Service Provider

Background

Versions

- 1.2
- 1.3 (since July ‘05)
- 2.0 (beta expected May ‘06)

Platform

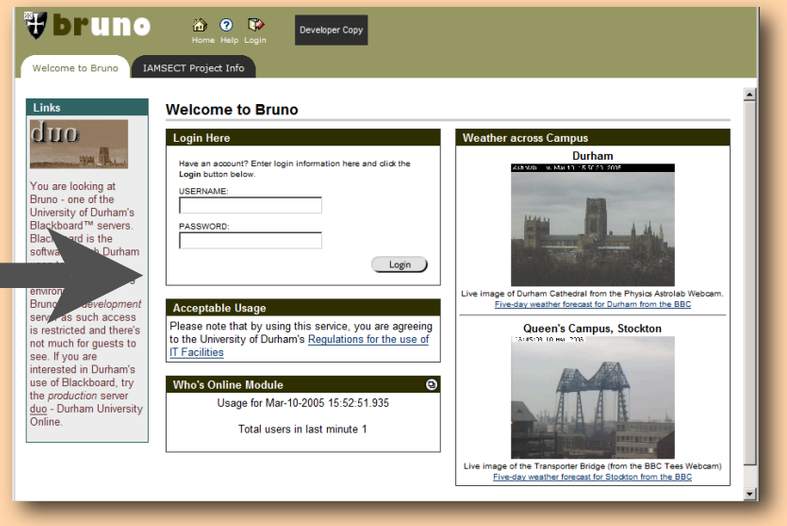
- cross-platform C++
  - Microsoft ISS via ISAPI
    - Apache httpd 1.3 & 2.0
- Java
  - shib 2.0

Service Provider

apache

mod_shib

shibd



Identity Provider

Building it

Binaries

- Redhat RPMs since 1.3
- much easier (if suitable)
- http://shibboleth.internet2.edu/latest.html

Documentation

- Dropped from shib docs as of 1.3
- in favour of wiki...
- ...but partially missing from wiki
- https://authdev.it.ohio-state.edu/twiki/
  - select “Shibboleth Web”

Install guide

- Not part of our original project plan...
- ...but in draft.

Dependencies: easy

- apxs (apache-dev)
- libssl-dev
- libcurl-dev

- Should be available with your O/S

Dependencies: intermediate

- opensaml
- libxml-security-c

Dependencies: harder

- xerces-c
  - via Internet2, bug in upstream
- log4cpp
  - via Internet2, project in limbo

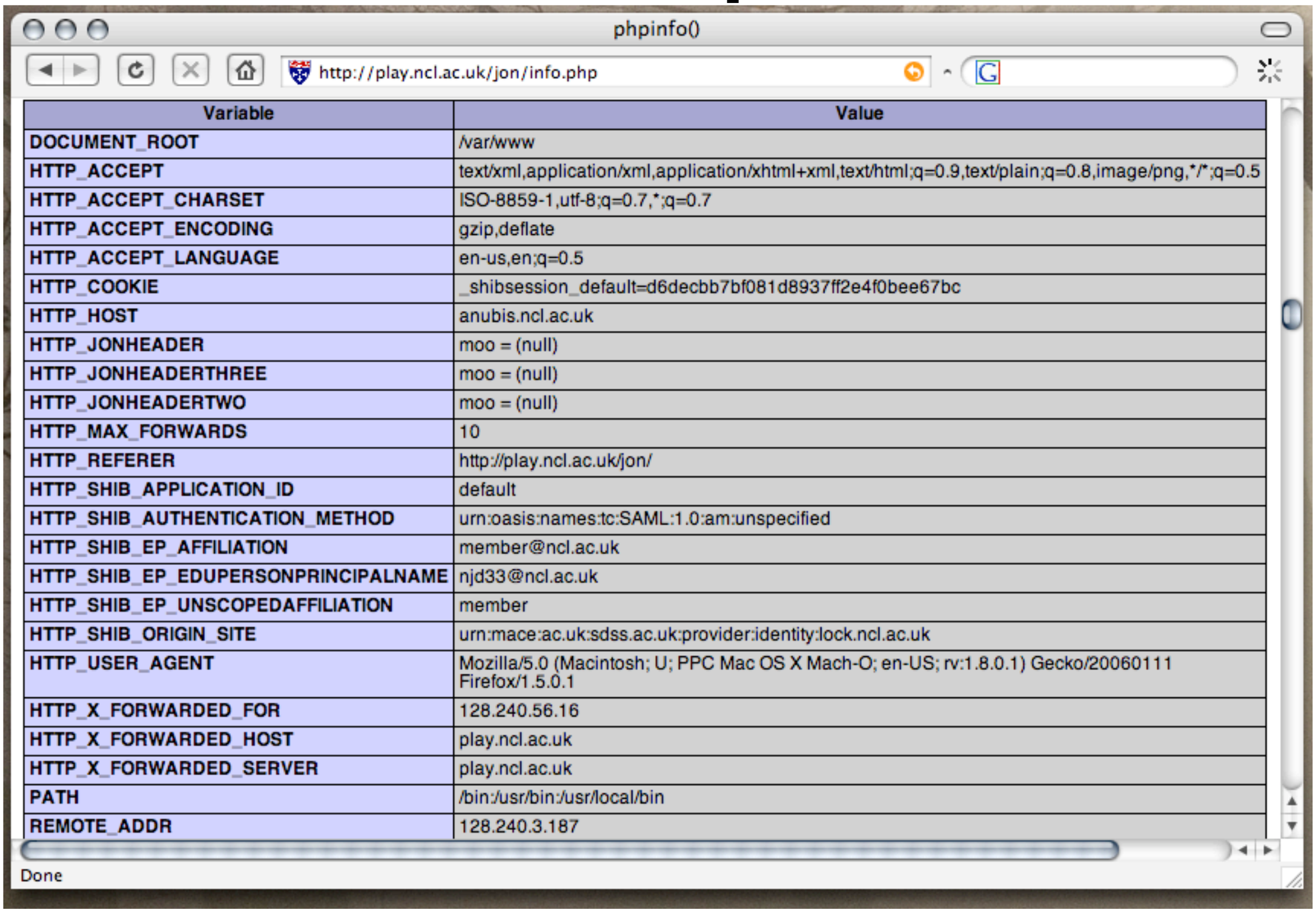
Other bits

- Service (/etc/init.d) script
- steal from the redhat packages
  - if your init.d works the same

First go

- Hello world
- local to apache server
- no internal Auth{N/Z} notion

example



Variable	Value
DOCUMENT_ROOT	/var/www
HTTP_ACCEPT	text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
HTTP_ACCEPT_CHARSET	ISO-8859-1,utf-8;q=0.7,*;q=0.7
HTTP_ACCEPT_ENCODING	gzip,deflate
HTTP_ACCEPT_LANGUAGE	en-us,en;q=0.5
HTTP_COOKIE	_shibsession_default=d6decbb7bf081d8937ff2e4f0bee67bc
HTTP_HOST	anubis.ncl.ac.uk
HTTP_JONHEADER	moo = (null)
HTTP_JONHEADERTHREE	moo = (null)
HTTP_JONHEADERTWO	moo = (null)
HTTP_MAX_FORWARDS	10
HTTP_REFERER	http://play.ncl.ac.uk/jon/
HTTP_SHIB_APPLICATION_ID	default
HTTP_SHIB_AUTHENTICATION_METHOD	urn:oasis:names:tc:SAML:1.0:am:unspecified
HTTP_SHIB_EP_AFFILIATION	member@ncl.ac.uk
HTTP_SHIB_EP_EDUPERSONPRINCIPALNAME	njd33@ncl.ac.uk
HTTP_SHIB_EP_UNSCOPEDAFFILIATION	member
HTTP_SHIB_ORIGIN_SITE	urn:mace:ac.uk:sdss.ac.uk:provider:identity:lock.ncl.ac.uk
HTTP_USER_AGENT	Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.1) Gecko/20060111 Firefox/1.5.0.1
HTTP_X_FORWARDED_FOR	128.240.56.16
HTTP_X_FORWARDED_HOST	play.ncl.ac.uk
HTTP_X_FORWARDED_SERVER	play.ncl.ac.uk
PATH	/bin:/usr/bin:/usr/local/bin
REMOTE_ADDR	128.240.3.187

First go

- set wayfURL to your local IDP
- self-signed certificates
- logout?

Authorization

access control

- by the server
- by the application
- by a framework

application-managed

server-managed

- apache httpd.conf / .htaccess files
- shibboleth 1.3b XML-based

apache-based

- Require entity-name [entity-name]

shibboleth-based

- relatively new, added in 1.3b
- performance questions

```
<AccessControl>
  <AND>
    <OR>
      <Rule require="affiliation">member@dur.ac.uk</Rule>
      <Rule require="affiliation">member@ncl.ac.uk</Rule>
    </OR>
    <Rule require="entitlement">
       urn:mace:example.edu:exampleEntitlement
    </Rule>
  </AND>
</AccessControl>
```

dealing with walk-ins

- "kiosk"-types, e.g. library terminals
- mod_auth_location
- http://staff.washington.edu/fox/authlocation/module.html

framework-managed

- Java AuthN & AuthZ Services (JAAS)
- Active Directory Federated Services (ADFS)

- covered later

Use Cases

A real service

- a local app with internal user auth{N/Z}
- hack in "trusting" an environment variable
  - e.g. $REMOTE_USER
- on-the-fly account creation
  - deletion?
- logout?

Example: sympa

- mailing list manager
- attributes via environment variables
  - app-configurable mapping
- authorization handled by apache
  - a canonical URL defined by sympa

Sympa's logout

- two-stage login:
  - authenticated by shibboleth
  - explicitly asked to be "logged in"
- (demo)

external services

- shibboleth/apache front-end
- “black-box” back-end

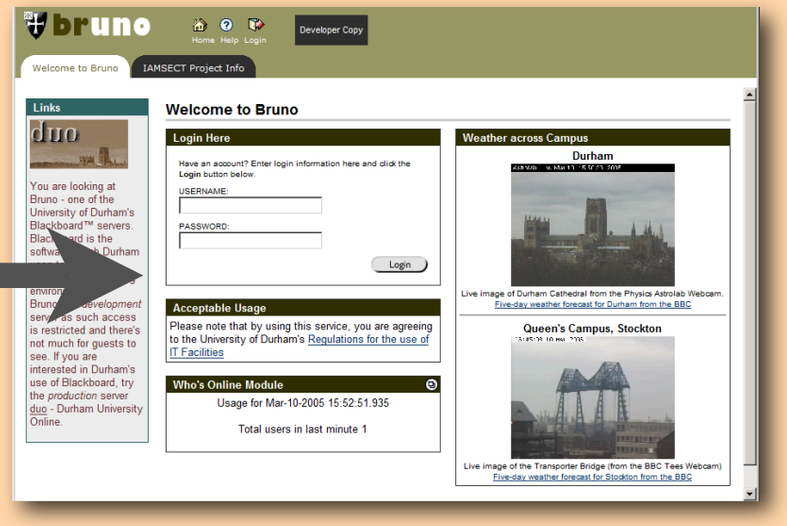
- e.g. proxying (via mod_proxy) or fastCGI

Service Provider

apache

mod_shib

shibd



Identity Provider

front-end

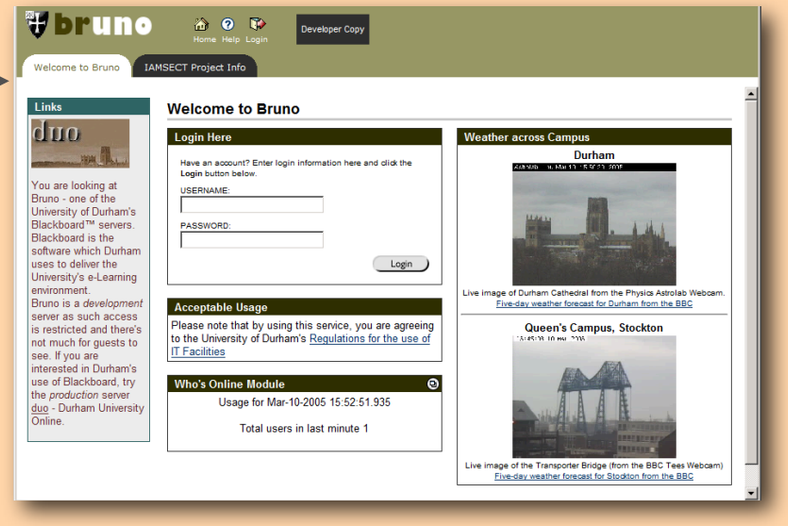
back-end

mod_proxy

apache

mod_shib

shibd



Identity Provider

mod_proxy front-end

```
ProxyPass        /jon http://front.ncl.ac.uk
ProxyPassReverse /jon http://front.ncl.ac.uk

<Location "/jon">
        AuthType shibboleth
        ShibRequireSession on
        Require valid-user
</Location>
```

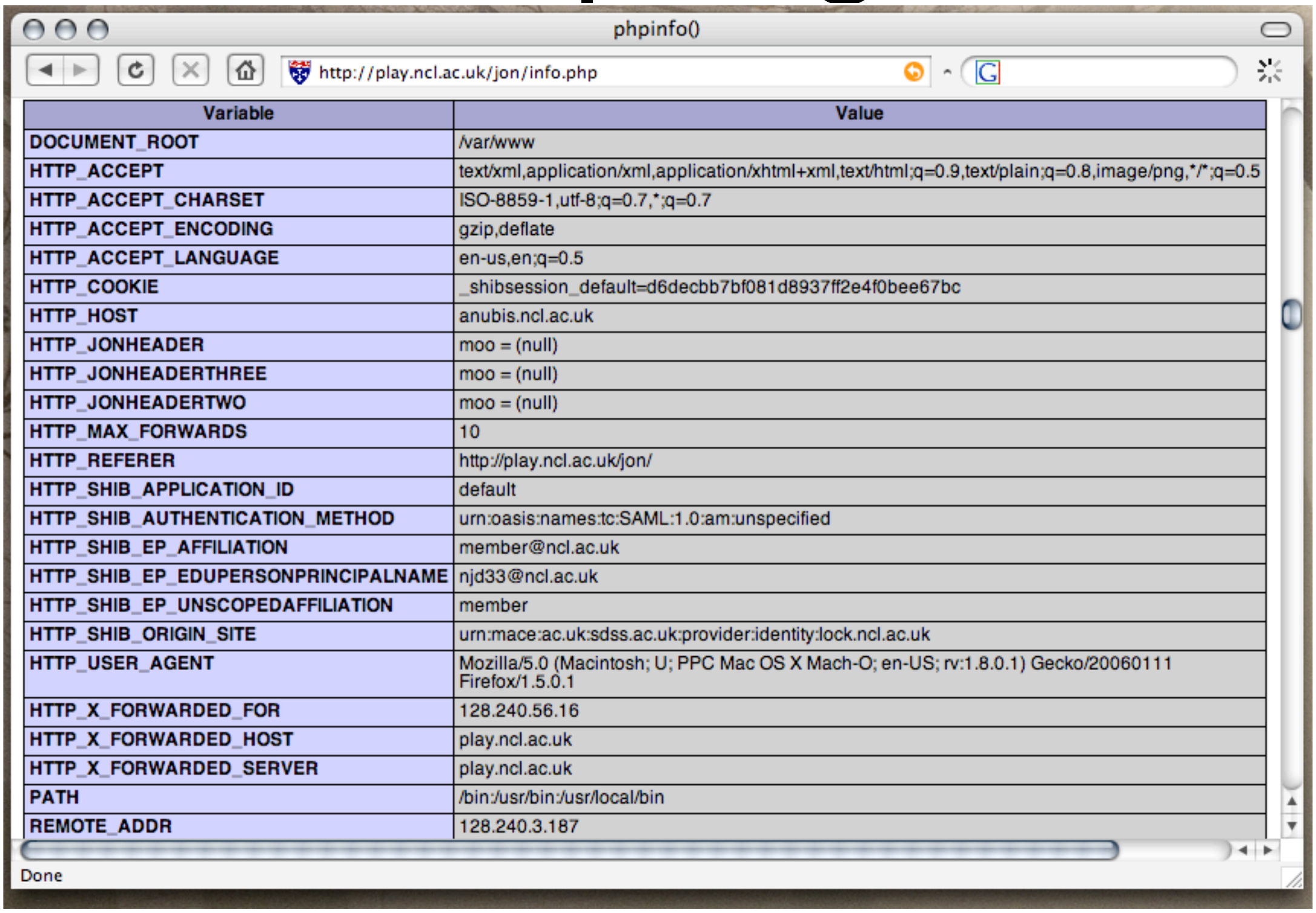
On the back-end

```
Order deny,allow
Deny from all
Allow from shib-front-end.ncl.ac.uk
```

Shortcomings

- IP spoofing on the back-end
- cookie scope
- certificate scope

example again



Variable	Value
DOCUMENT_ROOT	/var/www
HTTP_ACCEPT	text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
HTTP_ACCEPT_CHARSET	ISO-8859-1,utf-8;q=0.7,*;q=0.7
HTTP_ACCEPT_ENCODING	gzip,deflate
HTTP_ACCEPT_LANGUAGE	en-us,en;q=0.5
HTTP_COOKIE	_shibsession_default=d6decbb7bf081d8937ff2e4f0bee67bc
HTTP_HOST	anubis.ncl.ac.uk
HTTP_JONHEADER	moo = (null)
HTTP_JONHEADERTHREE	moo = (null)
HTTP_JONHEADERTWO	moo = (null)
HTTP_MAX_FORWARDS	10
HTTP_REFERER	http://play.ncl.ac.uk/jon/
HTTP_SHIB_APPLICATION_ID	default
HTTP_SHIB_AUTHENTICATION_METHOD	urn:oasis:names:tc:SAML:1.0:am:unspecified
HTTP_SHIB_EP_AFFILIATION	member@ncl.ac.uk
HTTP_SHIB_EP_EDUPERSONPRINCIPALNAME	njd33@ncl.ac.uk
HTTP_SHIB_EP_UNSCOPEDAFFILIATION	member
HTTP_SHIB_ORIGIN_SITE	urn:mace:ac.uk:sdss.ac.uk:provider:identity:lock.ncl.ac.uk
HTTP_USER_AGENT	Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.1) Gecko/20060111 Firefox/1.5.0.1
HTTP_X_FORWARDED_FOR	128.240.56.16
HTTP_X_FORWARDED_HOST	play.ncl.ac.uk
HTTP_X_FORWARDED_SERVER	play.ncl.ac.uk
PATH	/bin:/usr/bin:/usr/local/bin
REMOTE_ADDR	128.240.3.187