Acunetix ile Vulnerable Uygulama Tarama ve Gelen Zararlı Trafiği Dinleme

Bu makalede bir web zafiyet tarayıcısı yazılımıyla bir başka makinadaki zafiyetli web uygulamasının taranması ve bu tarama esnasında üretilen zararlı trafiğin karşı sistemce (zafiyete sahip web uygulamasının olduğu tarafça) dinlenmesi & dosyalanması gösterilmektedir.

Bu bahsedilen işlemler sırasında takip edilen adımlar şu şekildedir:

[Acunetix Tarafı]

a. Hedef web uygulaması iki yetkilendirme geçiş noktasına (http basic ve web app login) sahip olduğundan acunetix'e bu iki aşamayı geçebileceği kuralları öğretmemiz gerekmektedir.

-> Http basic yetkilendirmesi tarayıcıdan geçilir ve gelen çerez Acunetix-> Advanced->Custom Headers kısmına olduğu gibi (Authorization: sdlkfjdsklfjds) eklenir.

-> Ardından; web uygulamasında çeşitli aksiyonlar çerezler üzerinden gerçekleşiyorsa (örn; dvwa'da uygulama davranışı security çerezi üzerinden değişiklik arz etmekte) o zaman tarayıcıda uygulama oturumunu açıp F12 ile uygulama davranışını etkileyen çerezler etkin oldukları dizin yoluyla beraber (örn; dvwa'da security çerezi /dvwa dizininde etkinken PHPSESSID çerezi / dizininde etkindir) Acunetix->Advanced->Custom Cookies kısmına aşağıdaki gibi eklenmelidir.

Custom Cookies:

[url]	[çerezIsmi]=[çerezDegeri]
[url2]	[çerezIsmi2]=[çerezDegeri2]

-> Ardından; Acunetix taramaya başladığında hedef web uygulamasında oturum açabilmesi ve içeriyi de tarayabilmesi için Acunetix->General->Login Recorder->Use pre-recorded login sequence->New seceneği kullanılmalıdır. Gelen login olma adımları penceresinde ilk aşamada Login panelin yer aldığı URL, pencerenin adres çubuğuna ENTER'lanmalıdır. Sonra, gelen login panele hesap bilgileri girilmelidir ve oturum aç butonuna basılarak oturum açılmalıdır. Bu yapılan (gerçekleştirilen) adımlar sağ yan boşlukta satır satır sıralanır. Login islemi sonrası Next diyerek bir sonraki aşamaya (logout adımını gösterme aşamasına) geçilir ve logout butonuna / butonlarına tıklanarak "Restrict Request Using Exact Match" denir. Bu sayede acunetix logout yapan noktaları öğrenmiş olur. Bu logout vapan verler isaretlenerek (tıklanarak) sağ van boslukta satır satır sıralanacaktırlar. Ardından Next diyerek son aşamaya (yani login ve sonra logout aşamalarındaki adımlar / mekanizmalar sorunsuz çalışıyor mu testi aşamasına) geçilir ve ekrana "...successfully..." popup'ı gelir. Böylece iki aşamada sorun olmadığı görülür. Son olarak bulunulan aşamadaki (yani son aşamadaki) yan sağ boşlukta yer alan url incelenmelidir. Bu url acunetix'in tarama esnasında oturumu kaybedip kaybetmediğini test etmek için kullanacağı bir url olacaktır. Bu url sadece oturum açıkken erişilebilen bir url olmalıdır. Böylece acunetix tarama esnasında bu url'i test ederek halen oturumda mıyım yoksa oturum (örn; timeout gibi) bir nedenden dolayı sonlandırılmış mı kontrolü yapabilecektir. Sadece login'ken erişilebilen bir url, o boslukta url verine girilir ve Check Pattern ile girdiğimiz url'de problem / erişimde sıkıntı var mı kontrolü yapılarak son aşama tamamlanır. Ekrana gelen "...pattern verified..." popup'ı sonrası Finish diyerek Login Recorder işlemi tamamlanır.

b. Hedef web uygulamasında tarama esnasında tarama dışında tutulacak dizin ve dosya yolları için Acunetix->Crawl sekmesine gelinir ve Exclude Paths seçeneğine regexp pattern formatında dosya ve dizin yolları girilir. Bu, uygulamanın yapısında değişikliğe sebep olabilecek ve istenmeyen aktivitelere yol açabilecek (örn; uygulama veritabanını sıfırlama, uygulama hesap parolasını değiştirme,... gibi) dosya ve dizin yollarının tarama dışında tutulmasını sağlamak için vardır. Böylece Acunetix, uygulamanın yapısını bozmayak şekilde tarama yapabilir.

[Dvwa Tarafı]

a. Dvwa yüklü sanal makinanın ayakta olduğu tarafta wireshark açılır ve acunetix tarafından gelen trafik dinleme durumuna geçilir (wireshark filtresi: ip.src == acunetix_ip and ip.dst == dvwa_sanal_makina_ip).

b. Acunetix tarafından test amaçlı ping ile icmp paketleri DVWA tarafına gönderilir ve dvwa yüklü sanal makinanın olduğu tarafta wireshark icmp paketlerini görüntüler.

c. Wireshark ekranına sadece ama sadece acunetix tarafıdan gelen trafiğin gelebildiği görüldüğünde (yani filtrenin doğru şekilde çalıştığı görüldüğünde) göre acunetix taraması başlatılır.

d. Wireshark ekranına acunetix trafiği düşer ve nihayetinde tarama bittiğinde wireshark ekranına düşen son paket RST paketi olur. Böylece acunetix tarafı son yolladığı http talep paketinin tcp el sıkışmasını sürdürmek yerine artık sonlandırmış olur. Çünkü tarama, biter.

e. Wireshark ekranında listelenen acunetix trafiği dosyalanabilir. Böylece saf bir zararlı trafik dosya halinde toplanabilir (örn; *trafficComingFromAcunetix.pcap*).

f. (optional) Tarama sonrası wireshark ekranındaki filtrelemeyi

wireshark filtresi: ip.src == acunetix_ip and ip.dst == dvwa_sanal_makina_ip

yerine

wireshark filtresi: ip.src == dvwa_sanal_makina_ip and ip.dst == acunetix_ip

yaparak (yani ters düz ederek) acunetix tarafından gelen tarama paketlerine karşılık dvwa tarafının döndüğü paketleri ekranda listeleyebilir ve dvwa tarafının saldırı altındayken döndüğü yanıtları (yani dvwa'nın mukavemeti) bir dosya halinde toplanabilir (örn; *replyTrafficToAcunetixMachine.pcap*).

Uygulama

(+) Birebir denenmiştir ve başarılı olunmuştur.

Kişisel iş laptop'ımda wireshark çalıştırılacaktır ve bir yandan da aynı laptop'ımda DVWA yüklü ubuntu server sanal makinası ayağa kaldırılacaktır. Karşı taraftan (workstation iş laptop'ımdan) Acunetix çalıştırılacaktır ve kişisel iş laptop'ımdaki sanal makinada yer alan DVWA taramaya tabi tutulacaktır. DVWA yüklü sanal makinanın ayağa kaldırıldığı kişisel iş laptop'ımda wireshark ile Acunetix tarafından gelen trafik dinlenecektir. Kullanılan Araçlar

Wireshark - Ubuntu 18.04 LTS	// Kişisel Laptop	(Ana Makina)
DVWA - iK Test Makinesi (yt.14-6-19)	// Kişisel Laptop	(Sanal Makina)
Acunetix Scanner	// XYZ İŞ Laptop	(Diğer Makina)

Şimdi; xyz iş laptop'ımdan kişisel laptop'ımda ayağa kaldırılmış dvwa yüklü sanal makinadaki uygulamaya bir erişelim.

Workstation Laptop:

http://X.Y.Z.T

Acunetix-Kopyalama! - VMware Workstat	lion		٥	\times
File Edit View VM Tabs Help				
Library ×	192.168.0.28 × +	-	٥	×
C Type here to search C Type here to search Image: My Computer Image: My Computer Image:	 ← → C () 192.168.0.28 Oturum açın http://192.168.0.28 Bu siteye bağlantınız gizi değil Kullanıcı adı Şifre 	¥ 🥹	٢	I
	Oturum agn iptat	탄 뛰 4》 230	¹² [

(Hedef Web Uygulamasına Gitme)

Dvwa yüklü hedef web sunucu http basic yetkilendirme ile geçiş kontrolü yapmaktadır. Bilgileri (kullanıcı adı: admin, şifre: toka) girip bu yetkinlendirme aşamasını geçelim.

File Edit View VM Tabs Help I			
Library × + Q. Type here to search •			
Q Type here to search ✓ Image: Searc	-	٥	×
Wy Computer Acunetia: Kopyalanal WebScan-Netsparker PENTEST_PORTAL_2 http://192.168.028	0		
Pertet-Kali-201/ Bu siteye bağlantnız gizli değil Kullanıcı adı admin Şire ind Oturum açıı iptai) 233	02	

(Hedef Web Uygulaması Basic Yetkilendirmesine Bilgileri Girme)

Acunetix-Kopyalama! - VMware Workstat	ion		– • ×
File Edit View VM Tabs Help	III - 🖶 🖓 🖓 🖓 I 🖬 🖬 🗖		
Library ×	③ Index of / × +		– 0 ×
C Type here to search	← → C ① Güvenli değil 192.168.0.28		아 ☆ 🕹 😩 ፤
	Index of /		
Pentest-Kan-2017	Name	Last modified Size Description	
	Autocomplete Credential Calma Humilamaci/	2019 04 07 06-14	
	Phishing by Navigating Browser Tabs Uvgular	2019-04-07 06:14 -	
	Second Order Sol Injection Uvgulaması/	2019-04-07 06:14 -	
	WebGoat-5.4.zip	2018-07-11 15:31 113M	
	WebGoat-5.4/	2012-04-27 16:29 -	
	n 2 aaa	2019-04-26 09:48 246	
	backdoor.php	2019-04-26 19:38 571	
	dvwa/	2019-04-27 03:03 -	
	Apache/2.4.7 (Ubuntu) Server at 192.168.0.28 F	Port 80	2202
	🛋 🔎 🖽 🤤 😫 🌍 🖡	• • • • • • • • • • • • • • • • • • •	x ^R ^ D 닫 에 ^{23:03} 모

(Hedef Web Uygulaması Arayüzü Birden Fazla Uygulama İçerdiğini Gösterir)

Hedef sunucu test makinası olduğu için bir çok web uygulaması ve ilaveten web script'leri yer almaktadır. DVWA'ya gidelim.

Acunetix-Kopyalama! - VMware Workstat	ion	– o ×
File Edit View VM Tabs Help		
Library ×	📀 Login :: Damn Vulnerable Web A; x +	- 0 ×
Q Type here to search •	← → C ① Güvenli değil 192.168.0.28/dvwa/login.php	☆ 🥹 😩 :
 My Computer My Computer WebScan-Netspankar PRNTEST PORTAL_2 Pentest-Kali-2017 Shared VMs 	Username Password Login	
	Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project.	Ţ
	^ جم 🔰 🚦 🚺 🖬 🚺 🖬 🖗	した。 この3 23:03 21.06.2019

(DVWA Login Sayfası Gelir)

DVWA login ekranına giriş bilgilerini (kullanıcı adı: admin, şifre: password) girerek uygulamada oturum açalım.



(DVWA Login Ekranında Oturum Bilgileriyle Giriş Yapılır)



(DVWA Web Uygulaması Erişimi Tamamlanır)

Acunetix ile hedef web uygulaması DVWA'yı tarayabilmek için hedef makinada iki adet yetkilendirme aşamasından geçtik. Dolayısıyla Acunetix'e bu geçişleri yapabileceği kuralları girmemiz gerekmektedir.

XYZ İş Laptop:

https://localhost:3443/#/dashboard/

(*) Acunetix Web Arayüzünü Açar

Acunetix-Kopyalama! - VMware Workstat	tion					- 0	×
File Edit View VM Tabs Help	• ⊕ ₽ ₽ ₽						
Library ×	👩 Acunetix - Dashboard	× +				- 0	×
V Type here to search	← → C 🔒 https://local#	nost:3443/#/dashboard/				or 🕁 🥹) :
Wry Computer Acunetix-Kopyalamal webScan-Netsparker PINTEST_PORTAL_2 Pentest-Kali-2017	nacunetix					EMRE OZKOK 👻 🥹	P
D Shared VMs	Ē						Â
	🏠 Dashboard						
	⊙ Targets	22		190		34	
	🕷 Vulnerabilities						
	🕍 Scans	High Severity Vulr	erabilities Med	ium Severity Vulnerab	ilities Low Sever	ity Vulnerabilities	
	🖹 Reports						
	🌣 Settings	Scans Running	Scans Waiting	Total Scans Conducted	Open Vulnerabilities	Total Targets	
		0	0	13	246	4	
	© 2019 Acunetix Ltd						*
						16:45	
	🕂 🔎 🛱 🧲 🍯	O			Ŕ	く へ し に の 21.06.2019	\Box

Acunetix'e hedef web uygulaması adresi girilir.

Acunetix-Kopyalama! - VMware Workstat	ion		– o ×
File Edit View VM Tabs Help	📕 🗸 🖶 🖓 💭 💭 🗖		
Library ×	👩 Acunetix - Targets	× +	– 0 ×
C Type here to search -	$\leftarrow \rightarrow C$ https://localh	nost3443#/	야 삶 🙆 😩 :
□ ■ My Computer ④ Acunetic Kopyalamal ④ webScan-Netsparker ④ PENTEST_PORTAL_2 ④ Pentest-Kali-2017 ④ Shared VMs	acunetix	Add Target	EMRE OZKOK - Ø 🌲
	Œ	Address	ort CSV Tilter
	🏟 Dashboard	http://192.168.0.28/ <u>dvwa</u> /	
		h Description	nned on Jun 21, 2019 6:09:28 PM
			nned on Jun 21, 2019 5:18:27 PM
	}nn€ Vulnerabilities	<u></u> h	ined
	🕍 Scans	Add Target	nned on Jun 20, 2019 6:06:20 PM (Abortec Close
			nned on Jun 20, 2019 6:01:13 PM (Aborted
	🖹 Reports		
	🍄 Settings		
			• • • • • • • • • • • • • • • • • • •
	© 2019 Acunetix Ltd		
			23:12 D
	🕂 🖓 🗄 🤘		ダ へ D, 臣 印) 21.06.2019 レ

Acunetix-Kopyalama! - VMware Workstati	ion	- 0 ×
File Edit View VM Tabs Help	▼ ♣ ♀ ♀ ∎ ⊒ ≒ ⊑ ⊒	
Library ×	🙃 Acunetix - Configure Target - htt; 🗙 🕂	– 0 ×
C Type here to search -	← → C 🔒 https://localhost:3443/#/targets/6f54c860-d1c2-4993-b7ae-57d0b18871ad/general/?return	Url=%252F 🕶 🛠 🥴 😩 🗄
My Computer My Computer Comparison of the second	acunetix	емге одкок 👻 🥥 🌲
🛱 Shared VMs	T Can Save	
	Dashboard General Crawl HTTP Advanced	
	Target Info	
	Le Scans http://192.168.0.28/dvwa	/
	Reports Description	
	Settings Business Criticality Normal	•
	Scan Speed Slower Slow Mod	erate Fast
	© 2019 Acunetix Ltd	
	📲 🔎 🖽 🤮 🧕 🧑 🚍 👔	x ⁹ ヘ ট 탇 네) 23:13 모 21.06.2019 모

Tarama profilindeki Advanced sekmesine gelinir ve Custom Headers açılır. Bu seçenek ile hedef uygulama adresindeki http basic yetkilendirme aşaması geçildiğinde gelen çerezi ekleme işlemi uygulanacaktır.

UYARI:

Eğer HTTP Basic yetkilendirme çerezini önce bu bölüme koymazsan Acunetix'in Login Recorder seçeneğini kullanarak yazılıma Web App Login panelde login olma adımlarını öğretemezsin. Çünkü web app login'den önce bir başka yetkilendirme aşaması olan http basic yetkilendirmesi vardır. Acunetix ise http basic çerezini almadan web app login panelini göremeyeceğinden popup ile uyarı verecektir: "Lütfen Http Basic çerezi eklemesinde bulununuz". Dolayısıyla önce http basic yetkilendirme aşaması geçildiğinde gelen çerez Custom Headers alanına eklenir. Sonra Login Recorder kısmına geçip web app login panelde login olma adımları uygulanabilir.



Acunetix tarafından hedef uygulamaya tarayıcıdan erişilir ve http basic ekranı bizi karşılar.

Acunetix-Kopyalama! - VMware Worksta	ation		– o >	×
File Edit View VM Tabs Help	🛯 🗸 🖶 🖓 🙄 🚺			
Library ×	• Yeni Sekme 🛛 🗙	+	- a >	×
Library x Q. Type here to search • My Computer Acunetic Kopyalamal WebScan-Netsparker PENTEST PORTAL 2 Photest-Kali-2017 Shared VMs	• Yeni Sekme ×	Kimlik doğrulama gerekli X Image: State of the state of	- 5 >	×
	192.168.0.28 bekleniyor	\$ (5) (5)	^{23:16} ~ ①]

İlgili bilgiler (iK Test Makinesi http basic kullanıcı adı: admin, şifre: toka) girilir .

C Acunetix-Kopyalamal - VMware Workstation		٥	×
File Edit View VM Tabs Help 📙 🗸 🖶 💭 💭 💭 🔲 📟 🖽 🔁 📷			
Library × Yeni Sekme × +	-	٥	×
Image: Search Wight of the search with search		23:16	
	× ~ U E V 2	1.06.2019	~~

Hedef uygulama ekranına girildiğinde birçok alt uygulama olduğu görülecektir. DVWA uygulamasına dallanalım.



(Test Amaçlı Konulmuş Birden Fazla Uygulama Listelenir)

Acunetix-Kopyalama! - VMware Workstat	ion			-	٥	×
File Edit View VM Tabs Help	- ⊕ ₽ ₽ ₽ ■					
Library ×	Login :: Damn Vulnerable Web Appl 🗙	+		-	٥	×
Q Type here to search	← → ♂ ☆	🛈 🔏 192.168.0.28/dvwa/login.php	⊠ ☆	\		≡
Acuneta-Kopyalama		DVWA				^
		Username				
		Password				
		Login				
						ļ
		Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project.				~
	🔳 오 🛱 🤮 🔮	0 🖬 🧕	\$ ^ D D	(1)) 23: (1)) 21.06	17 2019 [
		(DVWA Login Paneli)				

DVWA uygulama hesap bilgileri (kullanıcı adı: admin, şifre: password) girilir.



(DVWA Login Noktası Bilgileri Girilir)

DVWA'da oturum açılır.



Artık tarayıcıdan DVWA'nın içerisine kadar girebildiğimize göre bu aşamada elimizdeki http basic ve sonra DVWA uygulama çerezini (çünkü DVWA'nın security seviyesi çerezi var ve bu tarama esnasında bize lazım olabilecek bir çerez) alıp Acunetix'e ekleyelim.

Aşağıda basic yetkilendirme çerezini almak için Burp ile tarayıcı trafiğinin arasına girip tarayıcı sayfasının yenilendiği gösterilmiştir.



Burp ekranına http talebi gelir.

Acunetix-Kopyalama! - VMware Worksta	tion	-	٥	×
File Edit View VM Tabs Help	II + 🖶 🖓 😩 💭 🔲 🖬 🖽 🛅			
Library × Q. Type here to search	Burp Suite Community Edition v1.7.36 - Temporary Project Burp Inituder Repeater Window Help	-	٥	×
Image: Big My Computer Image: Big My Computer <	Target Proof Splder Scanne Intruder Repeater Sequence Decoder Comparer Extender Project options User options Alerts Intercept HTTP hidror WebSockets history Options Options Intercept Interce	Comment this ite	-11	?
	GTT: / Arma/ index_php NTTP/1.1 Disr: 15.1.60.0.20 Uss: 15.1.60.0.20 Uss: 15.1.60.0.20 Uss: 16.0.100 Uss: 15.1.60.0.20 Uss: 15.1.7.7.7.7.7.7.7.7.7.7.7.7.7.7.7.7.7.7			*
	2 < + > Type a search terr		0 п	natches
	، 🖈 📃 🚺 🥥 🛄 🌖 🕌 🖉 👘	へ 🗓 🖫 🕬 23: 21.06	21 2019 [\Box

Custom Headers'a burp ile tuttuğumuz http talebindeki Authorization başlığı ilave edilir.



Acunetix-Kopyalama! - VMware Workstati	ion	– 🗆 ×
File Edit View VM Tabs Help	II • \$\oplus \$\oplus \oplus \oplus \$\oplus \oplus \oplus \oplus \oplus \$\oplus \oplus \oplus \oplus \oplus \$\oplus \oplus	
Library ×	🙃 Acunetix - Configure Target - htt; 🗙 🕂	- 0 ×
C Type here to search	← → C https://localhost:3443/#/targets/6f54c860-d1c2-4993-b7ae-57d0b18871ad/advanced/?returnUrl=%252F	여 ☆ 🙂 🗄 :
My Computer Acunetix-Kopyalamal webScan-Netsparker PENTEST_PORTAL_2 Pentest-Kali-2017	acunetix	EMRE OZKOK 🗸 🥹 🌲
ው Shared VMs	E Can Save	
	Dashboard General Crawl HTTP Advanced	Î
	⊘ Targets	
	₩ Vulnerabilities	
	🗠 Scans Custom Headers	
	Example: X-My-Header: My-Value Add	
	Settings Authorization: Basic YWRtaW45dG9rYQ== Remove	
	© 2019 Acunetix Ltd	
	# 2 目 😋 🧕 🧰 🧕 🤱	x ^Q ^ ① 문 예 ^{23:46} 모 21.06.2019 모

Acunetix aynı sayfada yer alan Custom Cookies'e ise tarayıcıda F12 yaparak uygulama çerezleri konur.





Acunetix-Kopyalama! - VMware Workstati	ion	-	٥	×
File Edit View VM Tabs Help				
Library ×	🙃 Acunetix - Configure Target - htt; 🗴 🕂	-	٥	×
C Type here to search	$\leftarrow \rightarrow \mathbf{C}$ \blacksquare https://localhost:3443/#/targets/6f54c860-d1c2-4993-b7ae-57d0b18871ad/advanced/treturnUrl=%252F	ন 🕁 🍪		:
My Computer Acunetix-Kopyalamal webScan-Netsparker PENTEST_PORTAL_2 Pentest-Kali-2017	acunetix	EMRE OZKOK 👻	Θ	
印 Shared VMs	E Scan Save			
	Dashboard Example: X-My-Header: My-Value Add			*
	Targets Authorization: Basic YWRtaW46dG9rYQ== Remove			
	新 Vulnerabilities			
	🗠 Scans Custom Cookies			
	Reports I Crawler can be instructed to use your custom cookie values. Insert your custom cookies below.			
	Settings http://192.168.0.28 PHPSESSID=7vmgmp6fu4mki2su8b2crppsv4	Ado	d	
	© 2019 Acunetix Ltd			Ŧ
			:48	
	Å 🚺 🥝 🔜 😲 😓 🛱 🎗 📲	へ [〕 [記 dii) 21.06	.2019	~J

Acunetix-Kopyalama! - VMware Workstati						
File Edit View VM Tabs Help						
Library ×	👩 Acunetix - Configure Target - htti 🗙 🕂		0 ×			
V lype here to search	← → C 🔒 https://localhost:3443/#/targets/6f54c860-d1c2-4993-b7ae-57d0b18871ad/advanced/?returnUrl=%252F	ন 👌 🍪	• :			
My Computer Acunetix-Kopyalamal webScan-Netsparker PENTEST_PORTAL_2 Pentest-Kali-2017	acunetix	EMRE OZKOK 👻 🌘	ə 🌲			
별 Shared VMs	E Carl Save					
	Dashboard Example: X-My-Header: My-Value Add		-			
	Targets Authorization: Basic YWRtaW46dG9rYQ== Remove					
	🕷 Vulnerabīlities					
	Custom Cookies					
	Reports Grawler can be instructed to use your custom cookie values. Insert your custom cookies below.		_			
	Settings thtp://192.168.0.28/dvwa security=low	Add				
	http://192.168.0.28 PHPSESSID=7vmgmp6fu4mk/2su8b2crppsv4	Remove	-			
	© 2019 Acunetix Ltd					
	a 2 日 C 🚺 💿 🔚 🌖 🛤	・ へ D に (10) 23:49 21.06.20	019 🖵			

Acunetix-Kopyalama! - VMware Workstat	ion	– a ×
File Edit View VM Tabs Help	II • \$\overline\$ \$\overline\$ \$\overline\$ \$\overline\$ \$\overline\$ \$\overline\$ \$\overline\$ \$\o	
Library ×	Acunetix - Configure Target - htt; × +	- 0 ×
Q Type here to search 👻	← → C https://localhost.3443/#/targets/6f54c860-d1c2-4993-b7ae-57d0b18871ad/advanced/?returnUrl=%252F	여 ☆ 👶 😩 :
回 團 My Computer	acunetix	EMRE OZKOK 👻 😧 🌲
巴 Shared VMs	E Back Scan Save	
	🚯 Dashboard	
	Targets Custom Cookies	
	Image: Transformer of the second se	
	Cookie URL Value	Add
	Reports http://192.168.0.28 PHPSESSID=7vmgmp6fu4mki2su8b2crppsv4	Remove
	http://192.168.0.28/dvwa security=low	Remove
	© 2019 Acunetix Ltd	
	م الله الله الله الله الله الله الله الل	^ D 臣 ☞ 23:50 ↓ 21.06.2019 ↓

Http basic çerezi eklemesi sonrası şimdi Acunetix'in General sekmesi altındaki Login Recorder seçeneğiyle yazılıma web app'teki login aşamasını geçme adımlarını öğretelim.

General sekmesi altındaki "Site Login" sürgüsü açılır ve "Use pre-recorded login sequence" radio button'u seçilir.

Acunetix-Kopyalama! - VMware Workstat	ion	– 🛛 ×
File Edit View VM Tabs Help	II • @ O O O II II II II II II II	
Library ×	Acunetix - Configure Target - htt: × +	- 0 ×
C Type here to search •	← → C https://localhost:3443/#/targets/184228ca-031b-45d9-bcc0-0dc6d6298903/general/?returnUrl=%252F	야 ☆ 🥹 😩 :
My Computer Acunetix-Kopyalamal webScan-Netsparker PENTEST_PORTAL_2 Pentest-Kali-2017	n acunetix	EMRE OZKOK 🗸 😧 🔎
ው Shared VMs	E Back Scan Save	
	Dashboard Slower Slow Moderate Fast	A
	O Targets Continuous Scanning	
	i Vulnerabilities	
	🗠 Scans	
•	Reports SSH Credentials	
	* Settings AcuSensor	
	© 2019 Acunetix Ltd	
	== 2 耳 😋 🥝 🕽	x ^A へ 🖏 🔛 🕬 16:48 💭



New ile sıfır bir Login Recorder (Login Adım Kaydedicisi) oluşturulur.



Açılan penceredeki Record Login Actions (Login Eylemlerini Kaydetme) bölümünde sağ yan boşluktaki ilk adım olarak gösterilen URL satırı login url'i esasında olmadığından onu silelim.



Acunetix-Kopyalama! - VMware Workstation	n	-	٥	×
File Edit View VM Tabs Help	H • \$ \$ \$ \$ \$ 1 D \$ \$ \$ \$ 1 D \$ \$ \$ \$ \$ \$ \$			
Library ×	Acunetix - Configure Target - htt; X +	-	٥	×
C Type here to search	← → C https://localhost3443/#/targets/0514cede-6853-4104-aabe-23b9dcafce25/general/?returnUrl=%252F	아 ☆ 🥹		+
My Computer Acureta Kopyalamai webScan-Netsparker PENTEST_PORTAL_2 Pentest-Kali-2017 PShared VMs	Record Login Sequence	EMRE OZKOK -	e ×	
	1. Record Login Actions 2. Record Restrictions 3. Detect User Ses	sion		
	C http://192.168.0.28/dwa/login.php			
	•			
	Username Dassword Action Properties	_		
	› A 🖬 🥃 🧐 🗐 🗐 🖓 🛱 🔍 📑	ヽ [] 臣 (ハ) 21.0	1:42 [6.2019 [$\overline{}$

Esas Login URL'i (adresi) ana ekranda görünen URL olduğundan adres çubuğundaki URL'i seçip ENTER'layalım.



Acunetix-Kopyalama! - VMware Workstation	-	٥	×
File Edit View VM Tabs Help 📙 🗸 🖧 💭 💭 💭 🔟 📟 🖼 🄁 🛅			
Library X Acunetix - Configure Target - htt X +	-	٥	×
C A type here to search ✓ C A type here to search ✓ C A type here to search ✓ C A type here to search ✓ C A type here to search ✓ C A type here to search ✓ C A type here to search ✓ C A type here to search ✓ C A type here to search ✓ C A type here to search ✓ C A type here to search ✓ C A type here to search ✓ A type here to search A type here to sea	0		
My Computer Acunctic Kopyalansi webScan-Netpsarker Pentest-Kali-2017 Shared VMs 1. Record Login Actions 2. Record Restrictions 3. Detect User Session ** * C			
 Nevigate to http://192.168.0.28/dr/vva/ogin.php Username Password 	•		l
Action Properties Action Properties 第 の前ででののではののでののではののでののではののでののではののでののではののでのので	21:- 21.06	44 2019 [[]	, T

Böylece login URL'i ilk adım olarak kayda girecektir. Daha sonra login ekranında username ve password kısımlarına sırasıyla dvwa hesap bilgilerini girelim ve Login butonuna basarak oturum açalım.





Oturum açılır. Sağ yan boşlukta, takip edilen adımların sırasıyla kayıt altına alındığı görülebilir. Şimdi Next butonu ile Logout adımını kaydetme sayfasına geçelim.



Record Restriction (Kısıtlayıcılığı Kaydet) bölümünde uygulamanın logout seçeneğine tıklanır ve



ekrana gelen "bu tık için Restrict" seçeneğine tıklanır. Böylece Acunetix logout butonunu öğrenmiş olur.





Şimdi login ve logout mekanizması açısından her şey yolunda mı diye sonraki (yani son) aşamaya geçilir.





Son aşamaya geçildiğinde ekrana gelen popup ile oturumun korunabilirliğinde sorun yoktur mesajı gelmiştir. Son olarak bulunulan bu son aşamadaki sağ yan boşlukta yer alan "Session Validation Request" kısmındaki URL incelenmelidir.



Acunetix tarama sırasında oturumu kaybedip kaybetmediğini (yani kapı dışarı kalıp kalmadığını) anlamak için son bir kurala ihtiyaç duyar. Bu da sadece oturum açıkken erişilebilir olan bir URL'i Session Validation Request bölümüne koymaktır.

NOT:

DVWA yapısal anlamda bir kusura sahip olduğundan index.php sayfası 200 OK ile login.php'ye yönlendirebilmektedir. Veya oturum açıkken halen login.php gelebilmektedir. Bu nedenle daha sağlam bir URL olarak sadece oturum açıkken içeriğine erişilebilen şu URL verilmiştir:

GET http://192.168.0.28/dvwa/vulnerabilities/brute/ HTTP/1.1

Bu url var olan önceki şekilde bırakıldığında ve tarama birkaç kez öyle yapıldığında / tekrarlandığında bulgularda kritik hiçbir zafiyet bulunamadığı görülmüştür. Fakat url bu şekilde dvwa'nın tasarımsal kusuru nedeniyle (index.php ve login.php ilişkisi dolayısıyla) düzenlendiğinde bulgularda kritik tüm zafiyetlerin sıralanabildiği görülmüştür.

Session Validation Request kısmındaki "http://192.168.0.28/dvwa/**index.php**" adresini sadece login'ken içeriğini görüntüleyebildiğimiz "http://192.168.0.28/dvwa/**vulnerabilities/brute**/" sayfası yapalım ve Check Pattern butonu ile yeni girdiğimiz URL'in talep edilmesi ve bunun sonucunda yanıt alınabilmesi noktasında bir sorun var mı kontrolünü yapalım.





Ekrana popup ile pattern'da sorun yoktur mesajı geldikten sonra son aşamaya Finish diyerek login olma adımları tamamen kaydedelim.



Böylece Acunetix tarama yapacağı zaman bu kayıt işleminde öğrendiği adımlar ile hedef uygulamada oturum açabilecektir ve tarama sırasında oturumu kaybetmemek için Logout'a gitmeyecektir ve ayrıca oturum örneğin zaman aşımına uğrama sonucu kapandı mı yoksa halen oturum açık mı kontrolleri yapabilmek için oturumun açık olup olmadığını sorgulayıcı url'e gidip gelecektir. Oturum kapandıysa oturum açma adımlarını tekrarlayacaktır.

Login Recorder tanımlaması tamam olduktan sonra tarama profilinin Crawl sekmesine gelinir ve Exclude Paths seçeneğine tarama sırasında taramaya dahil edilmemesi istenen dizin yolları girilir.

Acunetix-Kopyalama! - VMware Workstati	'n		– 0 ×
File Edit View VM Tabs Help	• 🕂 🖓 🙄 💭 🖬 🖬 🖼 🐻 👘		
Library ×	👩 Acunetix - Configure Target - http 🗙 🕂		– 0 ×
Q Type here to search ▼	← → C https://localhost:3443/#/targets/0514ced	e-6853-4104-aabe-23b9dcafce25/crawl/?returnUrl=%25	52F 🕶 🙀 🍪 😩 🗄
■ 一 My Computer	nacunetix		EMRE OZKOK 👻 😧 🌲
🖺 Shared VMs	正 Scan Sav		
	🙃 Dashboard General Crawl H	TP Advanced	
	◎ Targets		
	ℜ Vulnerabilities		
	User Scans	Agent Mozilla/5.0 (Windows NT 6.1; WOW64) AppleW	Choose
	Case Sensitive	Paths Auto 💌	
	🏶 Settings	Limit crawling to address and sub-directorie	is only
	b)> Excluded	Paths Enter a pattern	Add
		i Please note that the exclude paths are regular	r expressions (*) Regexp Pattern'ı istiyor sadece
	© 2019 Acunetix Ltd		
	🖷 🔎 🛱 🤮 🌖 🗐 📑 🔥		e ^R へ 🖡 巨 🕪 22:01 21.06.2019 🖵

Taranmasın denilen dizinler regexp pattern'ı formatında girilmek durumundadır. Çünkü "*Please note that the exclude paths are regular expression*" denmektedir.

Dolayısıyla DVWA'da setup.php sayfasının taranmaması için setup.\php , security.php sayfasının taranmaması için security\.php , vulnerabilities/csrf/ dizinin taranmaması için vulnerabilities\/csrf\/ girilmelidir.

Aşagıda setup.pnp sayfasi, security.pnp sayfasi ve vuinerabilities/csrf/ dizini dişlanmışti	Aşa	ığıda	setup.php	sayfası,	security.php	sayfası	ve vulner	abilities/o	csrf/	dizini	dışla	nmıştır	•
---	-----	-------	-----------	----------	--------------	---------	-----------	-------------	-------	--------	-------	---------	---

Acunetix-Kopyalama! - VMware Workstat	tion	– o ×
File Edit View VM Tabs Help		
Library X	Acunetix - Configure Target - htti × +	- 0 ×
C Type here to search 🔻	← → C https://localhost:3443/#/targets/0514cede-6853-4104-aabe-23b9dcafce25/crawl/?returnUrl=%252F	아 ☆ 🥹 😩 :
My Computer	n acunetix	EMRE OZKOK 👻 🥹 🌲
争 Shared VMs	E Back Scan Save	
	Dashboard	^
	O Targets User Agent MozIlla/5.0 (Windows NT 6.1; WOW64) AppleW Choose ↓	
	Case Sensitive Paths Auto 👻	
	Scans Imit crawling to address and sub-directories only Excluded Paths setup\php Add	
	Please note that the exclude paths are regular expressions	
	🍄 Settings	
	Import Files	
	© 2019 Acunetix Ltd	
	📲 ク 🛱 🤮 🥝 🔚 👔	^{22:04} 21.06.2019 ワ

🔲 Acunetix-Kopyalama! - VMware Workstati	ion	-	0	×
File Edit View VM Tabs Help				
Library ×	Acunetix - Configure Target - htt; × +	-	0	×
C Type here to search	← → C https://localhost:3443/#/targets/0514cede-6853-4104-aabe-23b9dcafce25/crawl/?returnUrl=%252F	on 🚖 🍪		:
My Computer Acunetix-Kopyalamal webScan-Netsparker PENTEST_PORTAL_2 Pentest-Kali-2017	acunetix	EMRE OZKOK 👻	θJ	4
D Shared VMs	Te Back Scan Save			
	Carwing) wavgauvi			•
	O Targets User Agent Mozilla/5.0 (Windows NT 6.1; WOW64) AppleW Choose →			
	ℜ Vulnerabilities Case Sensitive Paths Auto			l
	Scans			I
	Excluded Paths Security/pp Add Please note that the exclude paths are regular expressions			ľ
	Settings Setup\.php Remove			
				Ţ
	© 2019 Acunetix Ltd			
	A الله من ال	へ 🗍 হ 🕼 22:0 へ 🗍 🔁 🕼 21.06.	⁰⁷ 5	



Acunetix-Kopyalama! - VMware Workstati	ion			-	o ×	(
File Edit View VM Tabs Help	II • 🖶 🖓 💭 🖸 🖬 🖬 🗖 🗖					
Library ×	👩 Acunetix - Configure Target - htt; 🗙 🕂			-	o x	<
C Type here to search -	← → C https://localhost:3443/#/targets/0514cede-68	53-4104-aabe-23b9dcafce25/crawl/?returnUrl=%252F		on 👌 🥴	:	
My Computer Acunetix-Kopyalamal webScan-Netsparker PENTEST_PORTAL_2 Pentest-Kali-2017	nacunetix			EMRE OZKOK 🗸	θ 🖡	
争 Shared VMs	🗷 < Back Scan Save					
	Dashboard					*
	O Targets	t Mozilla/5.0 (Windows NT 6.1; WOW64) AppleW	Choose			ł
	Case Sensitive Path.	s Auto -				
	🗠 Scans	Limit crawling to address and sub-directories or Limit crawling to address and sub-directories or	nly			
	Excluded Path	Enter a pattern	Add			ľ
	🏶 Settings	vulnerabilities\/csrf\/	Remove			
		security\.php	Remove			
		setup\.php	Remove			-
	© 2019 Acunetix Ltd	-				
	🛋 A 🛱 🤮 🧕 🧊 📑 <u> </u>		۶ ^۹	へ 『見 早 di》 22:0 21.06.	09 .2019 🖵	

setup.php sayfası uygulamanın kullandığı veritabanını reset'lediğinden dışlanmıştır. security.php sayfası uygulamanın güvenlik seviyesini arttırdığından taramanın bulgularını azaltmasın diye dışlanmıştır. csrf/ dizini ise senaryosu gereği uygulamanın hesap parolasını değiştirdiğinden tarama dışında tutulması tercih edilmiştir.

Artık tarama profili hazır durumdadır. Şimdi Acunetix makinasından DVWA yüklü sanal makinaya gönderilen trafiği dinleme noktasında karşı tarafta Wireshark düzgün yapılandırılmış mı bir test edelim.

Acunetix tarafından CMD ekranı yoluyla test amaçlı karşı tarafa ICMP paketleri yollayalım ve karşıdan "sadece" DVWA makinasına gelen trafik anlık olarak görüntülenebiliyor mu bakalım.



Acunetix-Kopyalama! - VMware Workstation n × File Edit View VM Tabs Help | 🔢 🖛 | 🖶 | 💭 💭 💭 | 🚺 🚍 🖼 📮 | 🔚 Library × 👩 Acunetix - Configure Target - http: 🗙 🛛 🕂 • Q Type here to search ← → C 🔒 https://localhost:3443/#/targets/0514cede-6853-4104-aabe-23b9dcafce25/general/?returnUrl=%252F o- ☆ 0 😑 💻 My Computer Acunetix-Kopyalama acunetix PENTEST_PORTAL_2 Pentest-Kali-2017 Shared VMs Ē K Back Scan Save 🏠 Dashboard 🔤 Command Prompt - ping 192.168.0.28 × rosoft Windows [Version 10.0.17134.829] 2018 Microsoft Corporation. All rights reserved. ٥ Targets \Users\pentest>ping 192.168.0.28 瘷 inging 192.168.0.28 with 32 bytes of data: pply from 192.168.0.28: bytes=32 time=28ms TTL=64 pply from 192.168.0.28: bytes=32 time=128ms TTL=64 pply from 192.168.0.28: bytes=32 time=19ms TTL=64 Scans Ŀ Reports Settings ٠ Scan Speed Slower Moderate Slow へ 🗓 🖫 🕪 22:15 21.06.2019 🖓 Т

DVWA tarafı wireshark yazılımı aracılığıyla şu filtre

Wireshark (DVWA Tarafında):

ip.src == 192.168.0.29 and ip.dst == 192.168.0.28 // 29 : Acunetix, 28: DVWA

ile Acunetix tarafından gelen trafiği dinler durumdadır ve gelen icmp paketleri ekranına gelir.



Sonuç olarak Wireshark doğru bir şekilde sadece Acunetix tarafından gelen trafiği dinler vaziyettedir. Dolayısıyla Acunetix taramaya başladığında DVWA tarafında ekranımıza sadece Acunetix'ten gelen trafik düşecektir ve saf bir saldırı trafiği elde etmiş olacağız.

Saldırıyı başlatalım.

Acunetix-Kopyalama! - VMware Workstat	tion	-	٥	\times
File Edit View VM Tabs Help	II - & O O O I II = II - I II			
Library ×	🙃 Acunetix - Configure Target - htti 🗴 🕂	-	٥	×
Q Type here to search	← → C https://localhost:3443/#/targets/0514cede-6853-4104-aabe-23b9dcafce25/general/?returnUrl=%252F	on 🕁 🥴		:
My Computer My Computer Computer	acunetix	EMRE OZKOK 🗸	θ	
P Shared VMs	E Kack Scan Save			
	Ceneral Crawl HTTP Advanced			
	Targets Translate			
	₩ Vremerabilities			Ľ
	La Scans http://192.168.0.28/dvwa/			
	Reports Description			
	Settings Business Criticality Normal -			
	Scan Speed Slower Slow Moderate Fast			-
	© 2019 Acunetix Ltd			
	A 👔 🥃 🥥 🍯 🛱 🔍 🖿	へ ① 記 🗤 22 21.06	18 5.2019	$\overline{}$



Acunetix-Kopyalamal - VMware Workstation			o ×
File Edit View VM Tabs Help			
Library ×	Acunetix - Scans × +	-	o ×
Q Type here to search ➡ Myc Computer ➡ Acunetice-Kopyalamal ➡ WebScan-Nettsparker ➡ PENTEST-PORTAL_2 ➡ Pentest-Kali-2017 ➡ Shared VMs	← → C 🔒 https://localhost3443/#/scans/5e477ee8-a2a8-4463-aed9-88bebc747d1b/crawl/default/?status=open&returnUrl=%252Ftar	on 🕁 🍪	• :
	n acunetix	RE OZKOK 👻	0 ▲
	E Stop Scan Pause Scan Generate Report WAF Export *		
	Dashboard Scan Stats & Info Vulnerabilities Site Structure Events		
	₩ Vulnerabilities		
	Keans Keans		
	□ comig □ docs		
	dvwa Se., Vulnerability URL		=
	Settings about.php O Content Security Policy (CSP) not implemented http://192.168.028 confin	}/dvwa/	<u>^</u>
	Contrage Contrage Contrage Possible internal IP address disclosure http://192.168.0.28	/dvwa/	+
	© 2019 Acunetix Ltd		
	i ^ 월 🥶 🖬 🕹 📰 🗘 🕌	〕 ED (10) 22.06.2	4 2019 🖓

2 Acunetix-Kopyalamel - VMware Workstation				
File Edit View VM Tabs Help	Ⅱ - 🖶 🖓 🖓 🖓 🔳			
Library ×	👩 Acunetix - Scans 🛛 🗙	+		– 0 ×
C Type here to search	← → C	t3443/#/scans/5e477ee8-a2a8-4463-aed9-88bebc74	7d1b/vulns/default/?status=open&returnUrl=%252Ftar 💁 😁	☆ 🥹 😩 :
My Computer My Computer My Computer My Computer PowebScan-Netsparker PowebScan-Netsparker Powets-Kali-2017 Powets-Kali-2017	n acunetix		EMRE ÖZK	юкт 🛛 🌲
望 Shared VMs	⊒	Back Stop Scan Pause Scan Generate Re	port WAF Export + Group By: None + Status:	Open 🗱 🔻 Filter
	ණ Dashboard	can Stats & Info Vulnerabilities Site Structure	Events	
	⊙ Targets	Co. Male and Ultra	100	
	☆ Vulnerabilities	Se Vulnerability		Paran =
		Bund SQL Injection	http://192.168.0.28/dvwa/vulnerabilities/sqli_blind/	id
	🖮 Scans	Code execution	http://192.168.0.28/dvwa/vumerabilities/exec/	ıp
	B. Decenter	Cross site scripting	http://192.158.0.28/dvwa/vumerabilities/view_source.php	
	E Reports	Cross site scripting (verified)	http://192.108.0.28/0/wa/vulnerabilities/ws_s/	name
	🌣 Settings	Cross site scripting (verified)	http://192.106.0.28/d/wwa/vulnerabilities/wss_s/	mcxnes:
		Cross site scripting (vernied)	http://iszites.org/uvwa/vumerapinues/xss_s/	
	© 2019 Acunetix Ltd			
	🖶 P 🖽 🧲 🍯	🧿 🚍 🌒 👔	대 2 · 2	4») 00:27 22.06.2019 ∽
To direct input to this VM, move the mouse p	ointer inside or press Ctrl+G.			a 🖶 📣 🛔 🚡 🗩
🕂 🔎 🖽 🤤 🍯	🌻 🚍 😚 💶 🚿		へ Ĉ 늘 덮 ⊄× 1	TUR 22.06.2019

Acunetix-Kopyalama! - VMware Workstat	ion		– 🗗 🗙
File Edit View VM Tabs Help	- ⊕ ₽ ₽ ₽		
Library ×	👩 Acunetix - Scans	× +	– 0 ×
Q Type here to search ▼	← → C https://log	calhost:3443/#/scans/5e477ee8-a2a8-4463-aed9-88bebc747d1b/vulns/default/?status=c	ppen&returnUrl=%252Ftar 🗣 🙀 👶 😩 🗄
	nacunetix		EMRE 02KOK 🗸 🛛 🧟
🖆 Shared VMs	Ē	▲ Back Stop Scan Pause Scan Generate Report WAF Export ▼	Group By: None 👻 Status: Open 🕷 🔻 Filter
	🏠 Dashboard	Scan Stats & Info Vulnerabilities Site Structure Events	
	⊙ Targets		
	👻 Mulanun hillitet	Se Vulnerability URL	Paran =
	, me votnerabilities	Directory traversal http://192.168.0.28/dvwa	/vulnerabilities/fi/ page
	🖿 Scans	File inclusion http://192.168.0.28/dvwa	/vulnerabilities/fi/ page
		PHP allow_url_include enabled http://192.168.0.28/dvwa	/phpinfo.php
	■ Reports	Remote file inclusion XSS http://192.168.0.28/dvwa	/vulnerabilities/fi/ page
	🌣 Settings	Apache JServ protocol service http://192.168.0.28/	
		Application error message http://192.168.0.28/dvwa	/vulnerabilities/xss_s/ mtxHes: -
	© 2019 Acunetix Ltd		
	🚛 🔎 🖽 🧲	😆 🧑 🛤 😆 🚯	x ⁸ ^ ট 달 예) ^{00:31} 모

DVWA tarafında Acunetix makinasından gelen trafik ekrana anlık olarak düşer.

Activit	ies	Cum 22:22	👻 🕤 👘 🗘 👘
- 🚍			
9	df		
٩	W	*wtp2s0 • • •	
9	Http Range Başlığı.	File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	
0	docx	ip.src == 192.168.0.29 and ip.dst == 192.168.0.28 x = x = x = x = x = x = x = x = x =	
	254 GB Volume HDD'ye Atulacaklar X55 cheatsheet	Three Source Destination Protect length Mo. Destination Protect length Mo. 2421 247 2475 2477.95733 30 CC 252.168.0.29 102.168.0.28 HTTP 425 GT //Max/Vulserabilities/trute/source and HTP/1.1 (pplication/same of the same oit (Ubuntu 14.04.175) [Running]- Oracle VM VirtualBox Import Devices Help Informitig Informitig Import Devices Help Khernet I, Miadde 081:00:2715:a:14b:ed S.55.255.05 Import Devices Help Old Oracle XM Devices IV2: (146 or 255.855.255.05 Import Devices Help Import Devices Help Old Oracle XM Devices IV2: (146 or 255.855.855.05 Import Devices Help Import Devices Help Old Oracle XM Devices IV2: (146 or 255.855.855.05 Import Devices Help Import Devices Help Old Oracle XM Devices IV2: (146 or 255.855.05 Import Devices Help Import Devices Interview USM Carlos Interview IV2: (146 or 255.855.05 Import Devices Interview IV2: (146 or 255.95 Import Devices Interview IV2: (146 or 255.95 Import Devices Interview IV2: (146 or 255.95 USM Carlos Interview IV2: (146 or 255.95 Import Devices Interview IV2: (146 or 255.95 Import Devices Interview IV2: (146 or 255.95 Import Devices Interview IV2: (146 or 255.95 USM Carlos Interview IV2: (146 or 255.95 Import IV2: (146 or 255.95 Import IV2: (146 or 255.95 Import IV2: (146 or 255.95 Import IV2: (146 or 255.95 USM Carlos Interview IV2: (146 or 255.95 Import IV2: (146 or 255.95 Import IV2: (146 or 255.95 Import IV2: (146 or 255.95 Import IV2: (146 or 255.95<	
· 🥢	.docx Mutillidae Video Serisi.txt	10000 35 Ga al 77 Da d5 36 00 Gc 28 77 F5 48 68 00 45 00 -71 (-5) -NE. 1010 05 27 69 00 66 00 50 14 74 co 48 48 00 10 45 00 -71 (-5) -NE. - - 1010 05 27 75 86 00 66 86 00 47 00 11 72 73 74 75 76 - - - - 1010 07 26 58 06 66 66 67 68 60 - - - - - 1010 77 51 52 03 64 65 66 67 68 60 - - - - - - 10210 77 51 52 03 64 65 66 67 68 60 - <	inteli minel 일 ⓒ 양 중 2 또 문 구 (J 한 Right Ctr Temel CMD Komutar.
	Basamaklar I.docx	○ 2 wireshark_wip2s0_20190621221414_ZVAaCS.pcapng Packets: 24734 - Displayed: 11711 (47.3%) Profile: Default	
	Trash	smartasp PhoMyAdm txz/cvayir in Basir login bilg	
		hickubekara Belgeleri buk Biglieri	

Acunetix taraması bittiğinde acunetix yazılımı son olarak karşı tarafla olan tcp handshake'i sonlandırıcı RST paketini yollar. Bu paket sonrası acunetix tarafından DVWA tarafına başka paket gelmez.

Not: Acunetix taraması sonrası, gelen trafiği dinleme ekranına başka bir paket düşmez. Çünkü tarama bitmiştir ve paket alışverişi Acunetix tarafının bağlantıyı sonlandırıcı son paketi RST ile tamamlanmıştır.



Bu acunetix tarafından gelen ve toplanmış saf zararlı trafik, dosyalanabilir.



EKSTRA

Ayrıyetten Acunetix'ten gelen değil de DVWA yüklü makinanın Acunetix tarafına yanıt olarak döndüğü trafik aynı wireshark ekranı açıkken filtrelemeyi

ip.src == 192.168.0.29 and ip.dst == 192.168.0.28 // 29 : Acunetix, 28: DVWA

yerine

ip.src == 192.168.0.28 and ip.dst == 192.168.0.29 // 29 : Acunetix, 28: DVWA

şeklinde ters düz ederek güncellersek (yani önceden src Acunetix ve dst DVWA iken bu sefer src DVWA ve dst Acunetix yaparsak) ekrana devasa trafik paketleri içerisinden sadece DVWA'nın Acunetix tarafına yanıt olarak döndüğü trafik gelecektir. Dolayısıyla bu şekilde DVWA yüklü makinanın Acunetix tarafına döndüğü yanıtları dosyalayabiliriz.



Böylece zararlı gelen trafiğe karşı uygulamanın döndüğü tepkiler bir trafik dosyası altında toplanabilir.