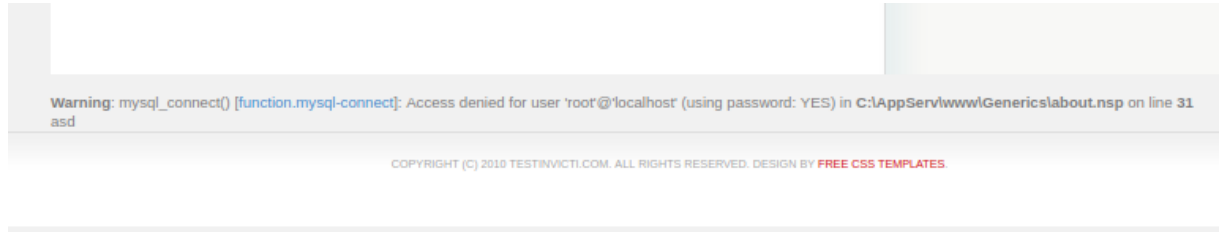
Yapılan web sızma testinde, web sitesi içerisinde ve hata mesajlarında ilgili teknoloji ve sürüm bilgisine rastlanmıştır.Aşağıdaki ekran görüntüsünde teknoloji/ sürüm bilgisi / port bilgisi görünmektedir.


```
1 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
2 <html><head>
3 <title>404 Not Found</title>
4 </head><body>
5 <h1>Not Found</h1>
6 <p>The requested URL /Generics/style.css was not found on this server.</p>
7 <hr>
8 <address>Apache/2.2.8 (Win32) PHP/5.2.6 Server at php.testsparker.com Port 80</address>
9 </body></html>
10
```

Aşağıdaki ekran görüntüsü ise ana-domainden alınmıştır. Sub-domainlere ait teknolojiler verilmektedir.

Name	URL	Technologies
ASP.Net - Testsparker	aspnet.testsparker.com	Windows, IIS, ASP.NET, MsSQL
PHP - Testsparker	php.testsparker.com	Windows, Apache, PHP, MySQL
SPA - Angular - Testsparker	angular.testsparker.com	Ubuntu, Apache, PHP, Angular 5, MySQL
API - REST - Testsparker	rest.testsparker.com	Ubuntu 18, Apache, PHP 7.1, MySQL

Aşağıdaki görselde ise sayfada oluşan hatadan kaynaklı bir mesaj oluşmuş; bu hatada mysql database kullanıldığı ve **root** user hakkında bilgi verilmiştir



Açıklığı Barındıran Sistemler:

- <http://php.testsparker.com/Generics/style.css>
- <http://php.testsparker.com/process.php?file=Generics/about.nsp>
- <http://www.testsparker.com/>

Cözüm Önerileri:

- Web sayfasının tüm dizinleri kontrol edilerek , çeşitli hata testleri yapılarak düzenlenmeli ve erişim halinde olan kişilere bu bilgiler verilmemelidir.

Composerın Herkese Açık Erişimi

Önem Derecesi : Orta

Açıklığın Etkisi: Sistem Hakkında Bilgi Sızması

Erişim Noktası: İnternet

Kullanıcı Profili : Anonim Kullanıcı

Bulgu Kategorisi : Web

Bulgu Sebebi : Uygulama Geliştirmedeki Eksiklik

Bulgu Açıklaması:

Web taraması yapılırken web sitesi üzerinde Composer installed.json dosyası keşfedildi. PHP'de bağımlılık yönetimi için bir araçtır. Projenizin bağlı olduğu kitaplıkları bildirmenize olanak tanır ve bunları sizin için yönetir (yükler/günceller). Bağımlılıkları yükledikten sonra, Composer bunların listesini dahili amaçlar için özel bir dosyada saklar.

Dosya herkese açık olduğundan, web uygulaması tarafından kullanılan bileşenlerle ilgili bilgilerin ifşa edilmesine yol açar. Aşağıdaki görseller installed.json dosyasından alınmıştır.

```
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
▼ packages:
  ▼ 0:
    name: "doctrine/instantiator"
    version: "1.4.0"
    version_normalized: "1.4.0.0"
    ▼ source:
      type: "git"
      url: "https://github.com/doctrine/instantiator.git"
      reference: "d56bf6102915de5702778fe20f2de3b2fe570b5b"
    ▼ dist:
      type: "zip"
      ▼ url: "https://api.github.com/repos/doctrine/instantiator/zipball/d56bf6102915de5702778fe20f2de3b2fe570b5b"
      reference: "d56bf6102915de5702778fe20f2de3b2fe570b5b"
      shasum: ""
    ▼ require:
      php: "^7.1 || ^8.0"
    ▼ require-dev:
      doctrine/coding-standard: "^8.0"
      ext-pdo: "*"
      ext-phar: "*"
      phpbench/phpbench: "^0.13 || 1.0.0-alpha2"
      phpstan/phpstan: "^0.12"
      phpstan/phpstan-phpunit: "^0.12"
      phpunit/phpunit: "^7.0 || ^8.0 || ^9.0"
    time: "2020-11-10T18:47:58+00:00"
    type: "library"
    installation_source: "direct"
```

JSON	Raw Data	Headers
Save	Copy	Collapse All Expand All Filter JSON
Doctrine\Instantiator\:	"src/Doctrine/Instantiator/"	
notification-url:	"https://packagist.org/downloads/"	
▼ license:		
0:	"MIT"	
▼ authors:		
0:		
name:	"Marco Pivetta"	
email:	"ocramius@gmail.com"	
homepage:	"https://ocramius.github.io/"	
▼ description:	"A small, lightweight utility to instantiate objects in PHP without invoking their constructors"	
▼ homepage:	"https://www.doctrine-project.org/projects/instantiator.html"	
▼ keywords:		
0:	"constructor"	
1:	"instantiate"	
▼ 1:		
name:	"myclabs/deep-copy"	
version:	"1.10.2"	
version_normalized:	"1.10.2.0"	
▼ source:		
type:	"git"	
url:	"https://github.com/myclabs/DeepCopy.git"	
reference:	"776f831124e9c62e1a2c601ecc52e776d8bb7220"	
▼ dist:		
type:	"zip"	
▼ url:	"https://api.github.com/repos/myclabs/DeepCopy/zipball/776f831124e9c62e1a2c601ecc52e776d8bb7220"	
reference:	"776f831124e9c62e1a2c601ecc52e776d8bb7220"	
.	..	

Açıklığı Barındıran Sistemler:

- <http://php.testsparker.com/vendor/installed.json>

Çözüm Önerileri:

- Web sayfasının tüm dizinleri kontrol edilerek /vendor erişiminin kaldırılması gerekir. Ayrıca benzer şekilde bilgiler içeren /twig erişiminin de kaldırılması gereklidir.

Referans:

Twig > <https://www.netsparker.com.tr/blog/web-guvenligi/dns-rebinding-ile-ethereum-lariniz-calinabilir/>

Açık Erişimli phpinfo Verileri

Önem Derecesi : Yüksek

Açıklığın Etkisi: Bilgi İfşası,Hizmet Aksaması

Erişim Noktası: İnternet

Kullanıcı Profili : Anonim Kullanıcı


Bulgu Kategorisi : Web

Bulgu Sebebi : Uygulama Geliştirmedeki Eksiklik

Bulgu Açıklaması:

phpinfo, PHP'nin yapılandırmasının çıktısını almak için yerleşik bir işlevdir. PHP uzantıları, işletim sistemi bilgileri, PHP lisansı ve çok daha hassas bilgiler gibi bilgileri verir. Bu işlev, geliştiricilerin belirli bir sistemde yapılandırma ayrıntılarını ve önceden tanımlanmış değişkenleri alması için kullanılır. Bir saldırgan için phpinfo tarafından yazdırılan bilgiler hayati öneme sahiptir. Saldırgan bu bilgiyi kullanarak başarılı bir saldırıyı verimli bir şekilde planlayabilir. Bu işlev PHP sürümünü gösterdiğinden, saldırgan PHP sürümünün sahip olduğu güvenlik açıklarını arayacaktır. Bu saldırı web uygulamasını yok etmeye kadar gidebilir.

Aşağıdaki ekran görüntüleri phpinfo dan alınmıştır.

PHP Version 5.2.6	
	
System	Windows NT IP-AC1E00C8 6.1 build 7601
Build Date	May 2 2008 18:01:20
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--with-gd=shared" "--with-extra-includes=C:\Program Files (x86)\Microsoft SDK\Include;C:\PROGRA~2\MICROS~2\VC98\ATL\INCLUDE;C:\PROGRA~2\MICROS~2\VC98\INCLUDE;C:\PROGRA~2\MICROS~2\VC98\MFC\INCLUDE" "--with-extra-libs=C:\Program Files (x86)\Microsoft SDK\Lib;C:\PROGRA~2\MICROS~2\VC98\LIB;C:\PROGRA~2\MICROS~2\VC98\MFC\LIB"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\Windows\php.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	enabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	php, file, data, http, ftp, compress.zlib
Registered Stream Socket Transports	tcp, udp

highlight.bg	#FFFFFF	#FFFFFF
highlight.comment	#FF8000	#FF8000
highlight.default	#0000BB	#0000BB
highlight.html	#000000	#000000
highlight.keyword	#007700	#007700
highlight.string	#DD0000	#DD0000
html_errors	On	On
ignore_repeated_errors	Off	Off
ignore_repeated_source	Off	Off
ignore_user_abort	Off	Off
implicit_flush	Off	Off
include_path	.;C:\php5\pear	.;C:\php5\pear
log_errors	On	On
log_errors_max_len	1024	1024
magic_quotes_gpc	Off	Off
magic_quotes_runtime	Off	Off
magic_quotes_sybase	Off	Off
mail.force_extra_parameters	no value	no value
max_execution_time	60	60
max_input_nesting_level	64	64
max_input_time	60	60
memory_limit	512M	512M
open_basedir	no value	no value
output_buffering	4096	4096
output_handler	no value	no value
post_max_size	256M	256M
precision	12	12
realpath_cache_size	256k	256k
realpath_cache_ttl	120	120

Apache Environment

Variable	Value
HTTP_HOST	php.testsparker.com
HTTP_USER_AGENT	Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_CONNECTION	keep-alive
HTTP_COOKIE	PHPSESSID=6aa26b30089e23a33d5921ff01107060
HTTP_UPGRADE_INSECURE_REQUESTS	1
PATH	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;c:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\c:\Program Files\Microsoft SQL Server\100\Tools\Binn\c:\Program Files\Microsoft SQL Server\100\Tools\Binn\c:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\VSShell\Common7\IDE;c:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Program Files\Amazon\cfn-bootstrap\
SystemRoot	C:\Windows
COMSPEC	C:\Windows\system32\cmd.exe
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
WINDIR	C:\Windows
SERVER_SIGNATURE	<address>Apache/2.2.8 (Win32) PHP/5.2.6 Server at php.testsparker.com Port 80</address>
SERVER_SOFTWARE	Apache/2.2.8 (Win32) PHP/5.2.6
SERVER_NAME	php.testsparker.com
SERVER_ADDR	172.30.0.200
SERVER_PORT	80
REMOTE_ADDR	185.135.108.48
DOCUMENT_ROOT	C:/AppServ/www/

safe_mode	Off	Off
safe_mode_exec_dir	no value	no value
safe_mode_gid	Off	Off
safe_mode_include_dir	no value	no value
sendmail_from	no value	no value
sendmail_path	no value	no value
serialize_precision	100	100
short_open_tag	On	On
SMTP	localhost	localhost
smtp_port	25	25
sql.safe_mode	Off	Off
track_errors	Off	Off
unserialize_callback_func	no value	no value
upload_max_filesize	256M	256M
upload_tmp_dir	no value	no value
user_dir	no value	no value
variables_order	EGPCS	EGPCS
xmlrpc_error_number	0	0
xmlrpc_errors	Off	Off
y2k_compliance	On	On
zend.ze1_compatibility_mode	Off	Off

apache2handler

Apache Version	Apache/2.2.8 (Win32) PHP/5.2.6
Apache API Version	20051115
Server Administrator	onur@netsparker.com
Hostname:Port	php.testsparker.com:0

Bu bilgiler ile dosya sistemi hakkında bilgi alacağından, dizin geçişi saldırısı yoluyla hassas dosyalara erişilebilir, siteler arası komut dosyası çalıştırma saldırısını tetiklemek için bilgileri kullanabilir, web uygulaması üzerinde SQL Injection saldırısı gerçekleştirebilir, işletim sistemi komutlarını temel alınan işletim sisteminde yürütebilir ve ağın dahili IP'lerine erişim sağlanabilir.

Açıklığı Barındıran Sistemler:

- <http://php.testsparker.com/phpinfo>

Cözüm Önerileri:

- Uygulamanın PHP yapılandırmasında phpinfo() işlevini devre dışı bırakın.
- phpinfo() işlevini çağıran tüm sayfaları kaldırın.

Kullanıcı Kimlik Bilgisi İçeriği

Önem Derecesi : Acil

Açıklığın Etkisi: Yetkisiz Erişim

Erişim Noktası: İnternet

Kullanıcı Profili : Anonim Kullanıcı

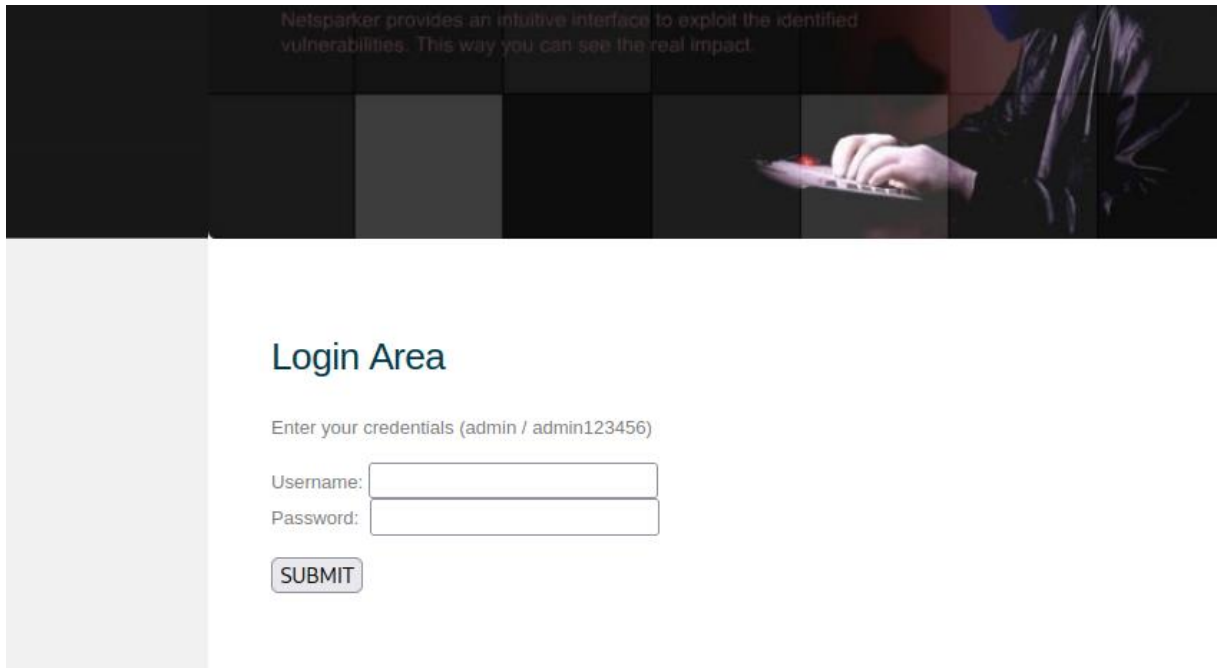
Bulgu Kategorisi : Web

Bulgu Sebebi : Uygulama Geliştirmedeki Eksiklik

Bulgu Açıklaması:

Yapılan web sızma testi esnasında kullanıcı giriş sayfası kullanıcı arayüzünde admin kullanıcısının kullanıcı adı ve şifresinin görüntülediği tespit edilmiştir.

Aşağıdaki ekran görüntüsü web sitesinin login sayfasına aittir.



Açıklığı Barındıran Sistemler:

- <http://php.testsparker.com/auth/login.php>

Cözüm Önerileri:

- Web sayfasının tekrar düzenlenerek kullanıcı giriş bilgileri kaldırılmalıdır. Admin kullanıcısı için büyük/küçük,ardışık olmayan ve sembollerin olduğu daha zor parolalar kullanılmalıdır.

CAPTCHA (Güvenlik Karakteri) Önlemi Eksikliği

Önem Derecesi : Yüksek

Açıklığın Etkisi: Yetkisiz Erişim

Erişim Noktası: İnternet

Kullanıcı Profili : Anonim Kullanıcı

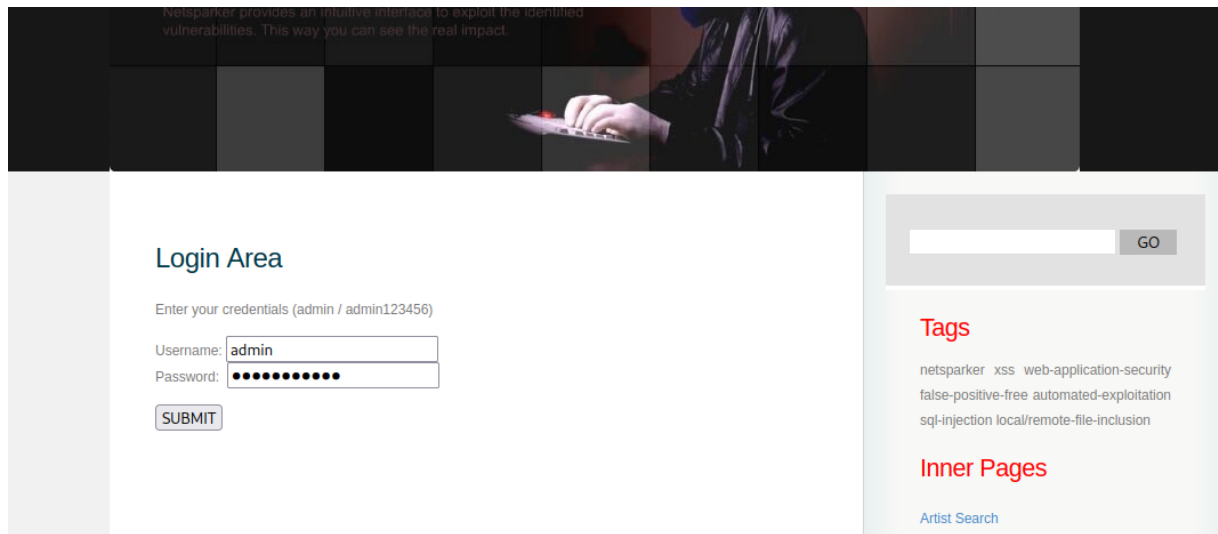
Bulgu Kategorisi : Web

Bulgu Sebebi : Uygulama Geliştirmedeki Eksiklik

Bulgu Açıklaması:

Yapılan web sızma testleri esnasında web sayfasına ait kullanıcı girişi yapılan bölümlerde captcha kullanılmadığı belirlenmiştir. Captcha, her oturum açma aşamasında rastgele karakterler çıkartılarak bunun kullanıcı tarafından girilmesi işlemidir. Bu yöntem saldırganların sistem üzerinde erişim elde edememeleri için uygulanan ek bir güvenlik önlemidir. Captcha kullanılmayan kimlik doğrulama arabirimlerinde, saldırganlar çeşitli otomatize araçlar kullanarak bu web formlarına sözlük ve kaba kuvvet saldırıları gerçekleştirebilirler. Bu şekilde kullanıcılara ait hesaplar veya yönetim panelindeki yönetici hesabı ele geçirilebilir. Kullanıcı adı ve parola girildikten sonra captcha girilmeden sisteme login olunabildiği görülmüştür.

Aşağıdaki ekran görüntüsünde siteye giriş denemesi yapıldığı ve CAPTCHA olmadığı görülmüştür.



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

Login Area

Enter your credentials (admin / admin123456)

Username:

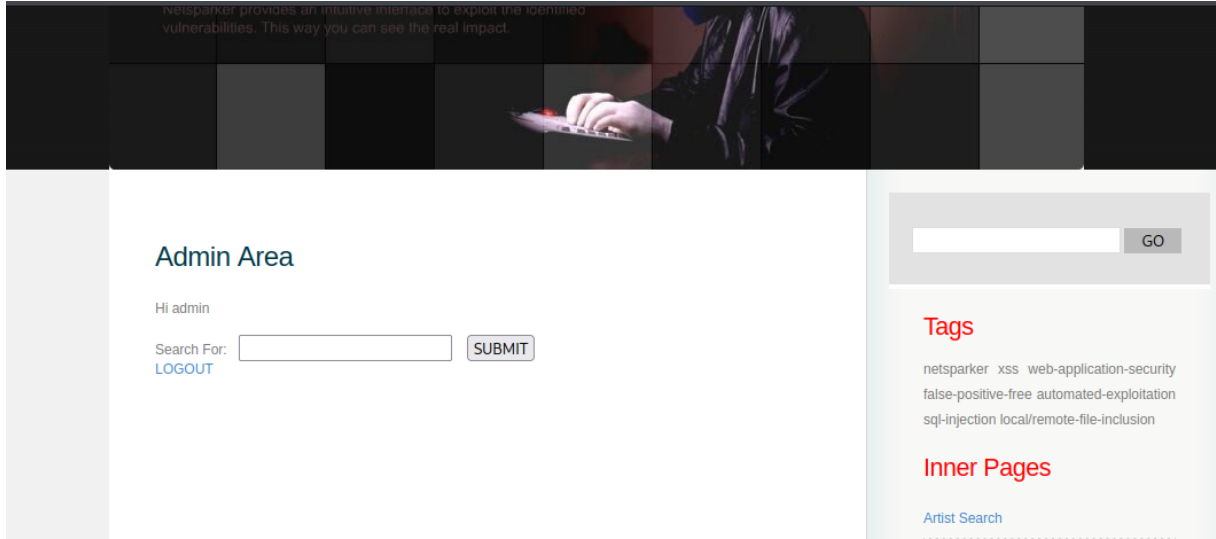
Password:

Tags

netsparker xss web-application-security
false-positive-free automated-exploitation
sql-injection local/remote-file-inclusion

Inner Pages

[Artist Search](#)



Açıklığı Barındıran Sistemler:

- <http://php.testsparker.com/auth/login.php>

Cözüm Önerileri:

- Captcha kontrolü yapılmadan sisteme direk olarak giriş yapılmamalıdır.

Referanslar:

- <http://en.wikipedia.org/wiki/CAPTCHA>
- <http://www.w3schools.in/php-tutorial/php-captcha/>
- <http://www.devmanuals.com/tutorials/java/jsp/captcha.html>

X-Frame Options Eksikliği - Clickjacking

Önem Derecesi : Yüksek

Açıklığın Etkisi: Yetkisiz Erişim, Zararlı Yazılım Enjeksiyonu

Erişim Noktası: İnternet

Kullanıcı Profili : Anonim Kullanıcı

Bulgu Kategorisi : Web

Bulgu Sebebi : Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

X-Frame Options 2009 yılında Clickjacking başta olmak üzere UI Redressing saldırılarına karşı önerilen ve bugün tüm major browserlar tarafından desteklenen bir güvenlik headerıdır.

Saldırılar basit olarak şu şekilde gerçekleşir. Hedef sistem içerisine bir iFrame yerleştirilir.Hedef sitedeki bilgilerin kullanıcı kandırılarak saldırganın sitesindeki arayüzlere girmesini sağlamak yada kullanıcının masum görünümlü site üzerinde gerçekleştiğine inandığı hareketleri hedef siteye yönlendirerek kullanıcı yetkileriyle erişim gerçekleştirmektedir.

Yerleştirilen iFrame in opaklık değeri düşük olduğu için iframe transparan hale gelir. Kullanıcı sitede işlem yaparken masum sitede etkileşim gerçekleştirdiğini sanarken aslında tıkladığı işlem zararlı sayfa üzerinde işlem gerçekleştirmektedir. Böylece saldırgan, kurbanı zararsız görünen bağlantılara tıklamaya ikna ederken, hedef sitedeki bir dizi aksiyonun tetiklenmesine yol açar.

```
http://php.testsparker.com/process.php?file=Generics/index.nsp
Host: php.testsparker.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://php.testsparker.com/hello.php?name=Visitor
Connection: keep-alive
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Sat, 27 Aug 2022 19:19:58 GMT
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Connection: close
Content-Type: text/html
Content-Length: 2993

.....
http://php.testsparker.com/favicon.ico
Host: php.testsparker.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
GET: HTTP/1.1 404 Not Found
Date: Tue, 23 Aug 2022 12:34:04 GMT
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Length: 302
Content-Type: text/html; charset=iso-8859-1

.....
```

Yapılan taramalarda yukarıdaki görsel websitesinin header bilgilerini içermektedir.X-Frame Option hakkında bir kısıtlama görülmemektedir.

X Frame Options ;

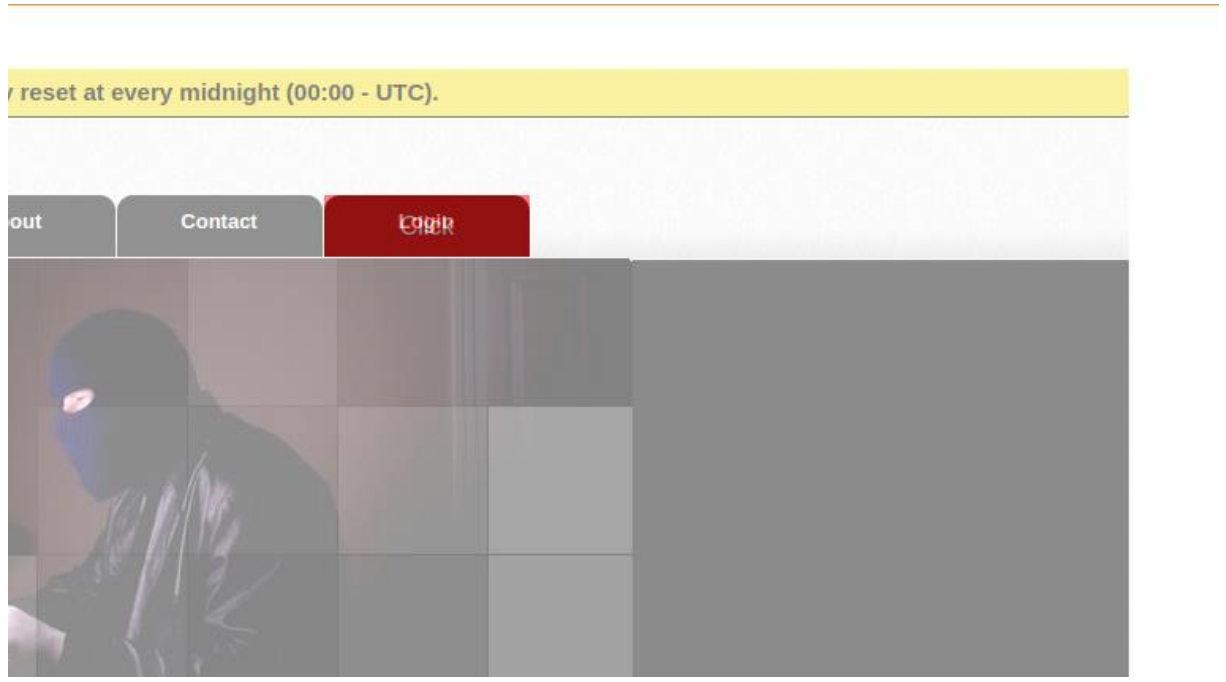
-Sameorigin

-Deny

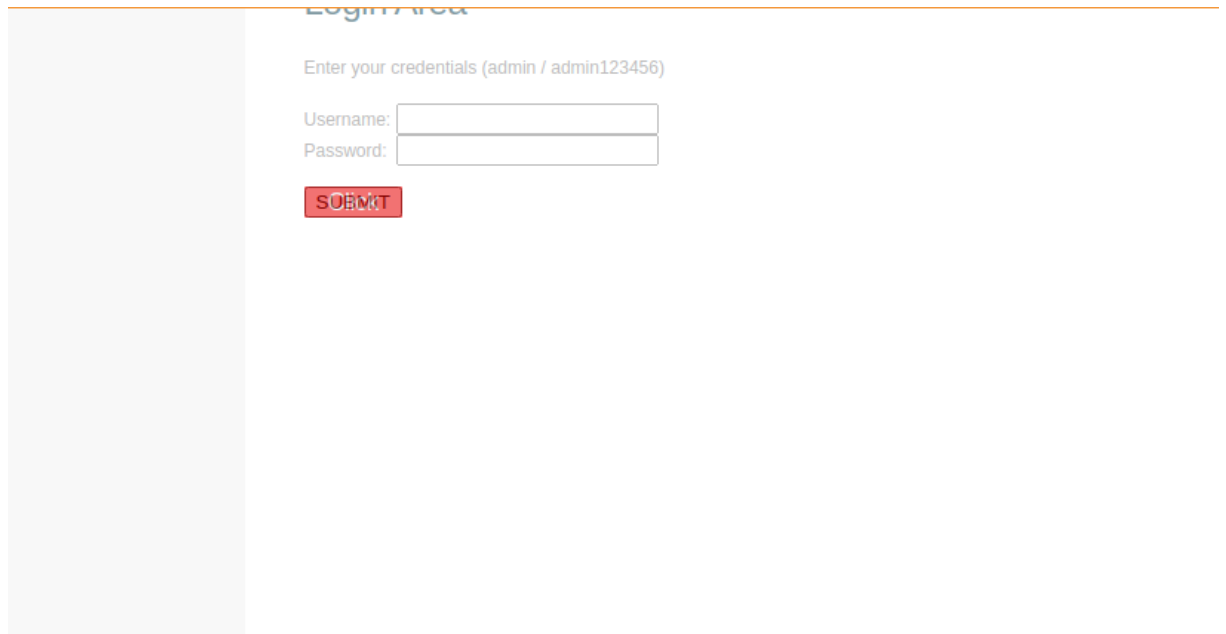
-Allow-From URL

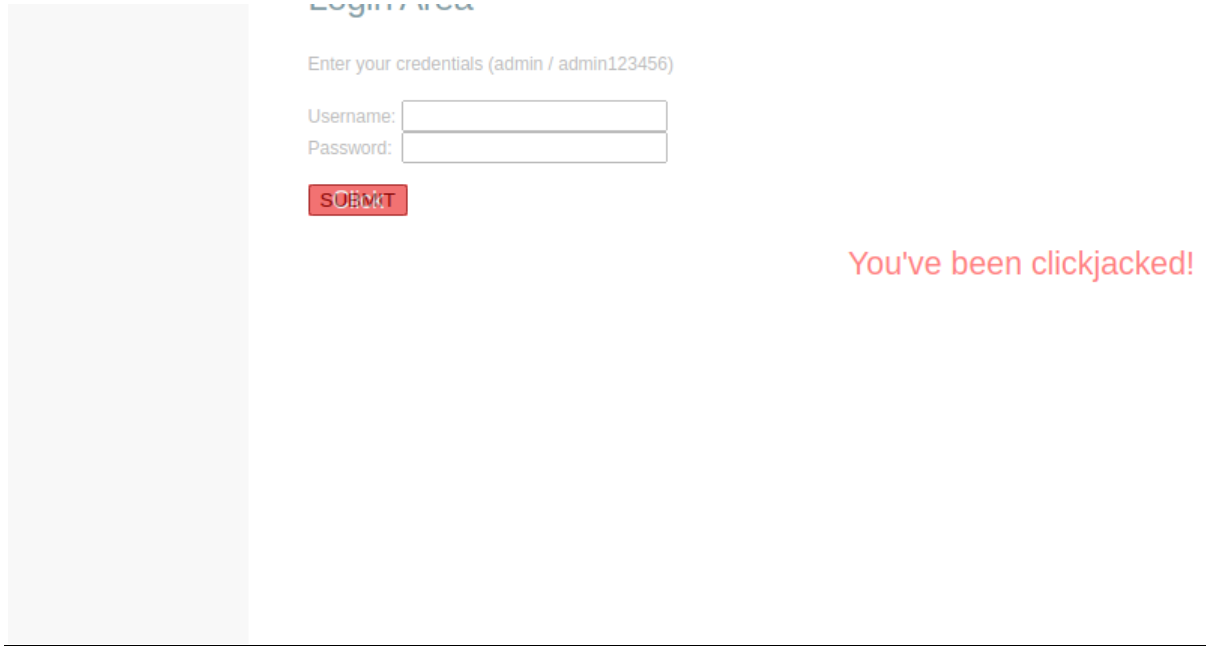
parametrelerini alacaktır.

Aşağıdaki ekran görüntüsü ise websitesine clickjacking uygulamasını içermektedir



Kullanıcının tıklayabileceği farklı butonlar üzerine opaklık değeri düşük farklı amaca hizmet eden yönlendirici butonlar yerleştirilmiştir.





En olası ihtimalle gerçekleşebilecek **login** işlemi sonrasında ise **clickjacking** gerçekleşmiştir.

Acıklığı Barındıran Sistem : <http://php.testsparker.com>

Cözüm Önerisi: Bu saldırıdan korunmak için Frame Busting başta olmak üzere, pek çok yöntem denenmiştir. Bunlardan en geçerli olan X-Frame-Options yöntemi ise 2009 yılında Microsoft tarafından IE browserlarına eklenmiştir.

Ziyaretçilerimizi Clickjacking vb. saldırılardan korunmanın en temel yolu, sayfalarımızın iframe, frame gibi yollarla embed edilmesini engellemek ya da buna bir kısıtlama getirmektir. Bunu yapmak için güvenlik headerlarından biri olan X-Frame-Options'ı kullanabiliriz.

Referanslar:

<https://www.netsparker.com.tr/blog/web-guvenligi/clickjacking-bastigin-yerleri-buton-diyerek-gecme/>

clientaccesspolicy.xml Yapılandırması

Önem Derecesi : Orta

Açıklığın Etkisi: Yetkisiz Erişim

Erişim Noktası: İnternet

Kullanıcı Profili : Anonim Kullanıcı

Bulgu Kategorisi : Web

Bulgu Sebebi : Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Etki alanları arası ilke dosyası, Java, Adobe Flash, Adobe Reader vb. gibi bir web istemcisinin farklı etki alanlarındaki verilere erişmek için kullandığı izinleri belirtir. İstemci erişim ilkesi dosyası, etki alanları arası ilkeye benzer ancak Silverlight uygulamaları için kullanılır. Aşırı izin veren yapılandırmalar, Siteler Arası İstek Sahteciliği saldırılarını etkinleştirir ve üçüncü tarafların kullanıcıya yönelik hassas verilere erişmesine izin verebilir.

Web uygulamasından http-domain-policy güvenlik açığı kaynak kodu aşağıdaki gibidir:

```
/clientaccesspolicy.xml:
  <?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>
Extra information:
Trusted domains:*
```

Burada * işareti ile gösterilen domain değerleri kısıtlandırılmamış ve tüm isteklere açıktır.

Açıklığı Barındıran Sistem : <http://php.testsparker.com>

Cözüm Önerisi: clientaccesspolicy.xml güncellenmeli, * karakteri ile gösterilen izin verilen domainler kısıtlandırılmalıdır

Referanslar: <https://cwe.mitre.org/data/definitions/942.html>

X-Content Type Options Eksikliği

Önem Derecesi : Orta

Açıklığın Etkisi: Yetkisiz Erişim, Zararlı Yazılım Enjeksiyonu

Erişim Noktası: İnternet

Kullanıcı Profili : Anonim Kullanıcı

Bulgu Kategorisi : Web

Bulgu Sebebi : Yapılandırma Eksikliği/Hatası

Bulgu Açıklaması:

Content-Type headerı ile içeriğin tipi belirtilmediği takdirde, browser içeriği en doğru biçimde görüntülemeye çalışır.

Özellikle de upload fonksiyonlarıyla beraber, sniffing işlemi bir takım tehlikeler arz edebilir.

Örneğin, kullanıcının zararsız addedilen bir text dosyası upload ettiğini varsayalım. Eğer bu text dosyası HTML ve script tagları, Javascript kodları içeriyorsa ve biz bu yüklenen dosyayı tekrar kullanıcıya sunarken bir içerik tipi belirtmiyorsak, tarayıcı bu sayfanın içeriğini koklayarak bunun pek tabii bir text/html tipinde bir dosya olduğuna karar verecektir ve bu sayfadaki kodlar da çalışacaktır.

Yine sitemize upload edilen resim dosyaları dahi, kullanıcıya geri sunulurken, içerik tipi bilgisi içermelidir. Yoksa EXIF data olarak tabir edilen, resmin meta datalarını içeren kısma zararlı kodları enjekte edilerek, bu kodlar çalıştırılabilir.

İşte bu gibi durumlarda, tarayıcının sayfa içeriğini koklayarak, inceleyerek servis edeceği tipe karar vermesinin önüne geçmek için X-Content-Type-Options headerı kullanılmaktadır.

```
http://php.testsparker.com/process.php?file=Generics/index.nsp
Host: php.testsparker.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://php.testsparker.com/hello.php?name=Visitor
Connection: keep-alive
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Sat, 27 Aug 2022 19:19:58 GMT
Server: Apache/2.2.8 (Win32) PHP/5.2.6
X-Powered-By: PHP/5.2.6
Connection: close
Content-Type: text/html
Content-Length: 2993

.....
http://php.testsparker.com/favicon.ico
Host: php.testsparker.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://php.testsparker.com/process.php?file=Generics/index.nsp
GET: HTTP/1.1 404 Not Found
Date: Tue, 23 Aug 2022 12:34:04 GMT
Server: Apache/2.2.8 (Win32) PHP/5.2.6
Content-Length: 302
Content-Type: text/html; charset=iso-8859-1

.....
```

Clickjacking kontrolünde web sitesinin http headerını incelemiştik. X-Content Type eksikliği header da görülmektedir.

Açıklığı Barındıran Sistem : <http://php.testsparker.com>

Cözüm Önerisi: X-Content Type Options – “Nosniff” server apache headers.conf dosyasına eklenmelidir.

Referanslar: <https://www.keycdn.com/support/x-content-type-options#:~:text=A%20Chrome%20client%20makes%20a,is%20declared%20by%20the%20server.>

XSS (Cross Site Scripting) Zaafiyeti

Önem Derecesi : Kritik

Açıklığın Etkisi: Yetkisiz Erişim, Bilgi İfşası

Erişim Noktası: İnternet

Kullanıcı Profili : Anonim Kullanıcı

Bulgu Kategorisi : Web

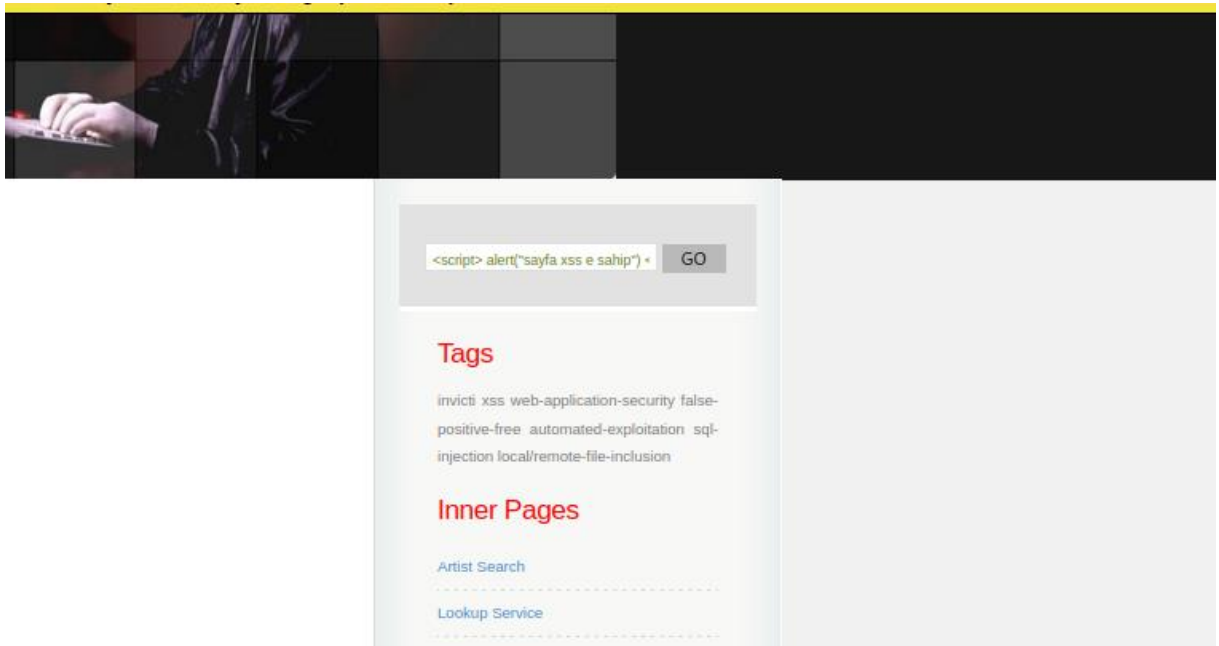
Bulgu Sebebi : Yapılandırma Eksikliği/Hatası

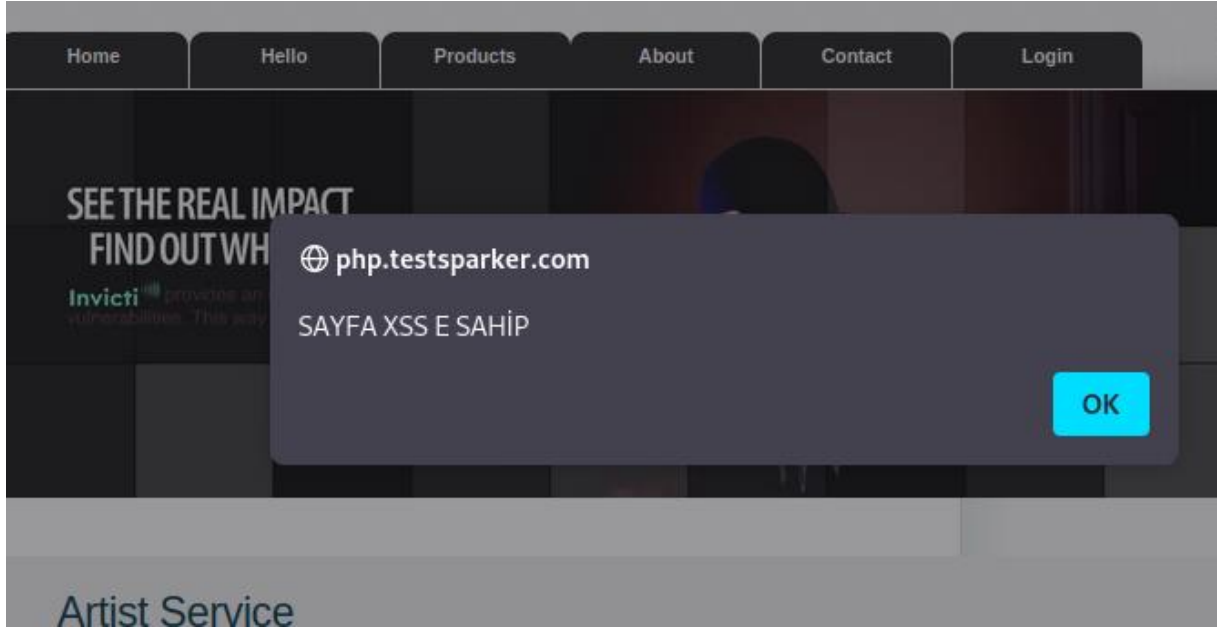
Bulgu Açıklaması:

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 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.

Aşağıdaki fotoğrafta ilgili websitesinin home alanındaki arama alanına script kodu girildiğinde script kodu engellenmemekte ve çalışmaktadır.Kullanıcı istediği bilgiyi ekrana basabilmektedir.





Yukarıdaki ekran görüntüsünde bahsedilen Reflected(Yansıyan) XSS saldırısına örnektir

Açıklığı Barındıran Sistem : <http://php.testsparker.com>

Cözüm Önerisi: Web uygulamalarında kullanıcının veri girişine izin verilen alanlarda filtreleme yaparak bu açıkları kapatabilirsiniz. Veri girişinin filtrelenmesi kadar veri çıkışının da incelenmesi web uygulamalarının güvenliğini arttıracaktır. Aşağıda belirtilen karakterlerin filtrelenmesi web uygulamaların güvenliğini sağlayacaktır.XSS sırasında kullanılan özel karakterler engellenebilir. Çerezlere “httponly” set edilmelidir.

Referanslar :

<https://bulutistan.com/blog/xss-cross-site-scripting-nedir/>

<https://www.ismailsaygili.com.tr/search/label/xss%20a%C3%A7%C4%B1%C4%9F%C4%B1%20kapatma>

Https (Güvenli Metin Aktarma Protokolü) Eksikliği

Önem Derecesi : Yüksek

Açıklığın Etkisi: Yetkisiz Erişim ve Bilgi İfşası

Erişim Noktası: Internet

Kullanıcı Profili : Anonim Kullanıcı

Bulgu Kategorisi : Web

Bulgu Sebebi : Yapılandırma Eksikliği

Bulgu Açıklaması:

Web sitesi üzerinde yapılan taramalarda internet protokolü olarak http kullandığı görülmüştür. Http eski bir teknoloji olup tasarlanma amacı olarak sadece veri taşımak için kullanılmaktadır. Veri güvenliği amacı taşımamaktadır. Https portu server ortamında açıktır.

Aşağıdaki ekran görüntüsü site ve sunucu arasındaki iletişim bilgilerinden alınmıştır.

```
2 Host: php.testsparker.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_
4 Accept: text/html,application/xhtml+xml,
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://php.testsparker.com/
8 Connection: close
```

Açıklığı Barındıran Sistem : <http://php.testsparker.com>

Çözüm Önerisi: Https (443) portu açık olduğu ve SSL sertifikası alarak sistem daha güvenli hale getirilmelidir. Http portu kapatılmalıdır.

Http Başlık Bilgileri İçerisinde Kullanıcı Adı ve Parola Taşınması

Önem Derecesi : Yüksek

Acıklığın Etkisi: Yetkisiz Erişim ve Bilgi Ifşası

Erişim Noktası: Internet

Kullanıcı Profili : Anonim Kullanıcı

Bulgu Kategorisi : Web

Bulgu Sebebi : Yapılandırma Eksikliği ve Hatası

Bulgu Açıklaması: Test gerçekleştirilen adresin http protokolünü kullandığı ve Http POST method ile iletilen http istekleri içerisinde kullanıcı adı ve parolanın http başlık bilgileri içerisinde taşındığı görülmüştür. Kullanıcı adı ve parolanın cleartext olarak token ile birlikte iletildiği tespit edilmiştir. Başarılı ve başarısız sonuçlar için elde edilen kullanıcı bilgileri aşağıdaki gibidir.

S...	Method	Domain	File	Initiator	Type	Transfe...	Size	Headers	Cookies	Request	Response	Timings
302	POST	php.testsparker.com	control.php	document	html	3.17 KB	2.79 KB					
200	GET	php.testsparker.com	internal.php	document	html	3.14 KB	2.79 KB					
404	GET	php.testsparker.com	favicon.ico	FaviconLoa...	html	cached	302 B					

3 requests

5.88 KB / 6.31 KB transferred

Finish: 1.39 s

DOMContentLoaded: 1.16 s

load: 1.20 s

Filter Request Parameters

Form data

username: "admin"

password: "admin123456"

token: "23483"

S...	Method	Domain	File	Initiator	Type	Transfe...	Size	Headers	Cookies	Request	Response	Timings
302	POST	php.testsparker.com	control.php	document	html	3.36 KB	2.99 KB					
200	GET	php.testsparker.com	login.php	document	html	3.34 KB	2.99 KB					
404	GET	php.testsparker.com	favicon.ico	FaviconLoa...	html	cached	302 B					

3 requests	6.27 KB / 6.70 KB transferred	Finish: 1.13 s	DOMContentLoaded: 1.10 s	load: 1.13 s
------------	-------------------------------	----------------	--------------------------	--------------

Açıklığı Barındıran Sistem : <http://php.testsparker.com>

Cözüm Önerisi: Protokol kullanımı olarak daha güvensiz olan http yerine https (güvenli aktarma protokolü) kullanılmalıdır. Https protokolü ve SSL, verilerin şifrelenerek sunucuya ulaşmasını sağlamaktadır.

SQL Injection

Önem Derecesi : Kritik

Açıklığın Etkisi: Yetkisiz Erişim ve Bilgi İfşası

Erişim Noktası: Internet

Kullanıcı Profili : Anonim Kullanıcı

Bulgu Kategorisi : Web

Bulgu Sebebi : Uygulama Geliştirmedeki Eksiklik ve Hata

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 Injection saldırıları, uygulamanın veri tabanına gönderdiği sorgularda herhangi bir yazım hatası syntax hatası olması durumunda veya sorgunun veri tabanında çalışması sonucu dönen verilerin, ekrana çıktı olarak verilmesi temeline dayanır.

http://php.testsparker.com adresi üzerinde sağ menüde Inner Pages > Artist Search kısmında tarayıcıdaki sorguya aşağıda belirtilen payloadı uyguladık.

URL :	http://php.testsparker.com/artist.php?id= 1 OR 1=1
HTTP TALEP TÜRÜ:	GET
PARAMETRE:	ID
PAYLOAD :	1 OR 1=1

Payload uygulandıktan sonra aşağıdaki sonuçlar alınmış ve database den veri çıkarılmıştır.

Results: 1 OR 1=1

ID	Name	SURNAME	CREATION DATE
2	NICK	WAHLBERG	2006-02-15 04:34:32
3	ED	CHASE	2006-02-15 04:34:32
4	JENNIFER	DAVIS	2006-02-15 04:34:32
5	JOHNNY	LOLLOBRIGIDA	2006-02-15 04:34:32
6	BETTE	NICHOLSON	2006-02-15 04:34:32
7	GRACE	MOSTEL	2006-02-15 04:34:32
8	MATTHEW	JOHANSSON	2006-02-15 04:34:32
9	JOE	SWANK	2006-02-15 04:34:32
10	CHRISTIAN	GABLE	2006-02-15 04:34:32
11	ZERO	CAGE	2006-02-15 04:34:32
12	KARL	BERRY	2006-02-15 04:34:32
13	UMA	WOOD	2006-02-15 04:34:32
14	VIVIAN	BERGEN	2006-02-15 04:34:32
15	CUBA	OLIVER	2006-02-15 04:34:32
16	FRED	COSTNER	2012-09-13 12:14:54 22
17	HELEN	VOIGHT	2012-09-13 12:14:54 22
18	DAN	TORN	2012-09-13 12:14:54 22
19	BOB	FAWCETT	2012-09-13 12:14:54 22
20	LUCILLE	TRACY	2012-09-13 12:14:54 22
21	KIRSTEN	PALTROW	2012-09-13 12:14:54 22
22	ELVIS	MARX	2012-09-13 12:14:54 22
23	SANDRA	KILMER	2012-09-13 12:14:54 22
24	CAMERON	STREEP	2012-09-13 12:14:54 22
25	KEVIN	BLOOM	2012-09-13 12:14:54 22
26	RIP	CRAWFORD	2012-09-13 12:14:54 22
27	JULIA	MCQUEEN	2012-09-13 12:14:54 22
28	WOODY	HOFFMAN	2012-09-13 12:14:54 22
29	ALEC	WAYNE	2012-09-13 12:14:54 22
30	SANDRA	PECK	2012-09-13 12:14:54 22
31	SISSY	SOBIESKI	2012-09-13 12:14:54 22
32	TIM	HACKMAN	2012-09-13 12:14:54 22
33	MILLA	PECK	2012-09-13 12:14:54 22
34	AUDREY	OLIVER	2012-09-13 12:14:54 22
35	JUDY	DEAN	2012-09-13 12:14:54 22
36	BURT	DUKAKIS	2012-09-13 12:14:54 22
37	VAL	BOLGER	2012-09-13 12:14:54 22
38	TOM	MCQUEEN	2012-09-13 12:14:54 22
39	GOLDIE	BRODY	2012-09-13 12:14:54 22
40	JOHNNY	CAGE	2012-09-13 12:14:54 22
41	JODIE	DEGENERES	2012-09-13 12:14:54 22
42	TOM	MIRANDA	2012-09-13 12:14:54 22

88	KENNETH	PESCI	2012-09-13 12:14:54 22
89	CHARLIZE	DENCH	2012-09-13 12:14:54 22
90	SEAN	GUINNESS	2012-09-13 12:14:54 22
91	CHRISTOPHER	BERRY	2012-09-13 12:14:54 22
92	KIRSTEN	AKROYD	2012-09-13 12:14:54 22
93	ELLEN	PRESLEY	2012-09-13 12:14:54 22
94	KENNETH	TORN	2012-09-13 12:14:54 22
95	DARYL	WAHLBERG	2012-09-13 12:14:54 22
96	GENE	WILLIS	2012-09-13 12:14:54 22
97	MEG	HAWKE	2012-09-13 12:14:54 22
98	CHRIS	BRIDGES	2012-09-13 12:14:54 22
99	JIM	MOSTEL	2012-09-13 12:14:54 22
100	SPENCER	DEPP	2012-09-13 12:14:54 22
101	SUSAN	DAVIS	2012-09-13 12:14:54 22
102	WALTER	TORN	2012-09-13 12:14:54 22
103	MATTHEW	LEIGH	2012-09-13 12:14:54 22
104	PENELOPE	CRONYN	2012-09-13 12:14:54 22
105	SIDNEY	CROWE	2012-09-13 12:14:54 22
106	GROUCHO	DUNST	2012-09-13 12:14:54 22
107	GINA	DEGENERES	2012-09-13 12:14:54 22
108	WARREN	NOLTE	2012-09-13 12:14:54 22
109	SYLVESTER	DERN	2012-09-13 12:14:54 22
110	SUSAN	DAVIS	2012-09-13 12:14:54 22
111	CAMERON	ZELLWEGER	2012-09-13 12:14:54 22
112	RUSSELL	BACALL	2012-09-13 12:14:54 22
113	MORGAN	HOPKINS	2012-09-13 12:14:54 22
114	MORGAN	MCDORMAND	2012-09-13 12:14:54 22
115	HARRISON	SALE	2012-09-13 12:14:54 22
116	DAN	STREEP	2012-09-13 12:14:54 22
117	RENEE	TRACY	2012-09-13 12:14:54 22
118	CUBA	ALLEN	2012-09-13 12:14:54 22
119	WARREN	JACKMAN	2012-09-13 12:14:54 22
120	PENELOPE	MONROE	2012-09-13 12:14:54 22
121	LIZA	BERGMAN	2012-09-13 12:14:54 22
122	SALMA	NOLTE	2012-09-13 12:14:54 22
123	JULIANNE	DENCH	2012-09-13 12:14:54 22
124	SCARLETT	BENING	2012-09-13 12:14:54 22
125	ALBERT	NOLTE	2012-09-13 12:14:54 22
126	FRANCES	TOMEI	2012-09-13 12:14:54 22
127	KEVIN	GARLAND	2012-09-13 12:14:54 22
128	CATE	MCQUEEN	2012-09-13 12:14:54 22
129	DARYL	CRAWFORD	2012-09-13 12:14:54 22
130	GRETA	KEITEL	2012-09-13 12:14:54 22
131	JANE	JACKMAN	2012-09-13 12:14:54 22
132	ADAM	HOPPER	2012-09-13 12:14:54 22

42	TOM	MIRANDA	2012-09-13 12:14:54 22
43	KIRK	JOVNOVICH	2012-09-13 12:14:54 22
44	NICK	STALLONE	2012-09-13 12:14:54 22
45	REESE	KILMER	2012-09-13 12:14:54 22
46	PARKER	GOLDBERG	2012-09-13 12:14:54 22
47	JULIA	BARRYMORE	2012-09-13 12:14:54 22
48	FRANCES	DAY-LEWIS	2012-09-13 12:14:54 22
49	ANNE	CRONYN	2012-09-13 12:14:54 22
50	NATALIE	HOPKINS	2012-09-13 12:14:54 22
51	GARY	PHOENIX	2012-09-13 12:14:54 22
52	CARMEN	HUNT	2012-09-13 12:14:54 22
53	MENA	TEMPLE	2012-09-13 12:14:54 22
54	PENELOPE	PINKETT	2012-09-13 12:14:54 22
55	FAY	KILMER	2012-09-13 12:14:54 22
56	DAN	HARRIS	2012-09-13 12:14:54 22
57	JUDE	CRUISE	2012-09-13 12:14:54 22
58	CHRISTIAN	AKROYD	2012-09-13 12:14:54 22
59	DUSTIN	TAUTOU	2012-09-13 12:14:54 22
60	HENRY	BERRY	2012-09-13 12:14:54 22
61	CHRISTIAN	NEESON	2012-09-13 12:14:54 22
62	JAYNE	NEESON	2012-09-13 12:14:54 22
63	CAMERON	WRAY	2012-09-13 12:14:54 22
64	RAY	JOHANSSON	2012-09-13 12:14:54 22
65	ANGELA	HUDSON	2012-09-13 12:14:54 22
66	MARY	TANDY	2012-09-13 12:14:54 22
67	JESSICA	BAILEY	2012-09-13 12:14:54 22
68	RIP	WINSLET	2012-09-13 12:14:54 22
69	KENNETH	PALTROW	2012-09-13 12:14:54 22
70	MICHELLE	MCCONAUHAY	2012-09-13 12:14:54 22
71	ADAM	GRANT	2012-09-13 12:14:54 22
72	SEAN	WILLIAMS	2012-09-13 12:14:54 22
73	GARY	PENN	2012-09-13 12:14:54 22
74	MILLA	KEITEL	2012-09-13 12:14:54 22
75	BURT	POSEY	2012-09-13 12:14:54 22
76	ANGELINA	ASTAIRE	2012-09-13 12:14:54 22
77	CARY	MCCONAUHAY	2012-09-13 12:14:54 22
78	GROUCHO	SINATRA	2012-09-13 12:14:54 22
79	MAE	HOFFMAN	2012-09-13 12:14:54 22
80	RALPH	CRUZ	2012-09-13 12:14:54 22
81	SCARLETT	DAMON	2012-09-13 12:14:54 22
82	WOODY	JOLIE	2012-09-13 12:14:54 22
83	BEN	WILLIS	2012-09-13 12:14:54 22
84	JAMES	PITT	2012-09-13 12:14:54 22
85	MINNIE	ZELLWEGER	2012-09-13 12:14:54 22
86	GREG	CHAPLIN	2012-09-13 12:14:54 22

131	JANE	JACKMAN	2012-09-13 12:14:54 22
132	ADAM	HOPPER	2012-09-13 12:14:54 22
133	RICHARD	PENN	2012-09-13 12:14:54 22
134	GENE	HOPKINS	2012-09-13 12:14:54 22
135	RITA	REYNOLDS	2012-09-13 12:14:54 22
136	ED	MANSFIELD	2012-09-13 12:14:54 22
137	MORGAN	WILLIAMS	2012-09-13 12:14:54 22
138	LUCILLE	DEE	2012-09-13 12:14:54 22
139	EWAN	GOODING	2012-09-13 12:14:54 22
140	WHOOPI	HURT	2012-09-13 12:14:54 22
141	CATE	HARRIS	2012-09-13 12:14:54 22
142	JADA	RYDER	2012-09-13 12:14:54 22
143	RIVER	DEAN	2012-09-13 12:14:54 22
144	ANGELA	WITHERSPOON	2012-09-13 12:14:54 22
145	KIM	ALLEN	2012-09-13 12:14:54 22
146	ALBERT	JOHANSSON	2012-09-13 12:14:54 22
147	FAY	WINSLET	2012-09-13 12:14:54 22
148	EMILY	DEE	2012-09-13 12:14:54 22
149	RUSSELL	TEMPLE	2012-09-13 12:14:54 22
150	JAYNE	NOLTE	2012-09-13 12:14:54 22
151	GEOFFREY	HESTON	2012-09-13 12:14:54 22
152	BEN	HARRIS	2012-09-13 12:14:54 22
153	MINNIE	KILMER	2012-09-13 12:14:54 22
154	MERYL	GIBSON	2012-09-13 12:14:54 22
155	IAN	TANDY	2012-09-13 12:14:54 22
156	FAY	WOOD	2012-09-13 12:14:54 22
157	GRETA	MALDEN	2012-09-13 12:14:54 22
158	VIVIAN	BASINGER	2012-09-13 12:14:54 22
159	LAURA	BRODY	2012-09-13 12:14:54 22
160	CHRIS	DEPP	2012-09-13 12:14:54 22
161	HARVEY	HOPE	2012-09-13 12:14:54 22
162	OPRAH	KILMER	2012-09-13 12:14:54 22
163	CHRISTOPHER	WEST	2012-09-13 12:14:54 22
164	HUMPHREY	WILLIS	2012-09-13 12:14:54 22
165	AL	GARLAND	2012-09-13 12:14:54 22
166	NICK	DEGENERES	2012-09-13 12:14:54 22
167	LAURENCE	BULLOCK	2012-09-13 12:14:54 22
168	WILL	WILSON	2012-09-13 12:14:54 22
169	KENNETH	HOFFMAN	2012-09-13 12:14:54 22
170	MENA	HOPPER	2012-09-13 12:14:54 22
171	OLYMPIA	PFEIFFER	2012-09-13 12:14:54 22
172	GROUCHO	WILLIAMS	2012-09-13 12:14:54 22
173	ALAN	DREYFUSS	2012-09-13 12:14:54 22
174	MICHAEL	BENING	2012-09-13 12:14:54 22
175	WILLIAM	HACKMAN	2012-09-13 12:14:54 22

165	AL	GARLAND	2012-09-13 12:14:54 22
166	NICK	DEGENERES	2012-09-13 12:14:54 22
167	LAURENCE	BULLOCK	2012-09-13 12:14:54 22
168	WILL	WILSON	2012-09-13 12:14:54 22
169	KENNETH	HOFFMAN	2012-09-13 12:14:54 22
170	MENA	HOPPER	2012-09-13 12:14:54 22
171	OLYMPIA	PFIEFFER	2012-09-13 12:14:54 22
172	GROUCHO	WILLIAMS	2012-09-13 12:14:54 22
173	ALAN	DREYFUSS	2012-09-13 12:14:54 22
174	MICHAEL	BENING	2012-09-13 12:14:54 22
175	WILLIAM	HACKMAN	2012-09-13 12:14:54 22
176	JON	CHASE	2012-09-13 12:14:54 22
177	GENE	MCKELLEN	2012-09-13 12:14:54 22
178	LISA	MONROE	2012-09-13 12:14:54 22
179	ED	GUINNESS	2012-09-13 12:14:54 22
180	JEFF	SILVERSTONE	2012-09-13 12:14:54 22
181	MATTHEW	CARREY	2012-09-13 12:14:54 22
182	DEBBIE	AKROYD	2012-09-13 12:14:54 22
183	RUSSELL	CLOSE	2012-09-13 12:14:54 22
184	HUMPHREY	GARLAND	2012-09-13 12:14:54 22
185	MICHAEL	BOLGER	2012-09-13 12:14:54 22
186	JULIA	ZELLWEGER	2012-09-13 12:14:54 22
187	RENEE	BALL	2012-09-13 12:14:54 22
188	ROCK	DUKAKIS	2012-09-13 12:14:54 22
189	CUBA	BIRCH	2012-09-13 12:14:54 22
190	AUDREY	BAILEY	2012-09-13 12:14:54 22
191	GREGORY	GOODING	2012-09-13 12:14:54 22
192	JOHN	SUVARI	2012-09-13 12:14:54 22
193	BURT	TEMPLE	2012-09-13 12:14:54 22
194	MERYL	ALLEN	2012-09-13 12:14:54 22
195	JAYNE	SILVERSTONE	2012-09-13 12:14:54 22
196	BELA	WALKEN	2012-09-13 12:14:54 22
197	REESE	WEST	2012-09-13 12:14:54 22
198	MARY	KEITEL	2012-09-13 12:14:54 22
199	JULIA	FAWCETT	2012-09-13 12:14:54 22
200	THORA	TEMPLE	2012-09-13 12:14:54 22
412	-1 OR 1=1	test	2012-09-13 12:14:54 22
413	-1 OR 1=1	test	2012-09-13 12:14:54 22
414	NSINO	test	2012-09-13 12:14:54 22
415	1 AND NS="ns	test	2012-09-13 12:14:54 22
416	" OR "ns"="ns	test	2012-09-13 12:14:54 22
417	-1 OR 17=10	test	2012-09-13 12:14:54 22
418	1 OR X="ns	test	2012-09-13 12:14:54 22
419	" OR "1"=1	test	2012-09-13 12:14:54 22
420	" OR "1"=1	test	2012-09-13 12:14:54 22

Cözüm 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 girdilerdeki bütün meta 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.nextgenss.com/papers/advanced_sql_injection.pdf

EK-1 : Raporda Geçen Teknik Terimler ve Kısaltmalar

-**Domain:** Alan adı, bir Web sitesinin İnternet'teki adı ve adresidir

-**Subdomain:** Alt alan adı, bir ana alan adına bağlı olan alt alanlardır.

-**Syntax:** Bilgisayar biliminde, bir bilgisayar dilinin sözdizimi, o dilde doğru yapılandırılmış ifadeler veya ifadeler olarak kabul edilen sembollerin kombinasyonlarını tanımlayan kurallar kümesidir.

-**Cleartext:** Açıkça anlaşılabilen, şifrelenmemiş bilgi.

-**Token:** Tek kullanımlık yaşam süresi olan hashlenmiş yada şifrelenmiş bir bilgi içeren metinlerdir.

-**Script:** Betik dili, betik yorumlamak için yazılmış özel çalışma-zamanı sistemlerinin yorumlayabileceği programlama dilleridir.

-**Header:** Başlık

-**Port(sanal):** Bilgisayar kullanırken ağ ve internet üzerinde veya bir yazılım vasıtasıyla yönlendirilen mantıksal bağlantı noktalarıdır.

EK-2 : Güvenlik Testleri Esnasında Kullanılan Araçlar

-Nikto

-Gobuster

-BurpSuite

-Http Header Live