- DISCLOSED VULNERABILITY REPORT -

By Prv | mail | github | bugcrowd |

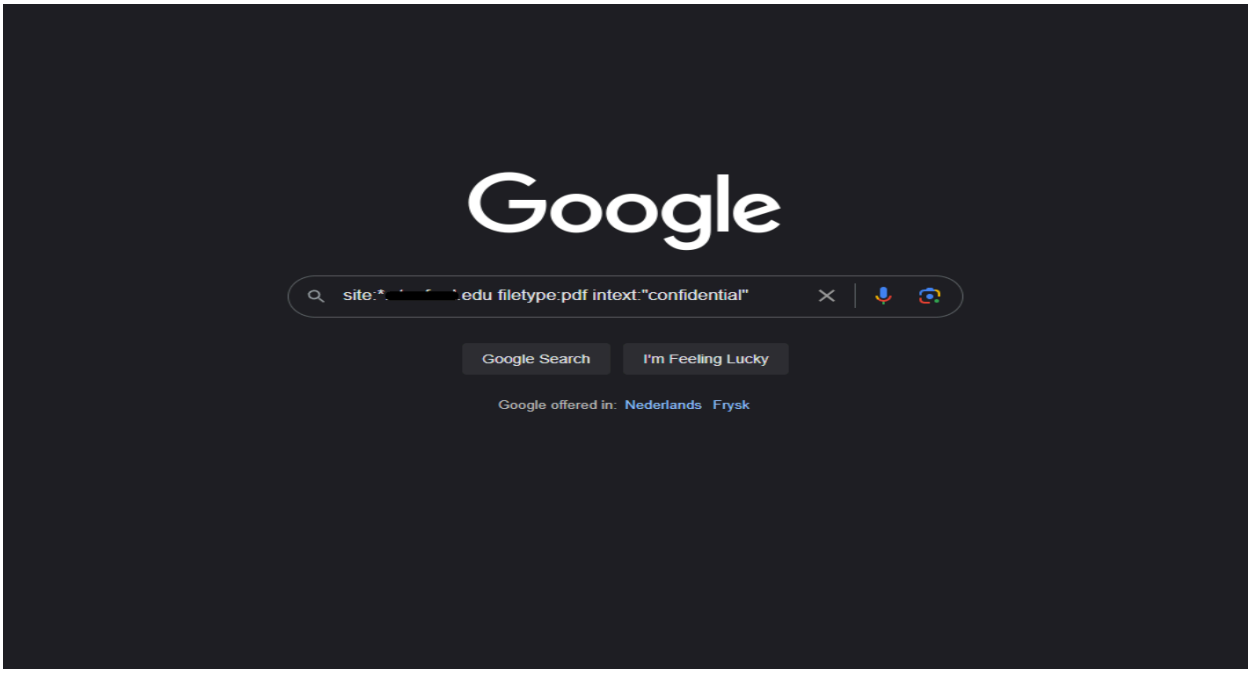
Name: PII & Internal Document Leakage Due To Improper Control Of File Storage and Access Control Measures on Large University Domain

Vulnerability type: Sensitive Data Exposure for Internal Asset

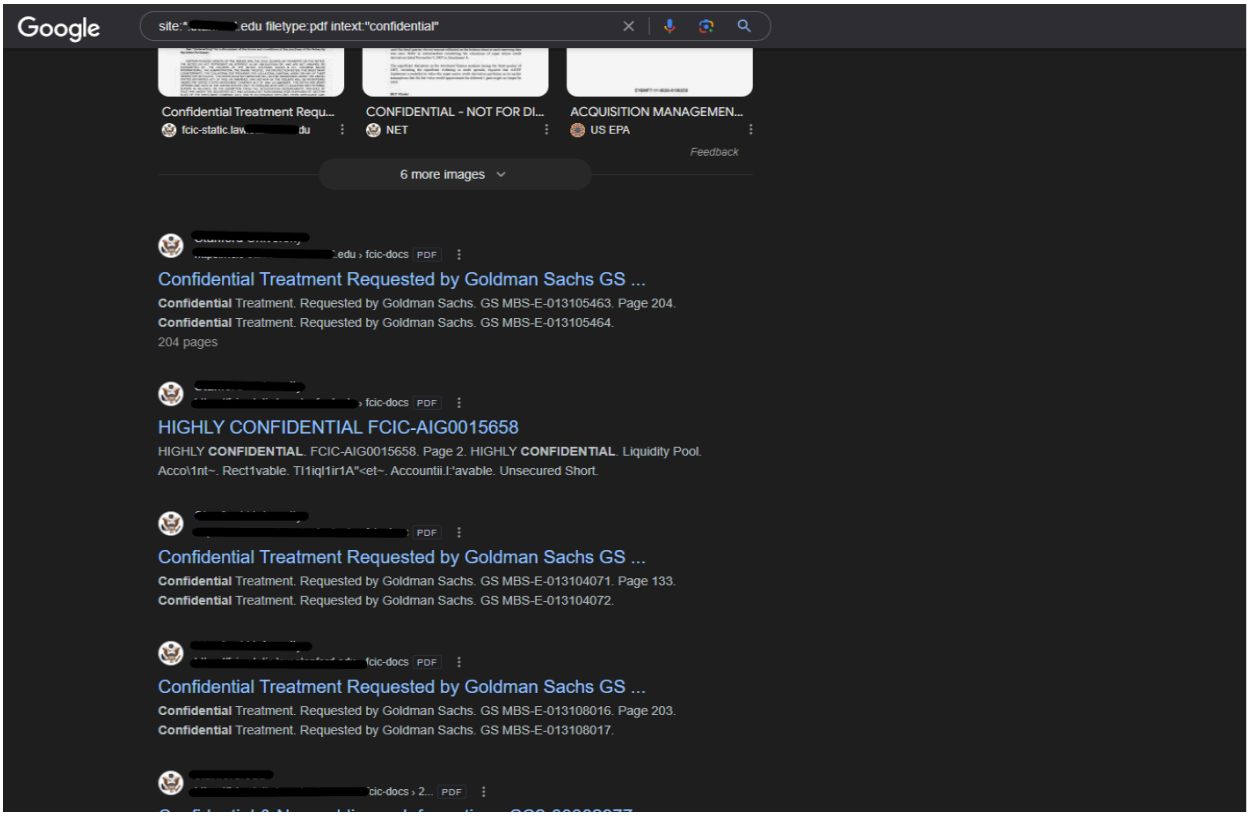
Severity: High⇒Critical

Overview:

During testing on a large university domain, I decided to look at the listed files on the website VIA the use of different queries and 'dorks'.



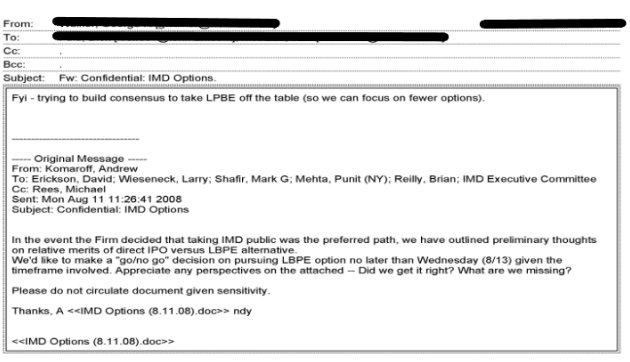
During this process, discovered many different files, some being irregularly listed or without proper context, upon visiting these publicly listed files, came across many that related to internal resources of both students and the universities internal database.



Some of these files contained numerous pieces of critical PII (publicly identifiable information) and confidential data, some of this data found was information such as:

Internal Confidential Emails Regarding Finance and Legal Situations of students and staff:

https://[redacted]~jbulow/Lehmandocs/docs/JPMORGAN/JPM-EXAMINER00000493.pdf
https://[redacted]~jbulow/Lehmandocs/docs/JPMORGAN/JPM-2004%200006510.pdf
https://[redacted]~jbulow/Lehmandocs/docs/JPMORGAN/JPM-2004%200002093-0002099.pdf
https://[redacted]~jbulow/Lehmandocs/docs/ERNST%20&%20YOUNG/EY-LE-LBHI-KEYPERS%203670023-3670024.pdf
https://[redacted]~jbulow/Lehmandocs/docs/DEBTORS/LBHI_SEC07940_653425-653426.pdf
https://fcic-static.law[redacted]/cdn_media/fcic-docs/2008-09-16%20FRBNY%20Email%20re%20Merrill%20Lynch%20Overnight%20Info.pdf
https://[redacted]~jbulow/Lehmandocs/docs/DEBTORS/LBEX-DOCID%202461203.pdf
https://[redacted]~jbulow/Lehmandocs/docs/DEBTORS/LBHI_SEC07940_648034-648036.pdf


From: [redacted]
To: [redacted]
Cc:
Bcc:
Subject: Fw: Confidential: IMD Options.

Fyi - trying to build consensus to take LPBE off the table (so we can focus on fewer options).

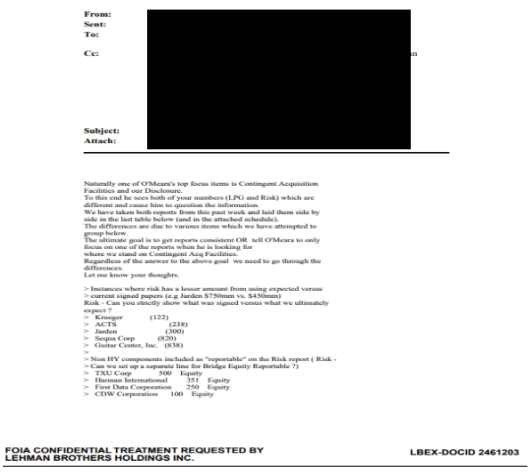
----- Original Message -----
From: Komaroff, Andrew
To: Erickson, David; Wieseneck, Larry; Shafir, Mark G; Mehta, Punit (NY); Reilly, Brian; IMD Executive Committee
Cc: Rees, Michael
Sent: Mon Aug 11 11:26:41 2008
Subject: Confidential: IMD Options

In the event the Firm decided that taking IMD public was the preferred path, we have outlined preliminary thoughts on relative merits of direct IPO versus LBPE alternative.
We'd like to make a "go/no go" decision on pursuing LBPE option no later than Wednesday (8/13) given the timeframe involved. Appreciate any perspectives on the attached -- Did we get it right? What are we missing?

Please do not circulate document given sensitivity.

Thanks, A <<IMD Options (8.11.08).doc>> ndy

<<IMD Options (8.11.08).doc>>


From:
Sent:
To:
Cc:
Subject:
Attach:

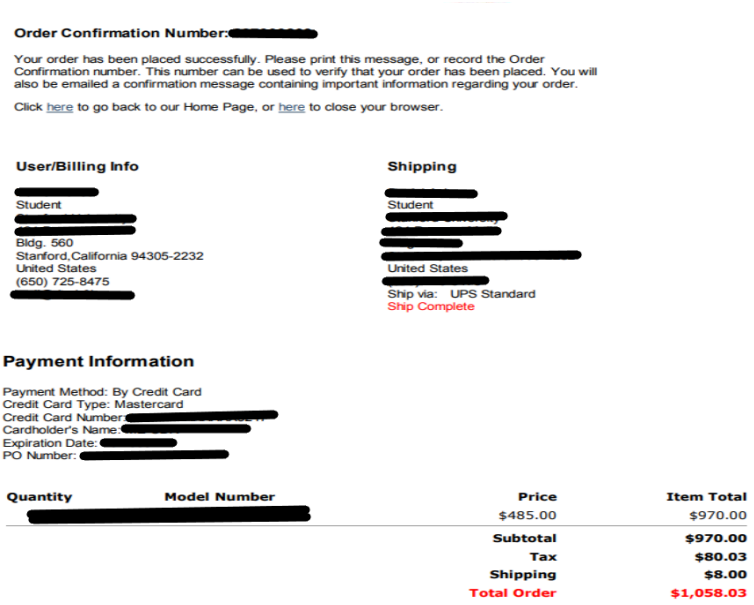
Naturally one of O'Meara's top focus items is Contingent Acquisition Facilities and our Disclosure.
To this end he sees both of your numbers (LPG and Risk) which are different and cause him to question the information.
We have taken both reports from this past week and laid them side by side in the last table below (and in the attached schedule).
The differences are due to various items which we have attempted to group below.
The ultimate goal is to get reports consistent OR tell O'Meara to only focus on one of the reports when he is looking for where we stand on Contingent Acq Facilities.
Regardless of the answer to the above goal we need to go through the differences.
Let me know your thoughts.

> Instances where risk has a lesser amount from using expected versus
> current signed papers (e.g Jarden $750mm vs. $450mm)
Risk - Can you strictly show what was signed versus what we ultimately expect ?
> Kroeger (122)
> ACTS (238)
> Jarden (300)
> Seqoia Corp (820)
> Guitar Center, Inc. (838)
>
> Non HY components included as "reportable" on the Risk report (Risk -
> Can we set up a separate line for Bridge Equity Reportable ?)
> TXU Corp 500 Equity
> Herman International 351 Equity
> First Data Corporation 250 Equity
> CDW Corporation 100 Equity

FOIA CONFIDENTIAL TREATMENT REQUESTED BY LEHMAN BROTHERS HOLDINGS INC.
LBEX-DOCID 2461203

Previous and Current Instances of Spam and Malware related evidence shown by malicious advertisements and pop ups, some being **phishing** and **pornography** related instances posted publicly on the universities pages.

Even credit card, Banking information and PII of students and staff:



Order Confirmation Number: [redacted]

Your order has been placed successfully. Please print this message, or record the Order Confirmation number. This number can be used to verify that your order has been placed. You will also be emailed a confirmation message containing important information regarding your order.

Click here to go back to our Home Page, or here to close your browser.

User/Billing Info

[redacted]
Student
[redacted]
Bldg. 560
Stanford,California 94305-2232
United States
(650) 725-8475
[redacted]

Shipping

[redacted]
Student
[redacted]
United States
[redacted]
Ship via: UPS Standard
Ship Complete

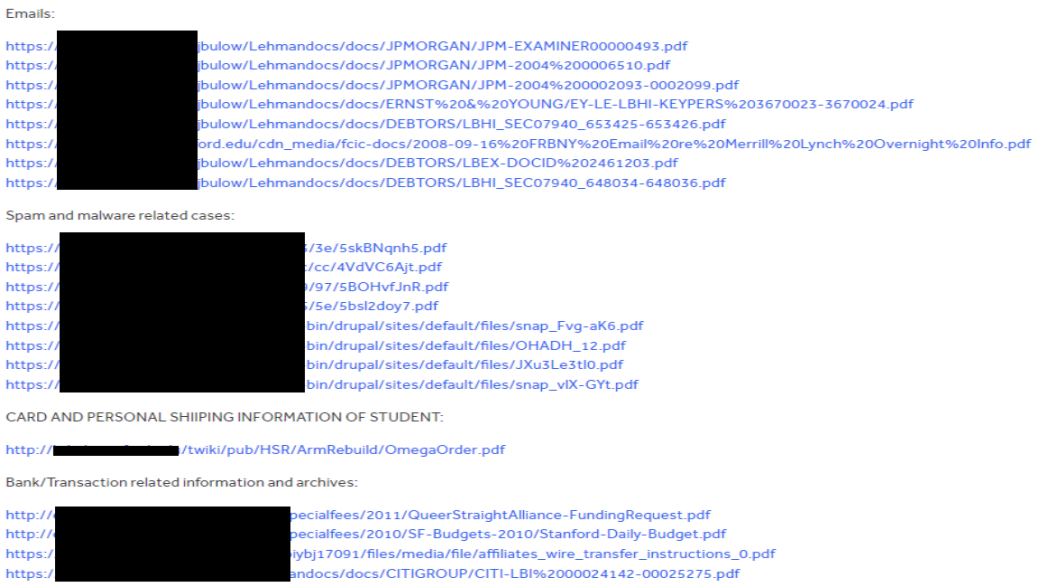
Payment Information

Payment Method: By Credit Card
Credit Card Type: Mastercard
Credit Card Number: [redacted]
Cardholder's Name: [redacted]
Expiration Date: [redacted]
PO Number: [redacted]

Quantity	Model Number	Price	Item Total
[redacted]		$485.00	$970.00
		Subtotal	**$970.00**
		Tax	**$80.03**
		Shipping	**$8.00**
		Total Order	**$1,058.03**

Much more than this shown was discovered, but due to the fact this matter has not been fully resolved and PII and banking information being leaked, cannot disclose anymore information in image format.

Instances of confidential file leakage:



Emails:

https://[redacted]bulow/Lehmandocs/docs/JPMORGAN/JPM-EXAMINER00000493.pdf
https://[redacted]bulow/Lehmandocs/docs/JPMORGAN/JPM-2004%200006510.pdf
https://[redacted]bulow/Lehmandocs/docs/JPMORGAN/JPM-2004%200002093-0002099.pdf
https://[redacted]bulow/Lehmandocs/docs/ERNST%20&%20YOUNG/EY-LE-LBHI-KEYPERS%203670023-3670024.pdf
https://[redacted]bulow/Lehmandocs/docs/DEBTORS/LBHI_SEC07940_653425-653426.pdf
https://[redacted]ord.edu/cdn_media/fcic-docs/2008-09-16%20FRBNY%20Email%20re%20Merrill%20Lynch%20Overnight%20Info.pdf
https://[redacted]bulow/Lehmandocs/docs/DEBTORS/LBEX-DOCID%202461203.pdf
https://[redacted]bulow/Lehmandocs/docs/DEBTORS/LBHI_SEC07940_648034-648036.pdf

Spam and malware related cases:

https://[redacted]/3e/5skBNqnh5.pdf
https://[redacted]/cc/4VdVC6Ajt.pdf
https://[redacted]/97/5BOHvfJnR.pdf
https://[redacted]/5e/5bsl2doy7.pdf
https://[redacted]bin/drupal/sites/default/files/snap_Fvg-aK6.pdf
https://[redacted]bin/drupal/sites/default/files/OHADH_12.pdf
https://[redacted]bin/drupal/sites/default/files/JXu3Le3tl0.pdf
https://[redacted]bin/drupal/sites/default/files/snap_vIX-GYt.pdf

CARD AND PERSONAL SHIIPING INFORMATION OF STUDENT:

http://[redacted]/twiki/pub/HSR/ArmRebuild/OmegaOrder.pdf

Bank/Transaction related information and archives:

http://[redacted]pecialfees/2011/QueerStraightAlliance-FundingRequest.pdf
http://[redacted]pecialfees/2010/SF-Budgets-2010/Stanford-Daily-Budget.pdf
https://[redacted]iybj17091/files/media/file/affiliates_wire_transfer_instructions_0.pdf
https://[redacted]andocs/docs/CITIGROUP/CITI-LBI%2000024142-00025275.pdf

Resolution:

The issue was fully documented and reported, the university was quickly made aware of this issue but is still ongoing, the majority of spam & malware related instances along with internal emails and banking information has since been removed from the public domain but instances may still exist.
