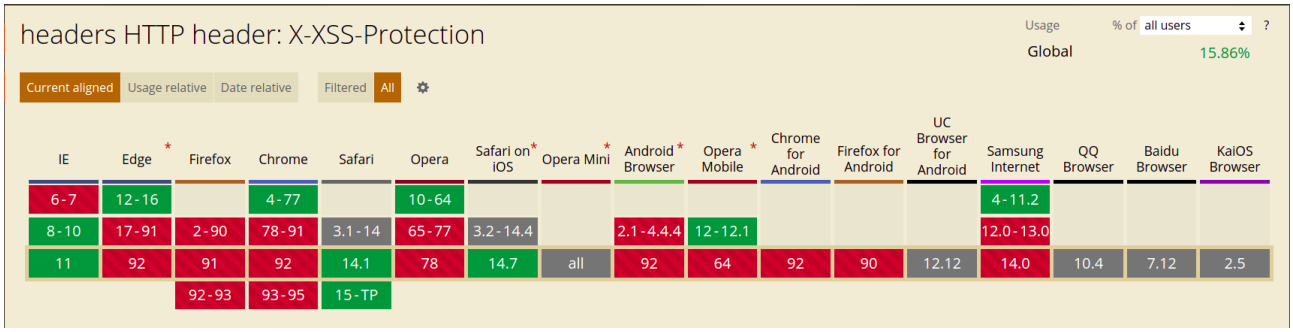
X-XSS-Protection Http Güvenlik Başlığı Uygulaması

a. X-XSS-Protection Nedir

X-XSS-Protection yanıt başlığı eski web tarayıcılarda XSS saldırılarını önleyen bir http güvenlik başlığıdır. Web tarayıcılarının görüntülediği web uygulamalarda xss payload'u gelirse bu xss payload'unun web tarayıcıda çalışmasını önler ve son kullanıcının güven içinde web uygulamada gezinmesini sağlar. Günümüzde daha kapsamlı olan Content-Security-Policy'ye yerini bırakmıştır. Fakat eski işletim sistemleri kullanan ve dolayısıyla eski web tarayıcılar kullanan kullanıcıları web uygulamalarda XSS saldırılarından korumak için bu http güvenlik başlığı kullanılmalıdır.

Bu başlık birçok web tarayıcının eski sürümlerinde tanımlıdır. Ancak örneğin Firefox web tarayıcıların hiçbir sürümünde tanımlı bir başlık olmamıştır.



Bu başlık ile eski web tarayıcılarda XSS önlenmektedir. Ancak XSS saldırılarından sadece Reflected XSS saldırılarını önlemektedir. Bu başlık ile örneğin Stored XSS saldırısı önlenememektedir.

b. Uygulama

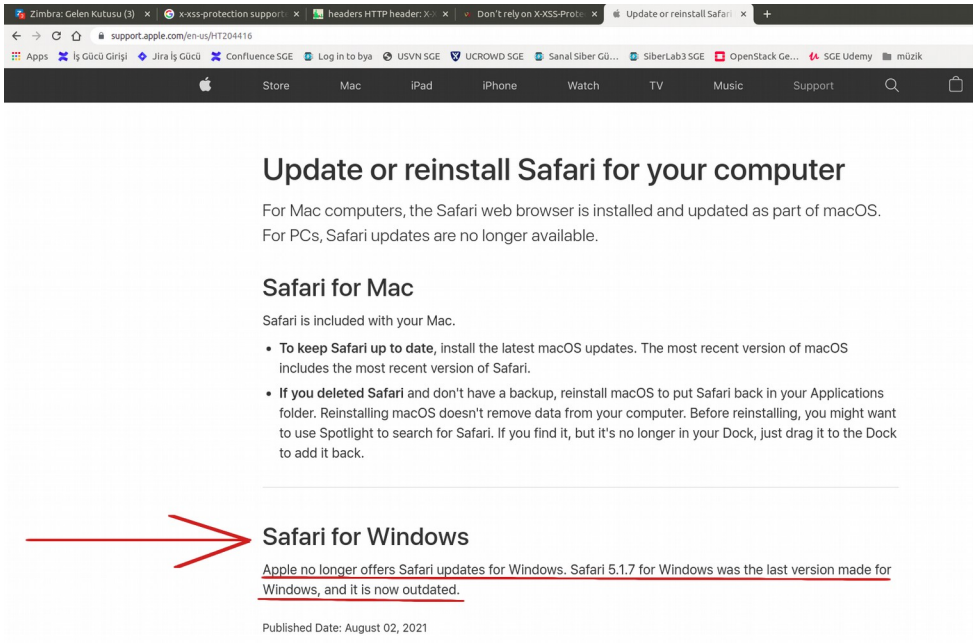
(+) Birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

Ubuntu 18.04 LTS - Apache	// Web Sunucu	(Ana Makina)
DVWA	// Web Uygulama	
Windows 7 Home Premium	// Son Kullanıcı Bilgisayarı	(Sanal Makina)
Safari 5.1.7 for Windows	// Son Kullanıcı Web Tarayıcısı	

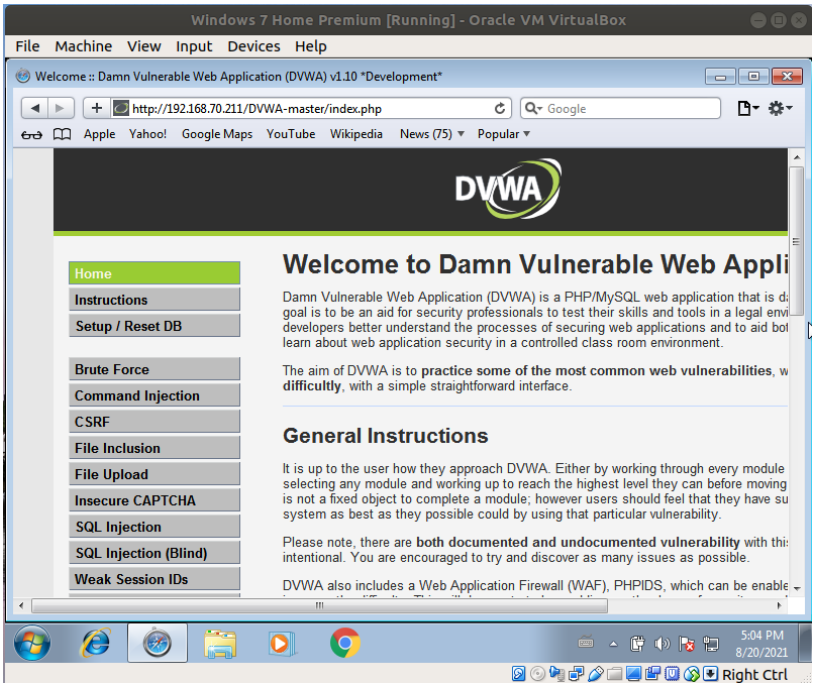
Not: Safari 5.1.7 kurulum dosyası ~/Downloads dizini altında Safari 5.1.7 Last Windows Version.zip dosyası ile yer almaktadır. Ayrıca Windows 7 Home Premium sanal makinasında yüklü durumdadır.

Safari web tarayıcılar windows platformunda artık sunulmamaktadır. Bundan önce sunulduğu zamanlarda en son sürüm olarak 5.1.7 yayınlanmıştır. Bu sürüm artık outdated olmuştur ve güncelleme gelmemektedir.

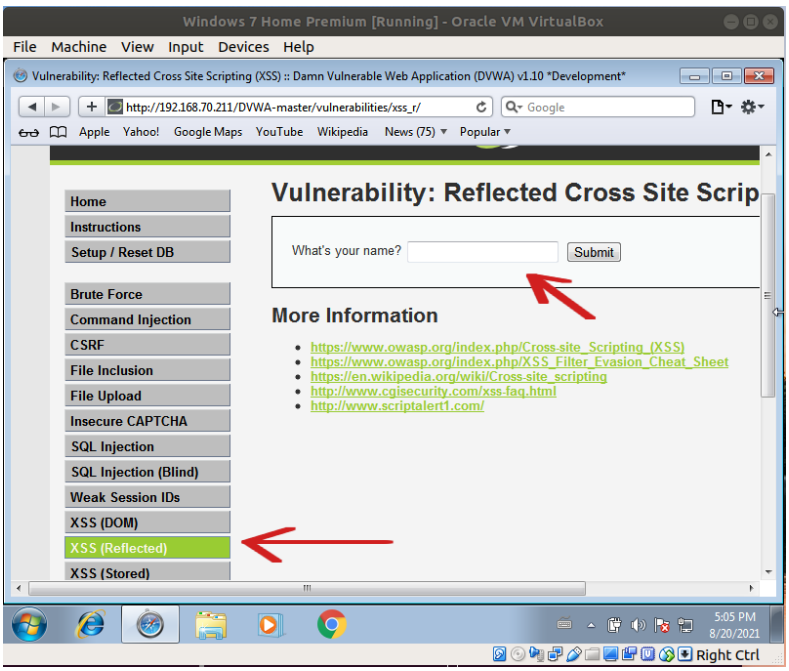


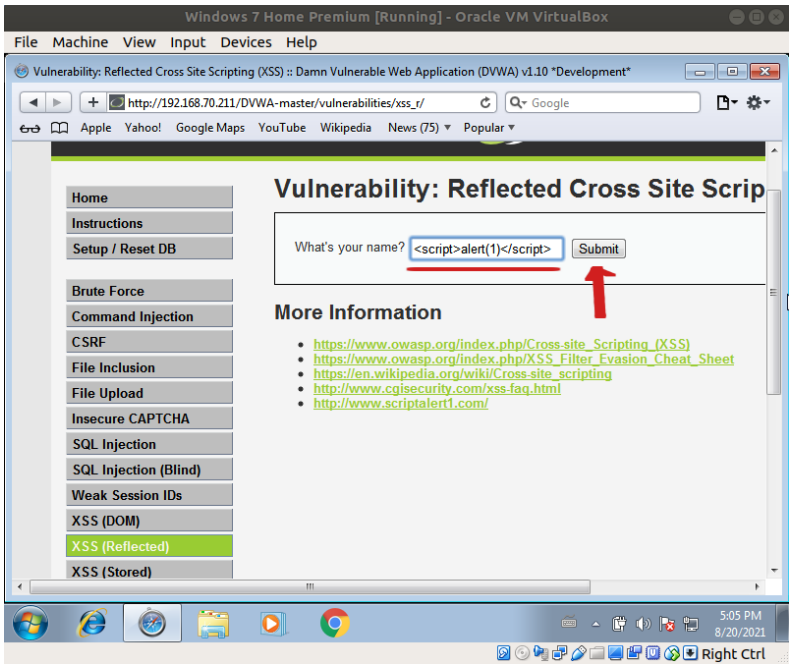
Safari web tarayıcıların bu eski sürümünde X-XSS-Protection yanıt başlığı tanımlıdır. Dolayısıyla bu web tarayıcı ile X-XSS-Protection yanıt başlığını kullanan bir web uygulama ziyaret edildiğinde XSS saldırısı yaşanırsa saldırı önlenecektir.

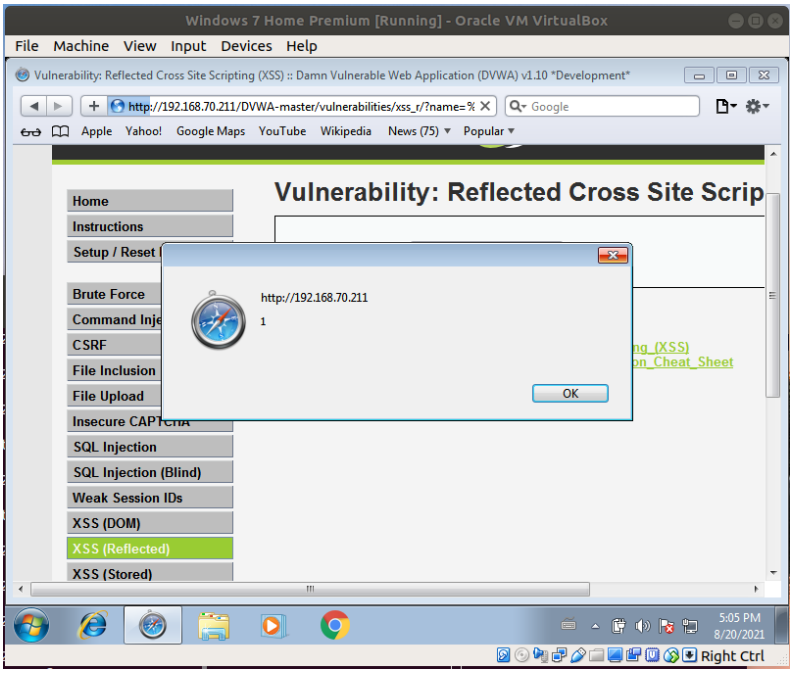
Şimdi uygulama gereği Ubuntu 18.04 LTS Apache web sunucuda yer alan DVWA web uygulamasını Windows makinada Safari 5.1.7 web tarayıcısı ile ziyaret edelim.



Safari web tarayıcıda web uygulamanın XSS zafiyeti olan sayfasına gidelim ve bir XSS saldırısı yiyelim.


Windows 7 Home Premium [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*
http://192.168.70.211/DVWA-master/vulnerabilities/xss_r/
Apple Yahoo! Google Maps YouTube Wikipedia News (75) Popular
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
Vulnerability: Reflected Cross Site Scrip
What's your name?
Submit
More Information
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/
5:05 PM
8/20/2021
Right Ctrl


Windows 7 Home Premium [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Vulnerability: Reflected Cross Site Scripting (XSS) :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*
http://192.168.70.211/DVWA-master/vulnerabilities/xss_r/
Apple Yahoo! Google Maps YouTube Wikipedia News (75) Popular
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
Vulnerability: Reflected Cross Site Scrip
What's your name?
<script>alert(1)</script>
Submit
More Information
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/
5:05 PM
8/20/2021
Right Ctrl



Görüldüğü gibi safari web tarayıcıda XSS açıklığı olan sayfa ziyaret edildiğinde XSS saldırısı gerçekleşmiştir. Şimdi DVWA web uygulaması sunucusunda konfigurasyon ayarı ile XSS önleyici X-XSS-Protection yanıt başlığını ekleyelim.

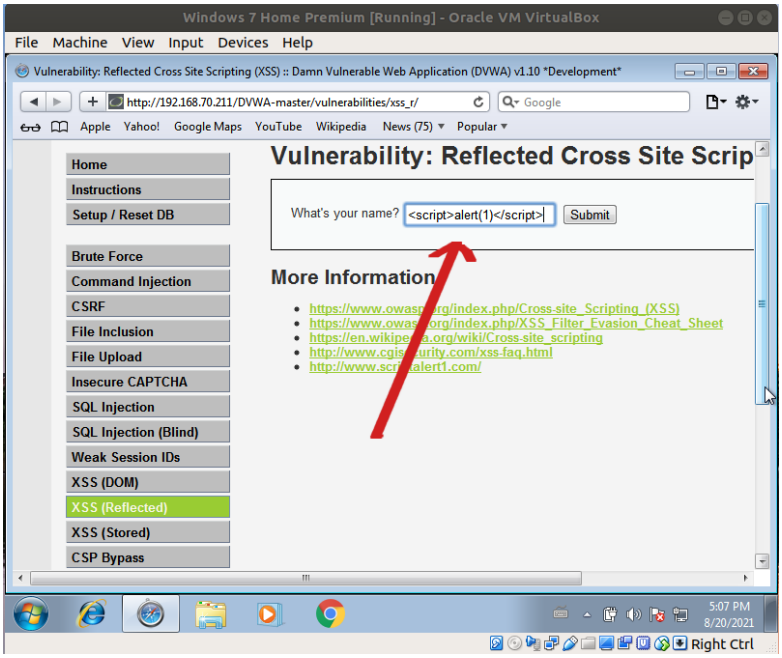
Ubuntu 18.04 LTS:

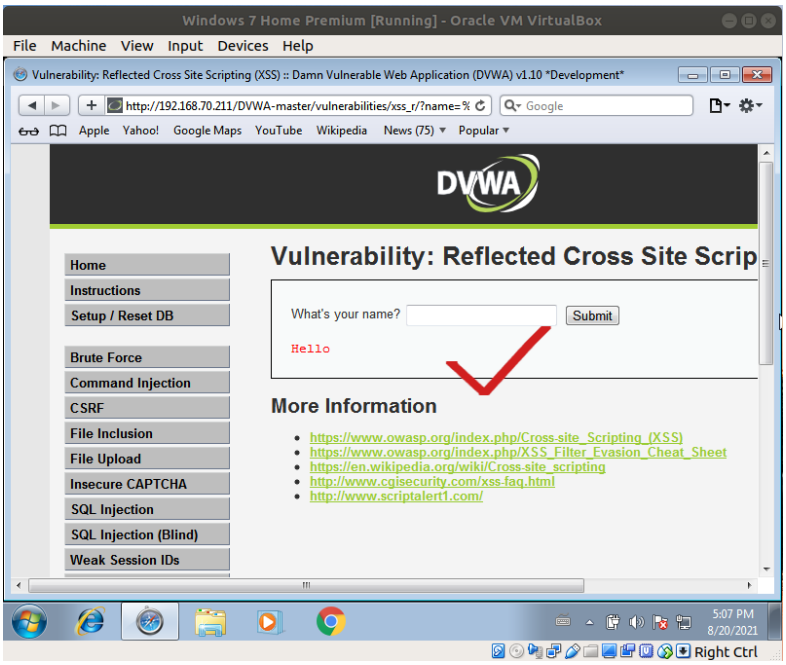
> sudo nano /etc/apache2/apache2.conf

(En Alta Eklenir)
…
…
Header set X-XSS-Protection "1"

> service apache2 restart

Web sunucuda bu ayar sonrası Safari web tarayıcıdan DVWA web uygulamasındaki XSS açıklığı olan sayfa tekrar ziyaret edildiğinde ve XSS saldırısı yeme uygulaması tekrarlandığında safari web tarayıcı web sunucudan gelen X-XSS-Protection yanıt başlığı direktifini kullanacaktır ve saldırıyı engelleyecektir.





Görüldüğü gibi X-XSS-Protection ayarı sonrası XSS saldırısı tekrarlandığında saldırı çalışmamıştır ve web sayfası filtrelenerek arayüze gelmiştir.

Bu güvenlik önlemini kontrol amaçlı pasifleştimek (yani kapamak) için DVWA web uygulama sunucusundaki X-XSS-Protection yanıt başlığı ayarı 1 değerinden 0'a çekilebilir.

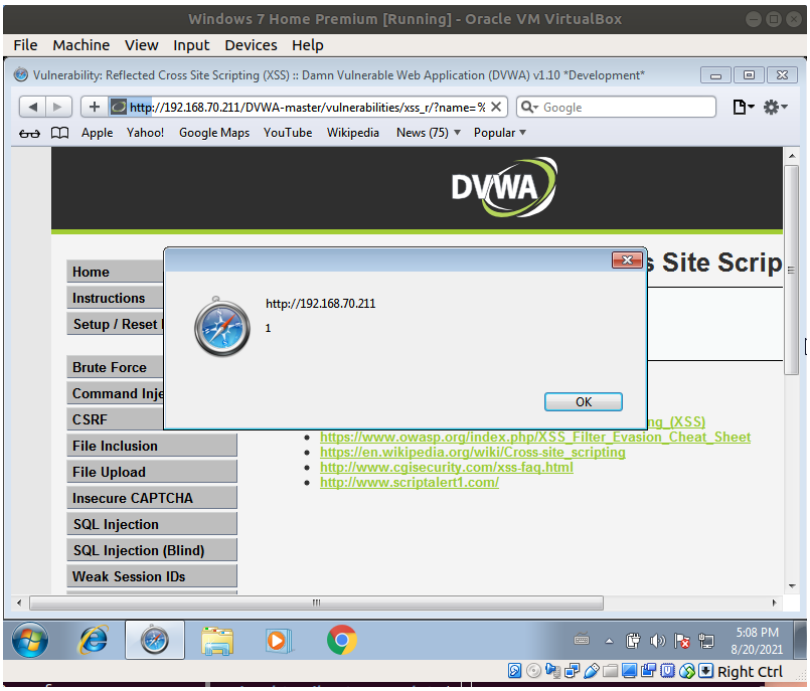
Ubuntu 18.04 LTS:

> sudo nano /etc/apache2/apache2.conf

(En Alta Eklenir)
…
…
Header set X-XSS-Protection "0"

> service apache2 restart

Web sunucuda bu ayar sonrası Safari web tarayıcıdan tekrar DVWA web uygulamasındaki XSS açıklığı olan sayfa ziyaret edildiğinde ve XSS saldırısı yeme uygulaması tekrarlandığında saldırı çalışacaktır.



XSS saldırılarının filtrelenmesi ve web sayfanın filtrelenmiş şekilde arayüze sunulması yerine web sayfanın komple bloklanması da sağlanabilir. Bunun için X-XSS-Protection yanıt başlığına mode=block eklemesi yapılır.

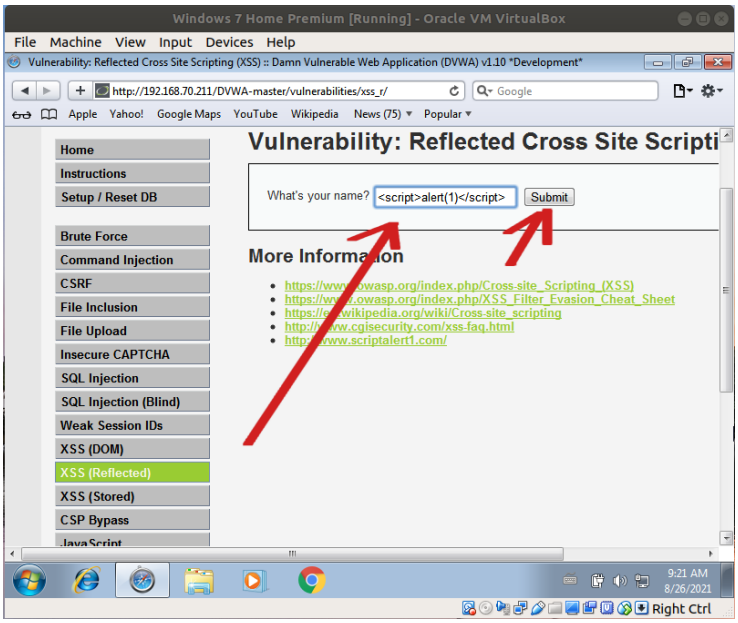
Ubuntu 18.04 LTS:

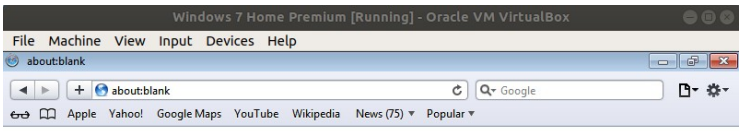
> sudo nano /etc/apache2/apache2.conf

(En Alta Eklenir)
…
…
Header set X-XSS-Protection "1; mode=block"

> service apache2 restart

Web sunucuda bu ayar sonrası safari web tarayıcıdan tekrar DVWA web uygulamasındaki XSS açıklığı olan sayfa ziyaret edildiğinde ve XSS saldırısı yeme uygulaması tekrarlandığında saldırının yaşandığı sayfa filtrelenerek ekrana gelmek yerine komple bloklanacaktır.





Görüldüğü gibi XSS saldırısının yaşanacağı sayfa komple bloklanmıştır.

Sonuç olarak eski web tarayıcılarda bir web uygulama sayfalarını gezerken XSS saldırısı yenildiğinde X-XSS-Protection yanıt başlığı varsa web tarayıcı saldırıyı önleyecektir. X-XSS-Protection yanıt başlığı güvenlik önleminde önerilen kullanım şekli mode=block ile tamamen bloklama şeklindedir.

Ekstra

(+) Birebir denenmiştir ve başarılı olunmuştur.

X-XSS-Protection yanıt başlığı sadece Reflected XSS saldırıları için önlem sunar. Örneğin Stored XSS için önlem sunmaz. Şimdi X-XSS-Protection başlığı mode=block ile tamamen bloklama modunda aktif olsun ve stored xss saldırısı yeme uygulaması yapalım.

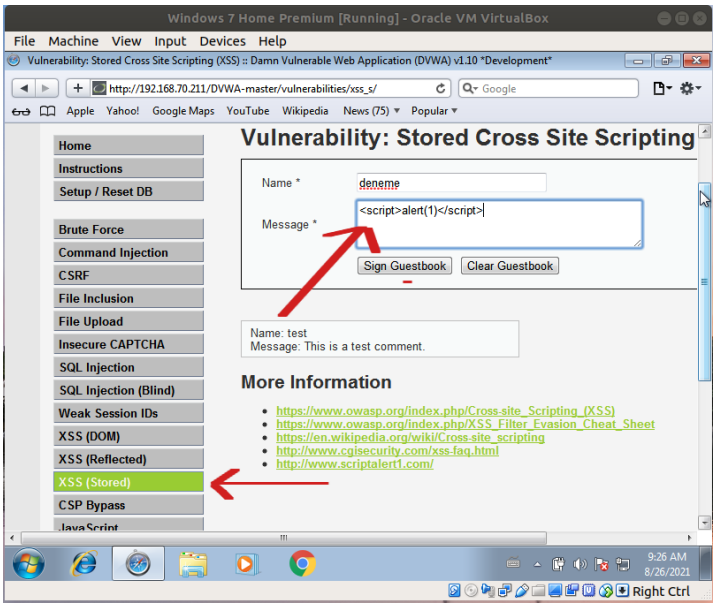
Ubuntu 18.04 LTS:

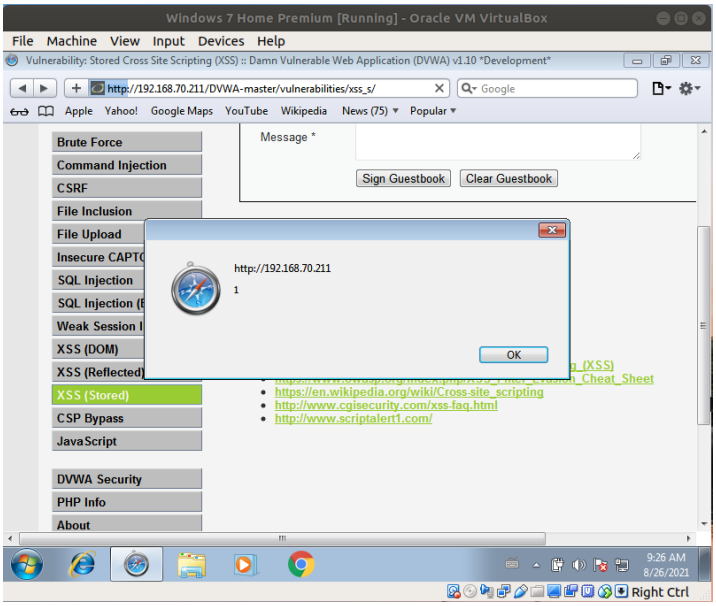
> sudo nano /etc/apache2/apache2.conf

(En Alta Eklenir)
…
…
Header set X-XSS-Protection "1; mode=block"

> service apache2 restart

Web sunucuda bu ayar sonrası Safari web tarayıcıdan DVWA web uygulamasındaki bu sefer Stored XSS açıklığı olan sayfayı ziyaret edelim ve XSS saldırısı yiyelim.





Görüldüğü üzere X-XSS-Protection başlığı aktifken Stored XSS açıklığı olan sayfa ziyaret edildiğinde saldırı engellenememiştir ve çalışmıştır. Sonuç olarak X-XSS-Protection yanıt başlığı sadece Reflected XSS saldırılarını önleyici bir başlıktır.

> Uyarı:
>
> Stored XSS zafiyetinin olduğu sayfada ilk kez xss payload'u girildiğinde ve akabinde sayfa görüntülendiğinde X-XSS-Protection saldırıyı engellemiştir. Ancak payload yerleştikten sonra sayfa tekrar ziyaret edildiğinde ve sonraki ziyaretlerde saldırı engellenememiştir. En başta engellemesinin muhtemel sebebi xss payload'u ilk kez girerken ve akabinde görüntülerken web tarayıcının saldırıyı reflected xss olarak algılaması olabilir. Sonraki ziyaretlerde ise payload girdisi yapılmadan daha önceden eklenmiş payload çalıştığından başlığın sunduğu güvenlik kapsamının dışına hitap etmiştir ve X-XSS-Protection başlığı saldırıyı engelleyememiştir.

Kaynaklar

https://caniuse.com/mdn-http_headers_x-xss-protection
https://jemurai.com/2018/11/28/dont-rely-on-x-xss-protection-to-protect-you-from-xss/
https://support.apple.com/en-us/HT204416