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 seçeneği 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 işlemi 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 yapan yerler işaretlenerek (tıklanarak) sağ yan boşlukta 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 boşlukta url yerine 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.

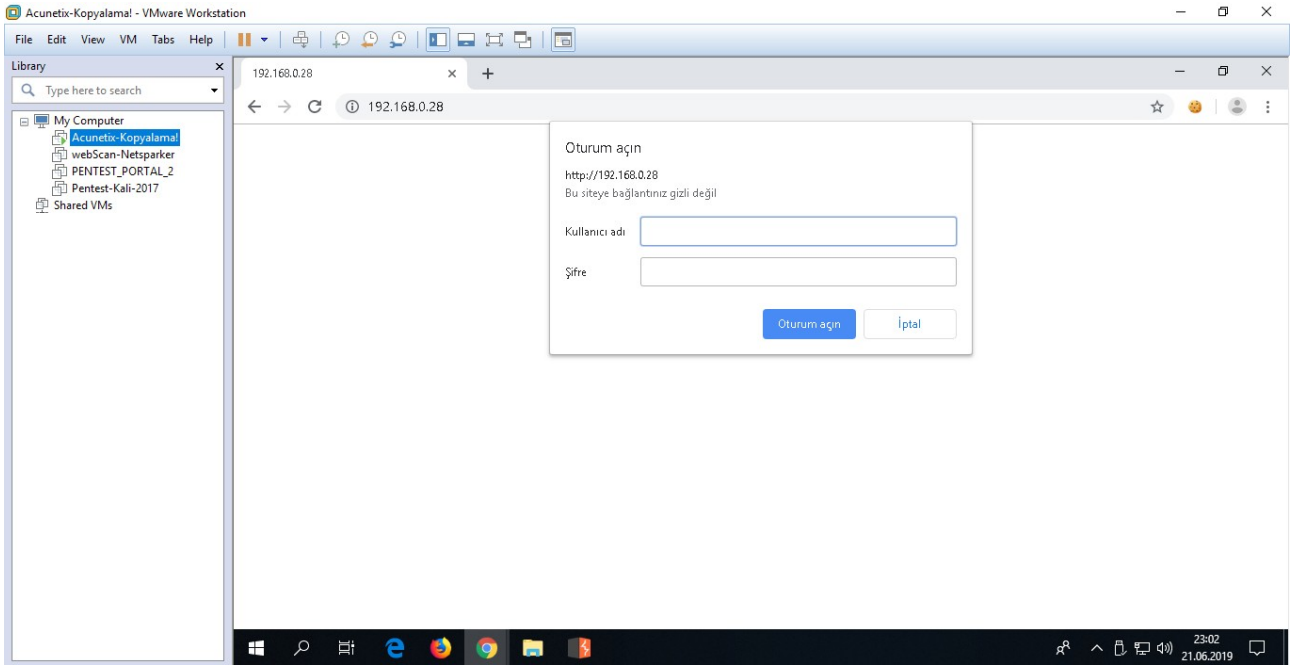
Kullanılan Araçlar

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.

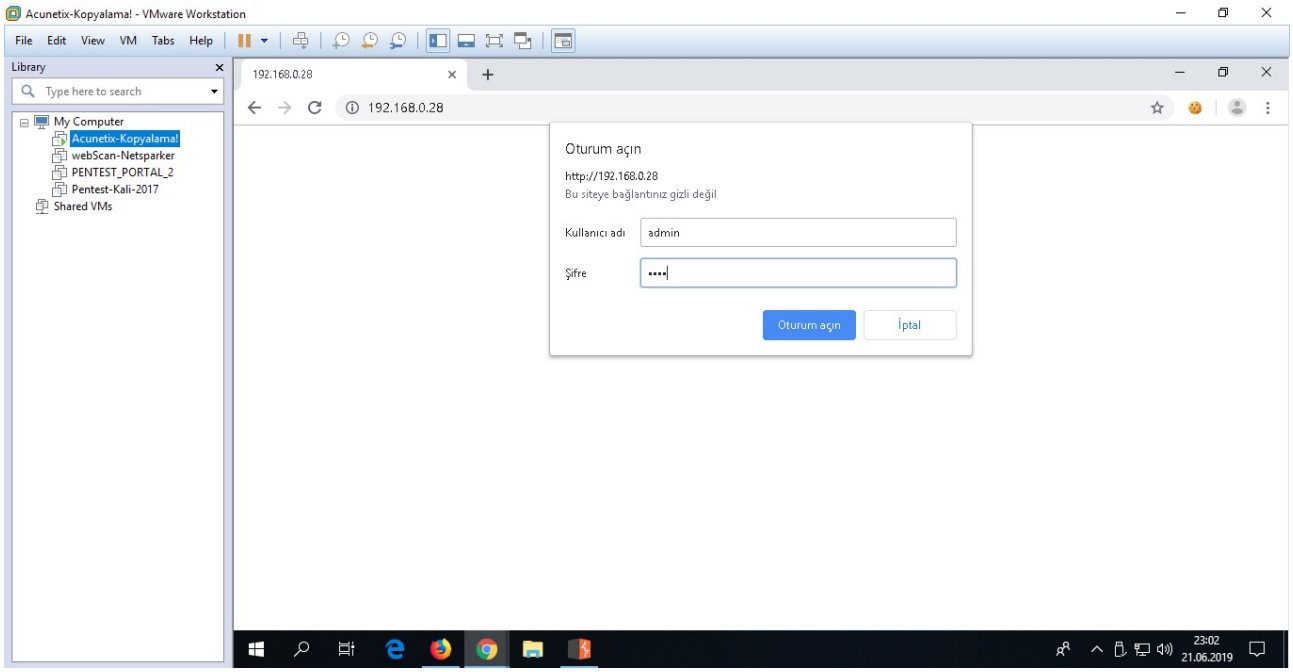
Workstation Laptop:

http://X.Y.Z.T

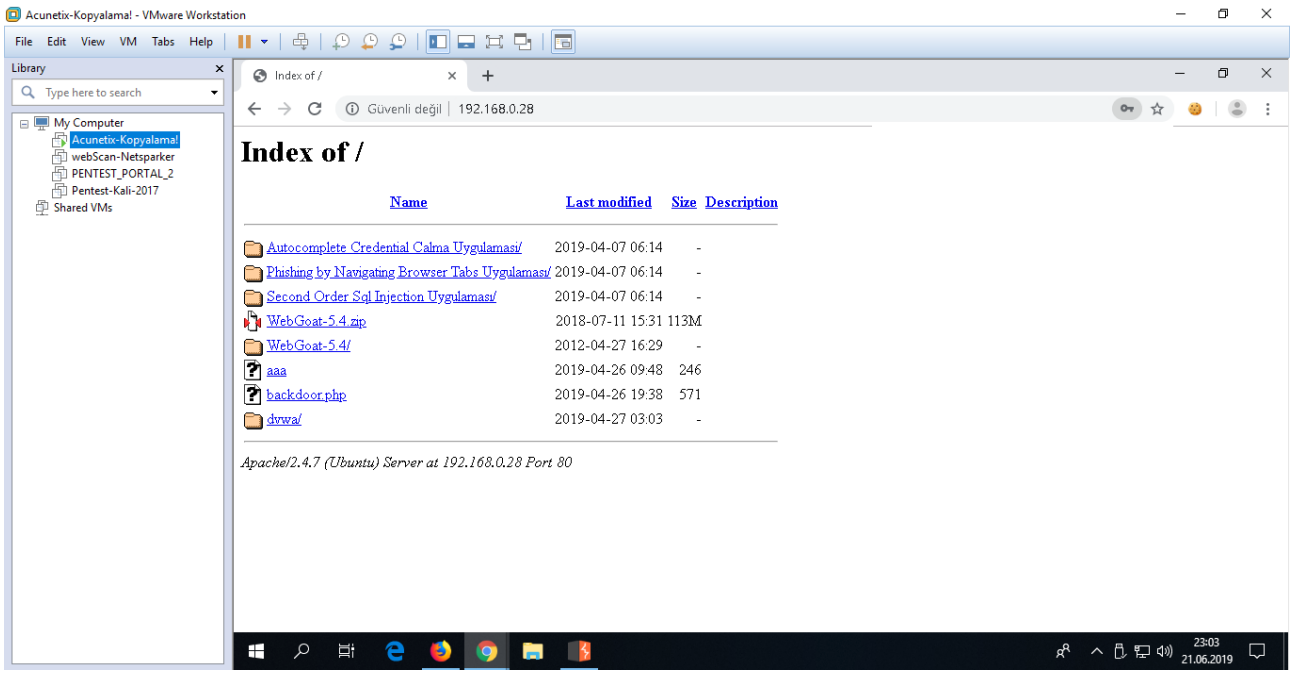


(Hedef Web Uygulamasına Gitme)

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

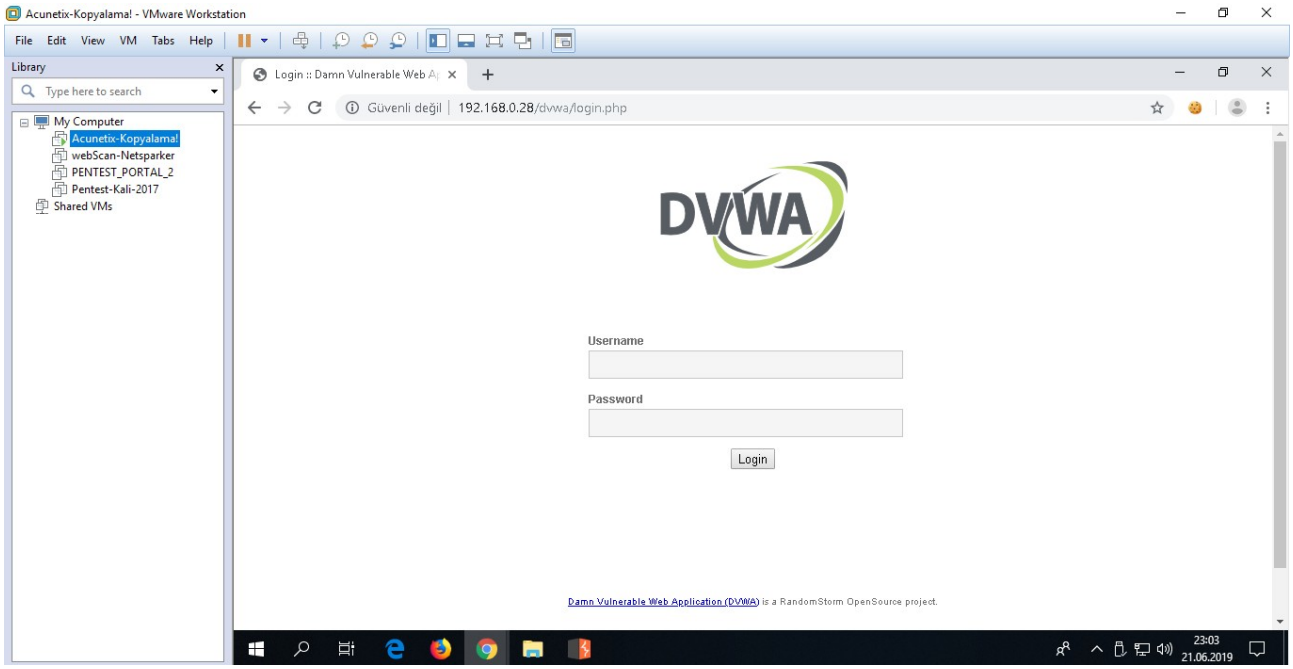


(Hedef Web Uygulaması Basic Yetkilendirmesine Bilgileri Girme)



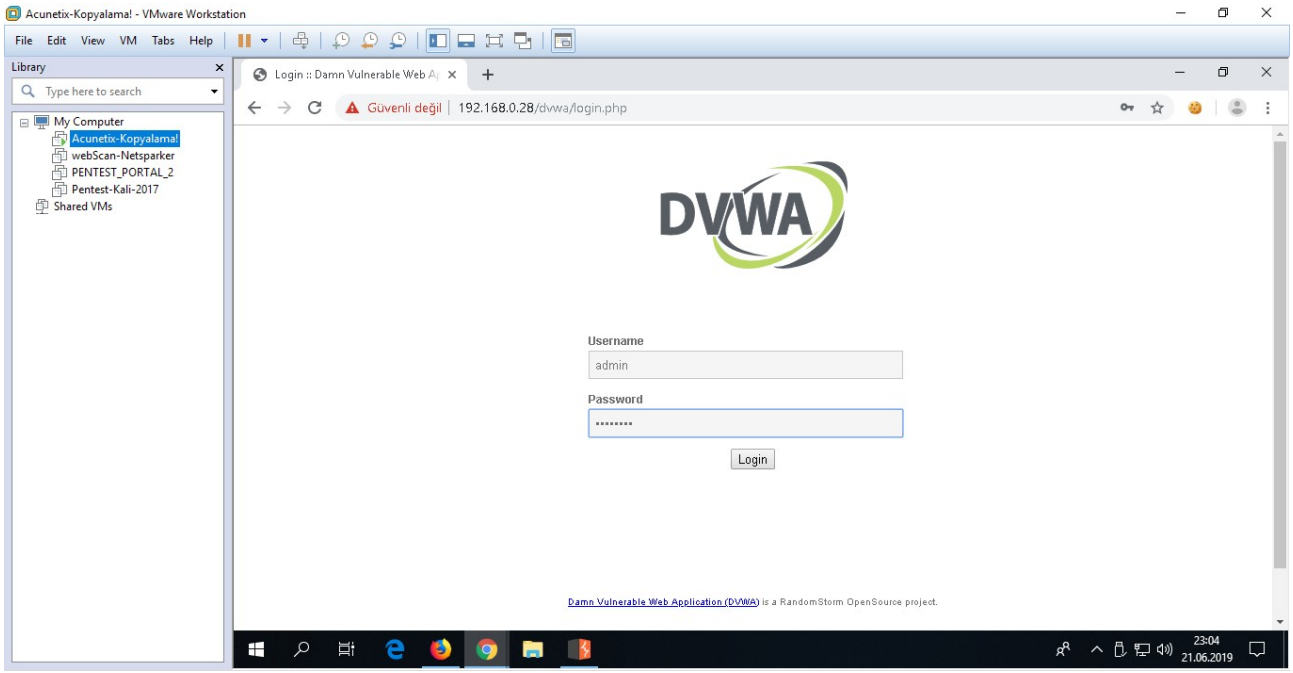
(Hedef Web Uygulaması Arayüzü Birden Fazla Uygulama İçerdiğini Gösterir)

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

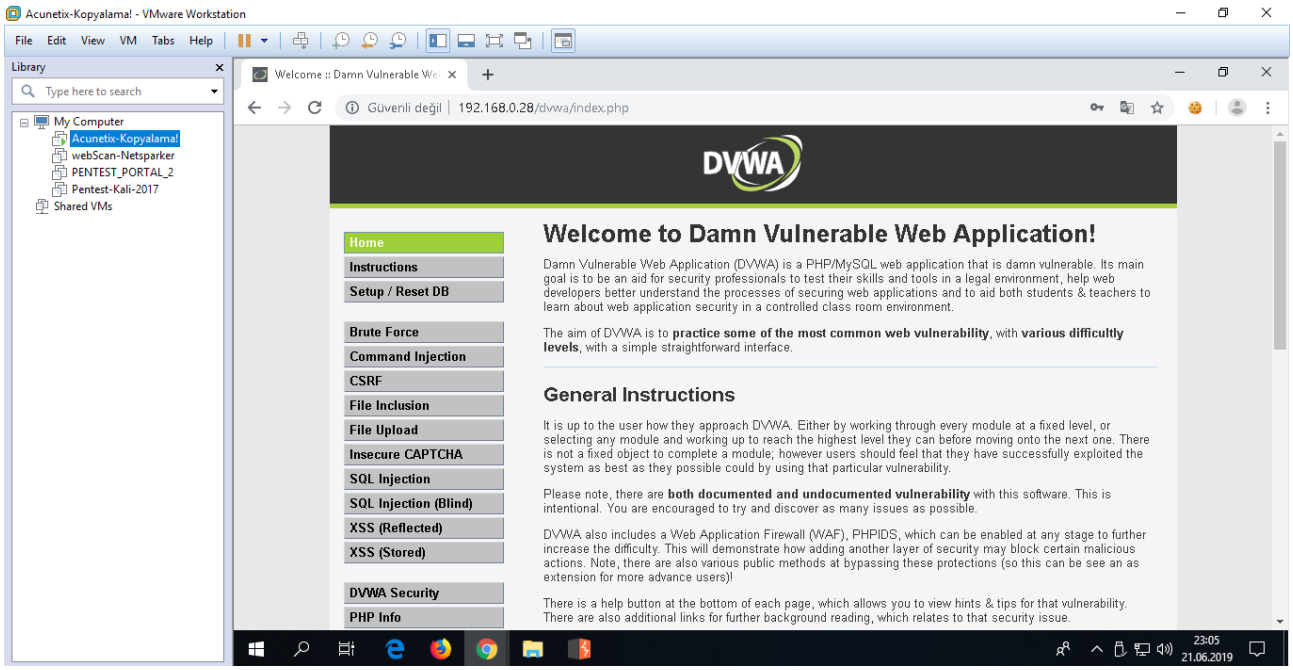


(DVWA Login Sayfası Gelir)

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



(DVWA Login Ekranında Oturum Bilgileriyle Giriş Yapılır)

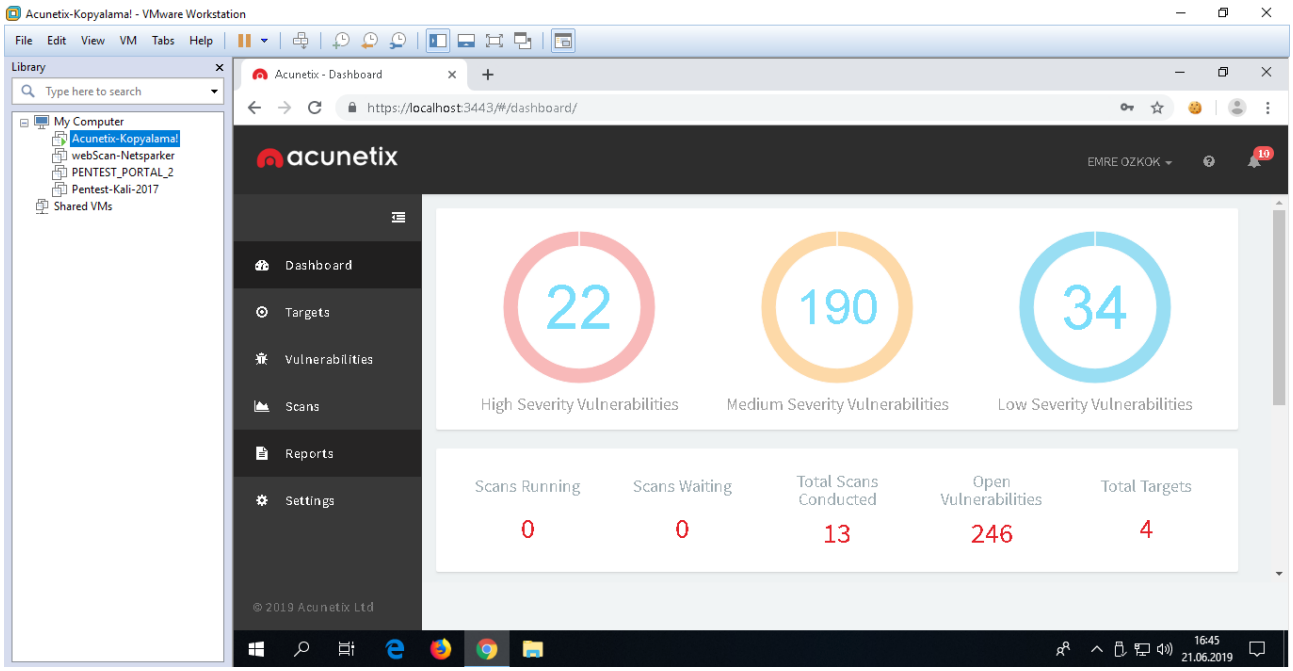


(DVWA Web Uygulaması Erişimi Tamamlanır)

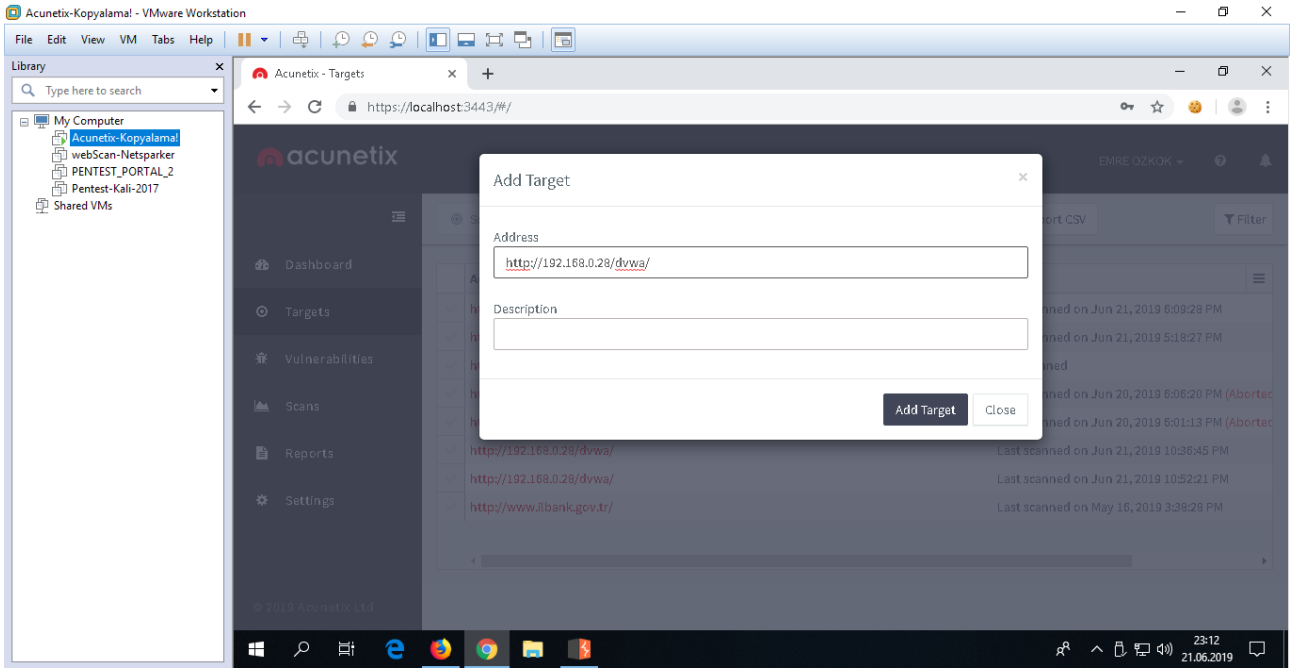
Acunetix ile hedef web uygulaması DVWA'yı tarayabilmek için hedef makinada iki adet yetkilendirme aşamasından geçtik. Dolayısıyla Acunetix'e bu geçişleri yapabileceği kuralları girmemiz gerekmektedir.

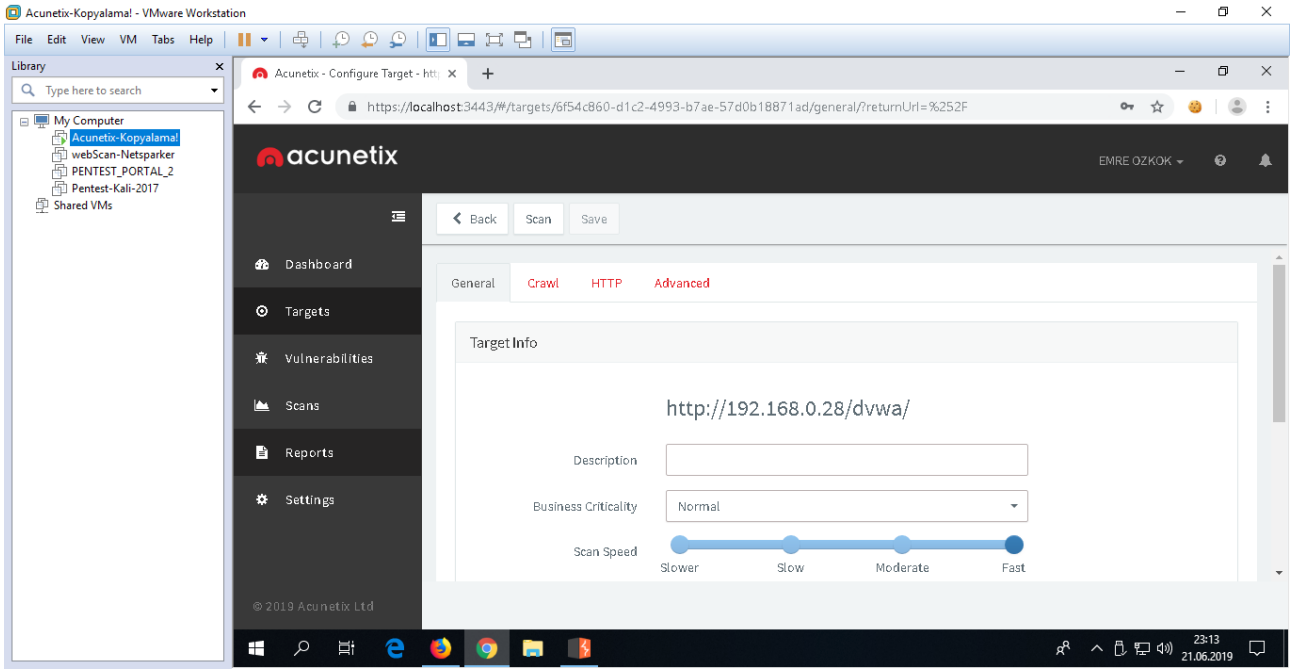
XYZ İş Laptop:

https://localhost:3443/#/dashboard/ (*) Acunetix Web Arayüzünü Açar



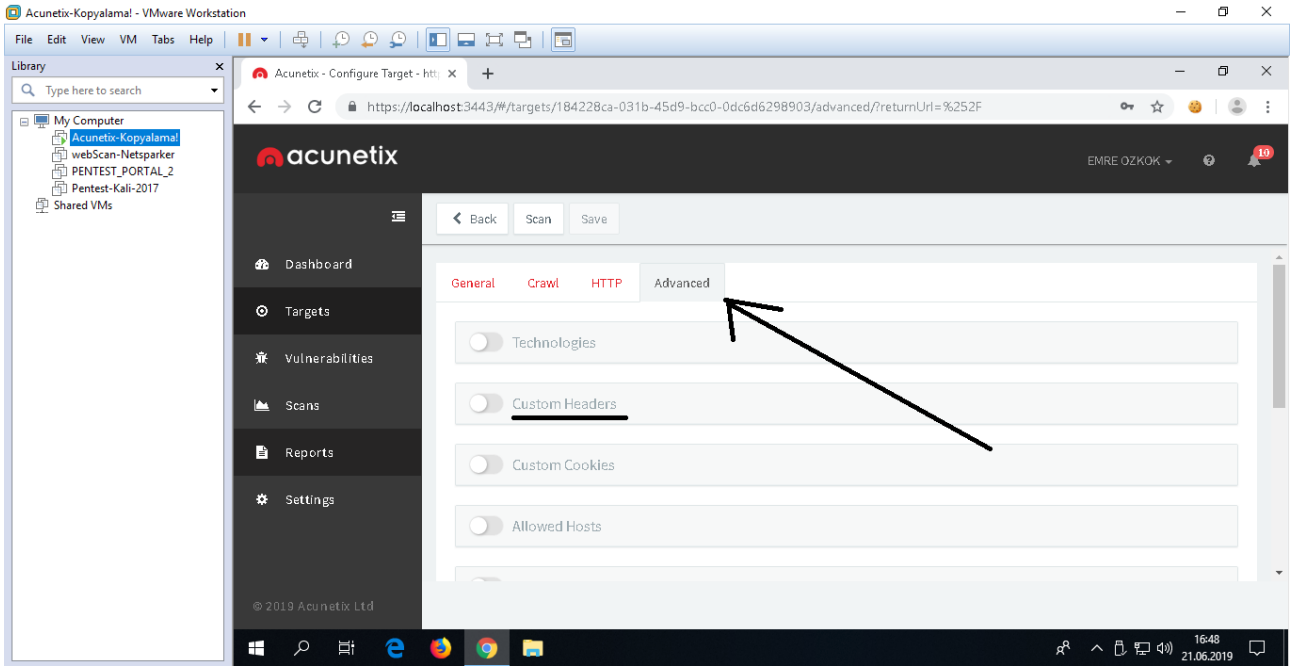
Acunetix’e hedef web uygulaması adresi girilir.



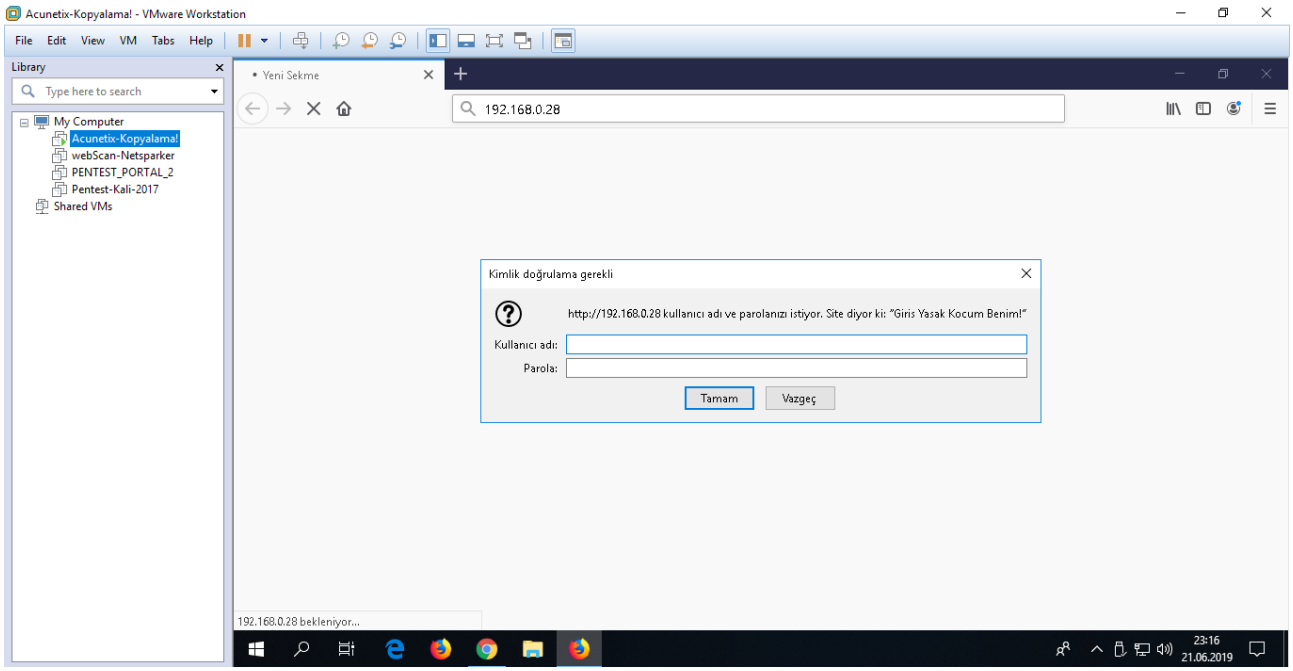


Tarama profilindeki Advanced sekmesine gelinir ve Custom Headers açılır. Bu seçenek ile hedef uygulama adresindeki http basic yetkilendirme aşaması geçildiğinde gelen çerezi ekleme işlemi uygulanacaktır.

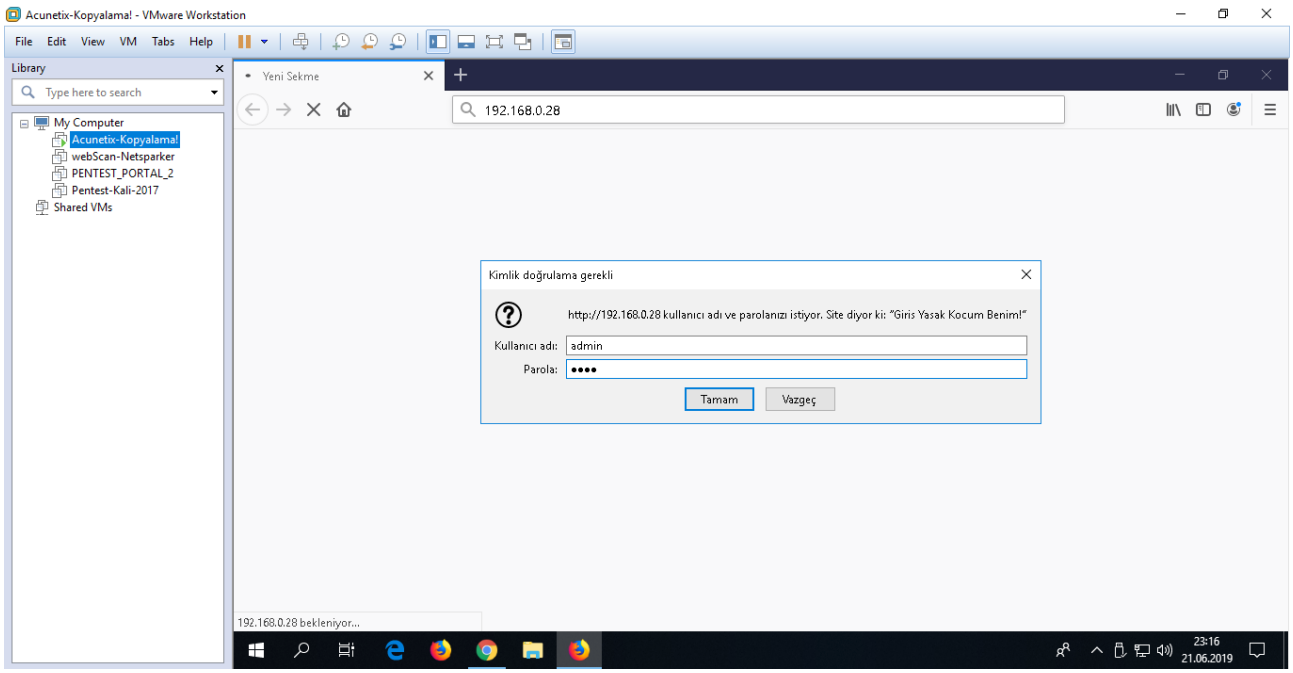
> *UYARI:*
>
> *Eğer HTTP Basic yetkilendirme çerezini önce bu bölüme koymazsan Acunetix'in Login Recorder seçeneğini kullanarak yazılıma Web App Login panelde login olma adımlarını öğretemezsin. Çünkü web app login'den önce bir başka yetkilendirme aşaması olan http basic yetkilendirmesi vardır. Acunetix 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.*



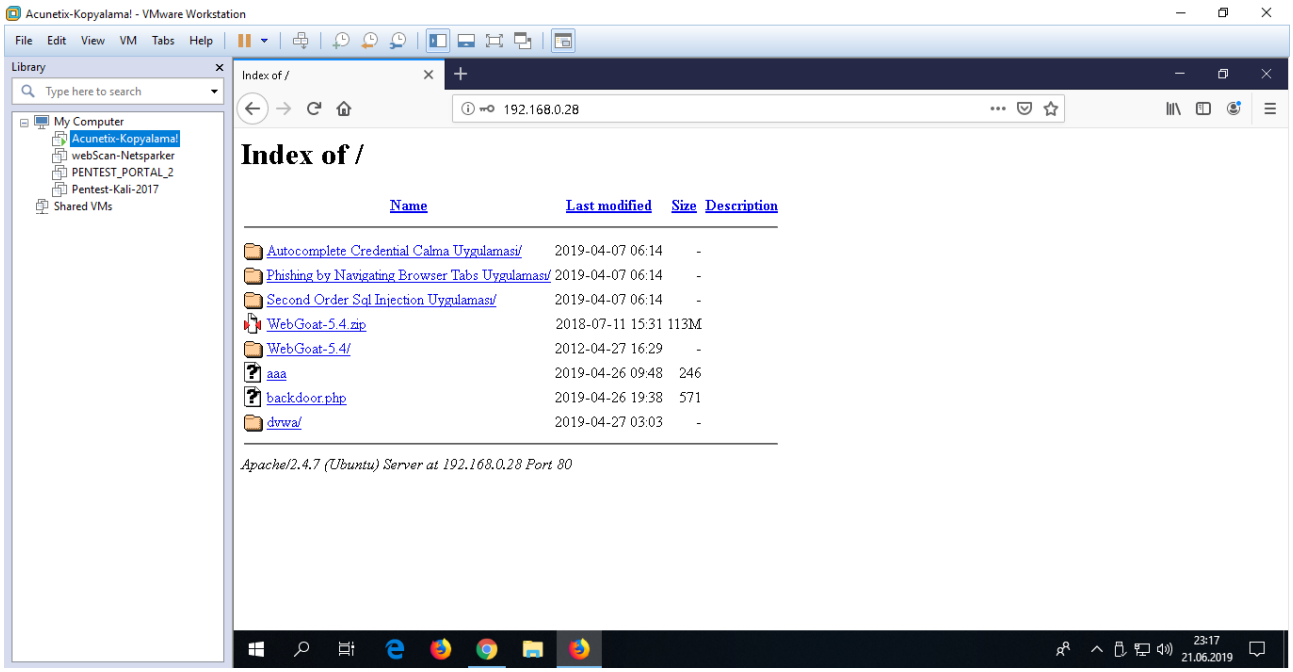
Acunetix tarafından hedef uygulamaya tarayıcıdan erişilir ve http basic ekranı bizi karşılar.



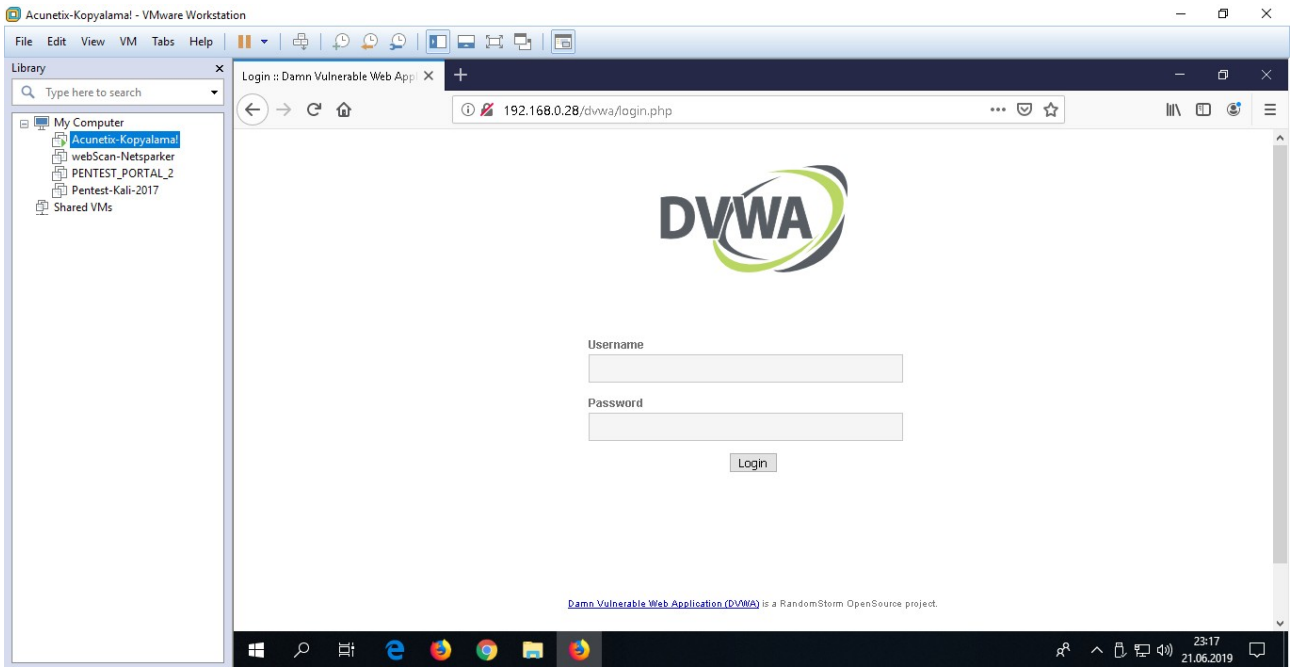
İlgili bilgiler (iK Test Makinesi http basic kullanıcı adı: admin, şifre: toka) girilir .



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

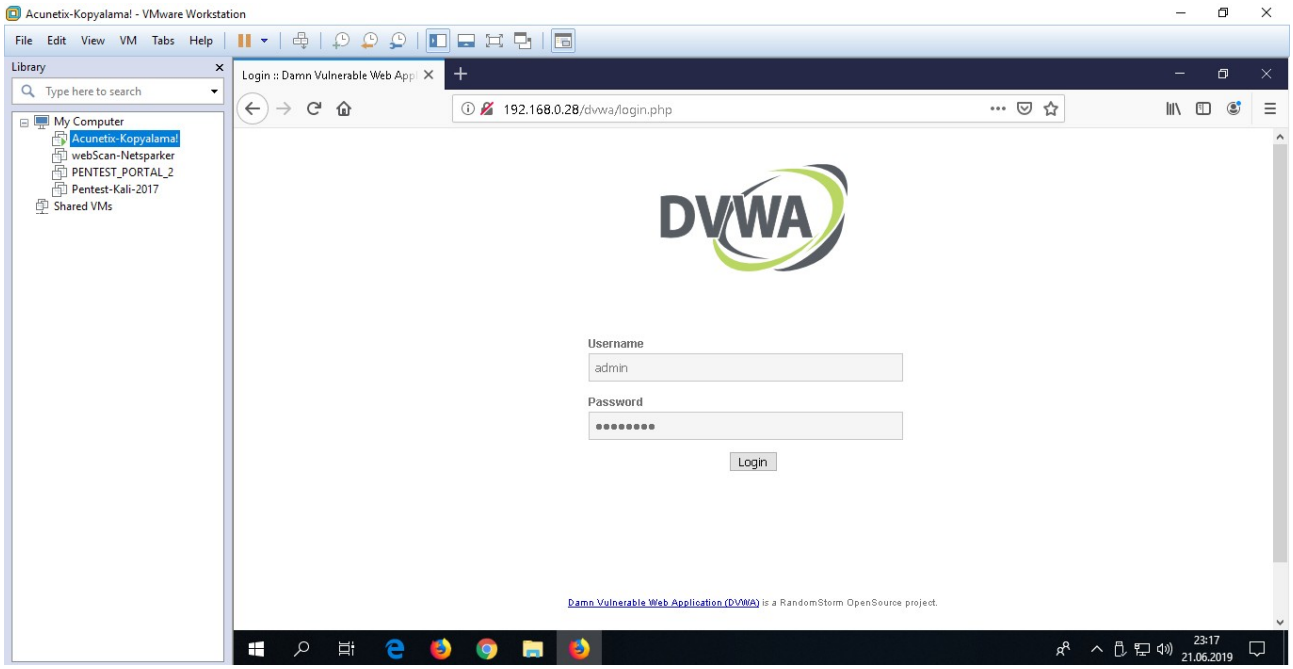


(Test Amaçlı Konulmuş Birden Fazla Uygulama Listelenir)



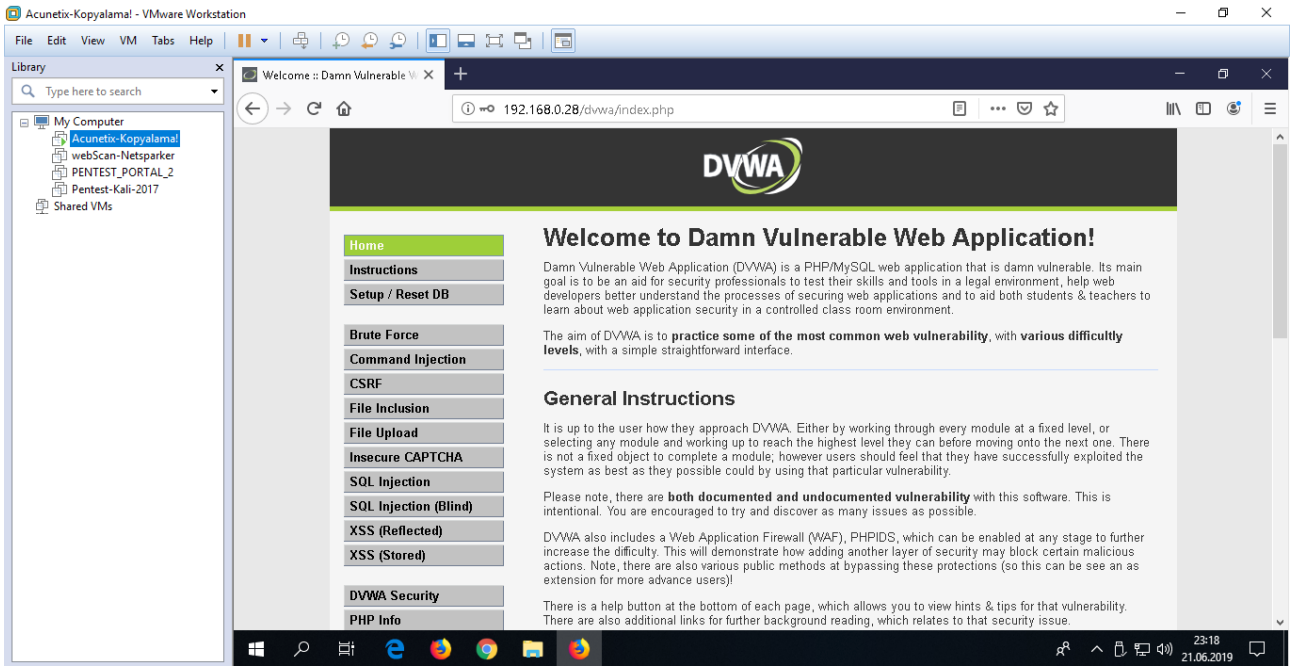
(DVWA Login Paneli)

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



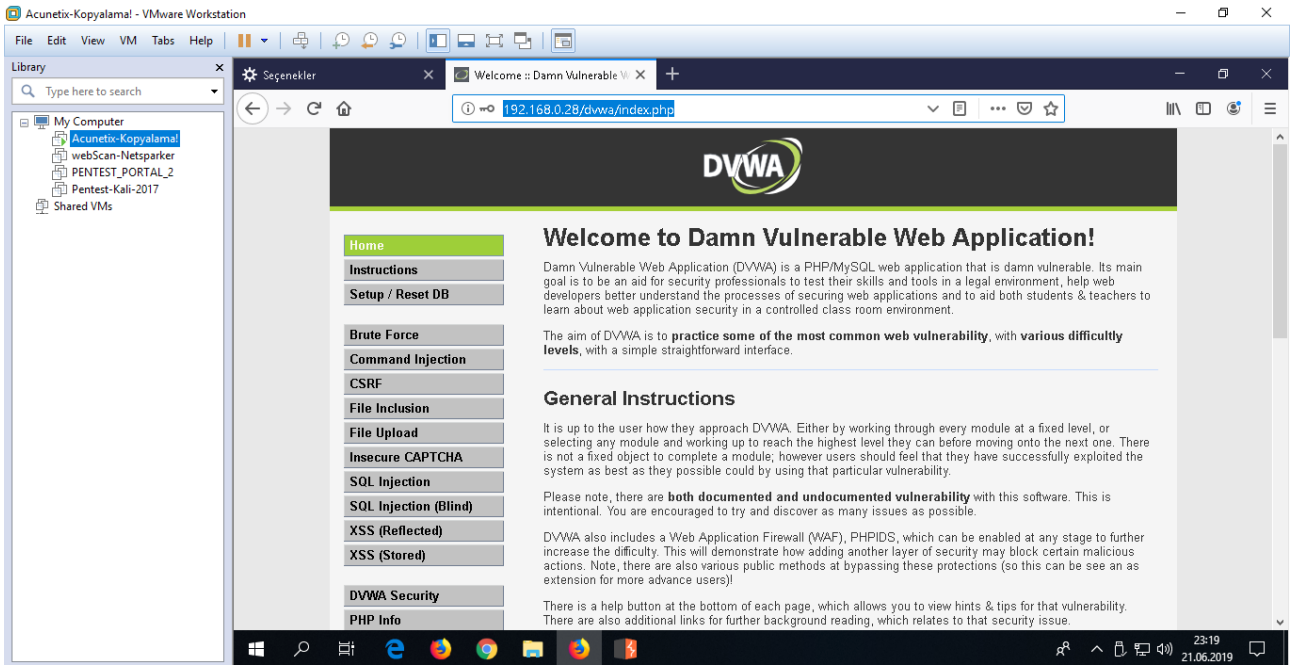
(DVWA Login Noktası Bilgileri Girilir)

DVWA'da oturum açılır.



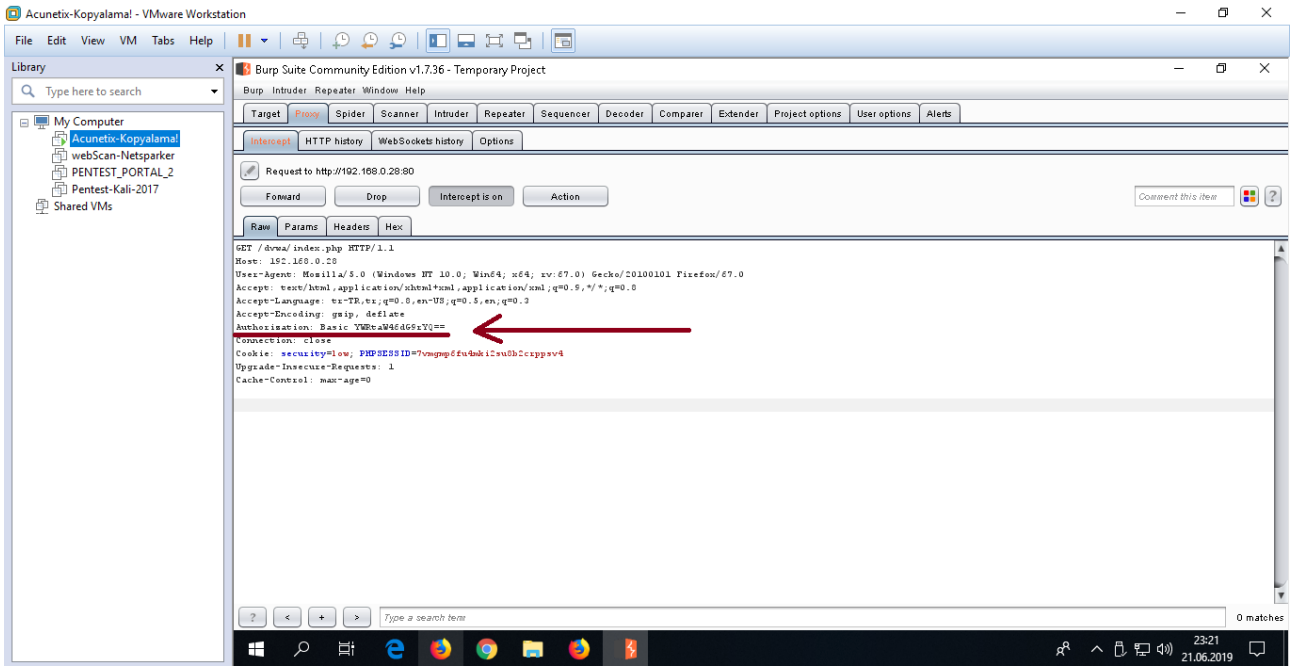
Artık tarayıcıdan DVWA'nın içerisine kadar girebildiğimize göre bu aşamada elimizdeki http basic ve sonra DVWA uygulama çerezini (çünkü DVWA'nın security seviyesi çerezi var ve bu tarama esnasında bize lazım olabilecek bir çerez) alıp Acunetix'e ekleyelim.

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

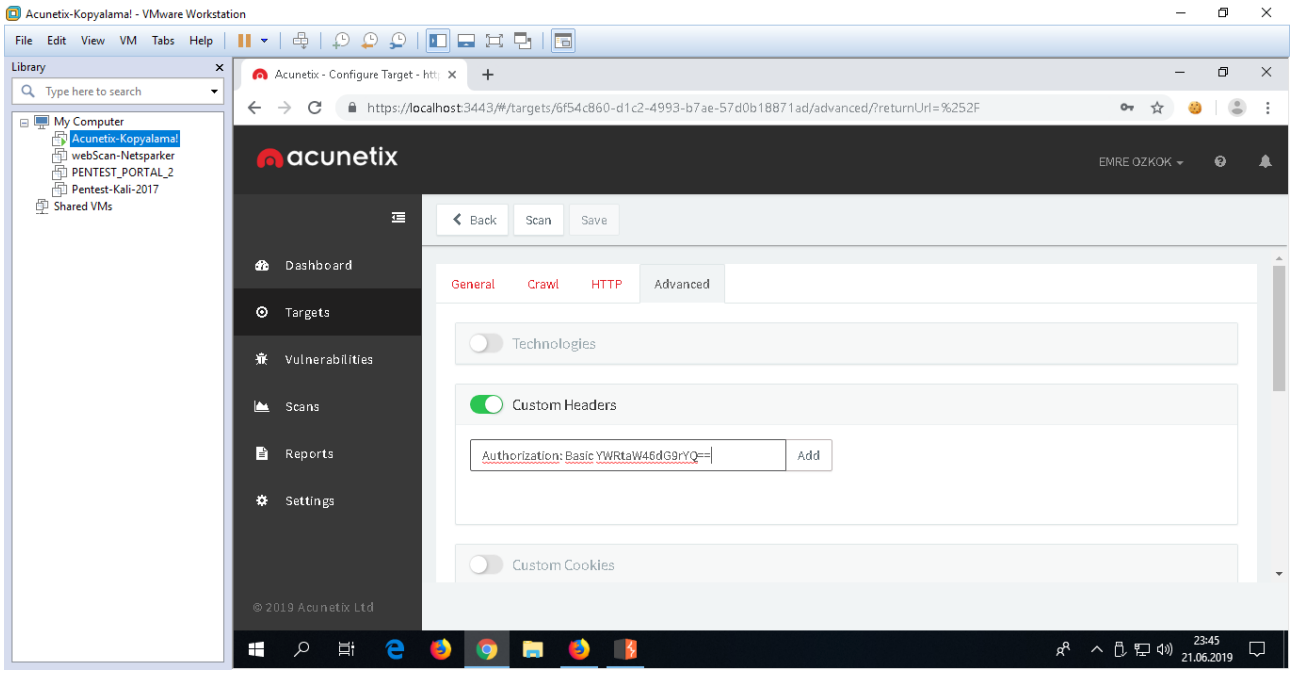


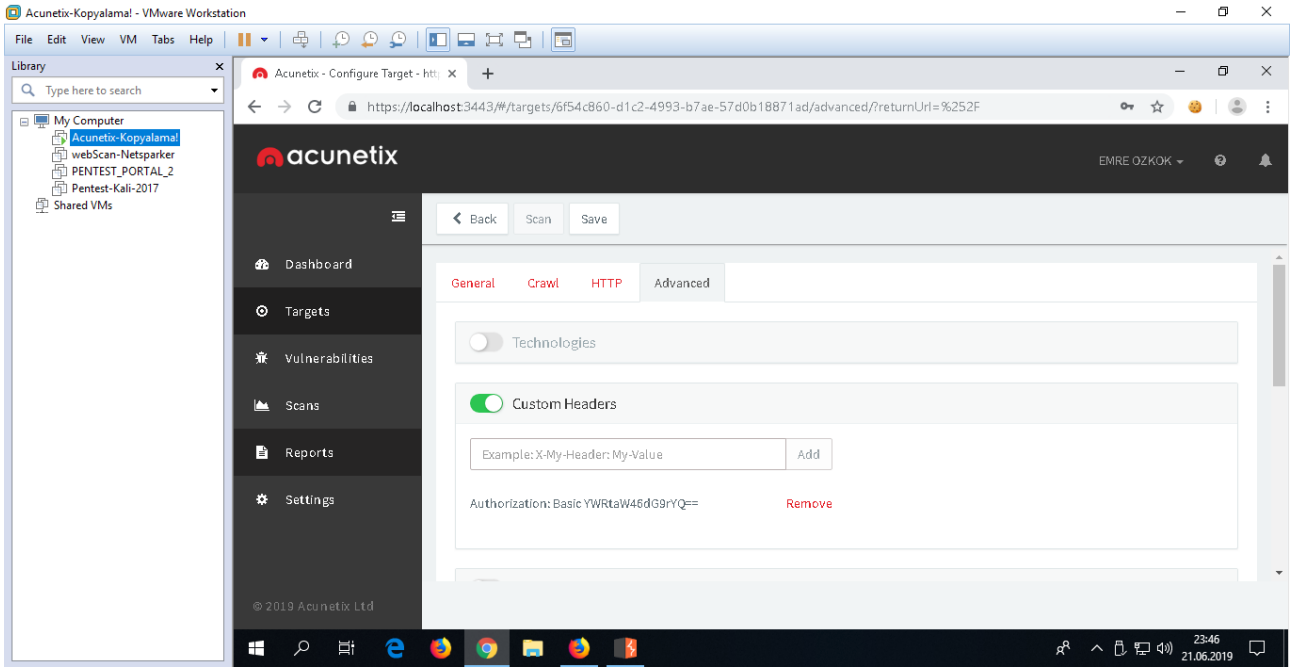
(Refresh)

Burp ekranına http talebi gelir.

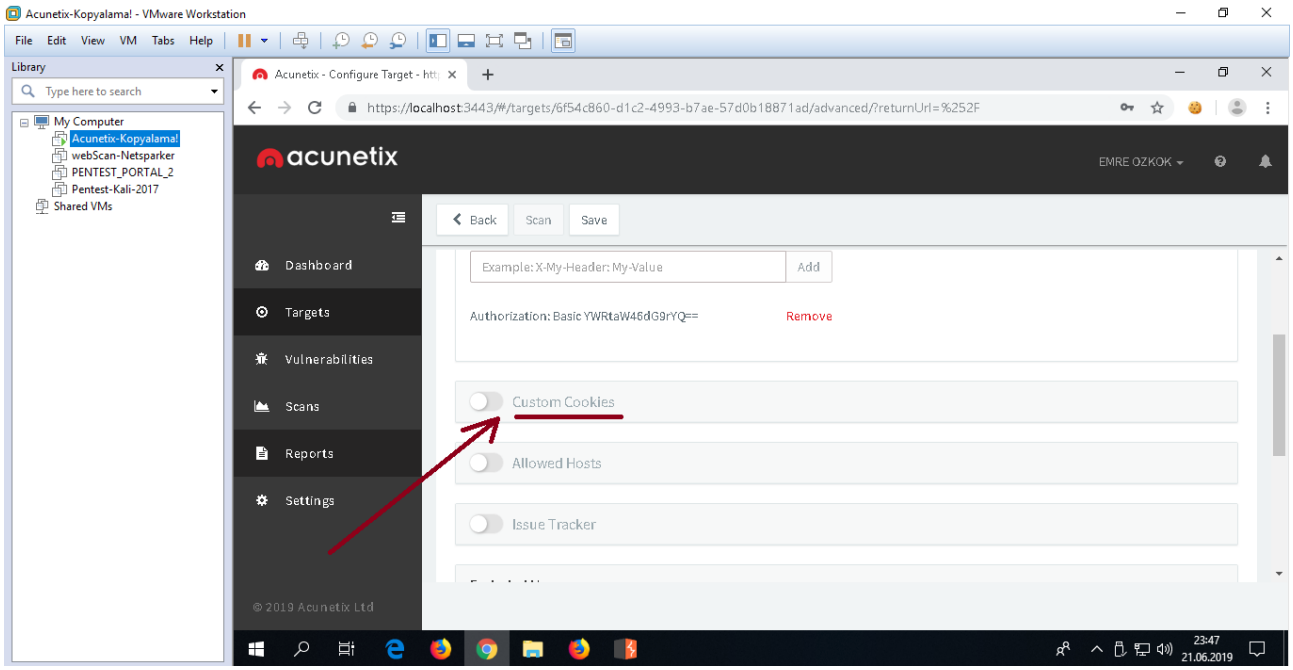


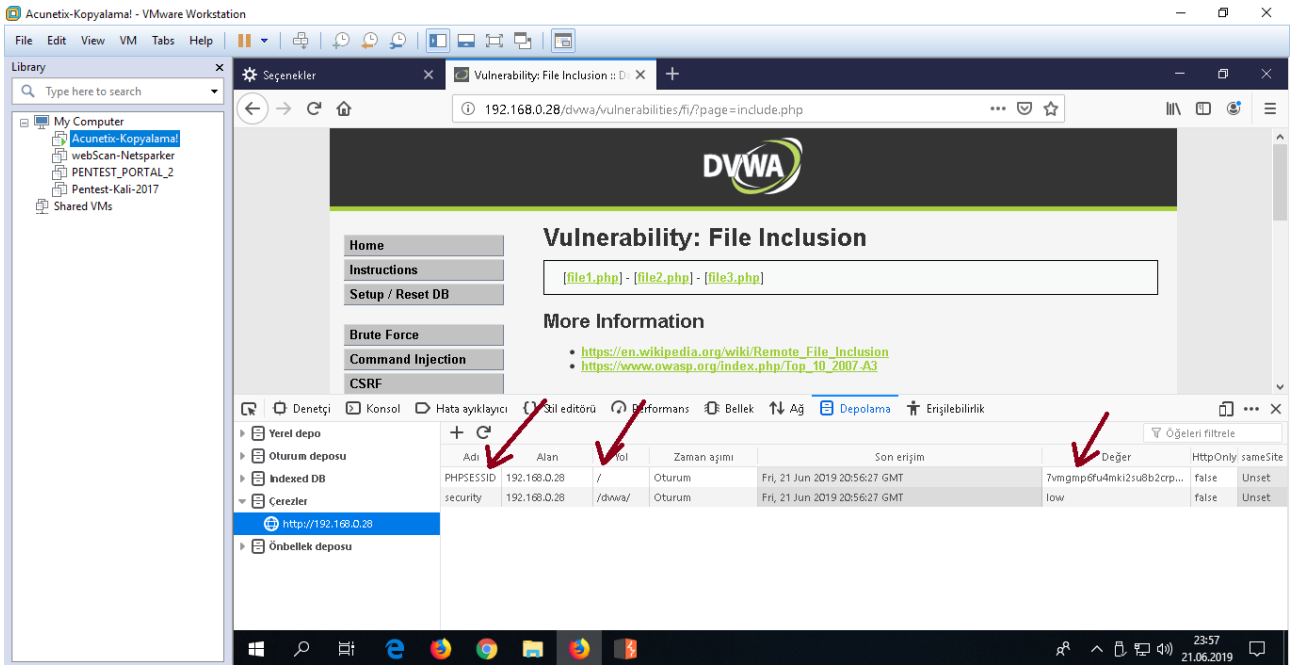
Custom Headers’a burp ile tuttuğumuz http talebindeki Authorization başlığı ilave edilir.

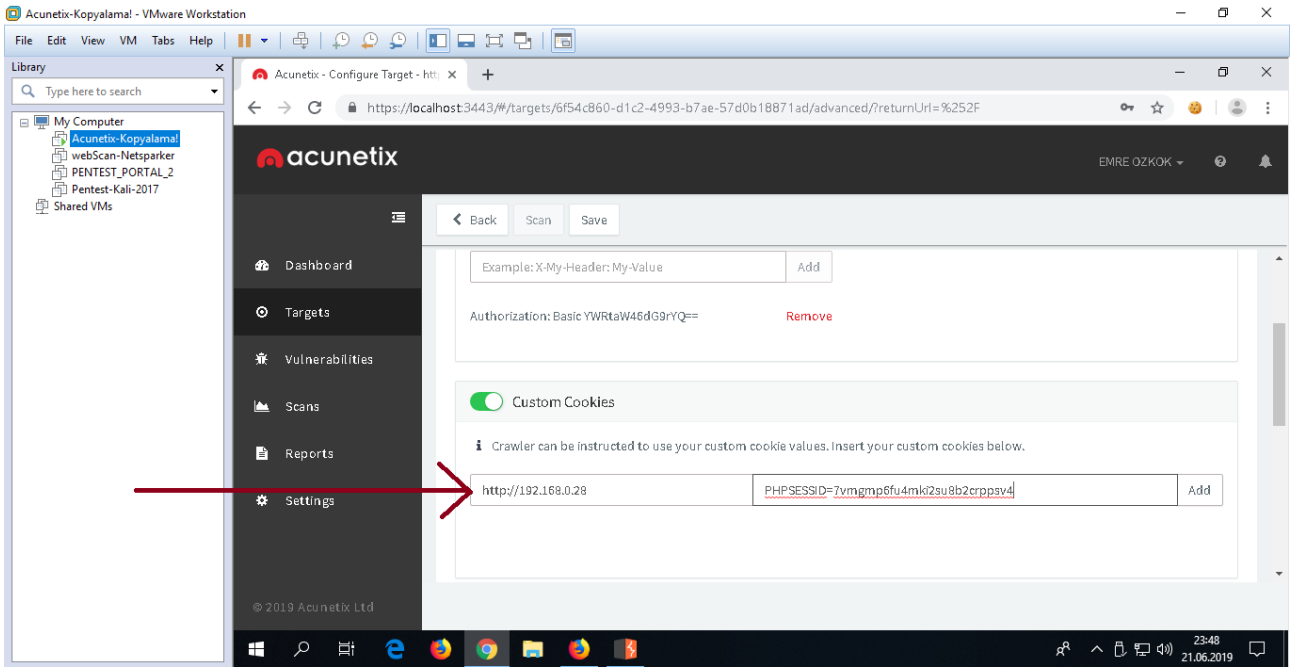


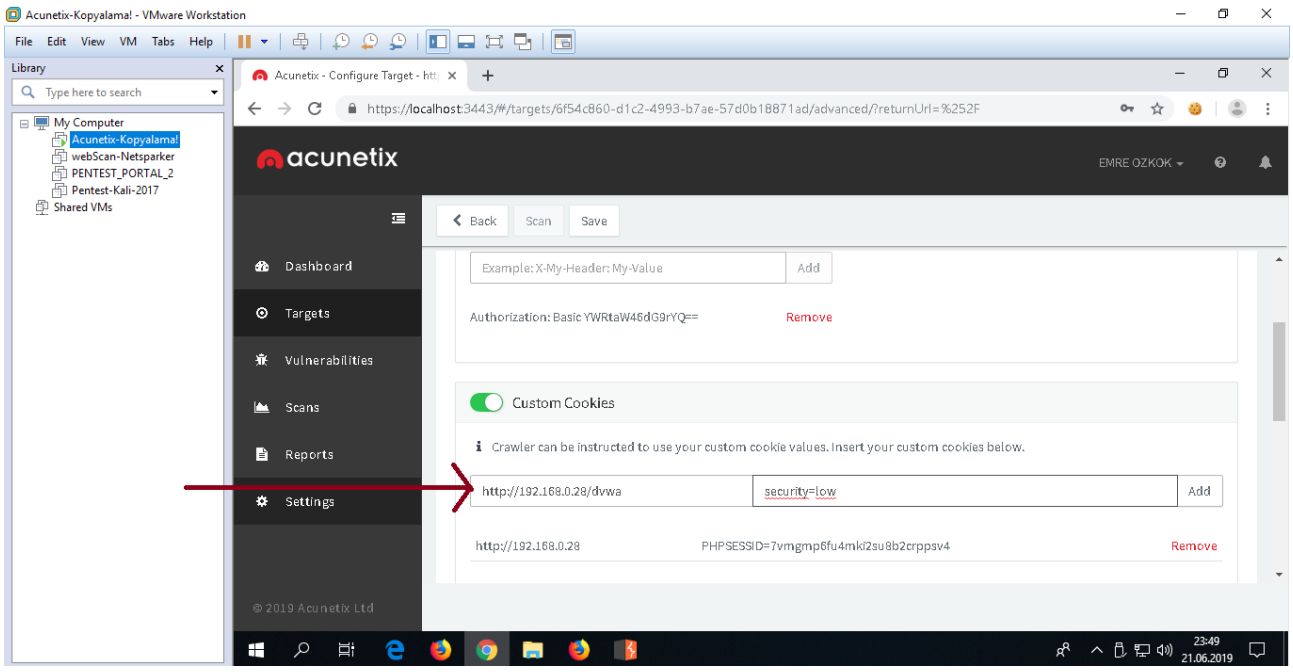


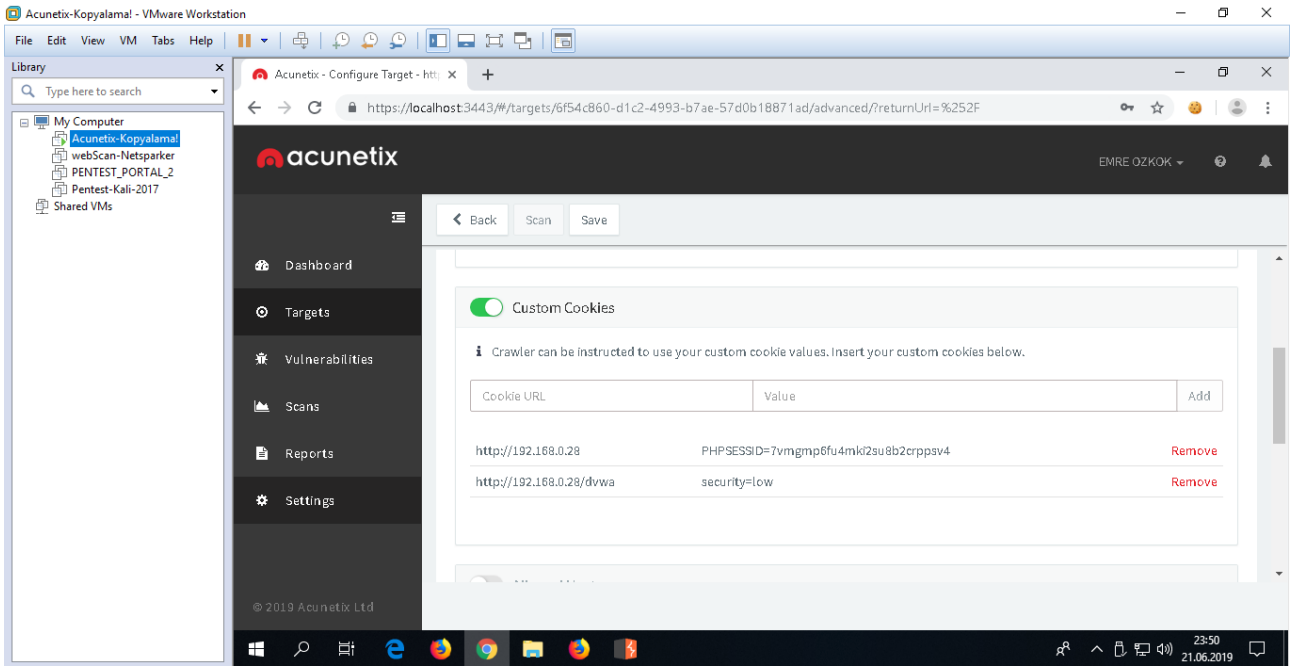
Acunetix aynı sayfada yer alan Custom Cookies'e ise tarayıcıda F12 yaparak uygulama çerezleri konur.


Acunetix-Kopyalama! - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Acunetix-Kopyalama!
webScan-Netsparker
PENTEST_PORTAL_2
Pentest-Kali-2017
Shared VMs
Acunetix - Configure Target - htt
https://localhost:3443/#/targets/6f54c860-d1c2-4993-b7ae-57d0b18871ad/advanced/?returnUrl=%252F
acunetix
EMRE OZKOK
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings
Back
Scan
Save
Example: X-My-Header: My-Value
Add
Authorization: Basic YWRtaW46dG9rYQ==
Remove
Custom Cookies
Allowed Hosts
Issue Tracker
© 2019 Acunetix Ltd
23:47
21.06.2019


Acunetix-Kopyalama! - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Acunetix-Kopyalama!
webScan-Netsparker
PENTEST_PORTAL_2
Pentest-Kali-2017
Shared VMs
Seçenekler
Vulnerability: File Inclusion
192.168.0.28/dvwa/vulnerabilities/fi/?page=include.php
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
Vulnerability: File Inclusion
[file1.php] - [file2.php] - [file3.php]
More Information
https://en.wikipedia.org/wiki/Remote_File_Inclusion
https://www.owasp.org/index.php/Top_10_2007-A3
Denetçi
Konsol
Hata ayıklayıcı
Stil editörü
Performans
Bellek
Ağ
Depolama
Erişilebilirlik
Yerel depo
Oturum deposu
Indexed DB
Çerezler
http://192.168.0.28
Önbellek deposu
Öğeleri filtrele
Adı
Alan
Yol
Zaman aşımı
Son erişim
Değer
HttpOnly
sameSite
PHPSESSID
192.168.0.28
/
Oturum
Fri, 21 Jun 2019 20:56:27 GMT
7vmgmp6fu4mki2su8b2crp...
false
Unset
security
192.168.0.28
/dvwa/
Oturum
Fri, 21 Jun 2019 20:56:27 GMT
low
false
Unset
23:57
21.06.2019

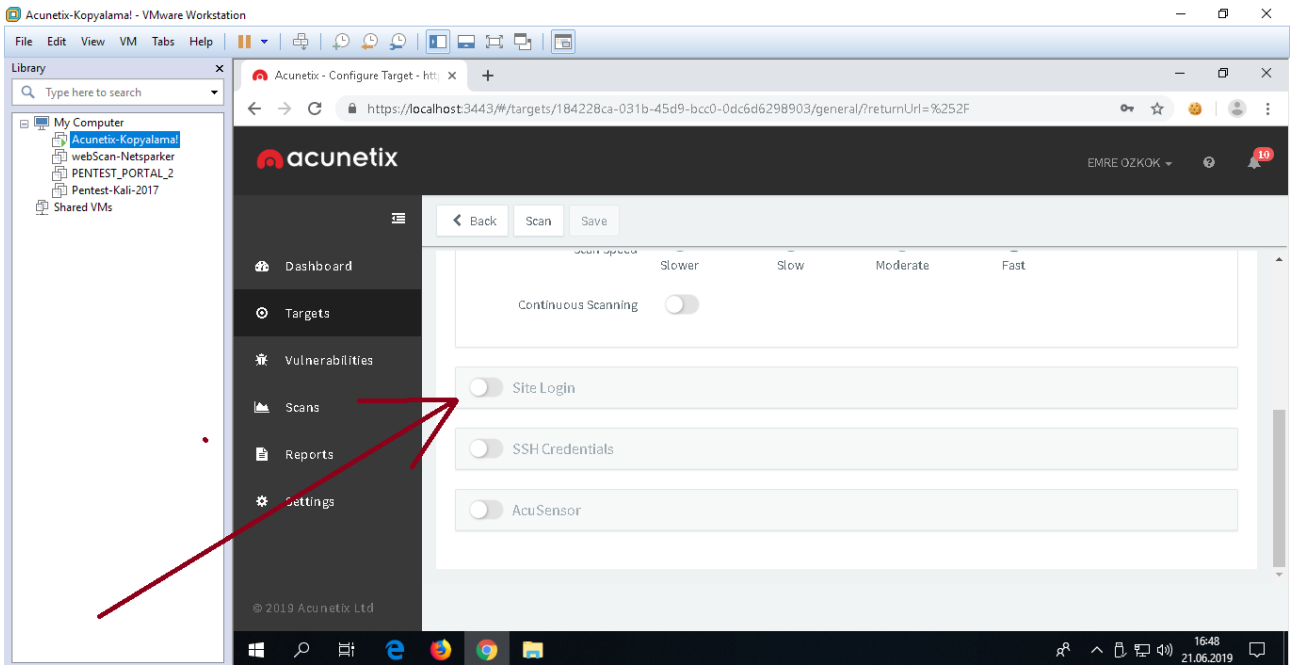

Acunetix-Kopyalama! - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Acunetix-Kopyalama!
webScan-Netsparker
PENTEST_PORTAL_2
Pentest-Kali-2017
Shared VMs
Acunetix - Configure Target - htt
https://localhost:3443/#/targets/6f54c860-d1c2-4993-b7ae-57d0b18871ad/advanced/?returnUrl=%252F
acunetix
EMRE OZKOK
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings
Back
Scan
Save
Example: X-My-Header: My-Value
Add
Authorization: Basic YWRtaW46dG9rYQ==
Remove
Custom Cookies
Crawler can be instructed to use your custom cookie values. Insert your custom cookies below.
http://192.168.0.28
PHPSESSID=7vmgmp6fu4mkl2su8b2crppsv4
Add
© 2019 Acunetix Ltd
23:48
21.06.2019

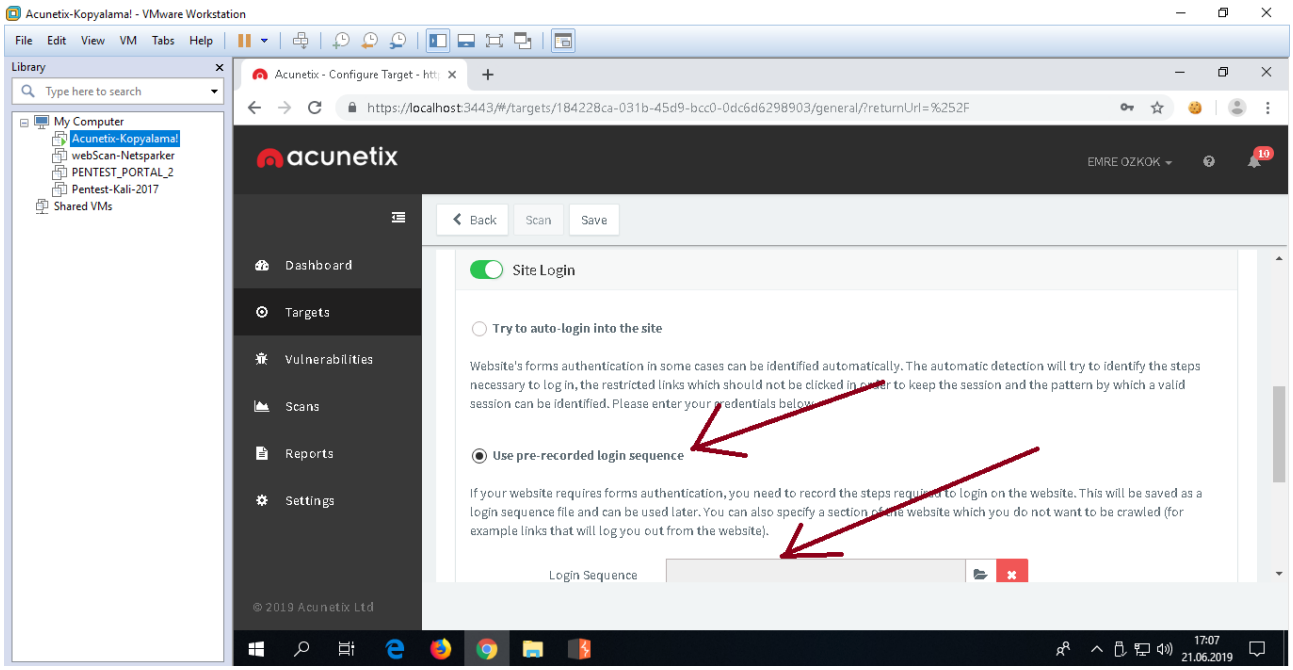

Acunetix-Kopyalama! - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Acunetix-Kopyalama!
webScan-Netsparker
PENTEST_PORTAL_2
Pentest-Kali-2017
Shared VMs
Acunetix - Configure Target - htt
https://localhost:3443/#/targets/6f54c860-d1c2-4993-b7ae-57d0b18871ad/advanced/?returnUrl=%252F
acunetix
EMRE OZKOK
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings
Back
Scan
Save
Example: X-My-Header: My-Value
Add
Authorization: Basic YWRtaW46dG9rYQ==
Remove
Custom Cookies
Crawler can be instructed to use your custom cookie values. Insert your custom cookies below.
http://192.168.0.28/dvwa
security=low
Add
http://192.168.0.28
PHPSESSID=7vmgmp6fu4mkl2su8b2crppsv4
Remove
© 2019 Acunetix Ltd
23:49
21.06.2019



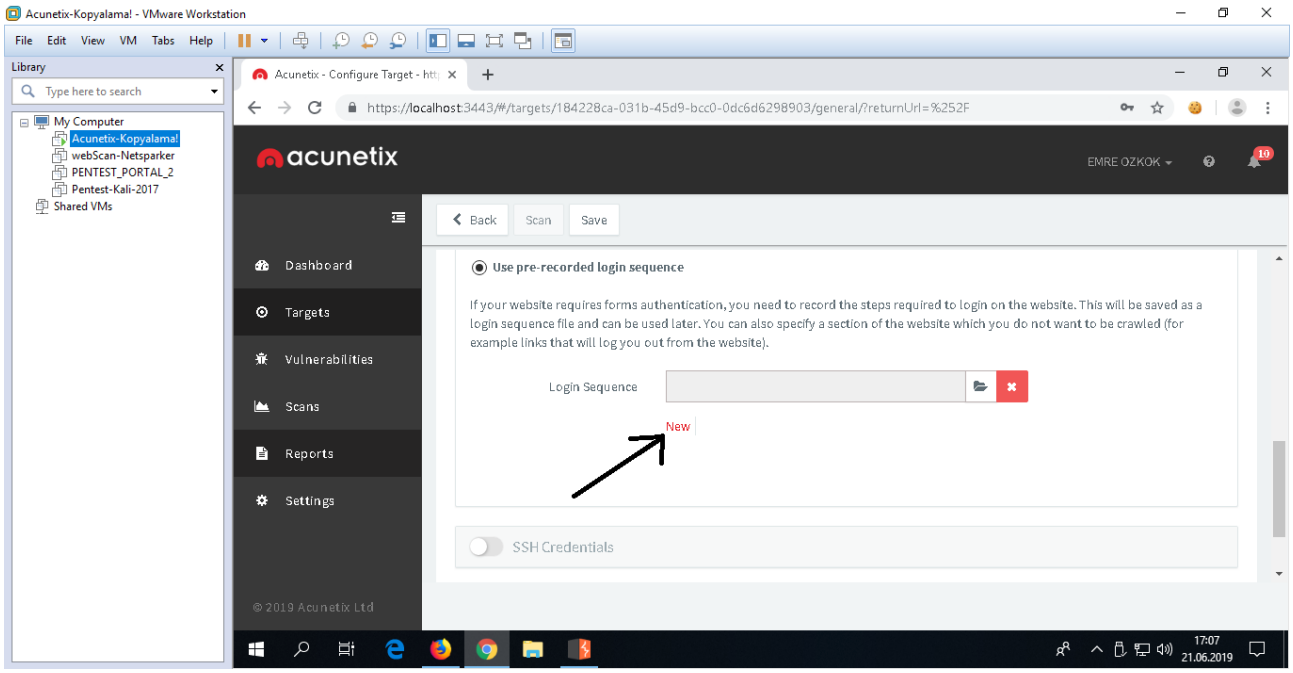
Http basic çerezi eklemesi sonrası şimdi Acunetix'in General sekmesi altındaki Login Recorder seçeneğiyle yazılıma web app'teki login aşamasını geçme adımlarını öğretelim.

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

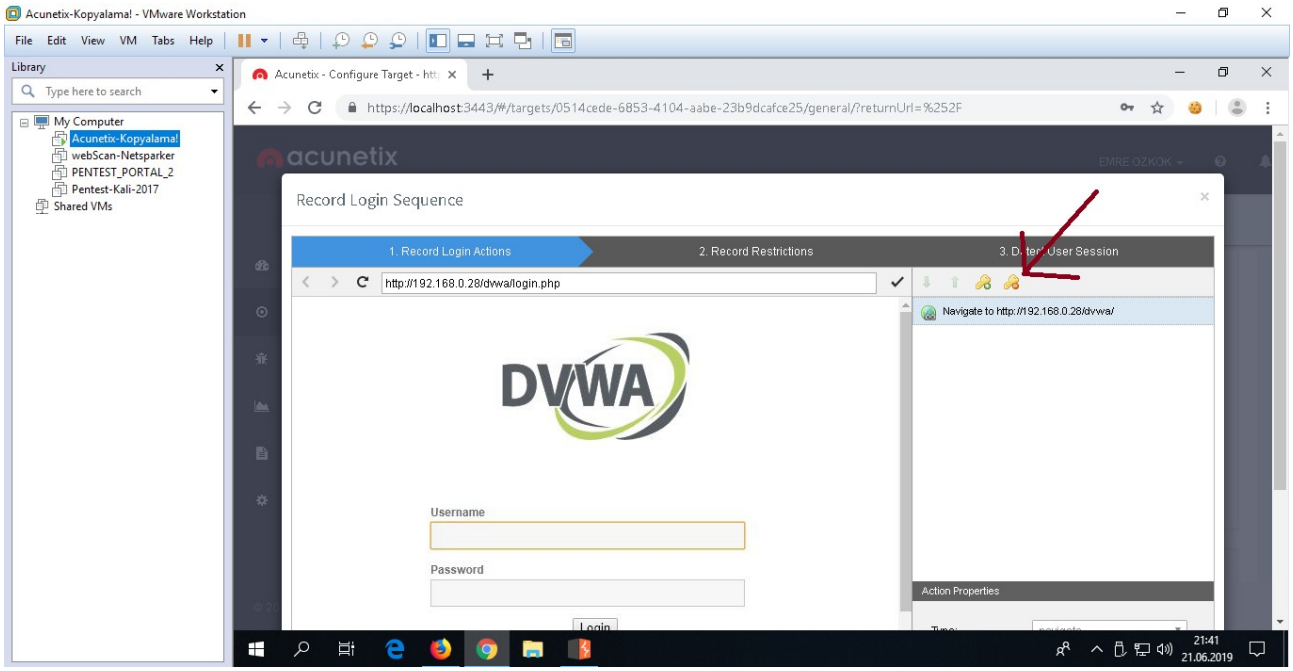


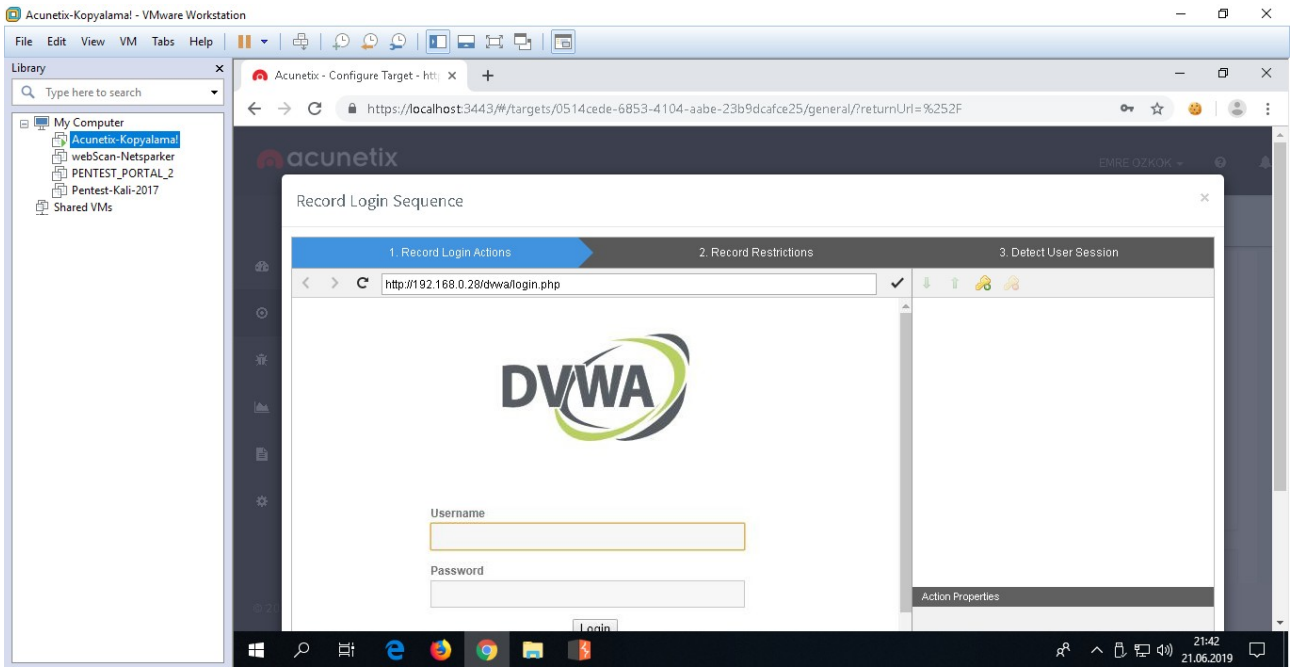


New ile sıfır bir Login Recorder (Login Adım Kaydedicisi) oluşturulur.

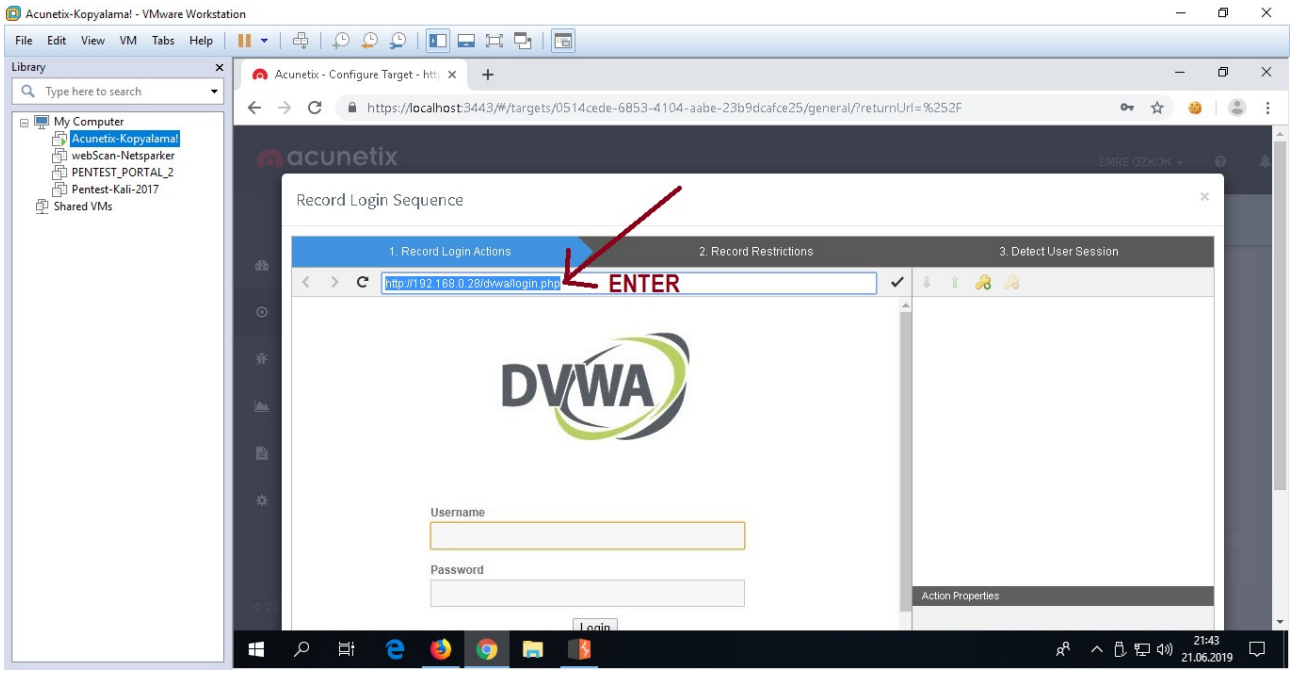


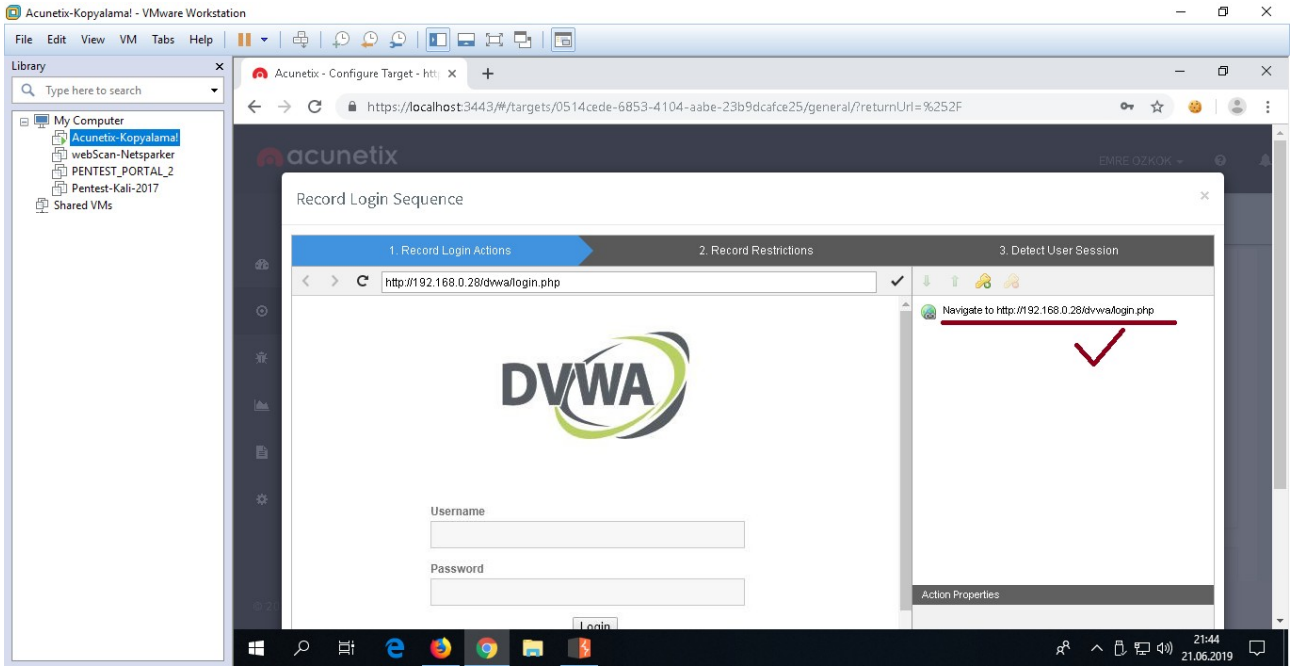
Açılan penceredeki Record Login Actions (Login Eylemlerini Kaydetme) bölümünde sağ yan boşluktaki ilk adım olarak gösterilen URL satırı login url'i esasında olmadığından onu silelim.



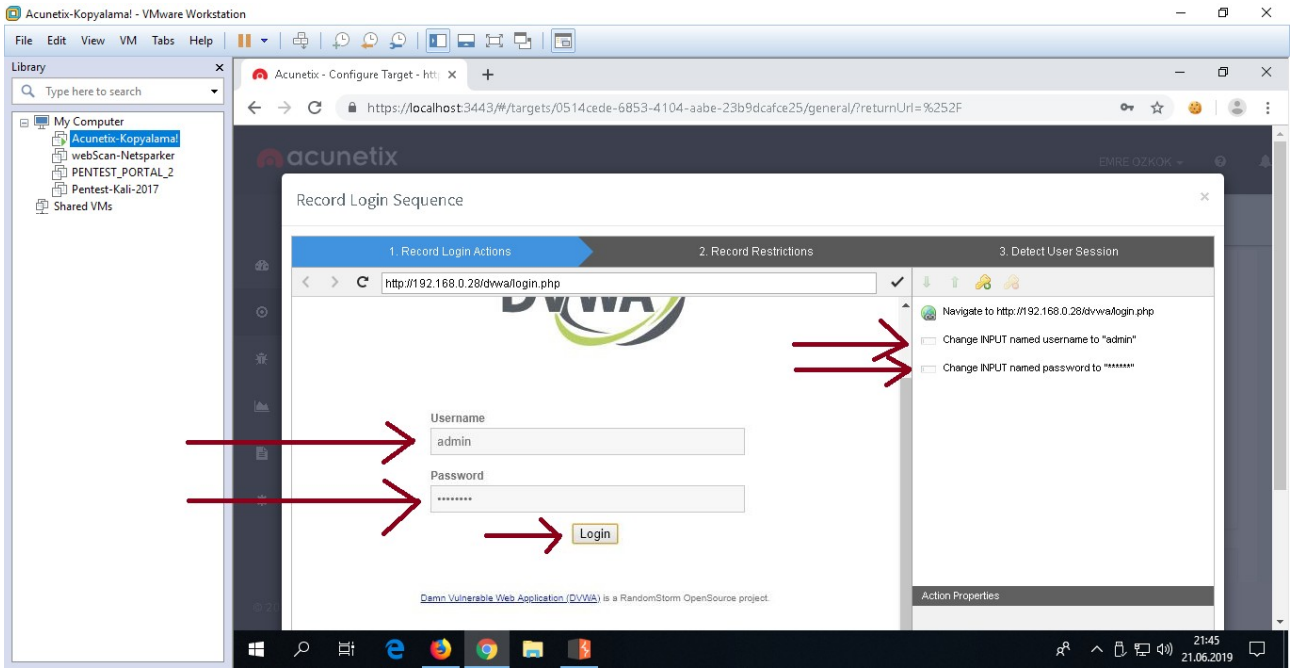


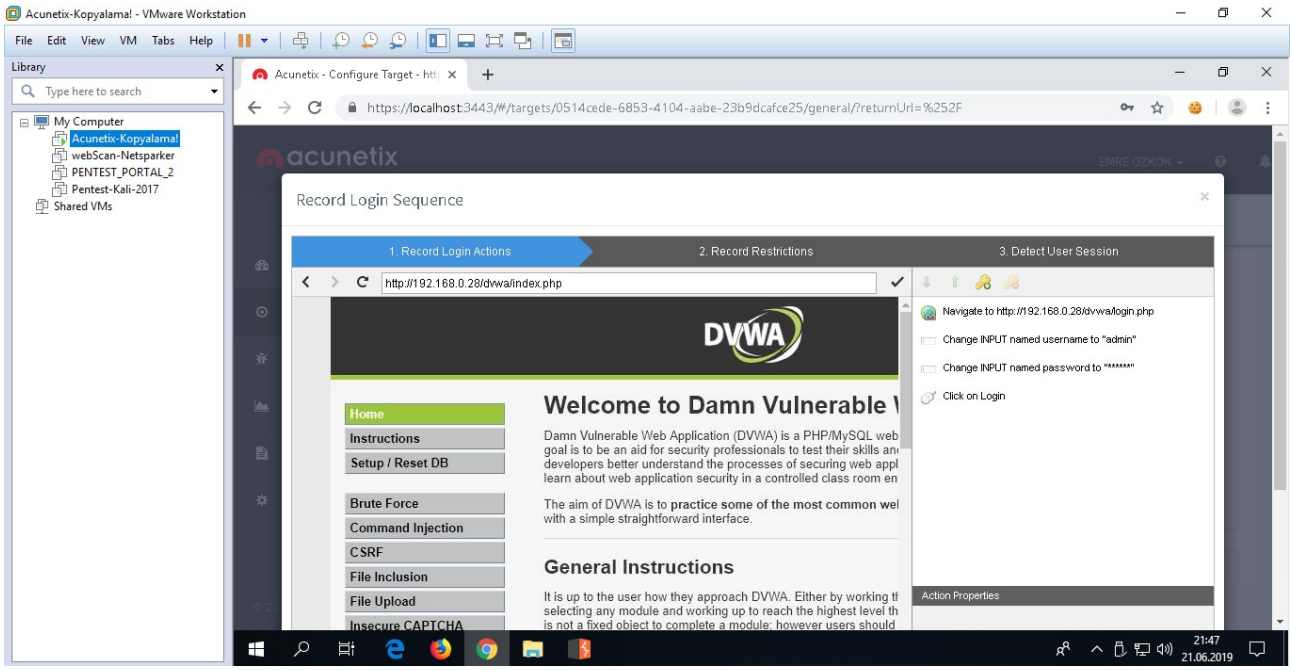
Esas Login URL'i (adresi) ana ekranda görünen URL olduğundan adres çubuğundaki URL'i seçip ENTER'layalım.



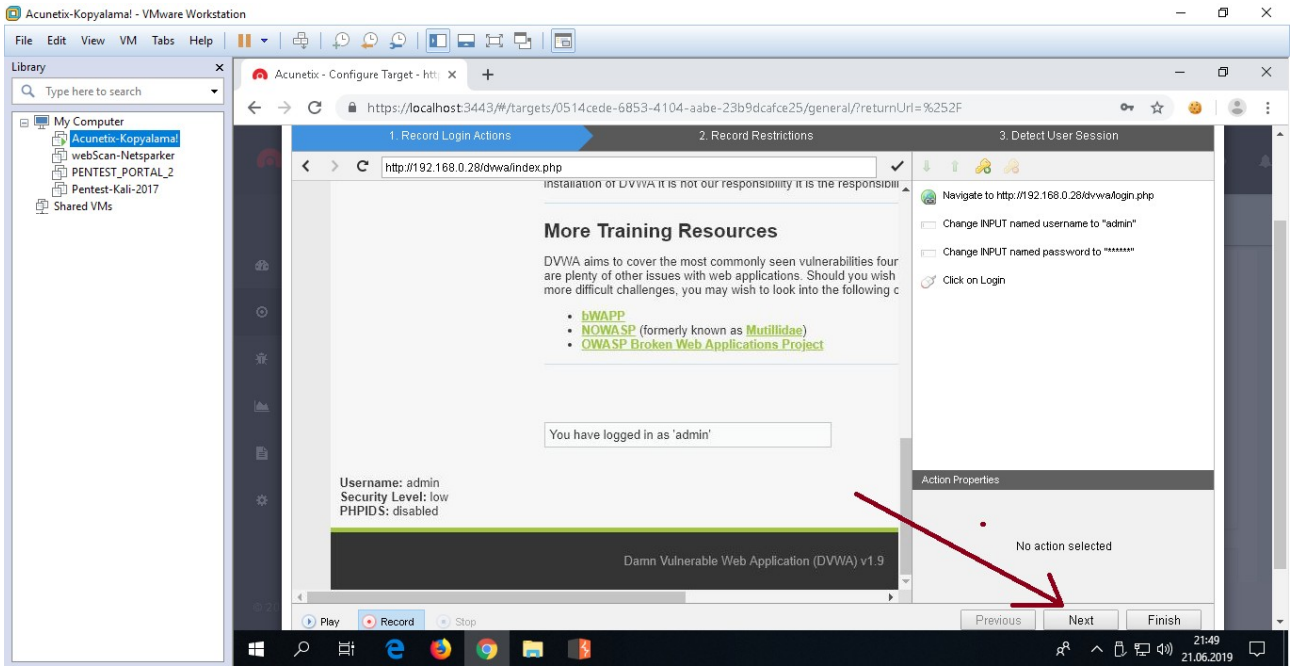


Böylece login URL'i ilk adım olarak kayda girecektir. Daha sonra login ekranında username ve password kısımlarına sırasıyla dvwa hesap bilgilerini girelim ve Login butonuna basarak oturum açalım.

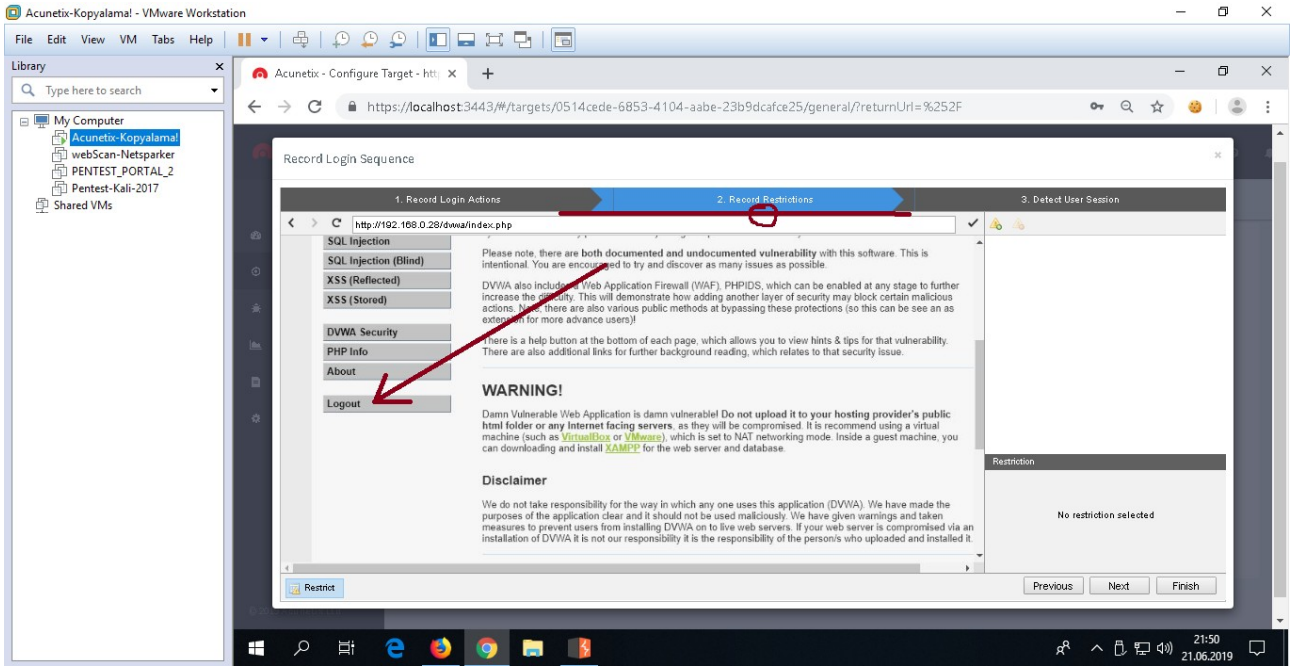




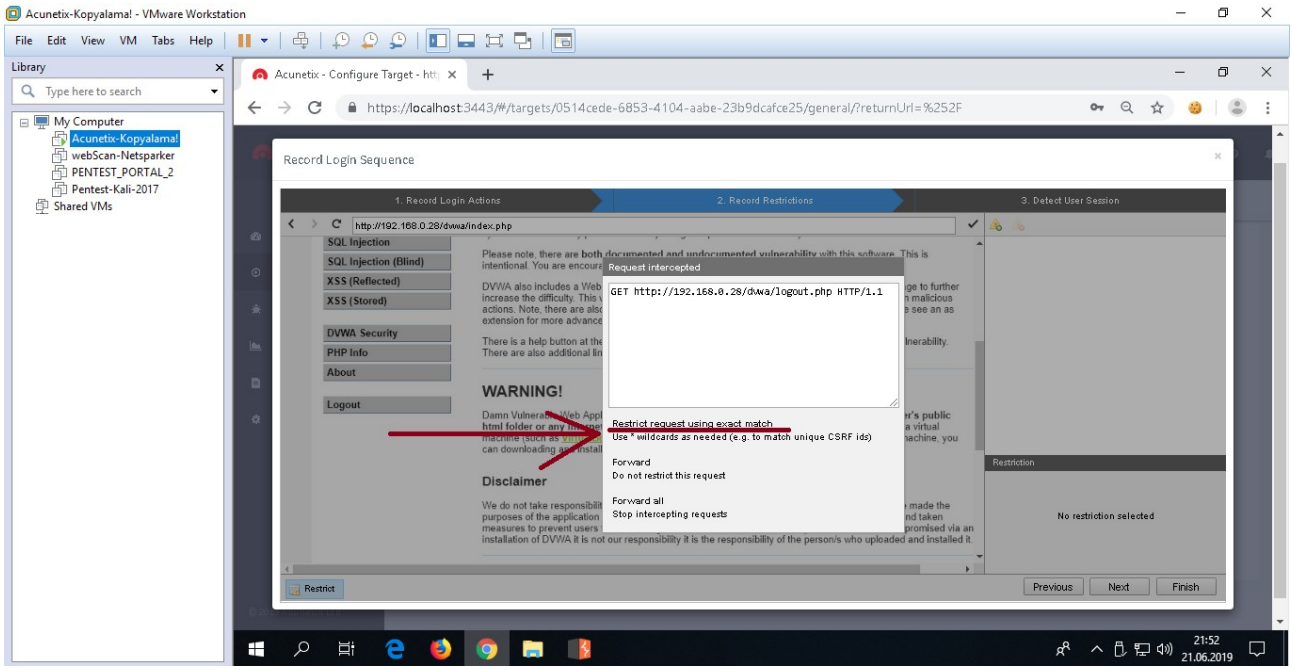
Oturum açılır. Sağ yan boşlukta, takip edilen adımların sırasıyla kayıt altına alındığı görülebilir. Şimdi Next butonu ile Logout adımını kaydetme sayfasına geçelim.

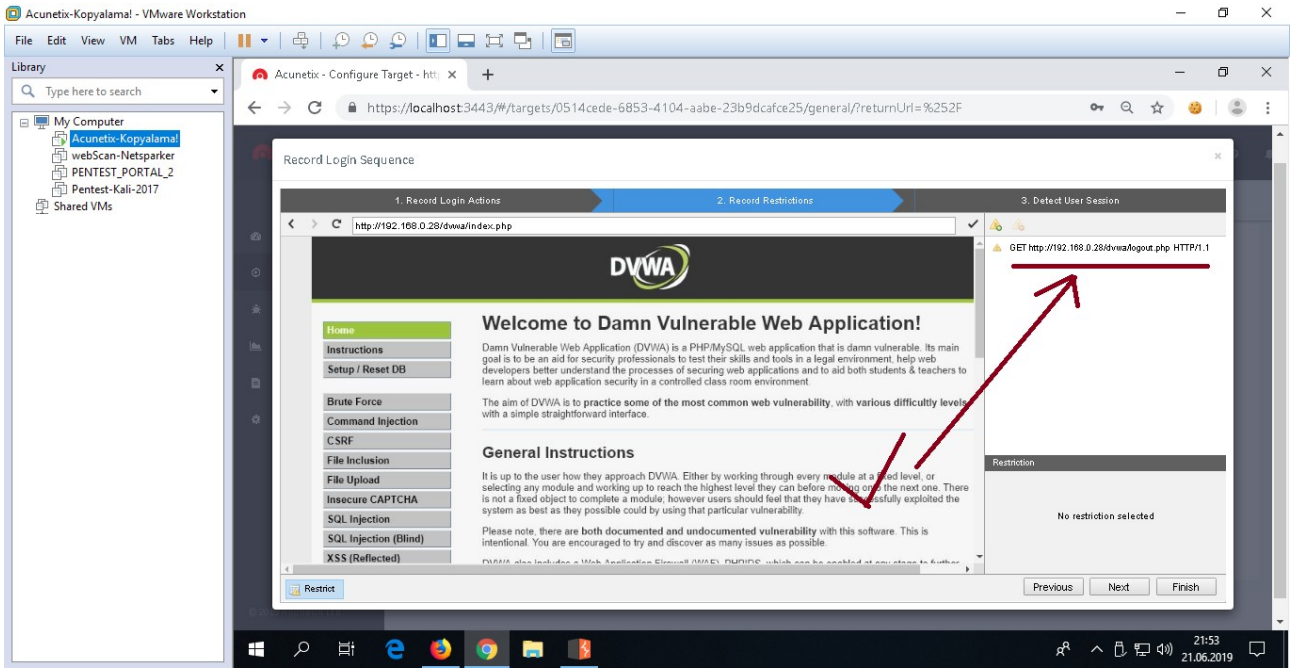


Record Restriction (Kısıtlayıcılığı Kaydet) bölümünde uygulamanın logout seçeneğine tıklanır ve

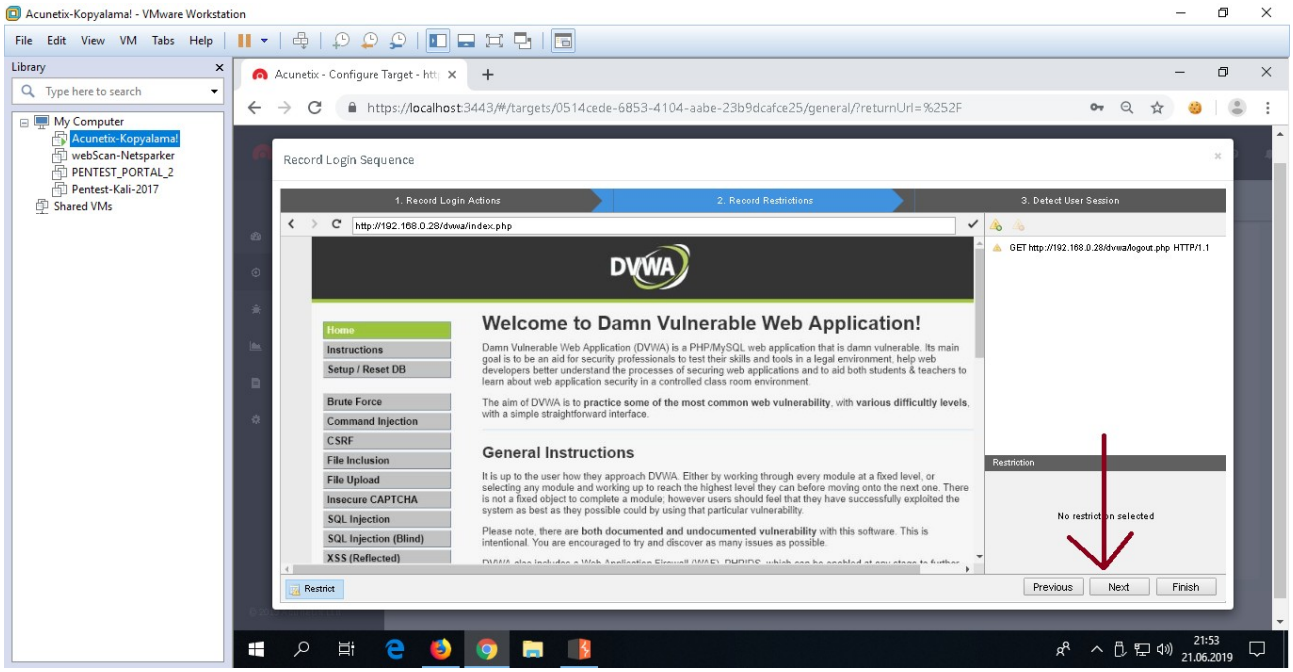


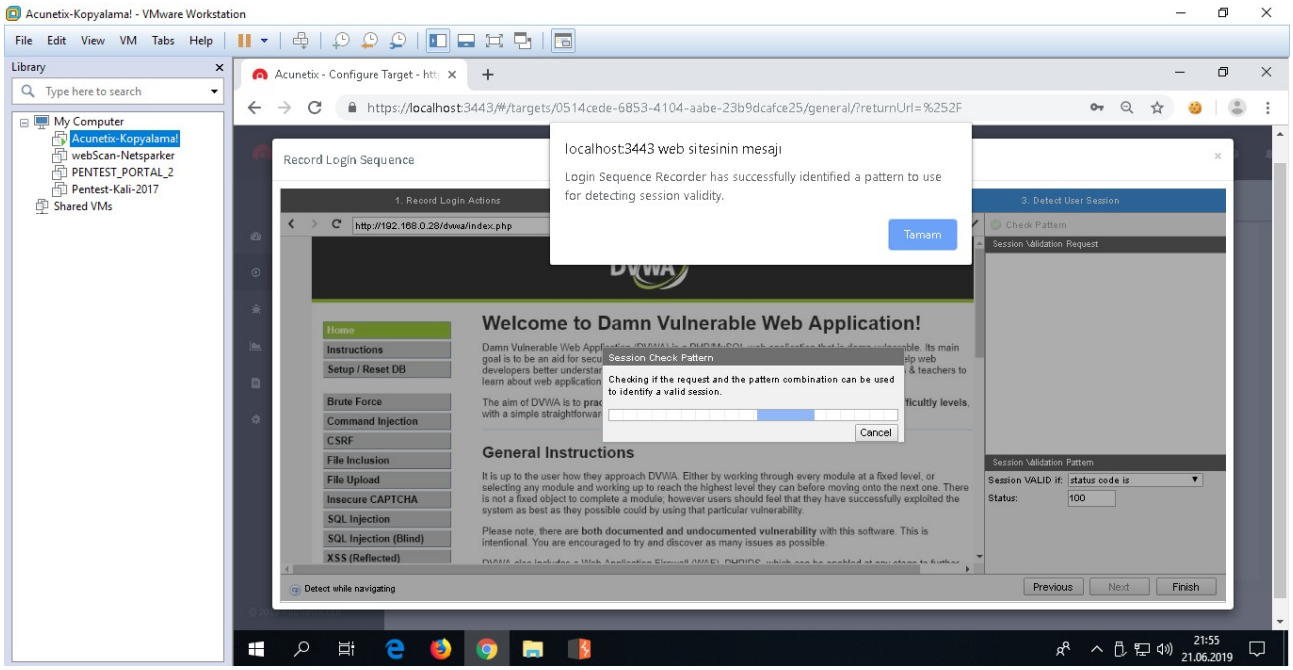
ekrana gelen “bu tık için Restrict” seçeneğine tıklanır. Böylece Acunetix logout butonunu öğrenmiş olur.



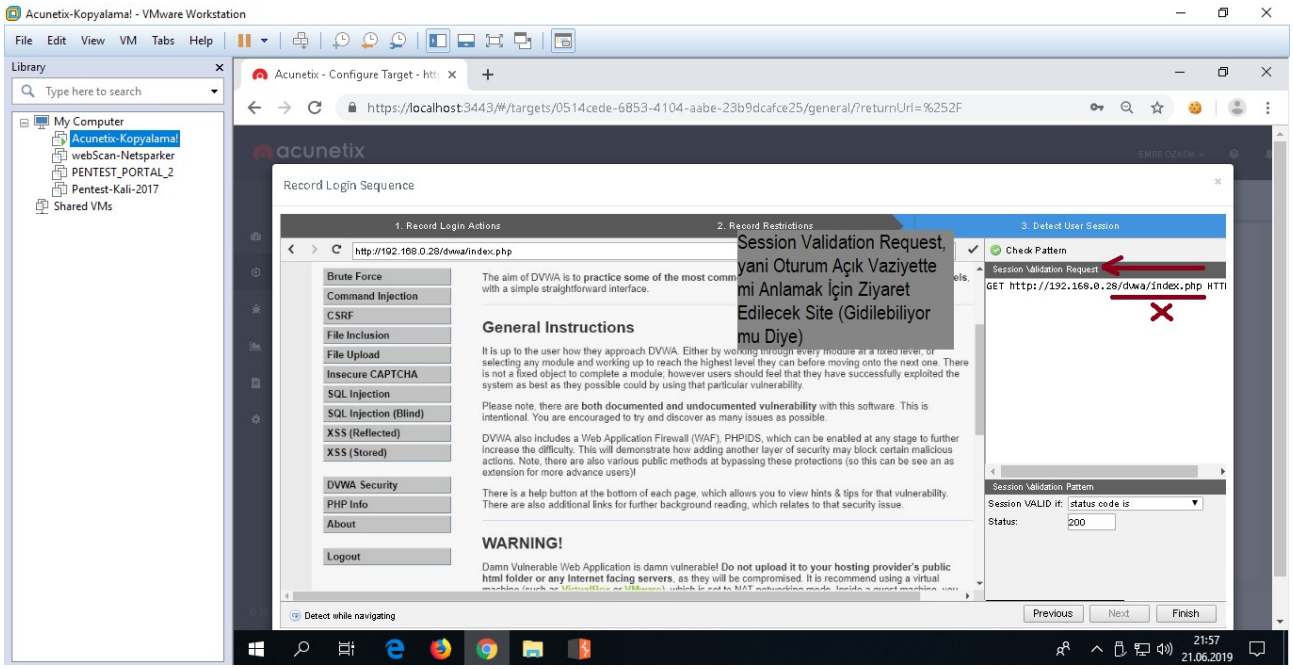


Şimdi login ve logout mekanizması açısından her şey yolunda mı diye sonraki (yani son) aşamaya geçilir.





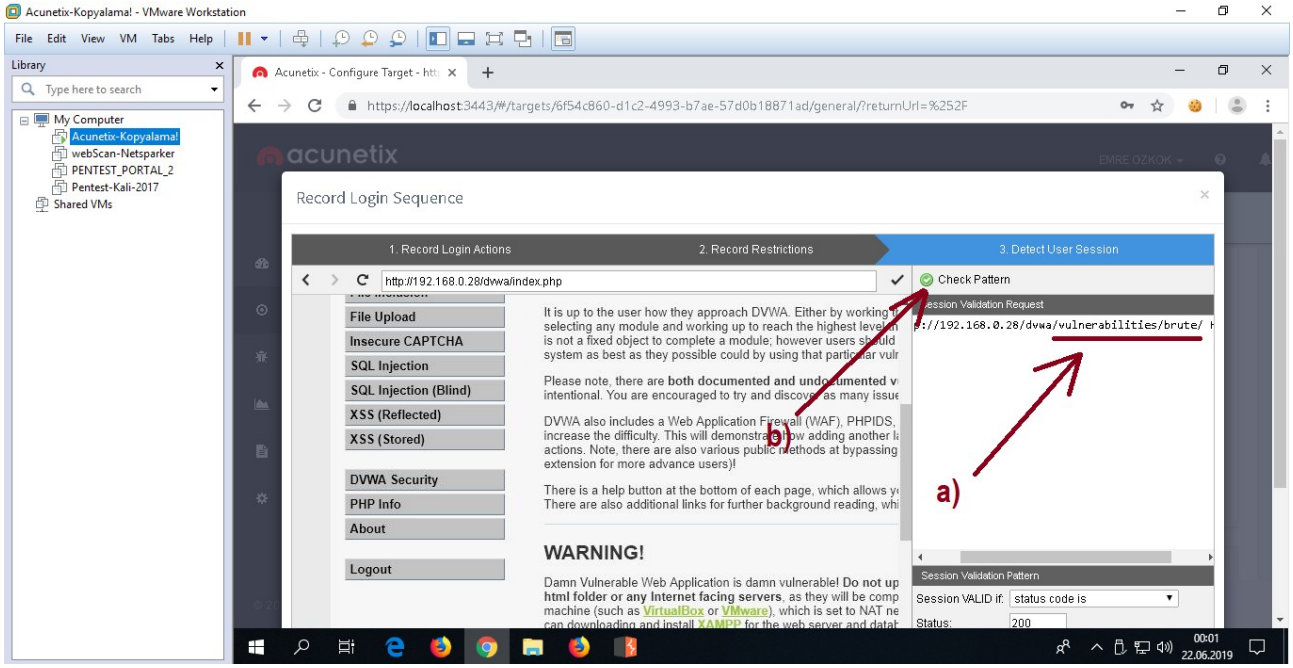
Son aşamaya geçildiğinde ekrana gelen popup ile oturumun korunabilirliğinde sorun yoktur mesajı gelmiştir. Son olarak bulunulan bu son aşamadaki sağ yan boşlukta yer alan “Session Validation Request” kısmındaki URL incelenmelidir.

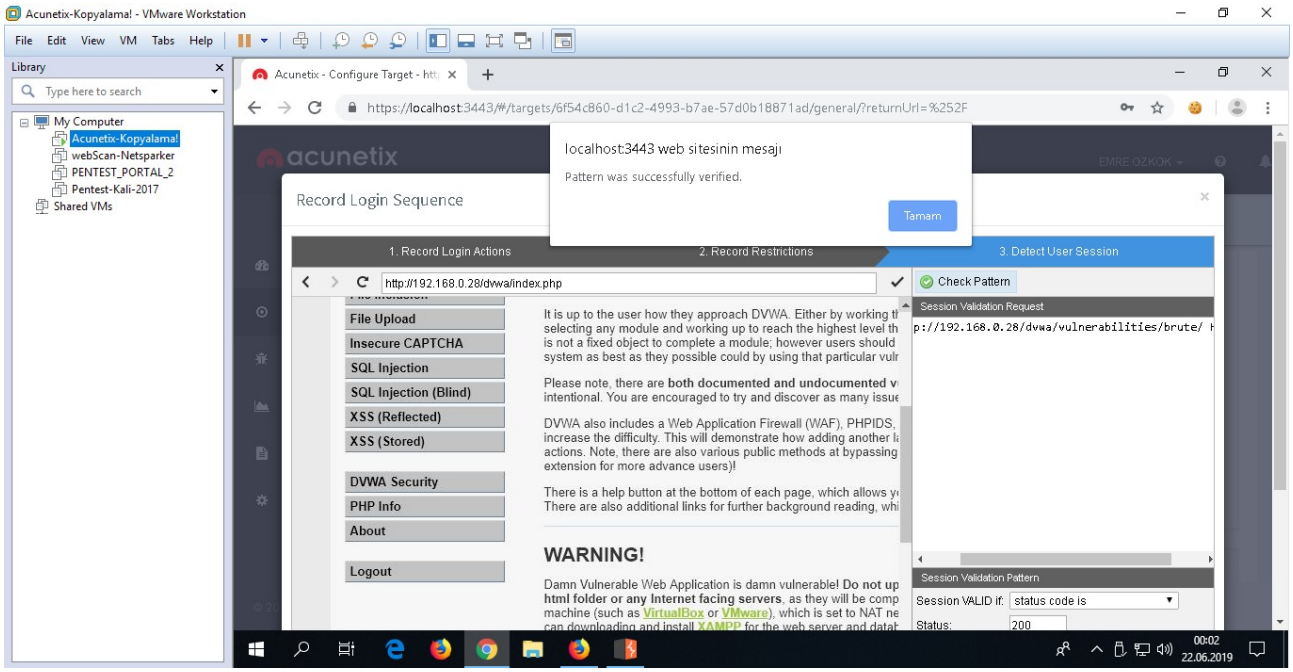


Acunetix tarama sırasında oturumu kaybedip kaybetmediğini (yani kapı dışarı kalıp kalmadığını) anlamak için son bir kurala ihtiyaç duyar. Bu da sadece oturum açıkken erişilebilir olan bir URL'i Session Validation Request bölümüne koymaktır.

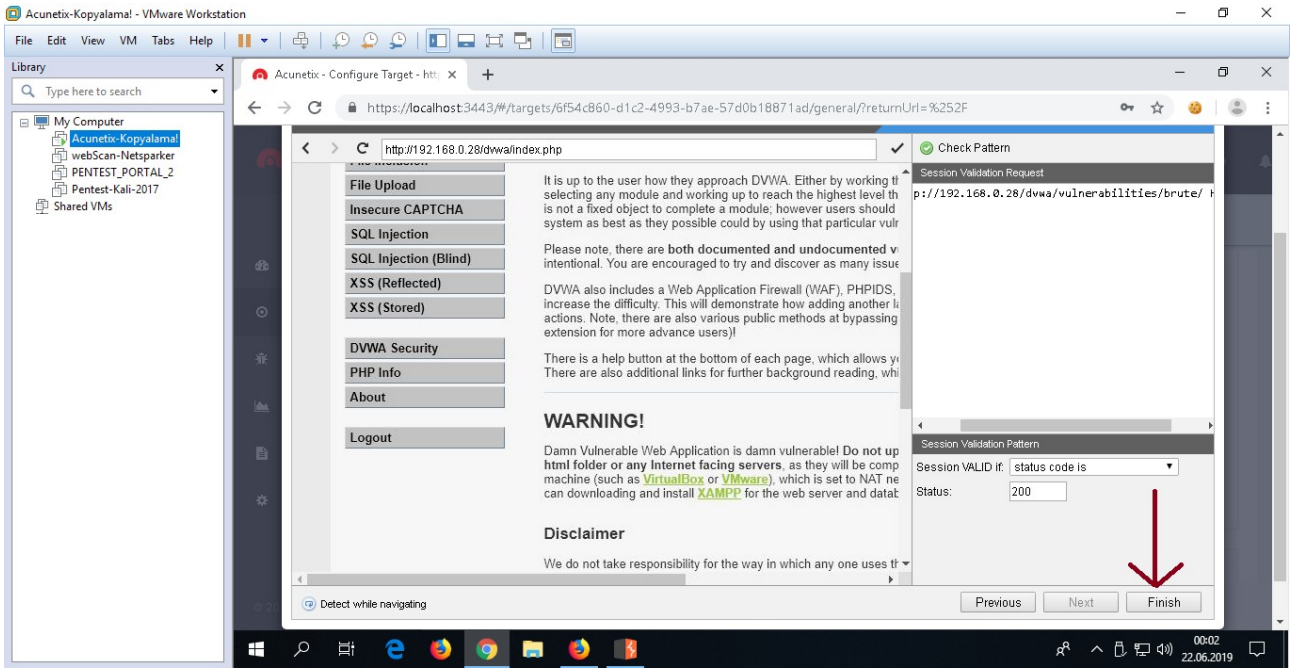
> NOT:
>
> DVWA yapısal anlamda bir kusura sahip olduğundan index.php sayfası 200 OK ile login.php'ye yönlendirebilmektedir. Veya oturum açıkken halen login.php gelebilmektedir. Bu nedenle daha sağlam bir URL olarak sadece oturum açıkken içeriğine erişilebilen şu URL verilmiştir:
>
> *GET http://192.168.0.28/dvwa/vulnerabilities/brute/ 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.



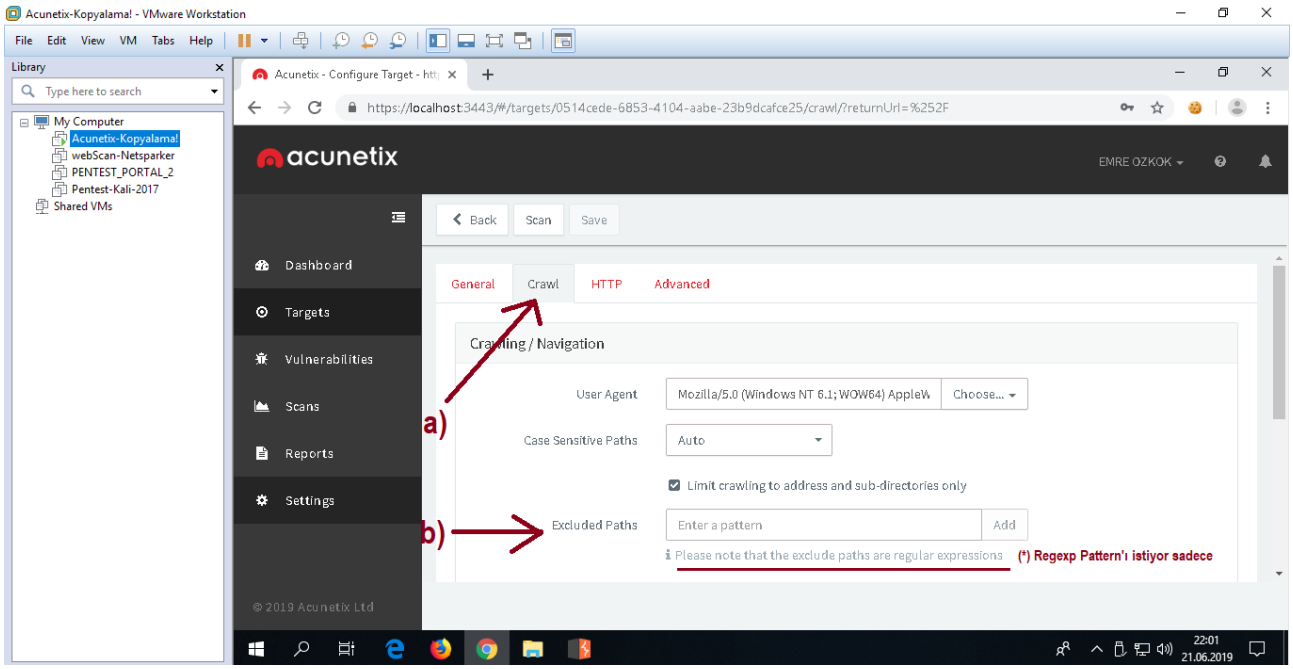


Ekrana popup ile pattern'da sorun yoktur mesajı geldikten sonra son aşamaya Finish diyerek login olma adımları tamamen kaydedelim.



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.

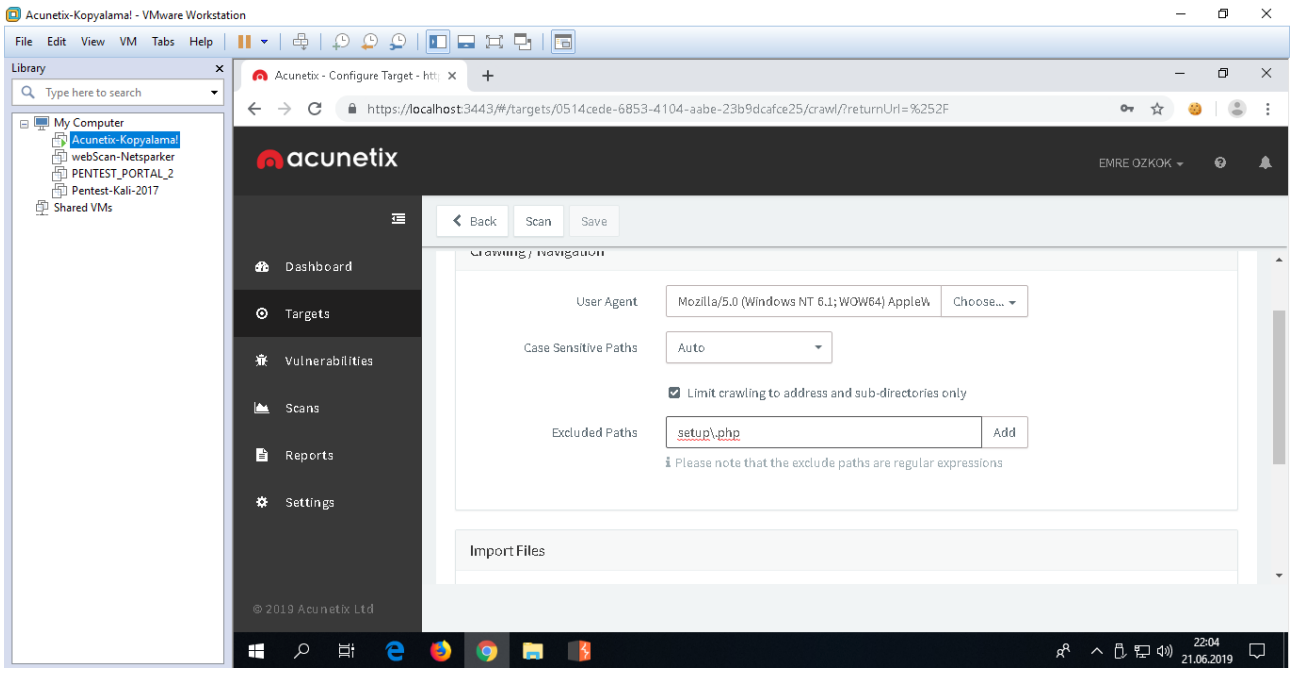
Login Recorder tanımlaması tamam olduktan sonra tarama profilinin Crawl sekmesine gelinir ve Exclude Paths seçeneğine tarama sırasında taramaya dahil edilmemesi istenen dizin yolları girilir.

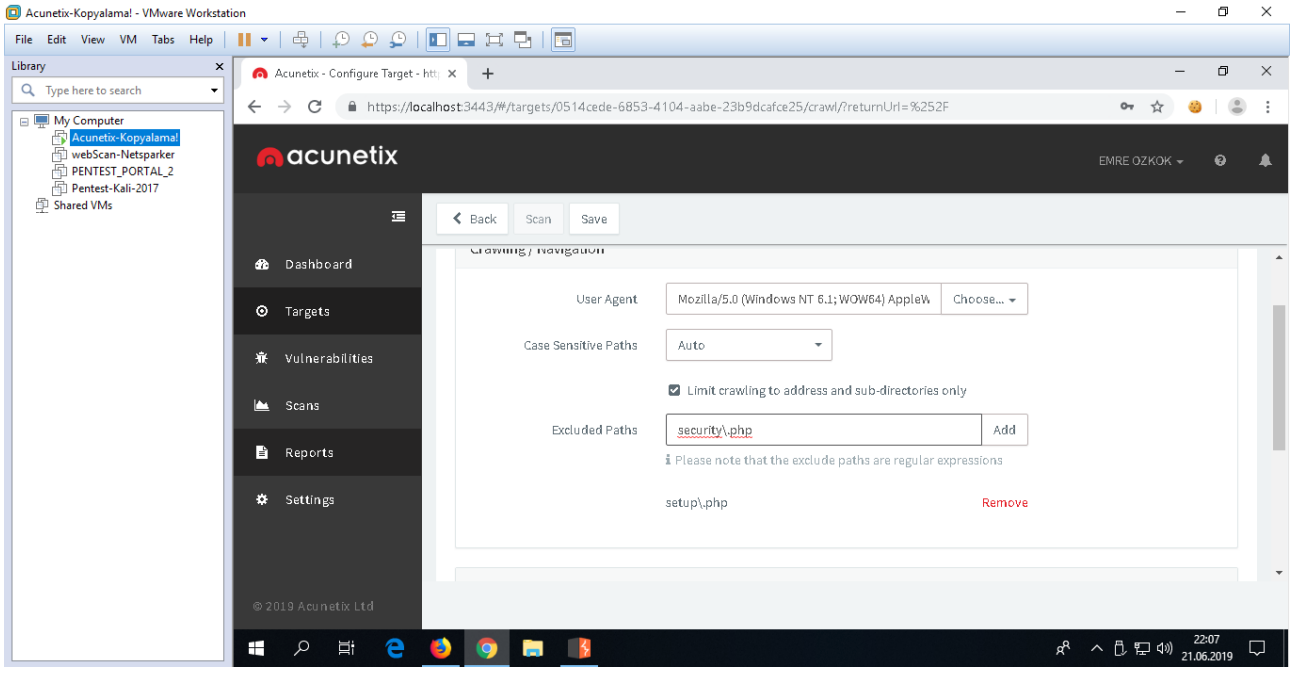


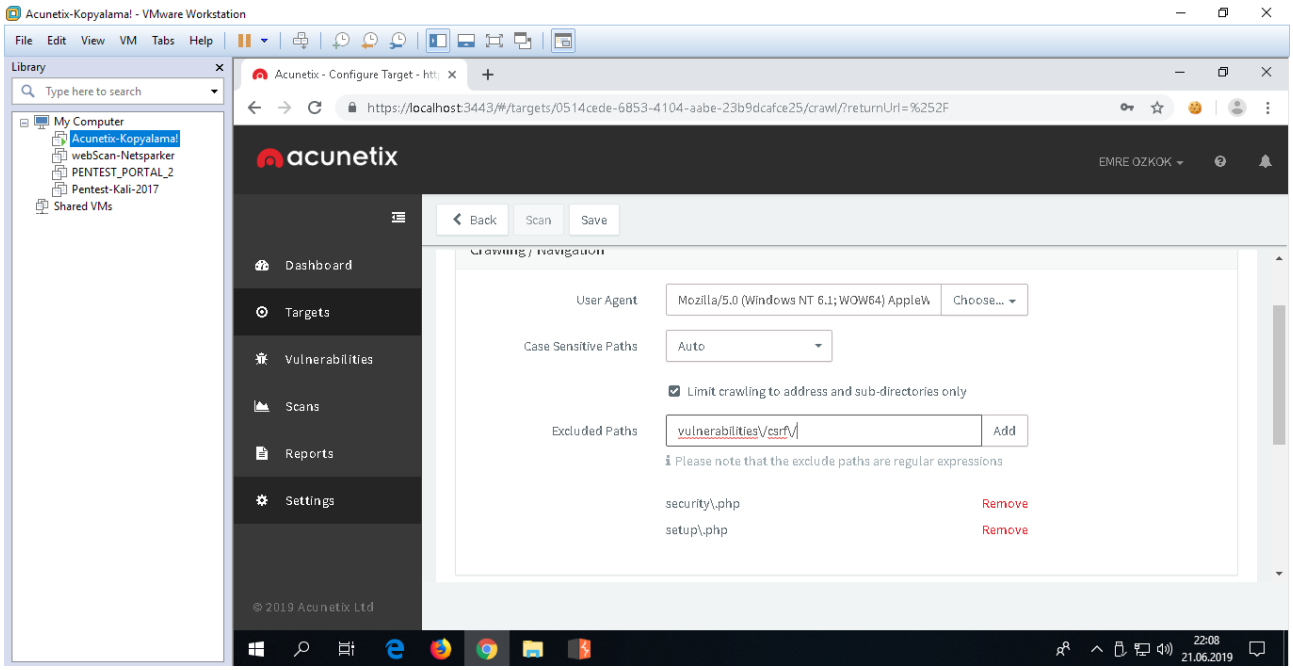
Taranmasın denilen dizinler regexp pattern'ı formatında girilmek durumundadır. Çünkü "*Please note that the exclude paths are regular expression*" denmektedir.

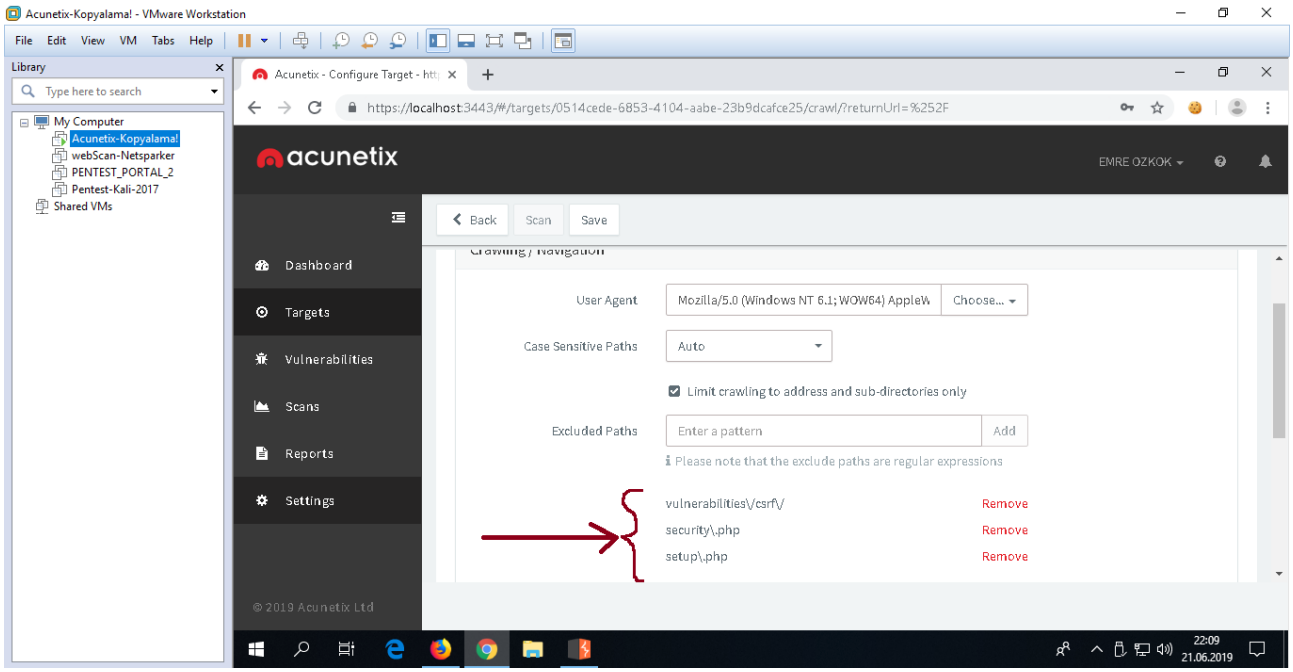
Dolayısıyla DVWA'da setup.php sayfasının taranmaması için setup.\php , security.php sayfasının taranmaması için security\.php , vulnerabilities/csrf/ dizinin taranmaması için vulnerabilities\/csrf\/ girilmelidir.

Aşağıda setup.php sayfası, security.php sayfası ve vulnerabilities/csrf/ dizini dışlanmıştır.





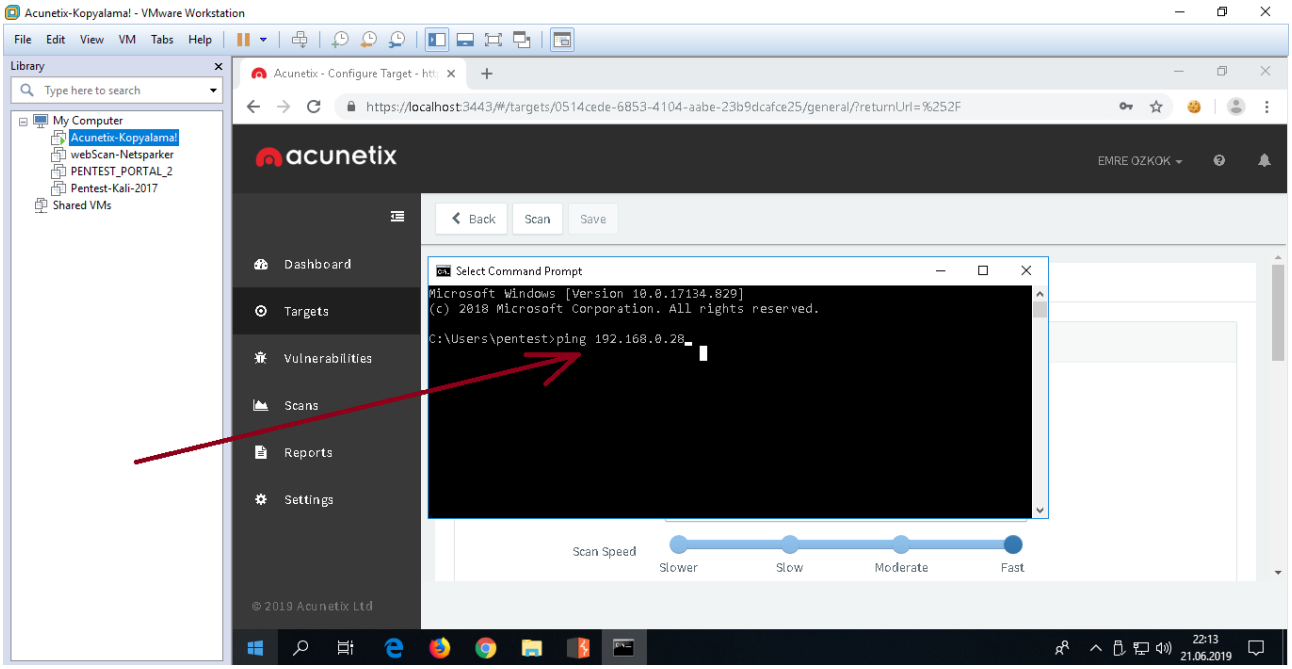


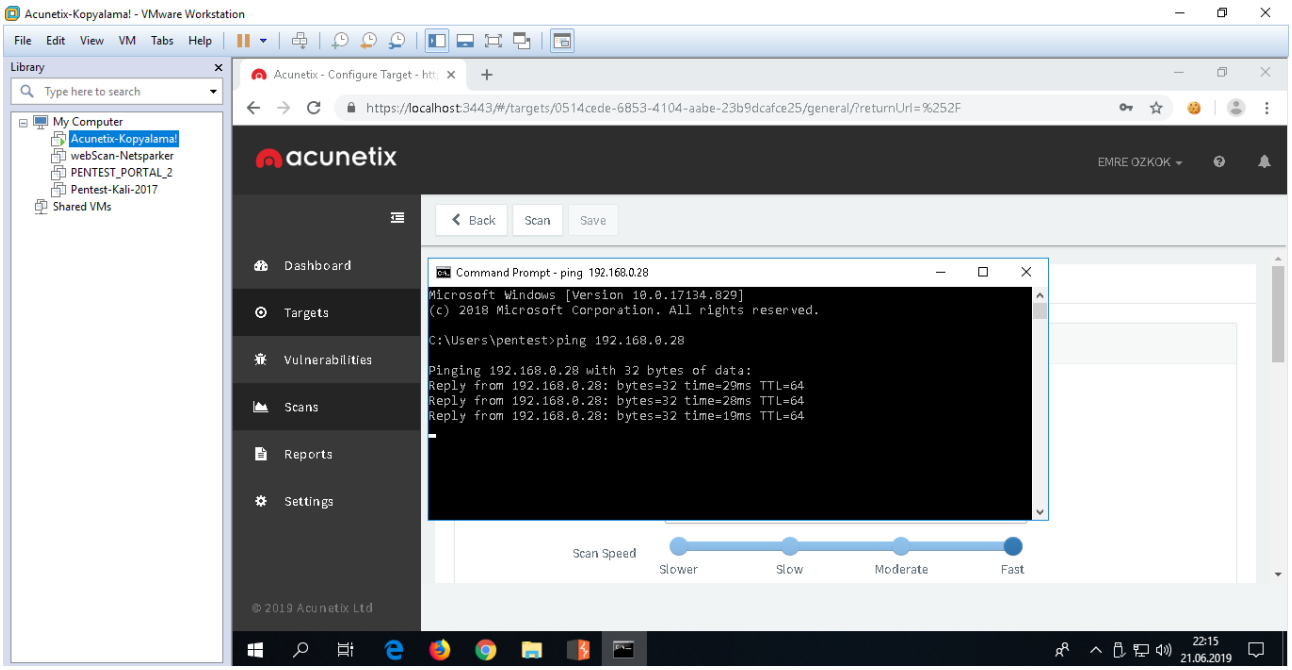


setup.php sayfası uygulamanın kullandığı veritabanını reset'lediğinden dışlanmıştır. security.php sayfası uygulamanın güvenlik seviyesini arttırdığından taramanın bulgularını azaltmasın diye dışlanmıştır. csrf/ dizini ise senaryosu gereği uygulamanın hesap parolasını değiştirdiğinden tarama dışında tutulması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



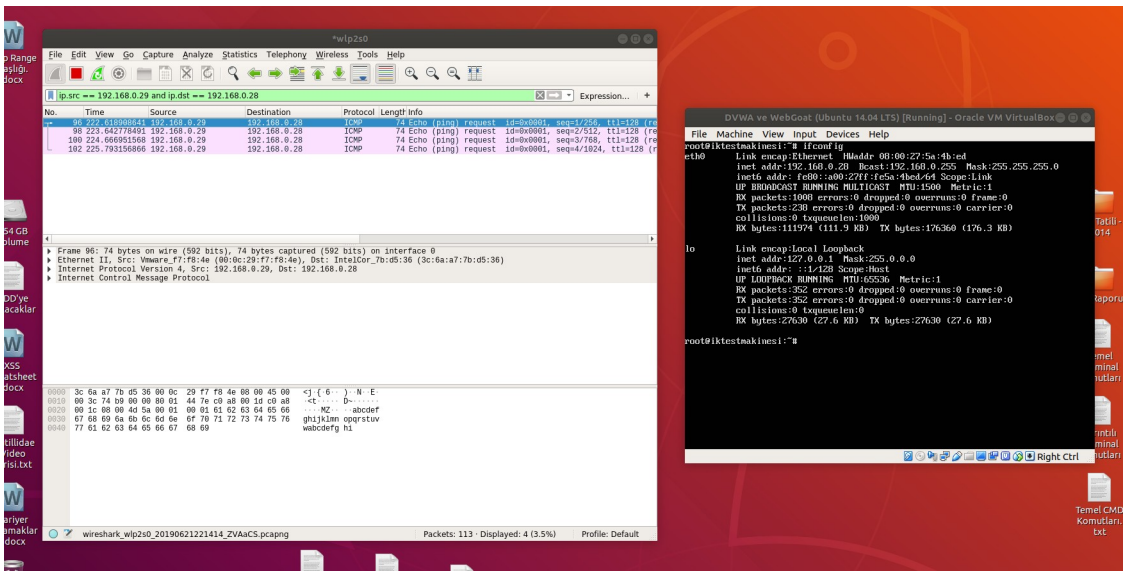


DVWA tarafı wireshark yazılımı aracılığıyla şu filtre

Wireshark (DVWA Tarafında):

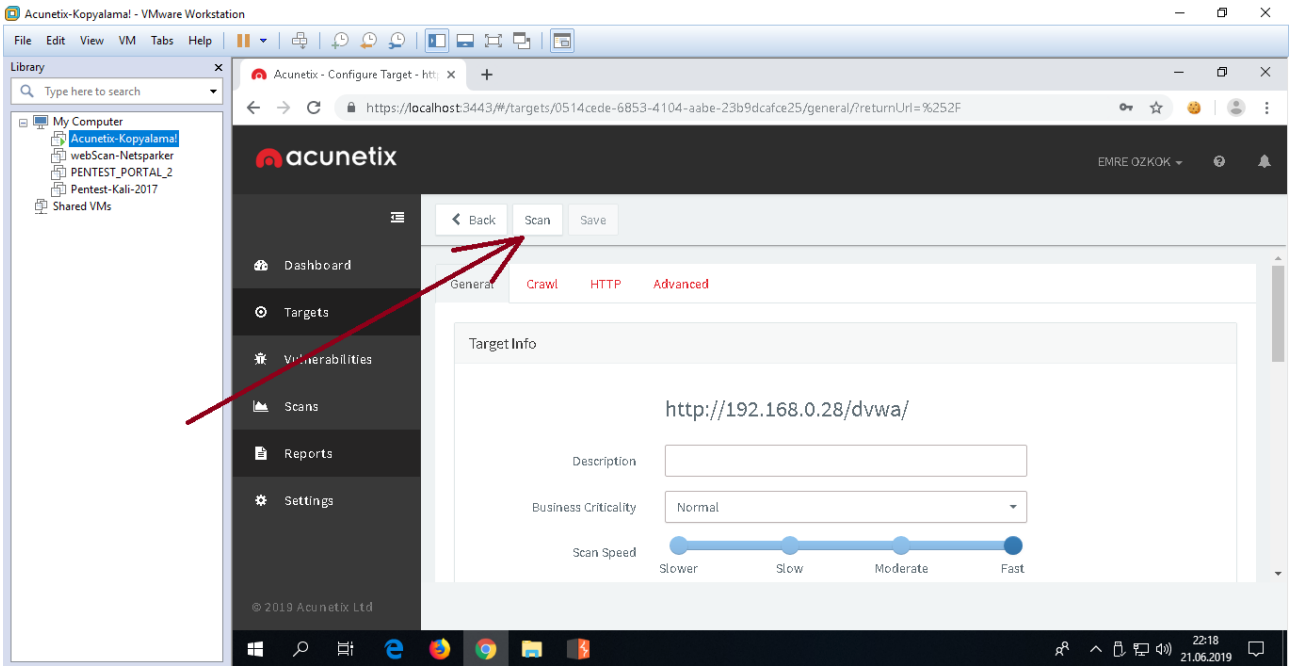
ip.src == 192.168.0.29 and ip.dst == 192.168.0.28 // 29 : Acunetix, 28: DVWA

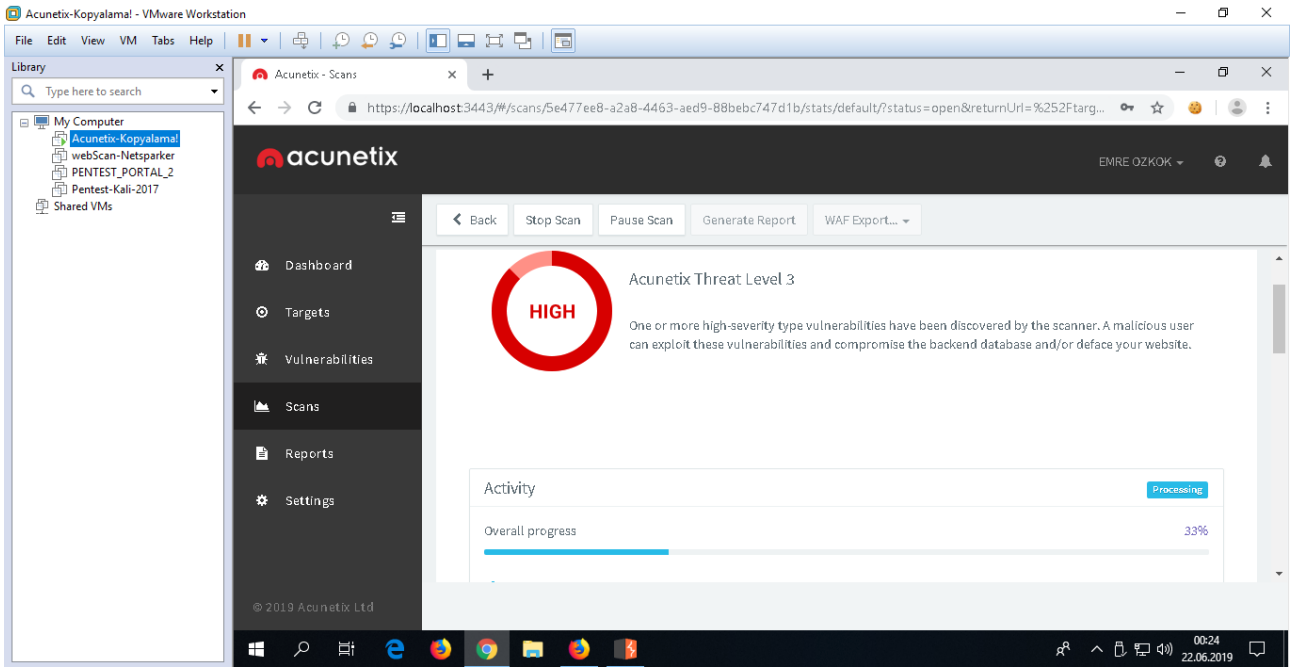
ile Acunetix tarafından gelen trafiği dinler durumdadır ve gelen icmp paketleri ekranına gelir.

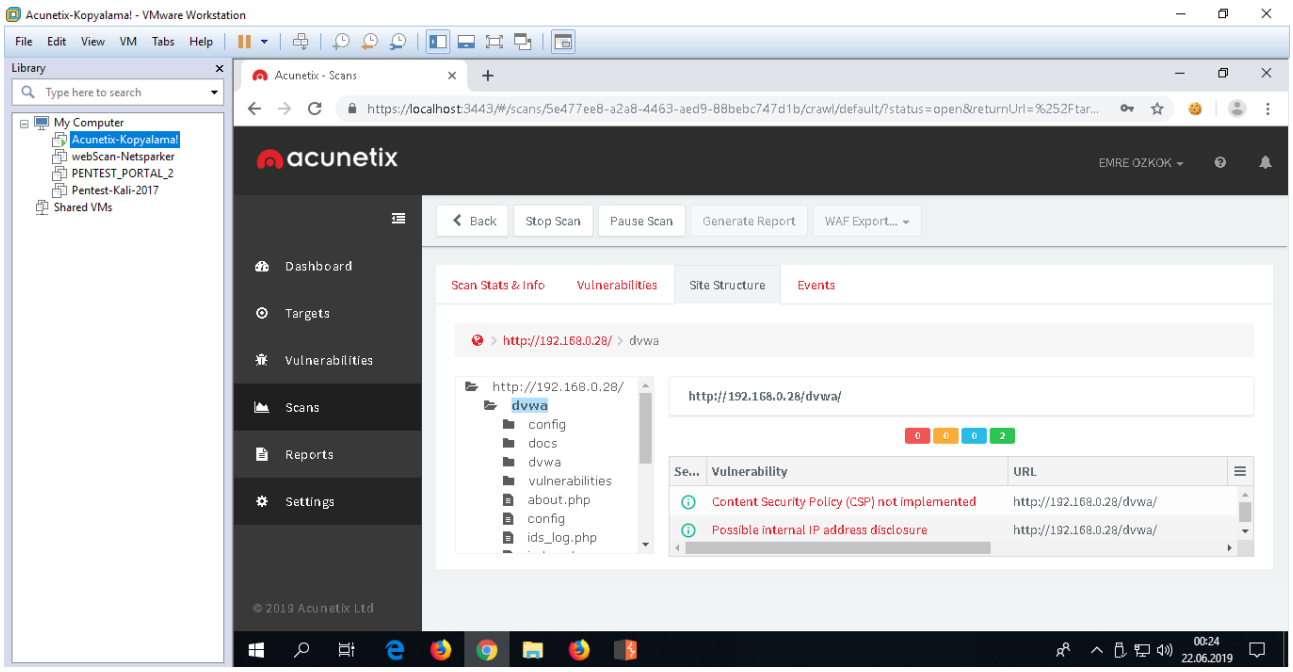


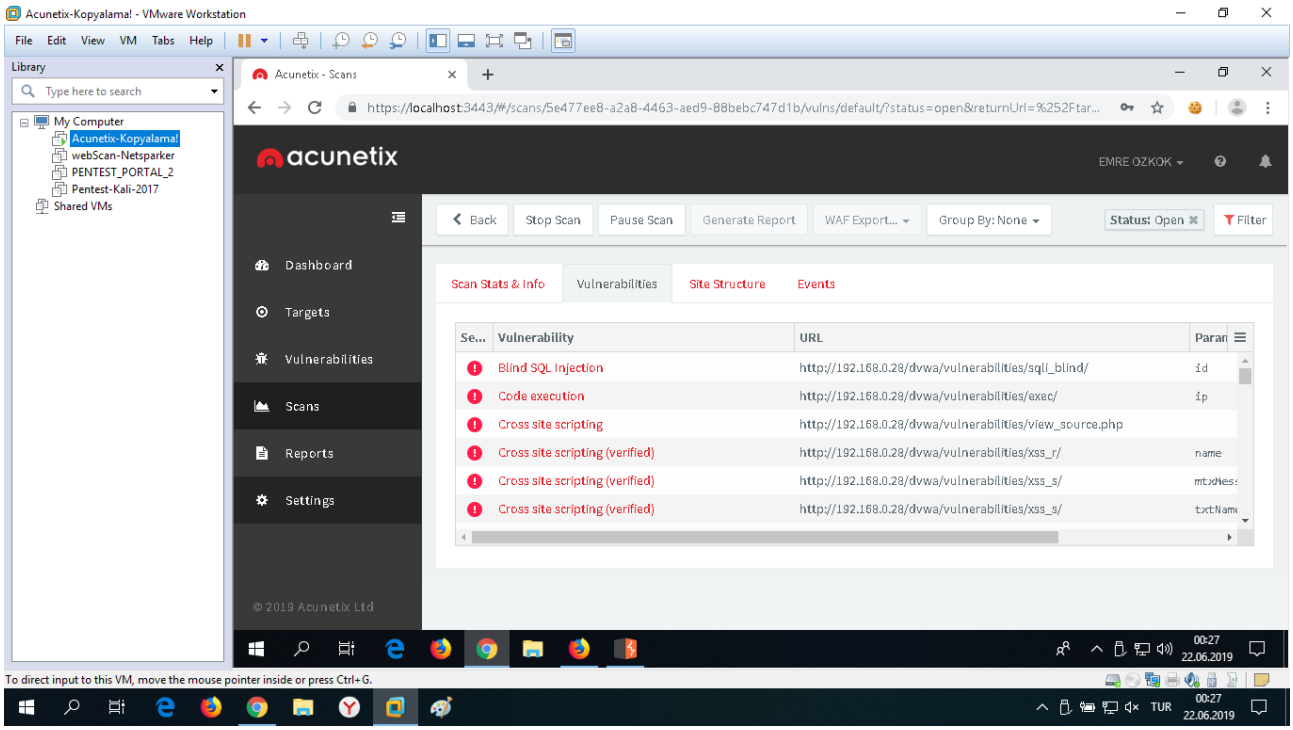
Sonuç olarak Wireshark doğru bir şekilde sadece Acunetix tarafından gelen trafiği dinler vaziyettedir. Dolayısıyla Acunetix taramaya başladığında DVWA tarafında ekranımıza sadece Acunetix'ten gelen trafik düşecektir ve saf bir saldırı trafiği elde etmiş olacağız.

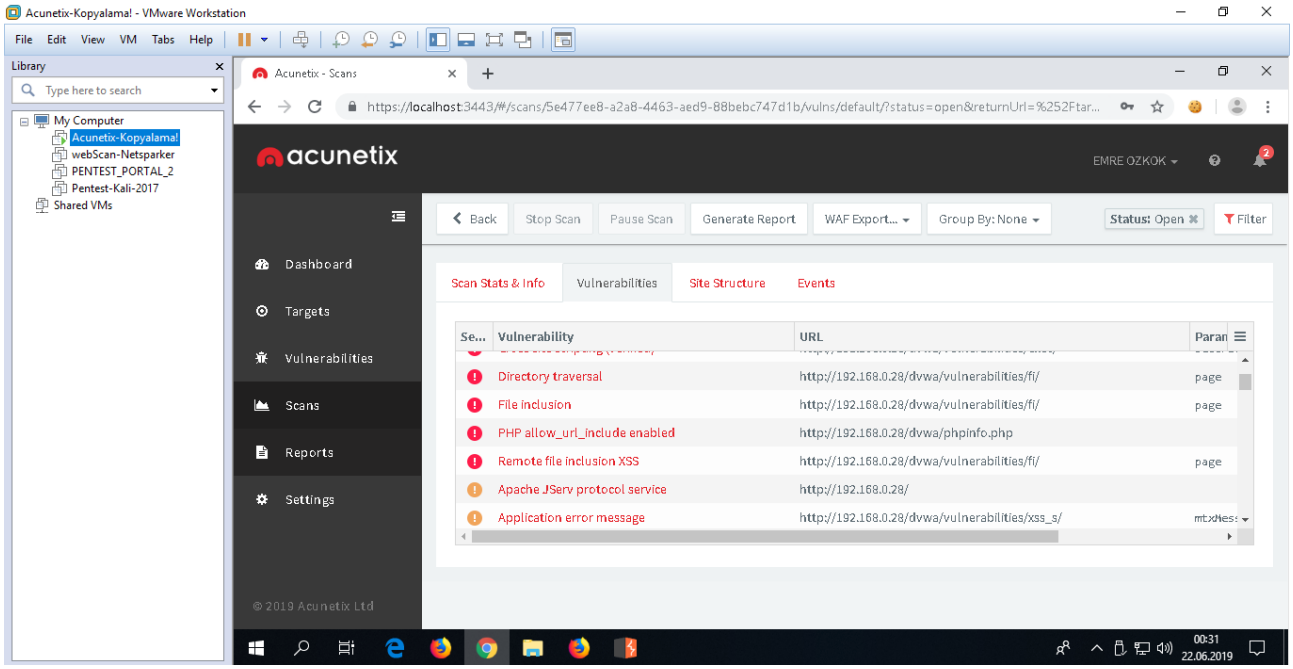
Saldırıyı başlatalım.



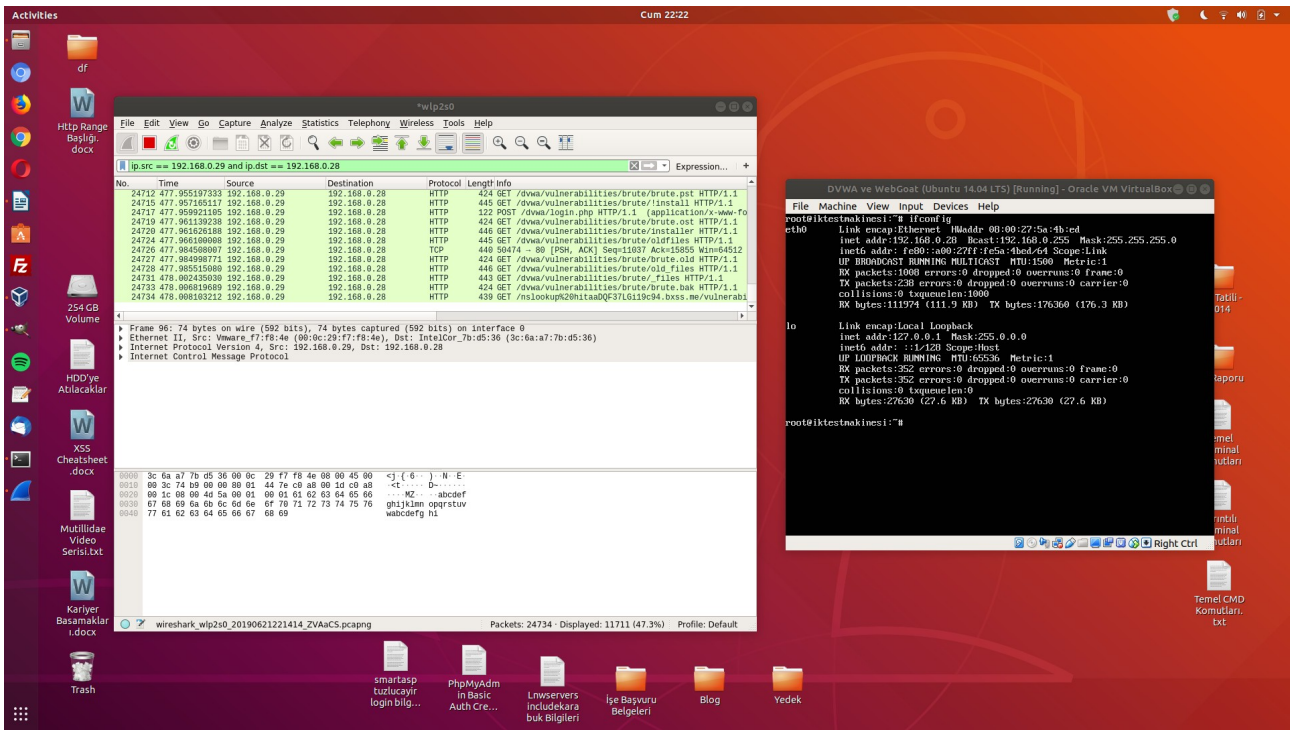

Acunetix-Kopyalama! - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Acunetix-Kopyalama!
webScan-Netsparker
PENTEST_PORTAL_2
Pentest-Kali-2017
Shared VMs
Acunetix - Scans
https://localhost:3443/#/scans/5e477ee8-a2a8-4463-aed9-88bebc747d1b/stats/default/?status=open&returnUrl=%252Ftarg...
acunetix
EMRE OZKOK
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings
Back
Stop Scan
Pause Scan
Generate Report
WAF Export...
HIGH
Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.
Activity
Processing
Overall progress
33%
© 2019 Acunetix Ltd
00:24
22.06.2019


Acunetix-Kopyalama! - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Acunetix-Kopyalama!
webScan-Netsparker
PENTEST_PORTAL_2
Pentest-Kali-2017
Shared VMs
Acunetix - Scans
https://localhost:3443/#/scans/5e477ee8-a2a8-4463-aed9-88bebc747d1b/crawl/default/?status=open&returnUrl=%252Ftar...
acunetix
EMRE OZKOK
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings
Back
Stop Scan
Pause Scan
Generate Report
WAF Export...
Scan Stats & Info
Vulnerabilities
Site Structure
Events
http://192.168.0.28/ > dvwa
http://192.168.0.28/
dvwa
config
docs
dvwa
vulnerabilities
about.php
config
ids_log.php
http://192.168.0.28/dvwa/
0 0 0 2
Se...
Vulnerability
URL
Content Security Policy (CSP) not implemented
http://192.168.0.28/dvwa/
Possible internal IP address disclosure
http://192.168.0.28/dvwa/
© 2019 Acunetix Ltd
00:24
22.06.2019



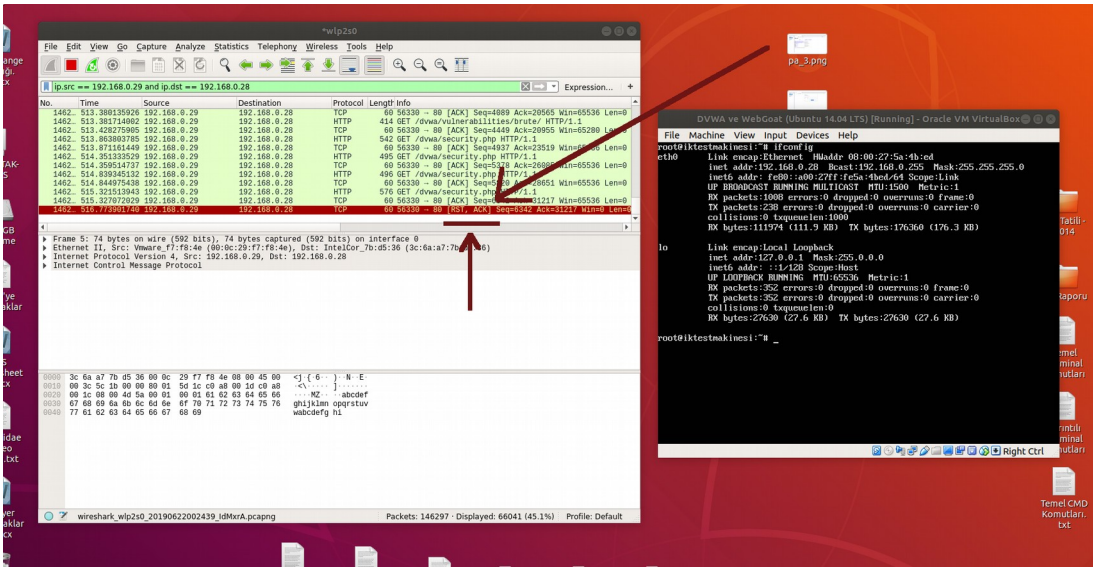


DVWA tarafında Acunetix makinasından gelen trafik ekrana anlık olarak düşer.

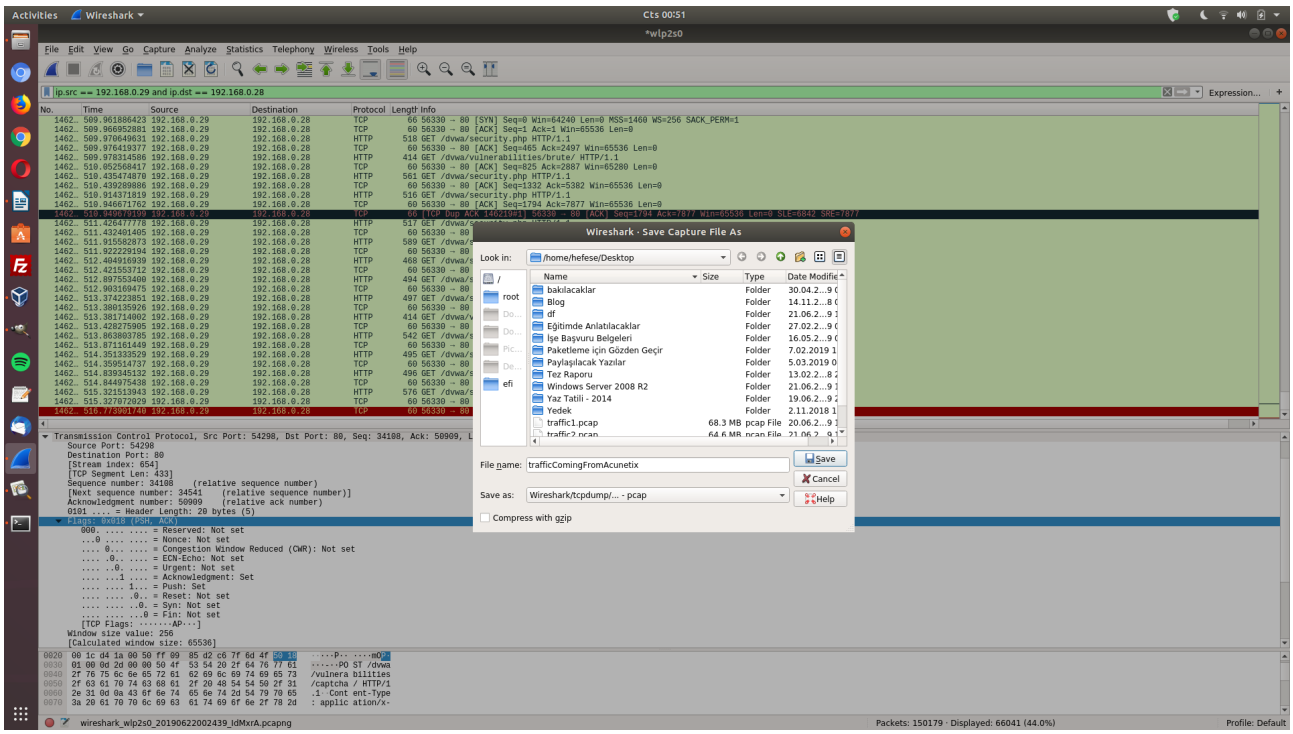


Acunetix taraması bittiğinde acunetix yazılımı son olarak karşı tarafla olan tcp handshake'i sonlandırıcı RST paketini yollar. Bu paket sonrası acunetix tarafından DVWA tarafına başka paket gelmez.

> 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

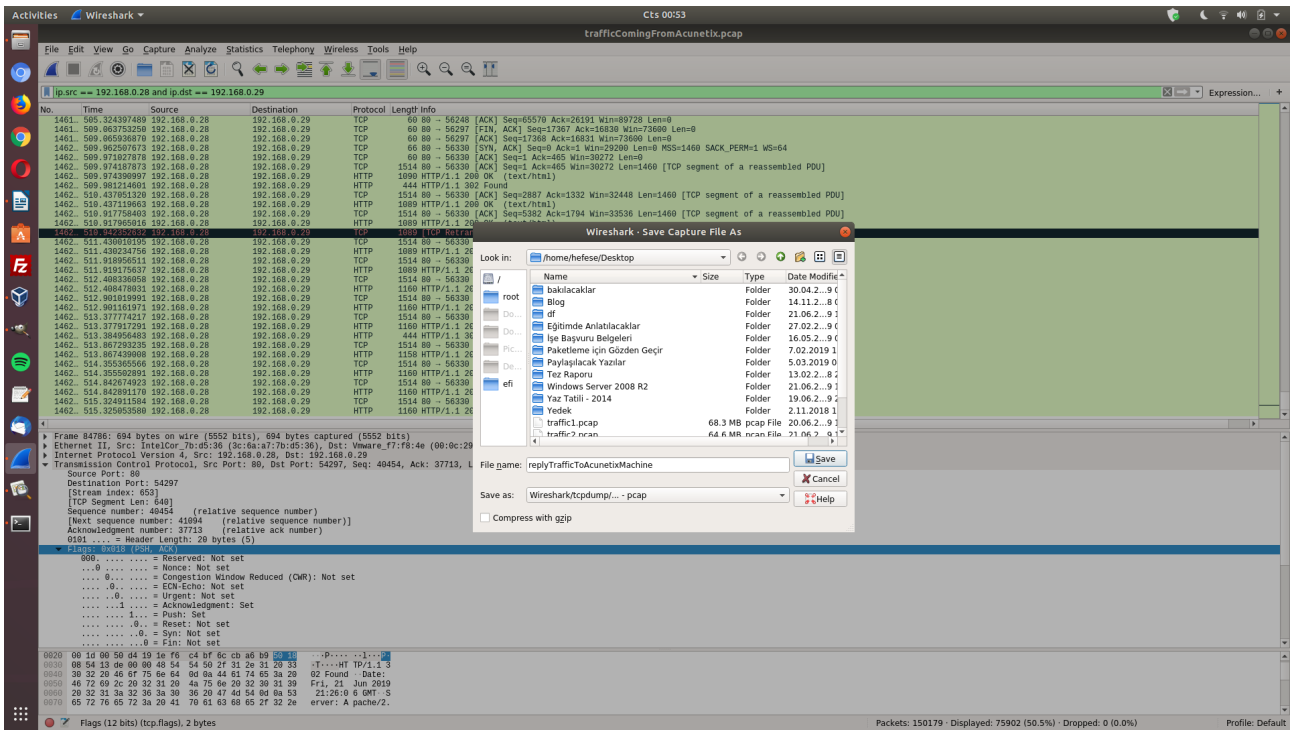
Ayrıyetten Acunetix'ten gelen değil de DVWA yüklü makinanın Acunetix tarafına yanıt olarak döndüğü trafik aynı wireshark ekranı açıkken filtrelemeyi

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.