MEDIAWIKI AUTHENTICATION

MARK A. HERSHBERGER
AUTHENTICATION

- Not Authorization
TYPES OF AUTHENTICATION AVAILABLE FOR MEDIAWIKI
REMOTEUSER
BOT PASSWORDS
LDAP
SAML
OPENID CONNECT (BASED ON OAUTH2)
WHICH DO YOU WANT TO USE?
A user has already authenticated themselves to the webserver itself
The webserver gives you an HTTP header (REMOTE_USER, usually)
You trust it and just need to tell MediaWiki to trust it
REMOTEUSER (CONTINUED)

- NTLM
- Kerberos
- Whatever your webserver can do
You want to write a bot for the wiki
You want to restrict the rights of the bot to a subset of your rights.
This will take special configuration if you use RemoteUser for authentication
Built into MediaWiki!
LDAP/ACTIVEDIRECTORY

• You work with a central repository for user information.
• LDAP can provide information more information that may be useful to your MW install
  - Gender
  - User's Language
  - Groups
  - Email
  - Timezone
On AD, this is usually combined with RemoteUser and NTLM to have MW use a SSO process.

- Authentication is handled using RemoteUser
- Authorization (MW Groups + Lockdown) and User info (email, name) is handled with LDAP queries
SAML

- Tends to be harder to configure
- Error reporting can be confusing
- But is provided by many companies as their preferred ID provider
**OPENID CONNECT**

- Let someone else handle the authentication
- Trusted provider's `/.well-known/openid-provider` url provides configuration

<table>
<thead>
<tr>
<th>Provider</th>
<th>OpenID Connect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google</td>
<td>well-known</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>Example tenant's well-known</td>
</tr>
<tr>
<td>Yahoo</td>
<td>well-known</td>
</tr>
<tr>
<td>PayPal</td>
<td>well-known</td>
</tr>
<tr>
<td>ORCiD</td>
<td>well-known</td>
</tr>
</tbody>
</table>
If you have an ORCiD, visit ORCiDWiki

```php
wfLoadExtension( "PluggableAuth" );
wfLoadExtension( "OpenIDConnect" );

$wgOpenIDConnect_Config = [
   'https://orcid.org/' => [
      'clientID' => 'APP-C9V0AYX46PFDV14A',
      'clientsecret' => 'sssh!',
      'name' => 'orcid',
      'preferred_username' => 'sub'
   ]
];
```