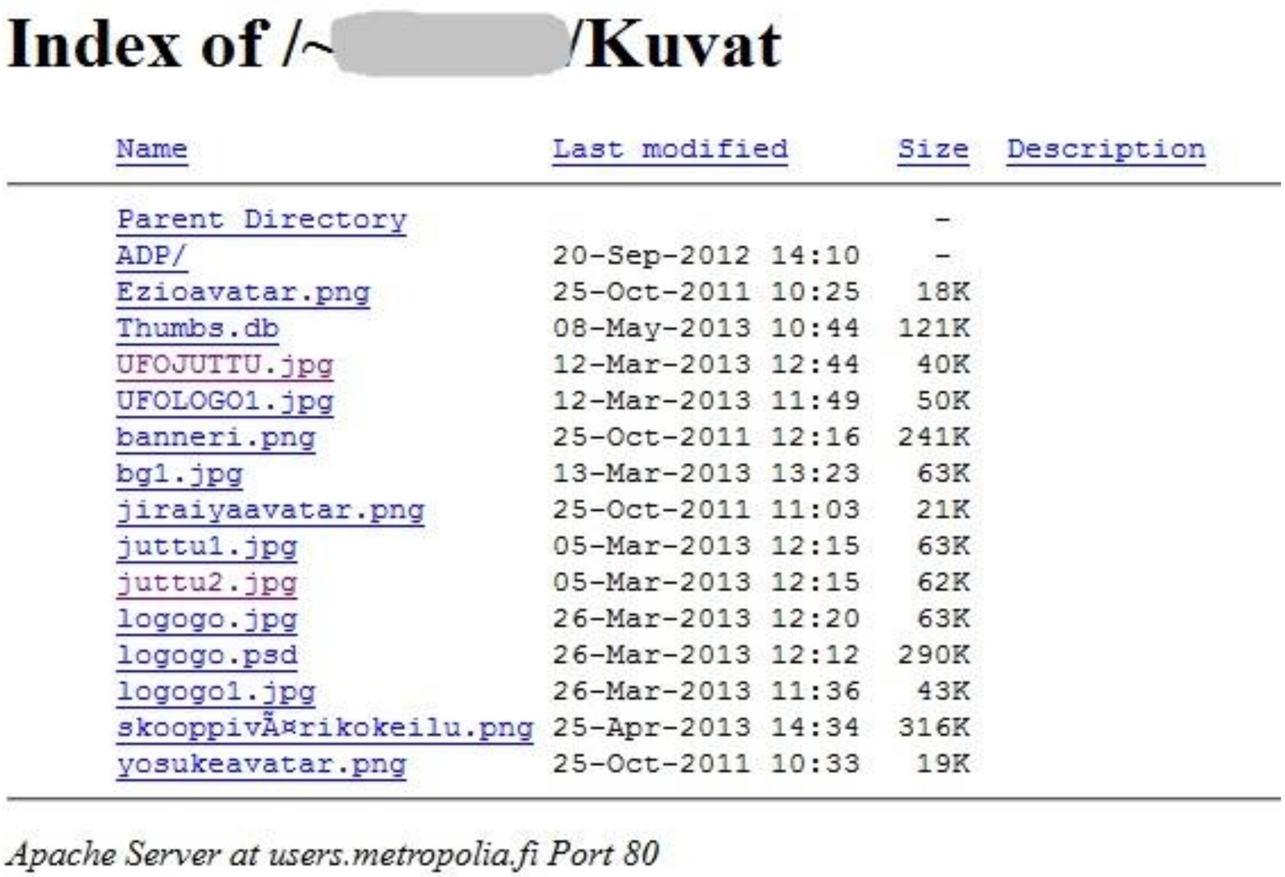
Unrestricted URL access

- Main cause
  - Failure to check access permissions for sensitive folders
- Access restrictions might be active for most parts of the website
  - Single error from developer can cause a vulnerability
- Hardest part is to locate the vulnerability
  - Protected but vulnerable URLs might not be visible or accessible trough normal webpages of website
  - URL fuzzers can be used to automate finding hidden folders and files

An example



Index of /~[redacted]/Kuvat

```
Name                    Last modified      Size  Description
--------------------------------------------------------------
Parent Directory                              -
ADP/                    20-Sep-2012 14:10     -
Ezioavatar.png          25-Oct-2011 10:25   18K
Thumbs.db               08-May-2013 10:44  121K
UFOJUTTU.jpg            12-Mar-2013 12:44   40K
UFOLOGO1.jpg            12-Mar-2013 11:49   50K
banneri.png             25-Oct-2011 12:16  241K
bg1.jpg                 13-Mar-2013 13:23   63K
jiraiyaavatar.png       25-Oct-2011 11:03   21K
juttu1.jpg              05-Mar-2013 12:15   63K
juttu2.jpg              05-Mar-2013 12:15   62K
logogo.jpg              26-Mar-2013 12:20   63K
logogo.psd              26-Mar-2013 12:12  290K
logogo1.jpg             26-Mar-2013 11:36   43K
skooppivÃ¤rikokeilu.png 25-Apr-2013 14:34  316K
yosukeavatar.png        25-Oct-2011 10:33   19K
--------------------------------------------------------------
```

Apache Server at users.metropolia.fi Port 80

Unrestricted URL access

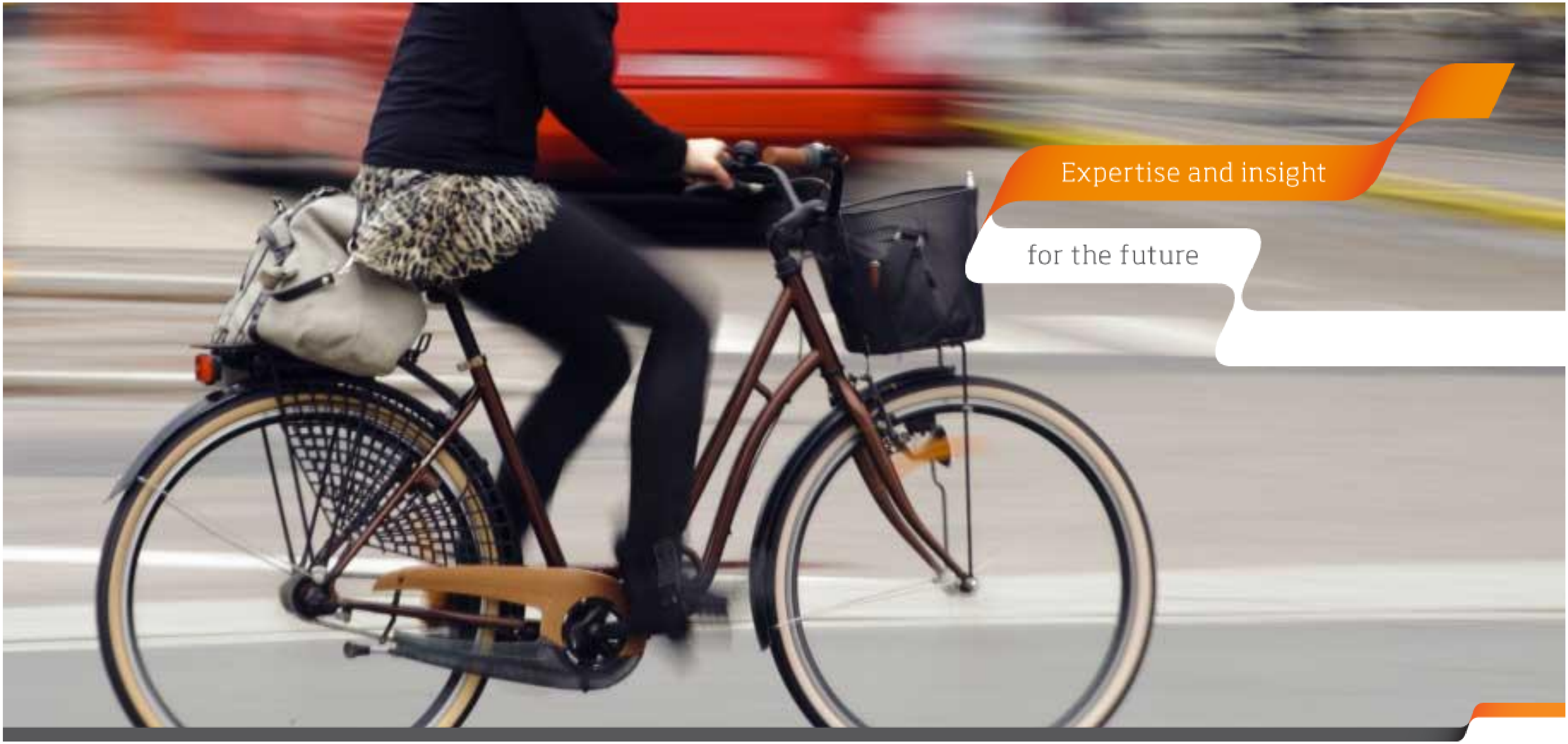
- Remember if the main site has restricted URL access there might be unrestricted access somewhere
  - So use directory bruteforcing (DirBuster)

Unsecure direct object references

- Vulnerability can happen if website uses parameters to construct the content of a webpage
- By maliciously modifying parameters confidential material could be accessed
  - Parameters can be used to fetch configuration files or HTML files
- This vulnerability is number four on OWASP top-10
  - And can lead to whole application compromise

An example

- Changing parameters to access confidential information
    - ttp://example.com/app/accountInfo?acct=notmyacct
    - http://example.com/app/accountInfo?acct=myaccount
- Viewing confidential files
    - http://example.com/open.php?file=pay.html
- Remember hidden parameters
    - So fire up your Burp proxy



THANK YOU!

www.metropolia.fi/en/
www.facebook.com/MetropoliaAMK
kimmo.sauren@metropolia.fi

Helsinki Metropolia University of Applied Sciences