الفصل السادس
ثغرة ال XPath Injection

المؤلف
د.م/ أحمد هاشم الفقي
استشارى أمن المعلومات و التحول الرقمي
Ahmed.Hashem.ElFiky@outlook.com

ثغرة ال XPath Injection

- قبل الخوض في تفاصيل ثغرة XPath Injection لنعرف أولًا ما هو الـ XPath في الأساس؟
- الـ XPath عبارة عن Query Language يتم استخدامها لجلب بعض البيانات المخزنة في XML Document
- تعريف مختصر وجميل، لنفصّل فيه الآن أكثر ..
- في بعض تطبيقات الويب (في الغالب التطبيقات البسيطة) يتم استخدام الـ XML Documents لتخزين بعض البيانات مثل : أسماء المستخدمين وبياناتهم، الصلاحيات، و أي نوع من البيانات التي يخدمها التطبيق ، على سبيل المثال تطبيق ويب يعرض قائمة بالكتب، قد يتم تخزين قائمة الكتب وتفاصيل كل كتاب (تاريخ النشر ، الكاتب ، الإصدار .. إلخ) في ملف XML

ثغرة ال XPath Injection (تكمله...)

- حتى يستطيع تطبيق الويب معالجة هذه البيانات (عرضها للمستخدم مثلًا) لابد من وجود آلية تُمكّن تطبيق الويب من جلب البيانات المخزنة في ملفات الـ XML
- الـ XPath هي اللغة -إن صح التعبير- التي تتيح لنا الوصول وتنفيذ Query على البيانات المخزنة في ملفات الـ XML
- XPath Injection
- يحدث هذا النوع من الثغرات عندما يقوم تطبيق الويب بمعالجة XPath query يتم بناءها بناءً على مُدخَل input يأتي من المستخدم، وهذا المُدخَل لا يتم معالجته بالشكل السليم، بالتالي قد يقوم المخترق بإستغلال هذا الخطأ البرمجي والتحكم بالـ XPath query التي يتم تمريرها للتطبيق،
- لنأخذ الكود التالي كمثال على هذه الثغرة:

ثغرة ال XPath Injection (تكمله...)

- الكود خاص بـ OWASP Mutillidae II، تحديدًا الصفحة التي تعرض بيانات المستخدم، تستطيع إيجادها في هذا المسار : mutillidae/user-info-xpath.php/

```
1 $lXPathQueryString = "//Employee[UserName='{USERNAME}' and Password='{PASSWORD}']";
2 $lXPathQueryString = str_replace("{USERNAME}", $lXPathUsername, $lXPathQueryString);
3 $lXPathQueryString = str_replace("{PASSWORD}", $lXPathPassword, $lXPathQueryString);
4 $lXMLQueryResults = $XMLHandler->ExecuteXPATHQuery($lXPathQueryString);
```

- السطر رقم 1 : يتم بناء الـ XPath query التي تقوم بالبحث في الـ Node المُسمّاه Employee وتمرّر لها قيمتين ، إسم المستخدم USERNAME و PASSWORD، هذه القيمتين يقوم المستخدم بإدخالها، وتُمرّر لتطبيق الويب عبر الـ URL Parameters كالتالي :

ثغرة ال XPath Injection (تكمله...)

Request

Raw | Params | Headers | Hex

```
1 GET /mutillidae/index.php?page=
  user-info-xpath.php&username=username&password=
  password&user-info-php-submit-button=
  View+Account+Details HTTP/1.1
2 Host: 192.168.162.122
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
  rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;
  q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Upgrade-Insecure-Requests: 1
```

ثغرة ال XPath Injection (تكمله...)

- السطر رقم 2 وَ 3 : يتم دمج القيم القادمة من الـ HTTP Request مع الـ query هنا مصدر الخَلل ، لم يتم معالجة المدخلات بالشكل السليم!
- السطر رقم 4 : يقوم هذا السطر بتنفيذ الـ Query
- لنأخذ مثال آخر:
- ملف الـ XML الذي سيتم تنفيذ الـ XPath query عليه كالآتي :
-

ثغرة ال XPath Injection (تكمله...)

```
<addressBook>
    <address>
        <firstName>William</firstName>
        <surname>Gates</surname>
        <password>MSRocks!</password>
        <email>billyg@microsoft.com</email>
        <ccard>5130 8190 3282 3515</ccard>
    </address>
    <address>
        <firstName>Chris</firstName>
        <surname>Dawes</surname>
        <password>secret</password>
        <email>cdawes@craftnet.de</email>
        <ccard>3981 2491 3242 3121</ccard>
    </address>
    <address>
        <firstName>James</firstName>
        <surname>Hunter</surname>
        <password>letmein</password>
        <email>james.hunter@pookmail.com</email>
        <ccard>8113 5320 8014 3313</ccard>
    </address>
</addressBook>
```

ثغرة ال XPath Injection (تكمله...)

- تعليمة الـ XPath التي تقوم بإسترجاع جميع الإيميلات ستبدو كالتالي :

```
//address/email/text()
```

- ولو أردنا عرض البيانات الخاصة بالمستخدم Dawes ستكون التعليمة كالتالي :

```
//address[surname/text()='Dawes']
```

- الآن لنفترض أن تطبيق الويب سيقوم بعرض بيانات الـ credit card بناءً على اسم المستخدم username وكلمة المرور password، سيتم تمرير هذه القيم من قبل المستخدم وستكون الـ query كالآتي :

ثغرة ال XPath Injection (تكمله...)

```
//address[surname/text()='Dawes' and password/text()='secret']/ccard/
text()
```

في حالة لم يقم المبرمج بمعالجة هذه المدخلات بالشكل السليم، قد يقوم المخترق بحقن القيمة التالية في حقل كلمة المرور :

```
' or 'a'='a
```

سيؤدي حقن القيمة السابقة إلى جعل التعليمة كالآتي :

```
//address[surname/text()='Dawes' and password/text()='' or 'a'='a']/
ccard/text()
```

والتي ستقوم بعرض قيم الـ credit cards لجميع المستخدمين

ثغرة ال XPath Injection (تكمله...)

- الممارسات الصحيحة لمنع ثغرات الـ XPath Injection
- لا تقم ببناء queries تستند على مُدخلات قادمة من المستخدم في المقام الأول
- إن كان ولا بد من بناء مثل هذه التعليمات، فتأكد بأنك تقوم بإختبار الـ parameters القادمة من المستخدم والتأكد بأنها تحتوي فقط على القيم المسموحة، مثل الأرقام والحروف فقط، بمعنى آخر إستخدم منهجية White List لإختبار المدخلات، ولا تقم بالإعتماد على تنقيح المدخلات Sanitization، حيث أن الطريقة الأخيرة لها طُرق تجاوز عدّة.

تم بحمد الله انتهاء الفصل السادس