ما هو AngularJS ؟

من إعداد

لا يخفى على الكثير من مبرمجي مواقع الانترنت "منصة الـ "AngularJS والتي يعود تاريخها الى عام 2012 , حيث قامت ببنائها شركة GOOGLEبناءً على مكتبات لغة الـ , JavaScript فقد جاءت هذه المنصة لتوفر السرعة والكفائة عبر الكثير من الاضافات والمميزات لتضفي تميزاً في مجال ال Front-End Developmentاي بما يتعلق بمظهر الموقع , وضف على ذلك انها مبنية على ال MVC Design Patternوالذي يعتبر من اشهر انماط البرمجة في وقتنا الراهن.

مثال بسيط على استخدام منصة الـAngularJS

سوف يظهر جمع 5 + 5 = 10

كيف يتم حقن قالب AngluarJS

```
<!DOCTYPE html>
<html>
<script
src="https://ajax.googleapis.com/ajax/libs/angularjs/1.6.4/angular.
min.js"></script>
<body>

<div ng-app>
<p>My first expression: {{ 5 + 5 }}</p>
</div>

</body>
</html>
```

في المثال السابق استخدمنا مصطلح متعارف عليه في ال AngularJsوهو ال Expressionوهو كل ما بين الاقواس

{{ expression }}وهو المكان الذي سنقوم فيه بحقن البايلود Payload وهو كود الJavaScript

هذا يعني : إن قام المستخدم بادخال {{ }} فان مترجم الـ **AngularJs**سيقوم بتحويله وينفذه مما سيؤدي الى

ثغرة **XSS – Cross Site Scripting** من خلال **Angular Expression**

ملاحظة : حقن قالب الـ AngularJs فقط يكون في عنصر ال Angularاي ng-app

كيف يحدث الحقن ؟

إن اي تجربة بسيطة لحقن بايلود ال XSSفي احدى قوالب ال AngularJsلا يؤدي الى ظهور ثغرة XSS ما لم يكن بالشكل المطلوب اولاً , وثانياً ما لم تتخطى ما يعرف بالـAngularJs Sandbox

ملاحظة : لمعرفة البارامتر او العنصر المصاب بهذه الثغرة او لا يمكنك ان تقوم بتجربة بدائية وهي {{7*7}} فان كانت النتيجة 49 فهو مصاب ويمكنك الاستمرار وفي بعض التطبيقات ممكن استخدام [[7*7]] وان نجحت بالتنفيذ فاستمر باستخدام [[ ]] في جميع البايلودات المستخدمة

1. مثال :ان قام المستخدم بحقن البايلود <script>prompt('XSS')</script>

فالنتيجة ستكون <script>prompt('XSS')</script>

هنا يظهر ان التطبيق آمن من ثغرة ال XSSلكن في الحقيقة نحن لم نتبع أساسيات الحقن فالبايلود ليس بالشكل المطلوب ولم نتخطى الSandbox

كيف نحسن Payload المستخدم ؟

هيا نحسن البايلود عبر اضافة فورمات الAngularJs

البايلود بالفورمات المطلوب{{prompt(‘XSS’)s}} :

النتيجة : ايضاً لم ينفذ البايلود وذلك بسبب حظره من قبل الAngularJs Expression Sandbox

لا ليس كما تظن, التطبيق الى الان ليس آمن وذلك حسب مرجع ووثائق الـ **AngularJs Documentation**فشـــركة الـ **GOOGLE**تنـوه الى ان تعابيـــر ال **AngularJs Expression**لا تقدم حمايـــة بل زد علـــى ذلك ان الـ **Expressino Sandbox**مهمته الرئيسية ليست الحماية او ايقاف الهاكر بل هي لفصل وتنظيم اجزاء التطبيق وعمله بكل سلاسة وبعيداً عن اي هشاشة فيه

كيف تتخطي AngularJs Expression Sandbox ؟

حتى عند الرجوع الى مرجع الـ AngularJS Documentationوخاصة ما يتعلق بالخلط بين الجهتين السيرفر والعميل-Mixing Server Side and Client-Side Templateفالثغرة تكون مؤثرة اكثر اي بمعنى آخر ان قام المستخدم بادخال بايلود وقامت جهة السيرفر بتحويله وتنفيذه فيمكننا الحصول على ثغرة من نوعXSS

لذلك ما سنقوم به هو الخروج من ال Sandboxويمكن ان يحدث ذلك عبر:

1. اعادة كتابة بعض ال Functionsالموجودة في منصة ال AngularJsمثل

charAt

fromCharCode

```
{{
    'a'.constructor.prototype.charAt=[].join;
    $eval('x=alert("XSS")')+''
}}
```

toString

1. استدعاء الـ AngularJs Constructor وقد انتشر في السابق الكثير من البايلودات من نفس النوع والي يمكن تنفيذه عبر استدعاء ال Constructorوسنسرد في نهاية المقال بعض المراجع وال Constructorهو built-in Function لاي Class موجودة , لكن في حالتنا هو Class وهو property اي خاصية تتبع ال Objectمثل الطول والعرض واللون ...الخ وممكن استدعائه مثله مثل اي خاصية اخرى

```
{{constructor.constructor('alert(1)')()}} الاصدار 1.3.2

{{0[a='constructor'][a]('alert(1)')()}} الاصدار 1.6.0
```

وهنا ما قمنا به هو عمل function يحتوي على (1 alert(وهو من نوع , anonymous فبحسب لغة الجافا سكريبت فيمكنك عمل function مثال

فالسطر الاول قمنا بإنشاء هذا ال Functionالذي لا اسم له والذي سيكون بنيته كما السطر 3,4,5

```
1  Function("alert(1)")
2
3  function anonymous(){
4  alert(1)
5  }
```

لذلك اذا اردنا ان نستعرض بنية هذا ال functionفيمكننا من خلال(constructor.constructor.alert(1

اما اذا اردنا تنفيذه بدون معرفة اسم هذا ال Functionفكل ما علينا فعله هو اضافة () ليصبح بذلك كما في الصورة ادناه

وممكن استدعاء ال Functionمن خلال ال scopeوهو عنصر اساسي في منصة ال AngularJsللتعامل مع ال Controllersوالعناصر الاخرى

```
1  constructor.constructor.alert(1)()
2
3  scope.constructor.constructor.alert(1)()
```

في النـهاية:

إن كنت تستخدم منصة AngularJs كـ Front-End فيجب عليك فلترة ال{{ }} او حتى ان كنت تستخدم Markup لغة ترميزية مثل ال[[ ]] فأيضاً يجب ان تقوم بفلترة المدخلات جيداً واعتبارها خطراً حقيقاً على الموقع , وينصح ايضاً بالابتعاد عن استخدام ال AngularJsمن جهة السيرفر بما يتعلق بترجمة مدخلات المستخدم

كما رأيتم فان هناك عدة طرق لتخطي الـ AngularJs Expression Sandbox وتكلمنا عن كيفية حدوث هذا التخطي ومنها انشاء Function جديدة تحتوي على كود الجافا سكريبت لتفعيل ال XSSاو من خلال اعادة كتابة Functions موجودين في المكتبة اصلاً , لكن تختلف في طريقة التطبيق والاستدعاء

مراجع:

الموقع الرسمي لـ : AngluarJS

https://docs.angularjs.org/guide/security

الاسغلالات المستخدمة " Payloads "

blog.portswigger.net/2016/01/xss-without-html-client-side-template.html

بعض من الثغرات المقدمة من خلال الهاكرز لبرامج المكافئات علي منصةHackerOne

– https://hackerone.com/reports/230234

– https://hackerone.com/reports/141463

– https://hackerone.com/reports/141240

Greetings to :

jericho * Larry W. Cashdollar * brutelogic* shadow_00715* 9aylas * djroot.dz * LiquidWorm* Hussin-X *D4NB4R * ViRuS_Ra3cH * yasMouh

Telegram : indoushka

Mobil : 00213771818860