ARTIKEL KAMSIB

Kamar Kamsib memiliki visi untuk meningkatan literasi keamanan informasi dan siber masyrakat Indonesia. Dengan pendekatan konten Instagram dan artikel mengenai *cyber security* yang mudah dipahami oleh seluruh kalangan masyarakat.

KAMSIB

Dokumen Terbatas Untuk Pembelajaran

Judul : Mengenal XXE XML External Entity Injection
Penulis : Anton Lepari
Tanggal : Januari 17, 2023
Keterangan : Bisa diakses dalam bentuk artikel web dan PDF

A. XML

Extensible Markup Language (XML) adalah bahasa markup dan format file untuk menyimpan, mentransmisikan, dan merekonstruksi data arbitrer. XML mendefinisikan seperangkat aturan untuk meng-*encoding* dokumen dalam format yang dapat dibaca manusia dan dapat dibaca mesin. Tujuan desain XML menekankan kesederhanaan, umum, dan kegunaan di Internet [1].

XML merupakan format data tekstual dengan dukungan kuat melalui Unicode untuk berbagai bahasa manusia. Meskipun desain XML berfokus pada dokumen, bahasa ini banyak digunakan untuk representasi struktur data arbitrer (*arbitrary data structures*) seperti yang digunakan dalam layanan web [1].

B. Injeksi XML external entity (XXE)

Injeksi Entitas Eksternal XML (*XXE Injection*) adalah kerentanan keamanan web yang memungkinkan penyerang mengganggu pemrosesan data XML oleh aplikasi. Seringkali memungkinkan penyerang untuk melihat file pada *filesystem* server aplikasi [2]. Serangan injeksi XXE memungkinkan penyerang untuk mengubah sintaks, konten, atau perintah sebelum diproses untuk sistem final [3].

Dalam beberapa situasi, penyerang dapat meningkatkan serangan XXE untuk mengkompromikan server yang mendasarinya (atau infrastruktur *back-end* lainnya) dengan memanfaatkan kerentanan XXE untuk melakukan serangan pemalsuan permintaan sisi atau *server server-side request forgery* (SSRF).

C. Serangan

Berikut adalah contoh payload yang bisa diinjeksi ke XML sehingga menjadi sebuah serangan File Disclosure [3]:

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/shadow"> ]>
<userInfo>
<firstName>Minsib</firstName>
<lastName>&ent;</lastName>
</userInfo>
```

Payload tersebut dimasukkan untuk mengubah request ke server. Sedangkan berikut ini adalah contoh bahasa dasar dari XML yang dikirimkan ke server [3]:

```
<!--?xml version="1.0" ?-->
<userInfo>
<firstName>Admin</firstName>
<lastName>Kamsib</lastName>
</userInfo>
```

D. Contoh CVE

Salah satu contoh serangan XXE yang menjadi sebuah CVE adalah CVE-2019-9670. Kerentanan tersebut ada pada mailboxd di Synacor Zimbra Collaboration Suite 8.7.x (< 8.7.11p10) seperti yang ditunjukkan oleh Autodiscover/Autodiscover.xml [4]. Kerentanan injeksi XXE yang diungkapkan pada Maret 2019 ini masih dipindai secara aktif untuk komponen kotak surat (mailboxd) yang rentan di Synacor Zimbra Collaboration Suite 8.7.x sebelum 8.7.11p10. Eksploitasi ini mencoba membaca file konfigurasi Zimbra yang berisi kata sandi LDAP untuk akun Zimbra [5].

E. Referensi

1. https://en.wikipedia.org/wiki/XML
2. https://portswigger.net/web-security/xxe
3. Sharif, Md Haris. (2022). Web Attacks Analysis and Mitigation Techniques. https://www.researchgate.net/publication/358547598_Web_Attacks_Analysis_and_Mitigation_Techniques
4. https://nvd.nist.gov/vuln/detail/CVE-2019-9670
5. https://isc.sans.edu/diary/CVE20199670+Zimbra+Collaboration+Suite+XXE+vulnerability/27570