Reflected File Download Zafiyeti ve Burp Plugin Aracılığı ile Tespiti

Giriş

Reflected File Download zafiyeti 2014 yılında Oren Hafif tarafından keşfedilen ve isimlendirilen web tabanlı bir zafiyet türüdür. Bu zafiyet 2014 yılında düzenlenen BlackHat Europe etkinliğinde "Reflected File Download a New Web Attack Vector" sunumu ile tanıtılmıştır. Bu yazıda

- Zafiyetin etkisi
- Zafiyetin oluşması için gereksinimler
- Manuel analiz teknikleri ile zafiyetin keşfi
- Zafiyetin giderilmesi
- Enforsec sızma testi ekibi olarak geliştirdiğimiz Burp Plugin aracılığı ile keşfi

konu alınacaktır.

Zafiyetin Etkisi

Reflected File Download zafiyetinin doğru şekilde istismar edilmesi sonucu saldırganların zararlı çalıştırılabilir dosyalarını (bat, cmd, vbs, vbe ve hta dosyaları gibi) google.com ve bing.com gibi güvenilir domain'lere yüklemişler gibi gösterebilmesi ve bu sayede hedef aldıkları kullanıcıların bu dosyaları indirmelerini sağlamaları mümkündür. Saldırganların zafiyet bulunan web sayfalarının güvenini kullanarak zararlı dosyaları hedef aldıkları kullanıcılara bir URL tıklaması ile yükletmesi ve bilgisayarlarının tamamen ele geçirilmesi mümkündür. Buna ek olarak Oren Hafif'in "Reflected File Download a New Web Attack Vector" sunumunda da gösterdiği üzere hedef alınan kullanıcılara ait internet tarayıcılarının same-origin-policy özelliği kapatılarak, internet tarayıcılarında tanımlı bulunan diğer web sayfalarına ait (gmail.com gibi) Cookie'ler ve tanımlı bulunan kayıtlı parolalar ele geçirilebilmektedir.

Reflected File Download Zafiyetinin Oluşması için gereksinimler

Reflected File Download zafiyetinin oluşması için aşağıdaki gereksinimler karşılanmalıdır.

1- Kullanıcı girdisinin web uygulamasında içerik olarak yansıtılması

   a. Shell komutlarının çalışabilmesi için saldırgan'a ait girdinin, bulunduğu veri alanının dışına (çoğu zaman string) çıkabilmesi ve kullanıcıya yansıtılıyor olması gereklidir.
   b. Saldırgan'a ait girdilerde '&' ve '|' gibi komut eklenen karakterlere izin verilmesi gerekmektedir

2- Dosya isminin kontrol edilmesi ve çalıştırılabilir dosyanın indirilmeye zorlanması

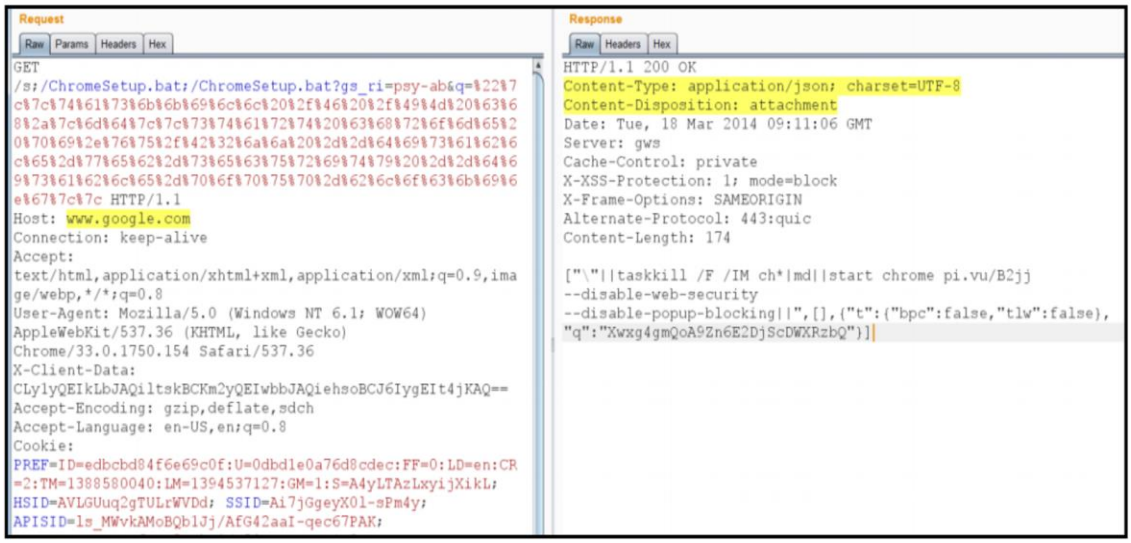
   Bunun gerçekleştirilebilmesi için 2 yöntem mevcuttur;

   a. Content-Disposition HTTP başlığı içerisinde filename özelliği gelmiyor ise indirilen dosyanın uzantısı URL'den alınmaktadır. Web sayfalarının yapısını ve akışını bozmadan uzantısının değiştirilebildiği çeşitli durumlar vardır.

i. Web sayfası/API'nin URL sonrası path'leri işleme almaması. Örneğin /services/search?callback=enforsec servisinin /services/search/update.bat?callback=enforsec URL'i ile de kullanılabiliyor olması.

ii. Web sayfası/API'nin URL'de ';' karakteri sonrası karakterleri işleme almaması. Örneğin /services/search?callback=enforsec servisinin /services/search;/update.bat?callback=enforsec URL'I ile de kullanılabiliyor olması. Safari hariç tüm internet tarayıcılarda bu zafiyeti test etmek için /services/search;/update.bat;/update.bat URL'i kullanılmalıdır.

Bir örnek vermek gerekirse, Oren Hafif, sunumunda belirttiği üzere google.com üzerinde Content-Disposition HTTP başlığının filename özelliği olmadan kullanılmadığını görmüş ve Reflected File Download zafiyetini keşfetmiştir. İlgili BlackHat Europe 2014 sunumunda (https://www.youtube.com/watch?v=dI1BJUNk8V4) gösterildiği üzere bir sosyal medya solucanına çevrilebilen Reflected File Download zafiyetinin tespitine ait ekran görüntüsü aşağıdaki gibidir;



https://www.blackhat.com/docs/eu-14/materials/eu-14-Hafif-Reflected-File-Download-A-New-Web-Attack-Vector.pdf

b. Content-Disposition HTTP başlığının olmadığı durumlarda, zararlı web sayfasında kullanıcının tıklayacağı linkin a tag'i içerisinde olması ve chrome/opera internet tarayıcıları tarafından desteklenen "download" tag'inin kullanılası gerekmektedir. Örnek zararlı HTML kodları aşağıdaki gibidir;

```
<a download href="http://hedef.com/services/search;/update.bat;">
https://hedef.com/services/search;/update.bat;</a>
<a href="http://hedef.com/services/search;/update.bat;"
download="update.bat" onclick="return false">Download</a>
```

Bknz: https://www.davidsopas.com/reflected-file-download-cheat-sheet/

Aşağıdaki grafik de hangi durumlarda zafiyetin oluşacağı anlatılmıştır.

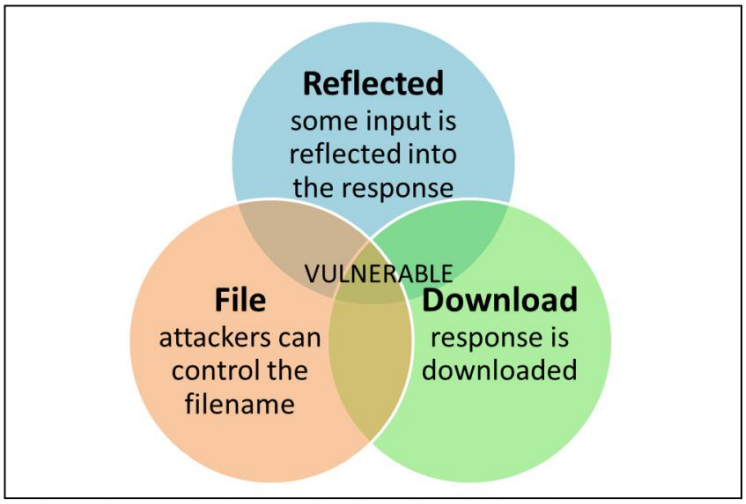


Figure 2 – A service is vulnerable if the three RFD requirements are met

Bknz: https://www.blackhat.com/docs/eu-14/materials/eu-14-Hafif-Reflected-File-Download-A-New-Web-Attack-Vector.pdf

Manüel analiz teknikleri ile zafiyetin keşfi

1. İlk adım olarak uygulamaya girilen girdilerin (input) web sayfası/API içerisinde kullanıcıya yansıtıldığı noktalar tespit edilmelidir. Bu noktaların sıklıkla bulunduğu durumlar aşağıdaki gibidir;

    a. Siteler arası betik çalıştırma (XSS) zafiyetine benzer şekilde bu adımda istek parametre değer/isimleri
    b. Uygulama hata sayfaları ve hata içerikleri
    c. Yerleşik siteler arası betik çalıştırma (Stored XSS) zafiyetine benzer şekilde sistem üzerinde tutulan ve kullanıcı kaynaklı veriler. Örneğin saldırgan forum benzeri bir web sayfasına kayıt olurken kullanıcı isminde bu zafiyeti tetikleyecek bir değer girebilir ve bu değer saldırgan'a ait profil sayfasında gözükecektir. Bu durumda saldırgan kendi profil sayfası ile Reflected File Download zafiyetini tetikleyebilir.
    d. JSONP callback değerlerine özellikle dikkat edilmelidir. JSONP callback değerleri uygulama üzerinde gezinirken (spider) keşfedilebilmektedir fakat bazı callback parametreleri API/web sayfalarında gizli olarak bulunabilmektedir. Bu sayfalara ve servislere parametreler eklenerek callback özelliğinin olup olmadığı tespit edilmelidir.

    Örneğin

    ```
    https://www.hedef.com/haberler/haber1?baslik=test
    ```

    URL'inde bulunan baslik parametresi saldırgan tarafından kontrol edilebilmektedir. Bu parametre değeri uygulama içeriği olarak link'e tıklayan kullanıcılara gösterilmektedir. HTTP cevabına ait body değeri aşağıdaki gibidir;

    ```
    {"id":"haber1", "baslik":"test"}
    ```

2. "baslik" parametresi ile alınan değer " değerleri arasında bir kelime (string) formatında kullanılmaktadır, bu değer komut satırı komutu içerisinde kullanılıyor olsa dahi bir kelime (string) olarak görülecek ve çalıştırılamayacaktır. Bu değerin çalıştırılabilir hale gelip gelmediğini kontrol etmek adına "baslik" parametresine aşağıdakine benzer bir istek yazılmalıdır.

https://www.hedef.com/haberler/haber1?baslik=**test“**

Reflected File Download zafiyetinin bulunduğu bir sistemde beklenen HTTP cevabına ait body değeri aşağıdaki şekilde olmalıdır;

{"id":"haber1", "baslik":"**test\”**"}

Bu değer uygulama içerisinde hala kelime (string) olarak gözükecektir fakat bu satırlar komut satırında komut olarak kullanılabildiğinde (bu kısmı bir sonraki başlıkta inceleyeceğiz) aşağıdaki örnek isteğe ait cevap çalıştırılabilir bir komut olacak ve hesap makinesi yazılımını çalıştırabilecektir. Örnek URL, HTTP cevabına ait body ve ekran görüntüsü aşağıdaki gibidir;

URL;

https://www.hedef.com/haberler/haber1?baslik=test**“||calc||**

HTTP cevabına ait body;

{"id":"haber1", "baslik":"test\”||calc||"}

Ekran görüntüsü;

3. Bu aşamada dosyanın indirilmeye zorlandığını varsayabiliriz, testler esnasına bu adımdaki amaç dosya uzantısını çalıştırılabilir bir format ile değiştirilebilir hale getirmek ve bununla beraber uygulamanın işleyişini bozmamak olacaktır. Bunun için aşağıdakilere benzer yapıda URL formatları denenmelidir.
   Orjinal URL

   https://hedefsite.com/haberler/**haber1?baslik=test**

Test edilecek URL formatları

```
https://hedefsite.com/haberler/haber1.bat?baslik="||calc||
https://hedefsite.com/haberler/haber1;update.bat?baslik="||
calc||
https://hedefsite.com/haberler/haber1/update.bat?baslik="||
calc||
https://hedefsite.com/haberler/haber1;/update.bat?baslik="|
|calc||
https://hedefsite.com/haberler/haber1;/update.bat;?baslik="
||calc||
```

Bknz: https://www.davidsopas.com/reflected-file-download-cheat-sheet/

Zafiyetinin Giderilmesi

Zafiyetin giderilmesi adına uygulanması beklenen 4 yöntem vardır. Bu yöntemlerden uygulama yapısına uygun olanlar kullanılmalıdır.

1. Callback benzeri kullanıcıdan veri alan ve bu veriyi uygulama çıktısına yansıtan parametrelerin değerleri bir beyaz listeden geçirilmelidir. Örneğin bu parametre gelmesi beklenen değerler sadece harften oluşuyor ise harf haricindeki karakterler kabul edilmemelidir. Özellikle “”, “|” ve “&” değerlerinin kullanımı engellenmelidir. Bu değerler engellenemiyorsa eğer ekranda gösterilirken encode edilmelidir. Örneğin “ değeri \x22 veya \u022 değeri ile değiştirilmelidir.
2. Content-Disposition HTTP başlığı kullanılacak ise eğer mutlaka filename özelliği eklenmeli ve bu değer boş bırakılmamalıdır. Google.com üzerinde Oren Hafif tarafından bulunan zafiyet bu yöntem ile giderilmiştir. Örnek HTTP cevabı aşağıdaki gibidir;

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=UTF-8
Date: Fri, 09 Dec 2016 06:07:30 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Disposition: attachment; filename="f.txt"
Server: gws
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
Alt-Svc: quic=":443"; ma=2592000; v="35,34"
Connection: close
Content-Length: 61834
```

3. Uygulama normalinde kullanılan URL’lerin arkasına veri eklenmesine izin verilmemelidir. Bu gibi durumlarda uygulama HTTP 404 cevabı vermeye zorlanmalıdır.
4. HTTP cevap başlıkları kullanılarak internet tarayıcılarının HTTP cevaplarına bakarak uygulama içeriği hakkında tahminde bulunmasının önüne geçilmelidir. Bu sayede uygulamaların HTTP cevabını çalıştırılabilir formatta görüp indirmesi engellenecektir. Örnek HTTP Başlığı aşağıdaki gibidir;

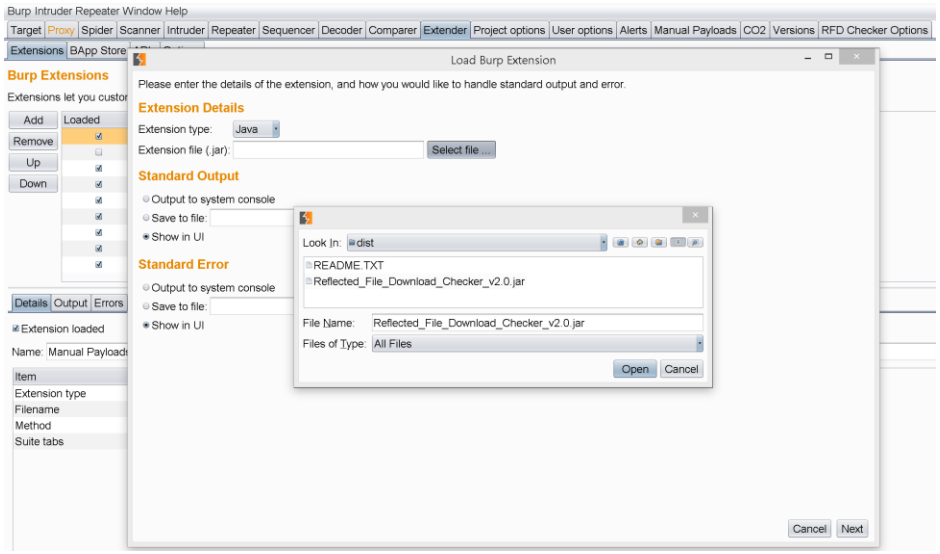
```
X-Content-Type-Options: nosniff
```

Enforsec Tarafından Geliştirilen Burp Plugin'i Aracılığı ile Zafiyetin Keşfi

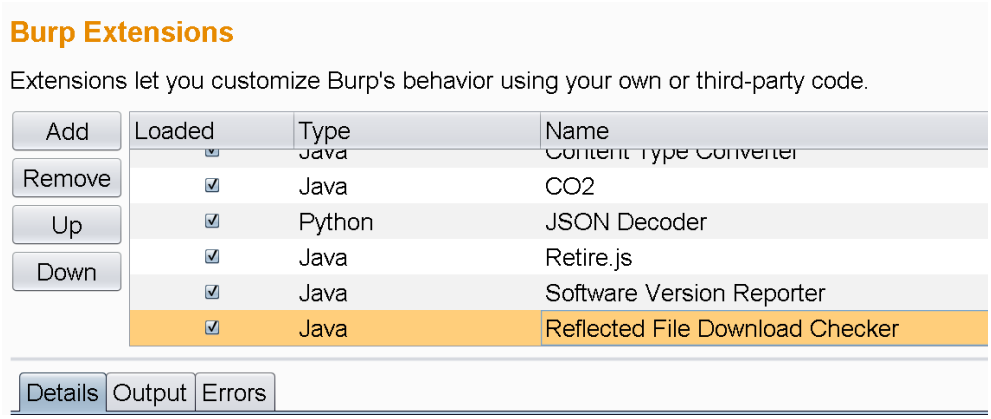
1. Burp Plugin'inin yüklenmesi

   Uygulama kaynak kodları https://github.com/onurkarasalihoglu/Reflected-File-Download-Checker-BurpSuite-Plugin.git sayfası üzerinden indirildikten sonra

   1.1. Burp Suite ekranında "Extender" tab'ına gelinir.
   1.2. Extender tab'ı içerisinde bulunan "Extensions" tab'ı açılır.
   1.3. Sol tarafta bulunan "Add" butonuna tıklanır, "Extension Details" bölünden "BurpExtender/dist" dizininde bulunan ilgili jar dosyası seçilir.



   1.4. Reflected File Download Checker plugin'inin doğru şekilde yüklendiği doğrulanır.

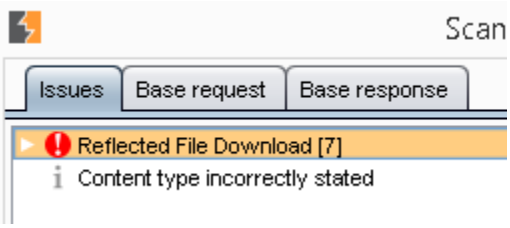


2. Burp Plugin'inin kullanımı

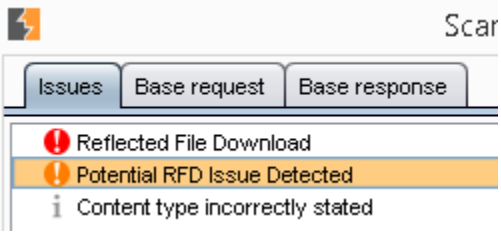
   Reflected File Download Checker plugin'i bir scanner modülü gibi çalışır. Beklenen şartlar sağlandığında Burp Suite'in mevcut bulguları tespit etmeye çalışması gibi zafiyetin tespiti için denemeler yapar ve zafiyet bulunduğunda "Scanner" ekranına eklenir. Reflected File

Download Checker plugin'i hem passive scan hem de active scan esnasında çalışmaktadır. Örnek bir zafiyet'e ait ekran görüntüleri aşağıdaki gibidir;

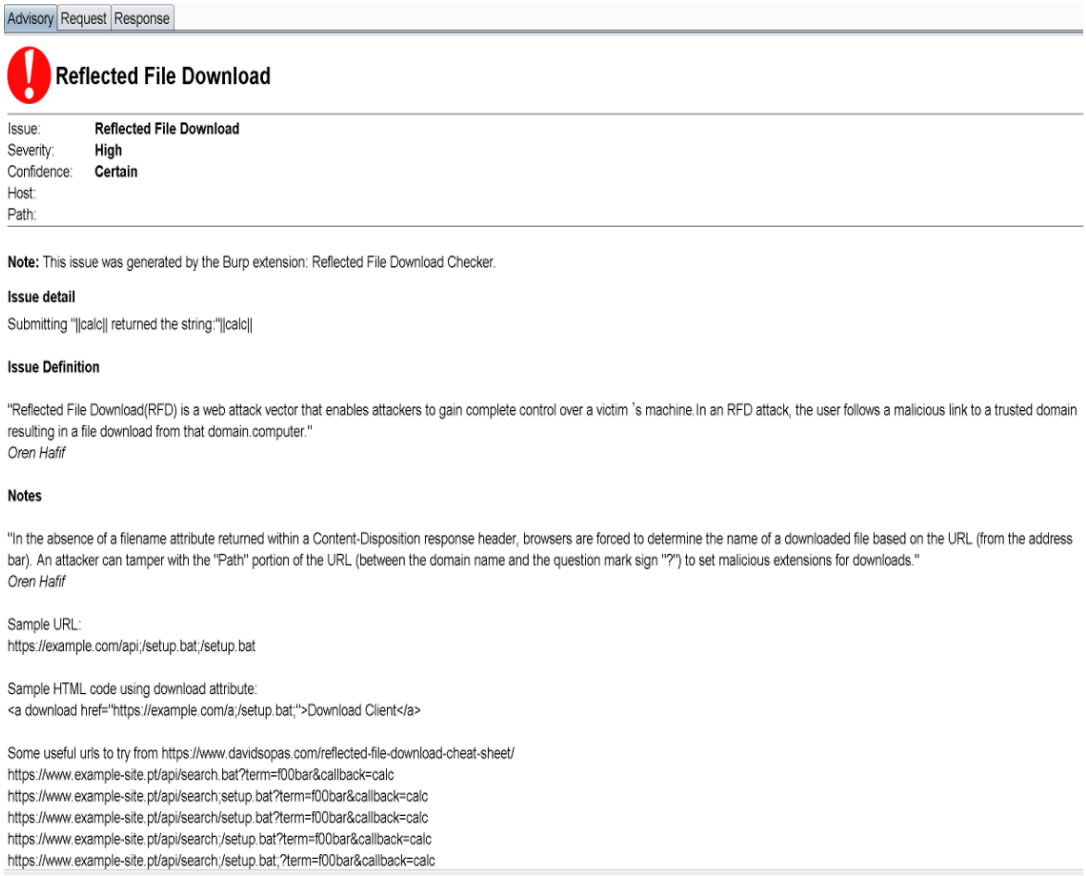
Active Scan esnasında bulunan zafiyetin ekran görüntüsü;



Passive Scan esnasında bulunan zafiyetin ekran görüntüsü;



Active Scan ile bulunan Reflected File Download bulgusunun içeriği;



Advisory | Request | Response

Reflected File Download

Issue: **Reflected File Download**
Severity: **High**
Confidence: **Certain**
Host:
Path:

Note: This issue was generated by the Burp extension: Reflected File Download Checker.

Issue detail

Submitting "||calc|| returned the string:"||calc||

Issue Definition

"Reflected File Download(RFD) is a web attack vector that enables attackers to gain complete control over a victim 's machine.In an RFD attack, the user follows a malicious link to a trusted domain resulting in a file download from that domain.computer."
Oren Hafif

Notes

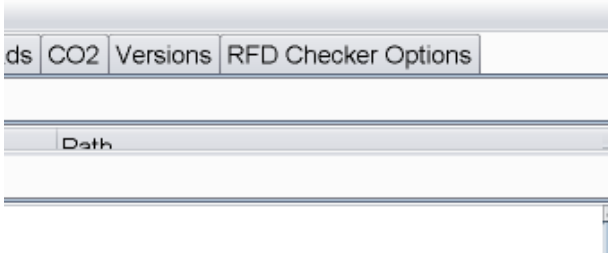
"In the absence of a filename attribute returned within a Content-Disposition response header, browsers are forced to determine the name of a downloaded file based on the URL (from the address bar). An attacker can tamper with the "Path" portion of the URL (between the domain name and the question mark sign "?") to set malicious extensions for downloads."
Oren Hafif

Sample URL:
https://example.com/api;/setup.bat;/setup.bat

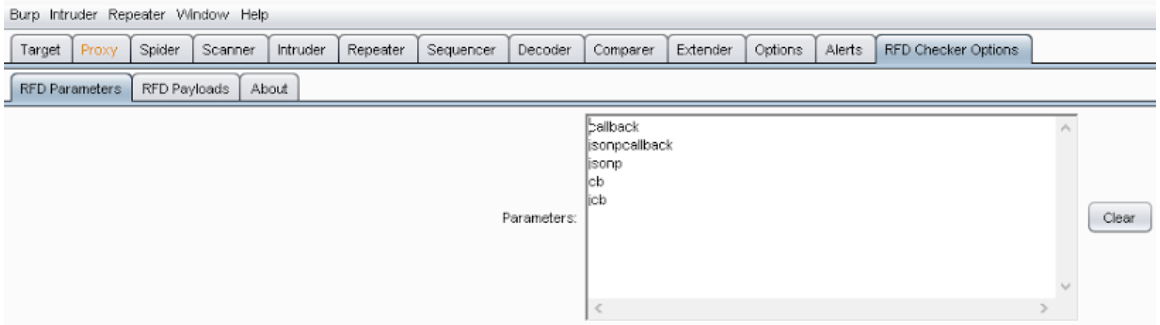
Sample HTML code using download attribute:
<a download href="https://example.com/a;/setup.bat;">Download Client

Some useful urls to try from https://www.davidsopas.com/reflected-file-download-cheat-sheet/
https://www.example-site.pt/api/search.bat?term=f00bar&callback=calc
https://www.example-site.pt/api/search;setup.bat?term=f00bar&callback=calc
https://www.example-site.pt/api/search/setup.bat?term=f00bar&callback=calc
https://www.example-site.pt/api/search;/setup.bat?term=f00bar&callback=calc
https://www.example-site.pt/api/search,/setup.bat;?term=f00bar&callback=calc

Plugin doğru şekilde yüklendikten sonra Burp Suite ekranında sağ üst köşede “RFD Checker Options” tab’ı aşağıdaki şekilde belirir.



Bu tab içerisinde “RFD Parameter”, “RFD Payloads” ve “About” tabları bulunmaktadır. “RFD Parameter” tabında plugin’in passive scan esnasında varlığını kontrol ettiği, active scan esnasında da test edilen web sayfasına parametre olarak eklediği parametre isimleri bulunmaktadır. Bu parametre isimlerinin sayısının arttırılması için ilgili metin kutusunun (text box) altına ekleme yapılmalıdır. “RFD Payload” dizininde ilgili parametreler üzerinde Reflected File Download zafiyetinin tespit edilmesi için kullanılan ve uygulama HTTP cevabında yansıması da aratılacak kelimeler (string) bulunmaktadır. Bu verilere yeni veri eklemek için ilgili metin kutusunun altına ekleme yapılmalıdır. “About” tabında ise Plugin’e ait geliştirici kontak bilgileri ve mevcut plugin’in versiyonu bulunmaktadır.



3. Bup Plugin’inin alt yapısı ve kod güncelleme/derleme

Plugin’in çalışma şeması aşağıdaki şekildedir;

Passive Scan Esnasında (doPassiveScan)

- Content-Type HTTP başlığının "json" veya "javascript" anahtar kelimelerini içerip içermediği kontrol edilir.

Eğer içeriyor ise callback benzeri parametrelerin varlığı kontrol edilir, bu parametrelerin listesi grafik ara yüzündeki “RFD Parameters” tab’ından alınmaktadır.

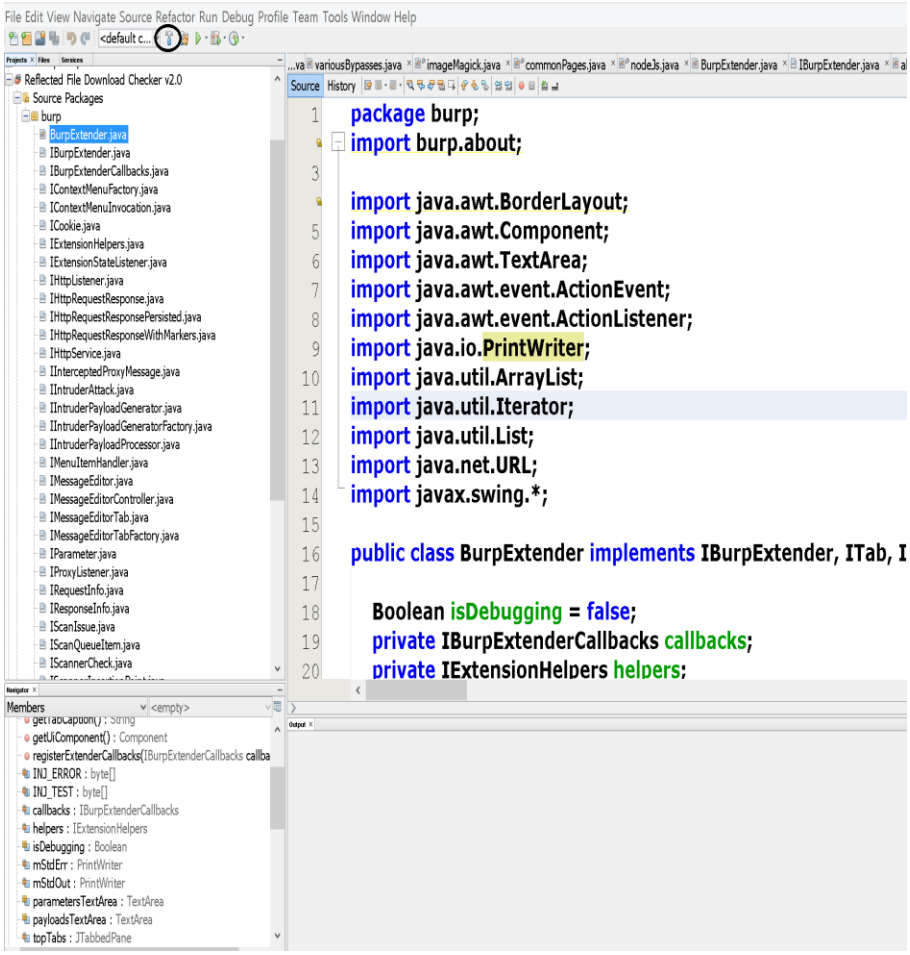
Eğer bu parametre isimlerinden herhangi biri kullanılmış ise "Potential RFD Issue Detected" zafiyeti bulgular tablosuna eklenir.

Active Scan Esnasında (doActiveScan)

- Eğer uygulama grafik ara yüzündeki “RFD Parameters” tab’ından alınan parametreleri içeriyor ise “RFD Payloads” kısmında bulunan değerler HTTP parametre değeri olarak atanır ve aynı parametre değerlerinin uygulama cevabında gösterilip gösterilmediği kontrol edilir.

- Eğer uygulama Content-Type HTTP başlığında json veya javascript değerlerini içeriyor ise fakat “RFD Parameters” tabında bulunan hiç bir parametre ismi ilgili istekde kullanılmamış ise bu parametre isimlerini “RFD Payloads” tabında bulunan kelimeler (string) ile ilgili isteğe eklenir ve HTTP cevabında varlığı kontrol edilir. Var ise “Reflected File Download” bulgusu zafiyetler tablosuna eklenir.

Uygulama kodu üzerinde değişiklik yapılmak istenir ise mevcut proje “Net Beans” yazılımı aracığılığı ile açılır ve “BurpExtender.java” dosyasında istenilen değişiklikler yapılır. İstenilen değişiklikler yapıldıktan sonra aşağıdaki ekran görüntüsünde gösterildiği şekilde proje derlenir. Proje doğru şekilde derlendiğinde Burp Suite üzerinden yüklenmesi gereken jar dosyası “\BurpExtender\dist” dizininde oluşacaktır.



Referanslar

https://www.blackhat.com/docs/eu-14/materials/eu-14-Hafif-Reflected-File-Download-A-New-Web-Attack-Vector.pdf

https://www.davidsopas.com/reflected-file-download-cheat-sheet/