

Outlook Money
<http://money.outlookindia.com/>

Directory Listing Allowed and Open access to
User's Personal information including
Name,Address,E-mail,Phone No.,Mobile No. etc

Reported by : Raxit Sheth
E-mail: raxitsheth2000@gmail.com
Author : Raxit Sheth

Disclosure Timeline

reported time: Jun 21,2009, 12:59 pm

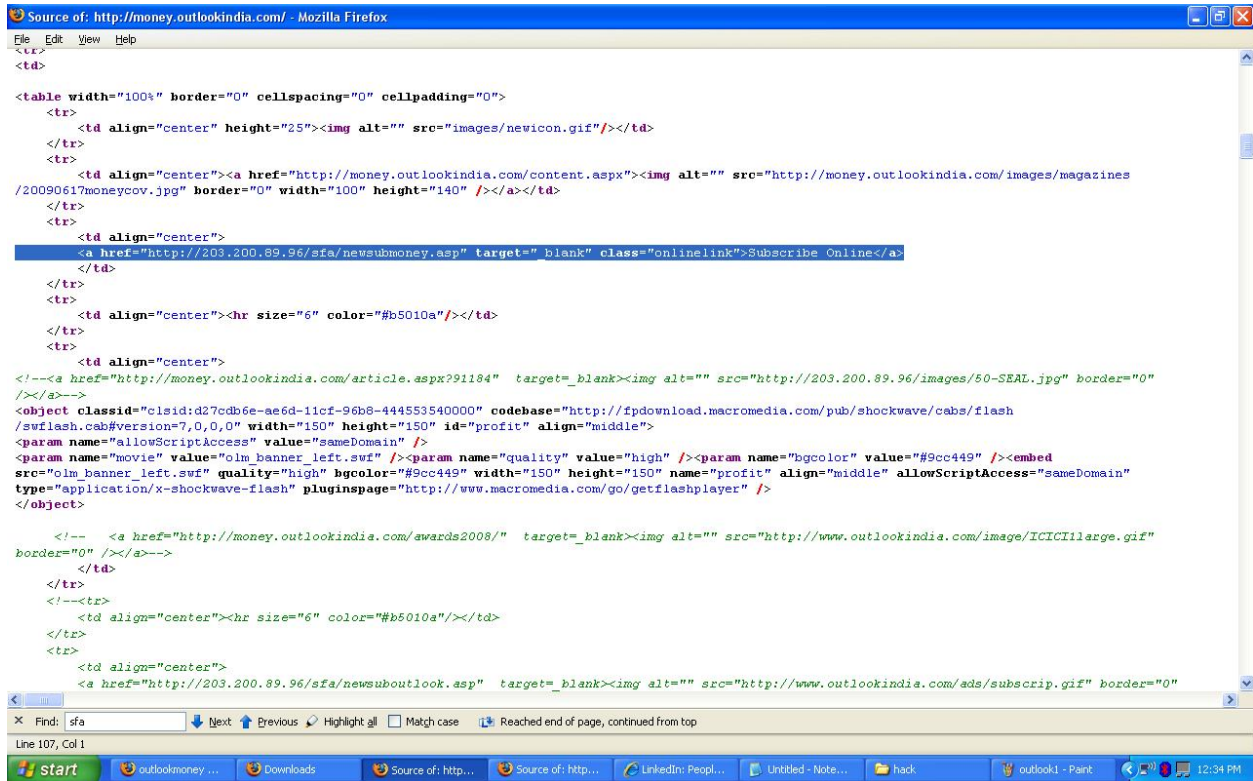
Fixed & Confirmation : Jun 22, 2009, 7:09 PM

Raxit Sheth [raxitsheth2000@gmail.com]

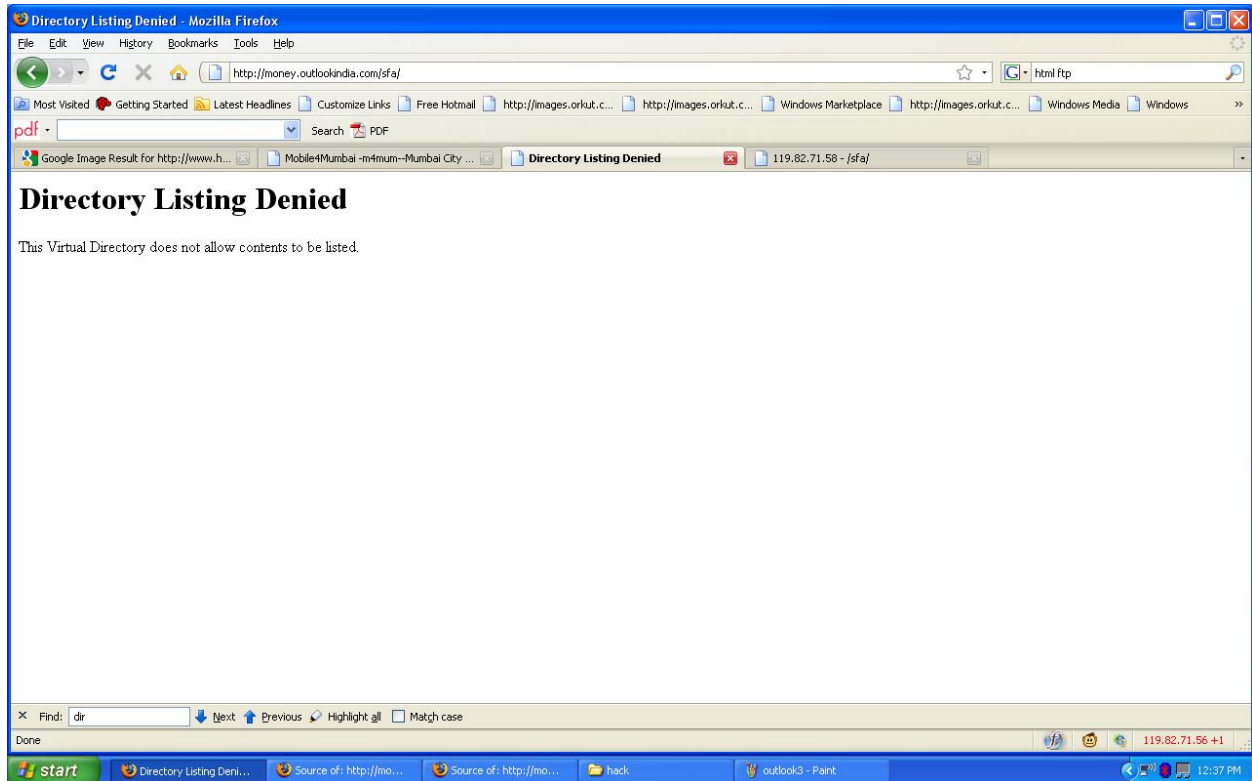
PoC and How to ?

[Plesae do not try this has been fixed.]

1. View source of <http://money.outlookindia.com/>

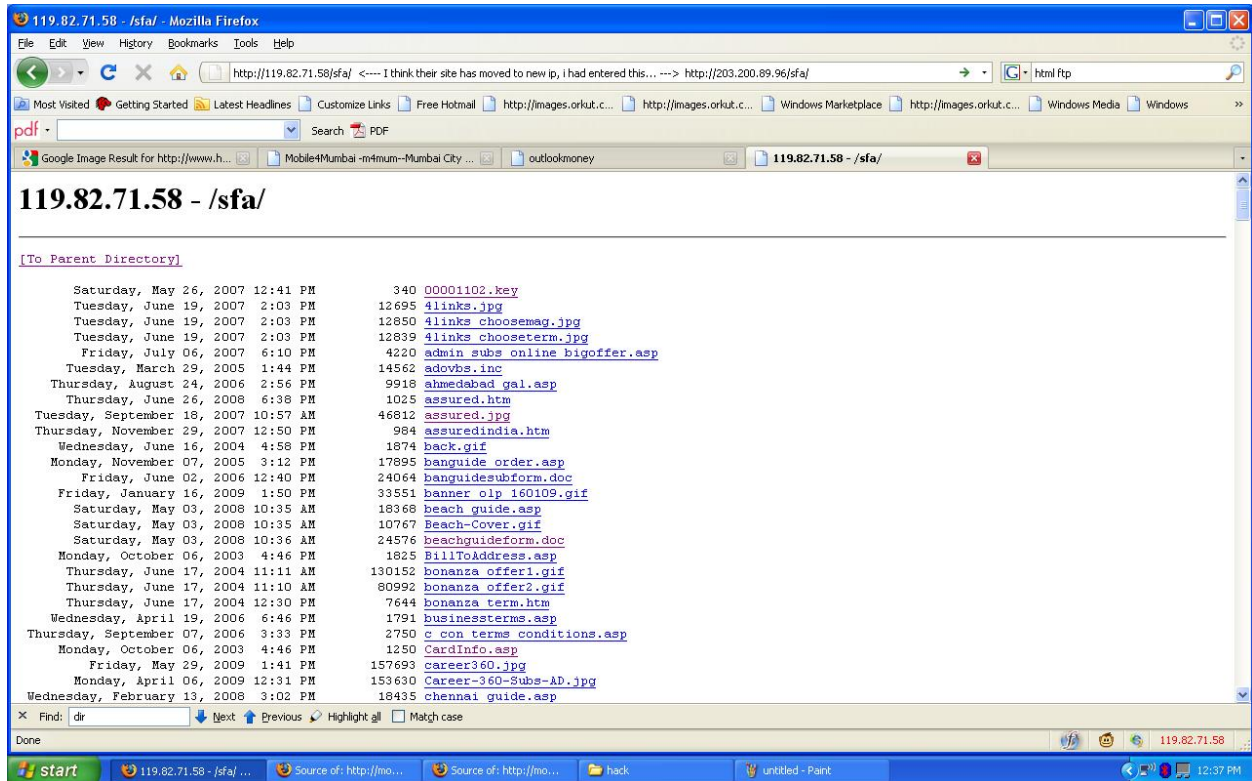


2. Trying <http://money.outlookindia.com/sfa/> [not worked !!! :(]

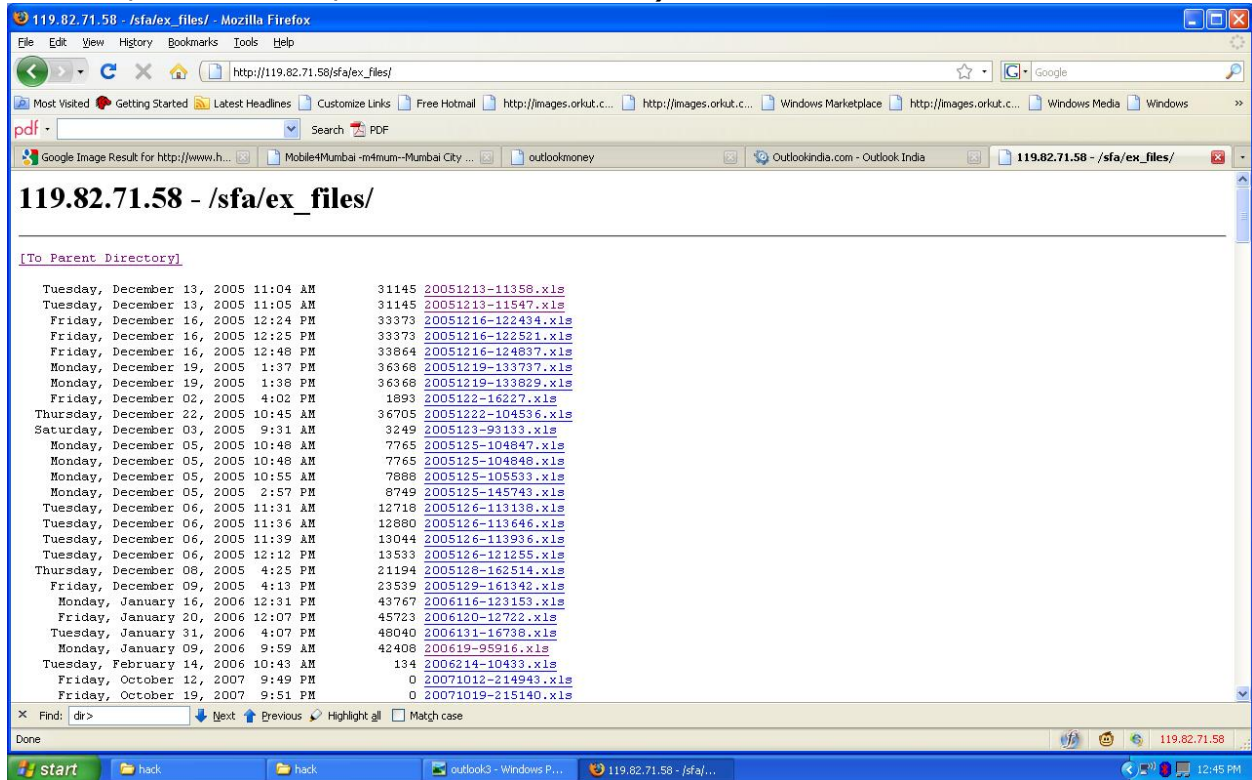


Raxit Sheth [raxitsheth2000@gmail.com]

3. Let me try with ip address !



4. Traversing more directories ! (this is just one sample directory out of few more ! with many xls file, which was containing personal informations like First name, last name, Postal address, E-mail, Phone No., Mobile No. etc !)



Lesson Learnt:

1. Proper configuration of web server so it should not show directory listing in anyway.
2. even it was not showing directory listing when we entered domain name, but when we tried with ip address, it was open :)
3. Do not put any file with critical information which can be directly accessible from web.