Status and futur of PHP LDAP extension

By Côme Chilliet – LDAPCon 2017

Maintaining and extending PHP-LDAP

- Working on FusionDirectory since 2011
- Using PHP-LDAP
- Missing features

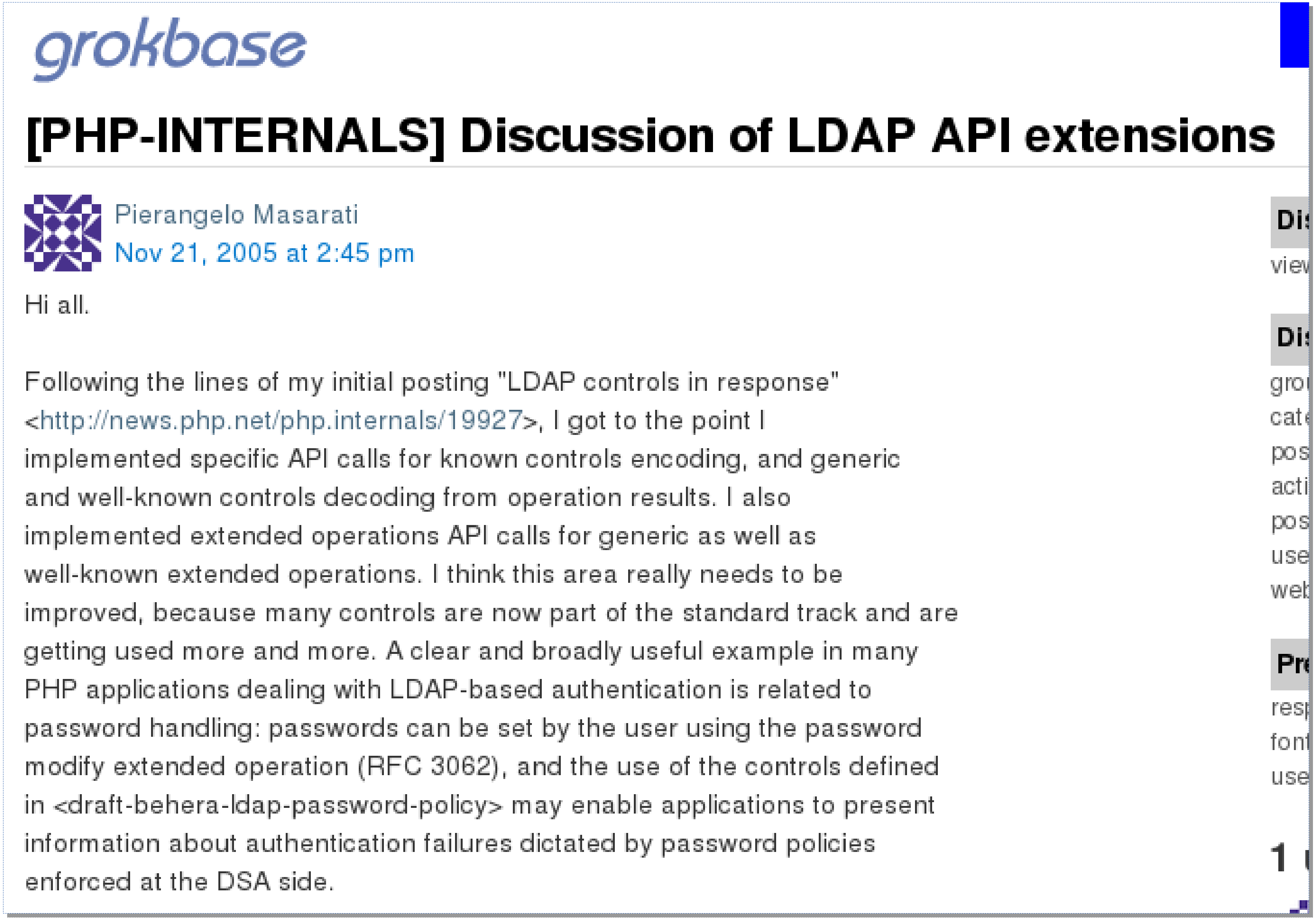
Maintaining and extending PHP-LDAP

- Using ppolicy through PHP-LDAP
- Extended Operations
- Controls

Maintaining and extending PHP-LDAP

- Bug tickets
- Patches
- Roadmap

Maintaining and extending PHP-LDAP



[PHP-INTERNALS] Discussion of LDAP API extensions

Pierangelo Masarati
Nov 21, 2005 at 2:45 pm

Hi all.

Following the lines of my initial posting "LDAP controls in response" <http://news.php.net/php.internals/19927>, I got to the point I implemented specific API calls for known controls encoding, and generic and well-known controls decoding from operation results. I also implemented extended operations API calls for generic as well as well-known extended operations. I think this area really needs to be improved, because many controls are now part of the standard track and are getting used more and more. A clear and broadly useful example in many PHP applications dealing with LDAP-based authentication is related to password handling: passwords can be set by the user using the password modify extended operation (RFC 3062), and the use of the controls defined in <draft-behera-ldap-password-policy> may enable applications to present information about authentication failures dictated by password policies enforced at the DSA side.

Maintaining and extending PHP-LDAP

- Patch from 2005 adding EXOP and controls
  - Ticket opened in 2006
  - Never merged
- Paged result controls patch from 2007
  - Merged in 2012 (PHP 5.4)
  - Limited
- Patch from 2012 to remove deprecated flag
- Ticket from 2012 asking for VLV support

Maintaining and extending PHP-LDAP

- Becoming maintainer
- Let’s accept patches!
- Where are they all gone?

Maintaining and extending PHP-LDAP

- Patches are outdated
- Implementing controls
- Chicken and egg situation

Maintaining and extending PHP-LDAP

- Starting slowly
- Removal of deprecated flag
  - ldap_sort deprecated in PHP7, removed in PHP8
- First break of PHP-LDAP
  - host:port syntax for ldap_connect

Extended Operations in PHP 7.2

resource **ldap_exop**(*resource* $link, *string* $reqoid
[, *string* $reqdata [, *array* $servercontrols [, *string* &$retdata
[, *string* &$retoid]]]])

bool **ldap_parse_exop**(*resource* $link, *resource* $result
[, *string* &$retdata [, *string* &$retoid]])

string **ldap_exop_whoami**(*resource* $link)

string **ldap_exop_passwd**(*resource* $link [, *string* $user
[, *string* $oldpw [, *string* $newpw]]])

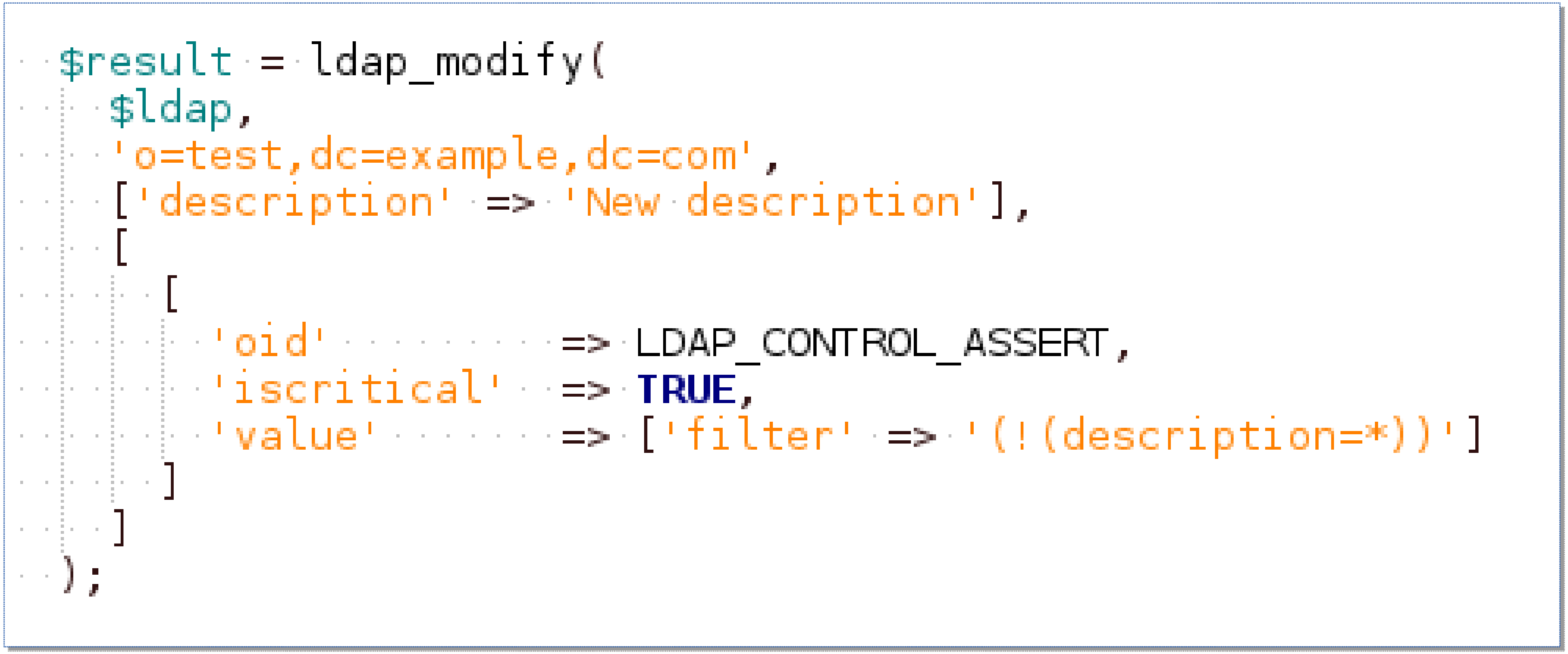
int **ldap_exop_refresh**(*resource* $link, *string* $dn, *int* $ttl)

Maintaining and extending PHP-LDAP

Controls in PHP 7.3

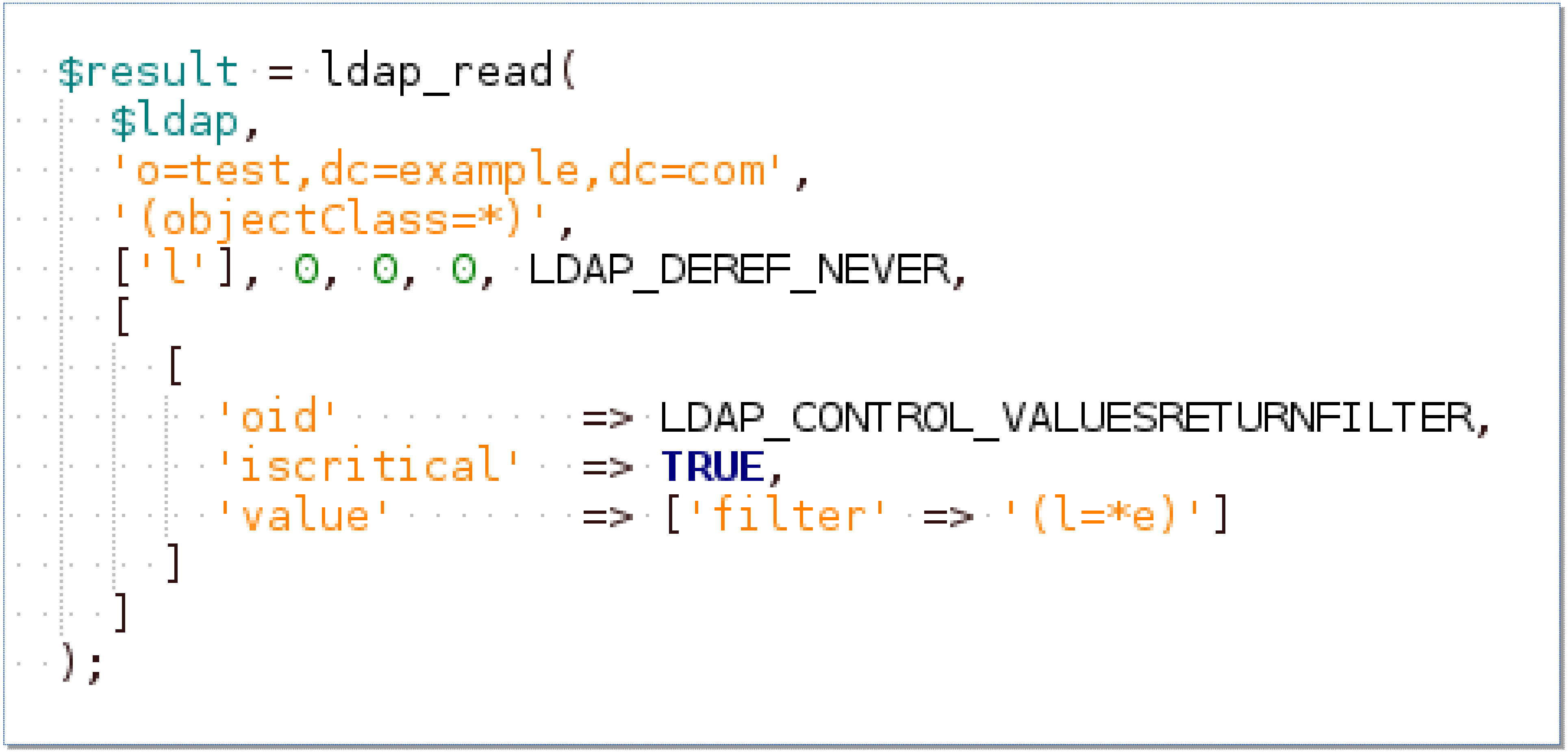
- Modified functions: ldap_add, ldap_mod_replace, ldap_mod_add, ldap_mod_del, ldap_modify, ldap_rename, ldap_compare, ldap_delete, ldap_modify_batch, ldap_parse_result, ldap_search, ldap_list, ldap_read
- Added functions: ldap_add_ext, ldap_bind_ext, ldap_delete_ext, ldap_mod_add_ext, ldap_mod_replace_ext, ldap_mod_del_ext, ldap_modify_ext, ldap_rename_ext

Maintaining and extending PHP-LDAP



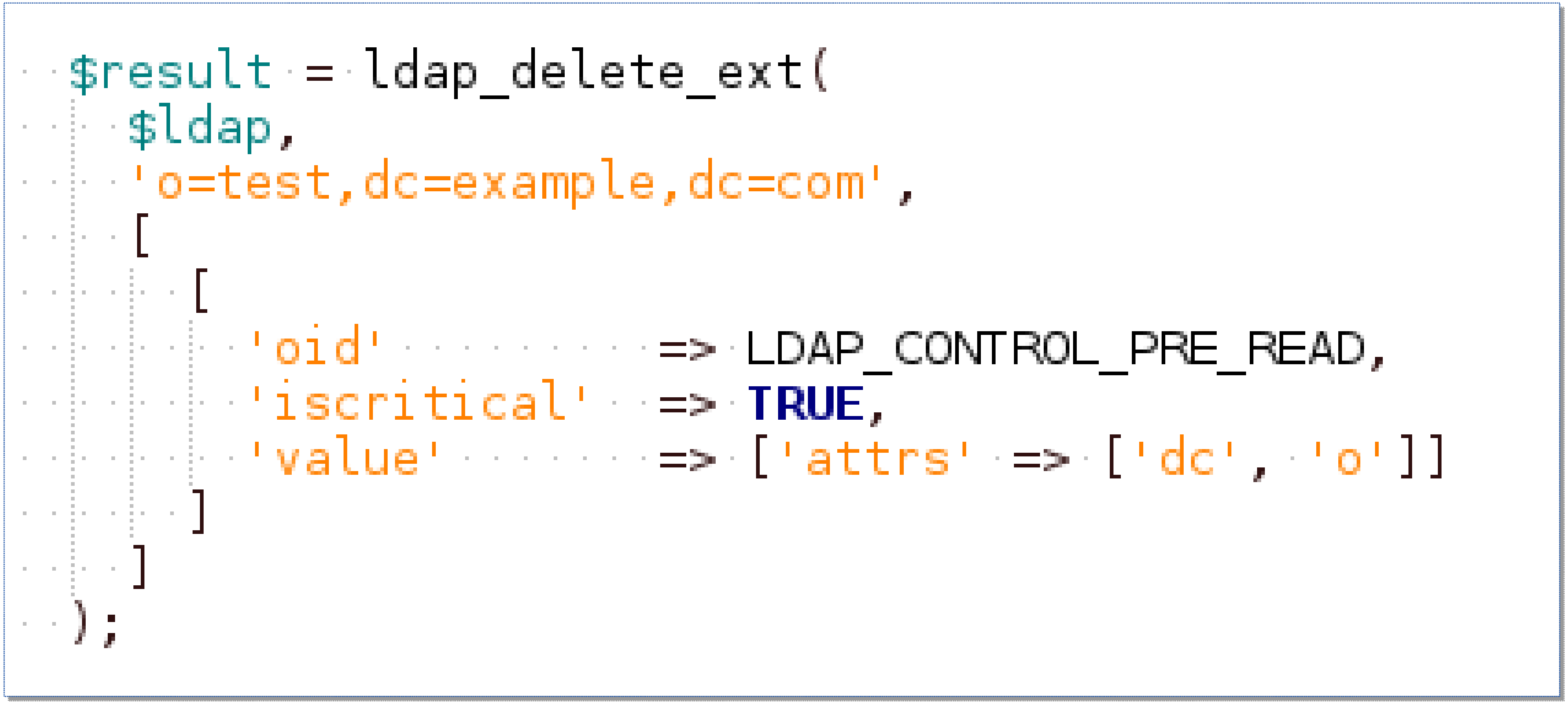
```
  $result = ldap_modify(
    $ldap,
    'o=test,dc=example,dc=com',
    ['description' => 'New description'],
    [
      [
        'oid'           => LDAP_CONTROL_ASSERT,
        'iscritical'    => TRUE,
        'value'         => ['filter' => '(!(description=*))']
      ]
    ]
  );
```

Maintaining and extending PHP-LDAP



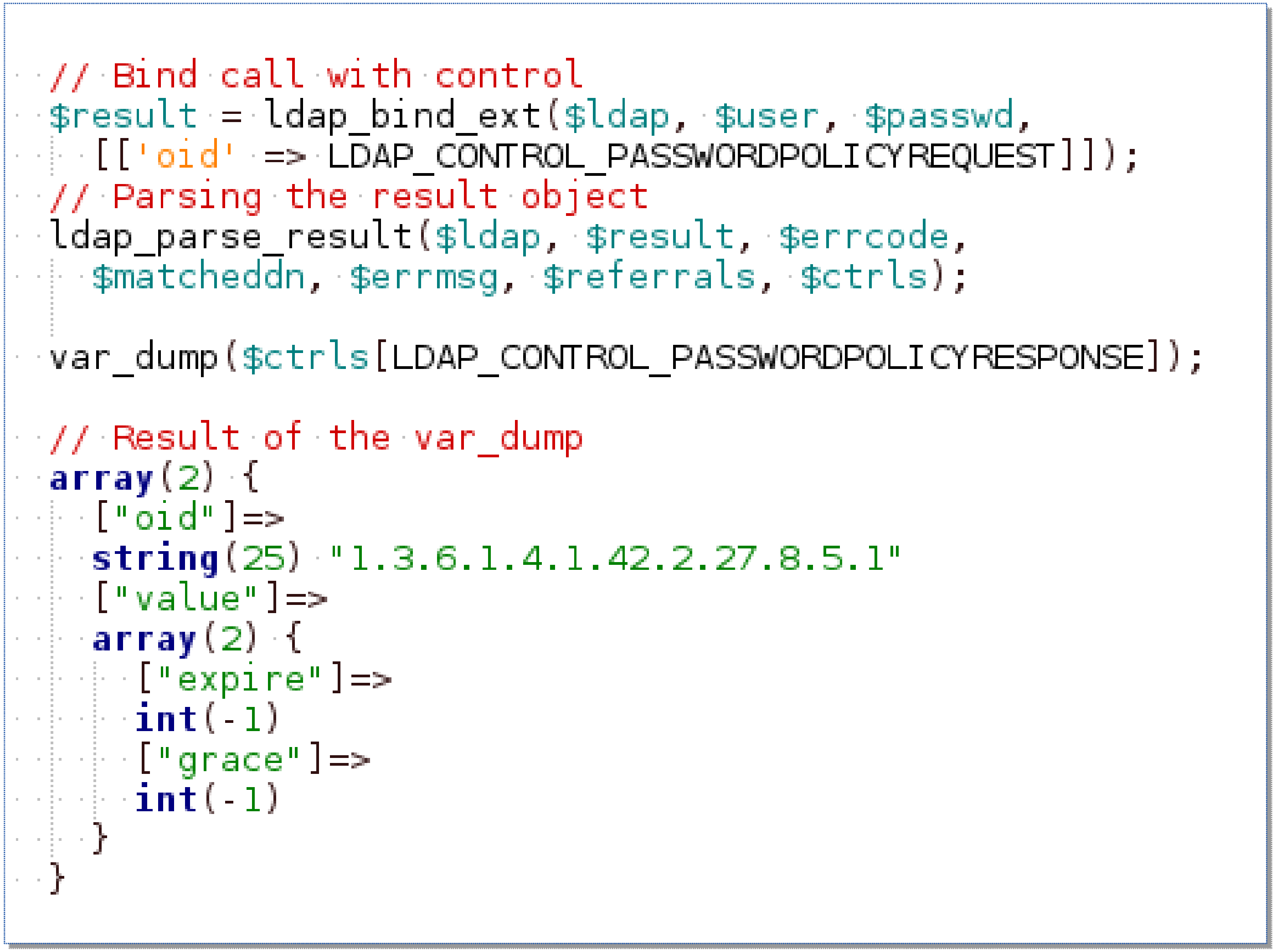
```
  $result = ldap_read(
    $ldap,
    'o=test,dc=example,dc=com',
    '(objectClass=*)',
    ['l'], 0, 0, 0, LDAP_DEREF_NEVER,
    [
      [
        'oid'        => LDAP_CONTROL_VALUESRETURNFILTER,
        'iscritical' => TRUE,
        'value'      => ['filter' => '(l=*e)']
      ]
    ]
  );
```

Maintaining and extending PHP-LDAP



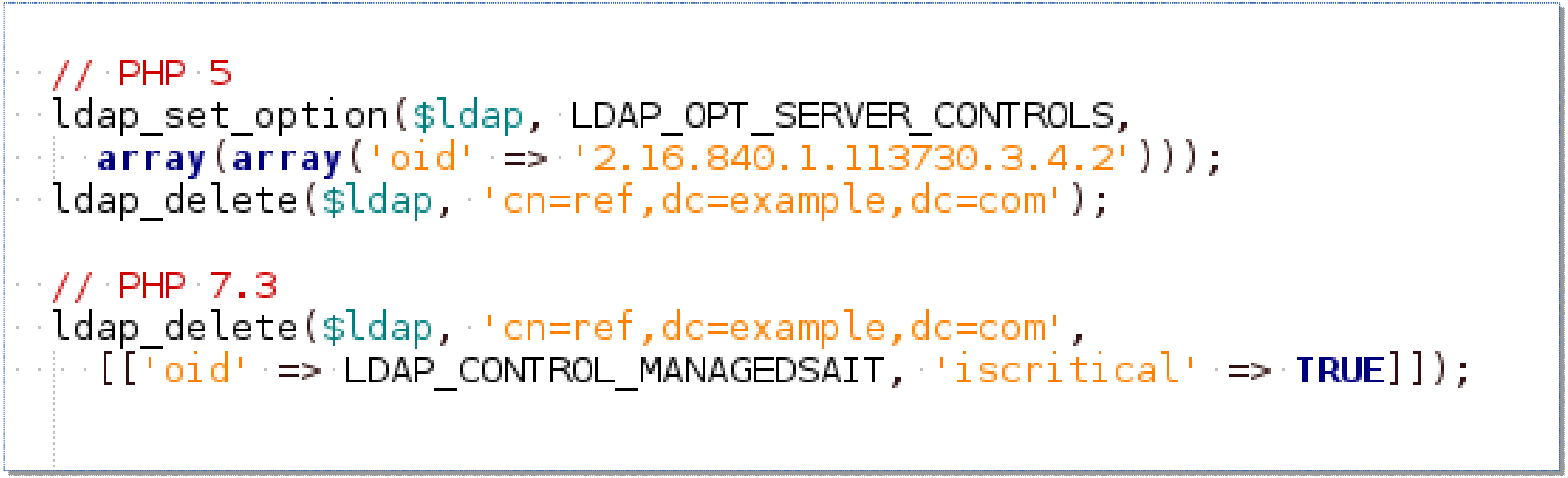
```
  $result = ldap_delete_ext(
    $ldap,
    'o=test,dc=example,dc=com',
    [
      [
        'oid'         => LDAP_CONTROL_PRE_READ,
        'iscritical'  => TRUE,
        'value'       => ['attrs' => ['dc', 'o']]
      ]
    ]
  );
```

Maintaining and extending PHP-LDAP



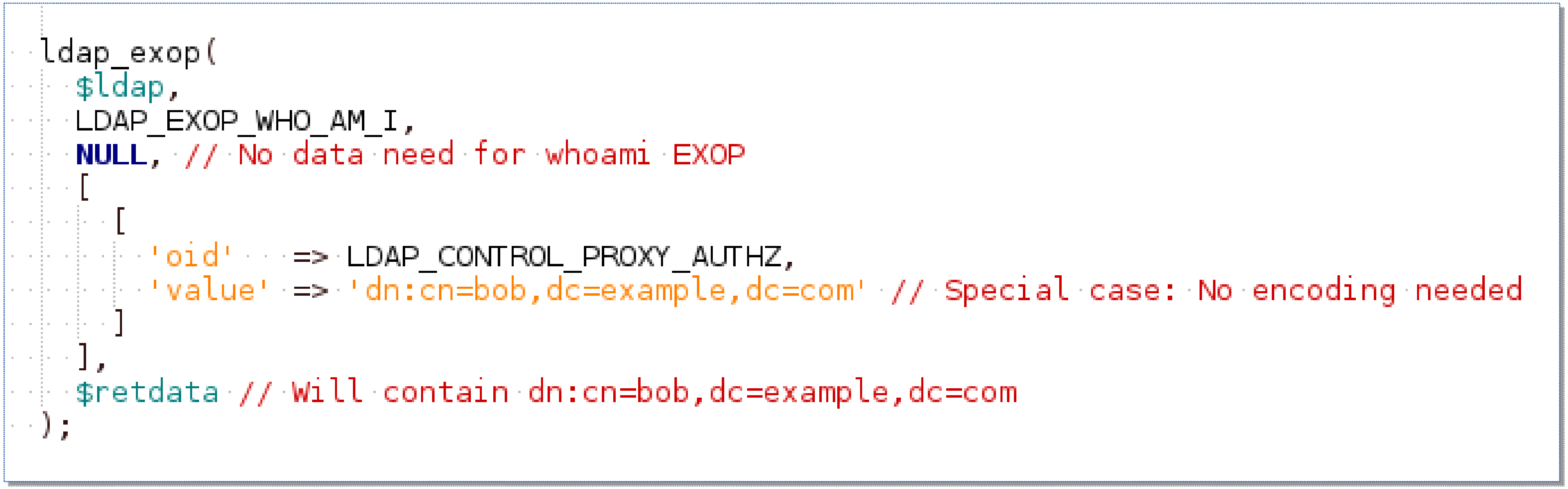
```
// Bind call with control
$result = ldap_bind_ext($ldap, $user, $passwd,
    [['oid' => LDAP_CONTROL_PASSWORDPOLICYREQUEST]]);
// Parsing the result object
ldap_parse_result($ldap, $result, $errcode,
    $matcheddn, $errmsg, $referrals, $ctrls);

var_dump($ctrls[LDAP_CONTROL_PASSWORDPOLICYRESPONSE]);

// Result of the var_dump
array(2) {
    ["oid"]=>
    string(25) "1.3.6.1.4.1.42.2.27.8.5.1"
    ["value"]=>
    array(2) {
        ["expire"]=>
        int(-1)
        ["grace"]=>
        int(-1)
    }
}
```

Maintaining and extending PHP-LDAP



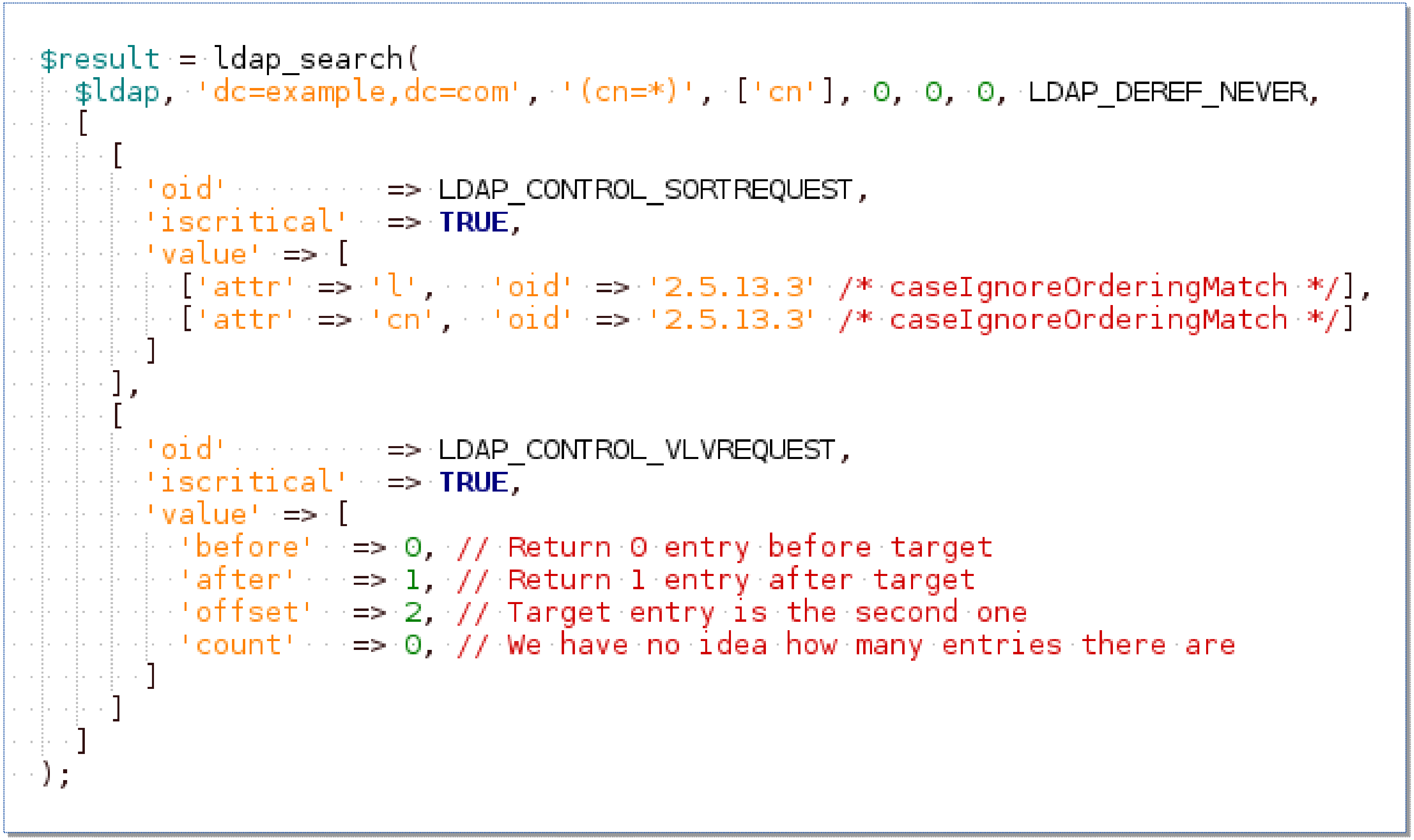
```
// PHP 5
ldap_set_option($ldap, LDAP_OPT_SERVER_CONTROLS,
  array(array('oid' => '2.16.840.1.113730.3.4.2')));
ldap_delete($ldap, 'cn=ref,dc=example,dc=com');

// PHP 7.3
ldap_delete($ldap, 'cn=ref,dc=example,dc=com',
  [['oid' => LDAP_CONTROL_MANAGEDSAIT, 'iscritical' => TRUE]]);
```

Maintaining and extending PHP-LDAP



```
ldap_exop(
    $ldap,
    LDAP_EXOP_WHO_AM_I,
    NULL, // No data need for whoami EXOP
    [
        [
            'oid'   => LDAP_CONTROL_PROXY_AUTHZ,
            'value' => 'dn:cn=bob,dc=example,dc=com' // Special case: No encoding needed
        ]
    ],
    $retdata // Will contain dn:cn=bob,dc=example,dc=com
);
```

Maintaining and extending PHP-LDAP



```php
$result = ldap_search(
    $ldap, 'dc=example,dc=com', '(cn=*)', ['cn'], 0, 0, 0, LDAP_DEREF_NEVER,
    [
        [
            'oid'          => LDAP_CONTROL_SORTREQUEST,
            'iscritical'   => TRUE,
            'value' => [
                ['attr' => 'l',   'oid' => '2.5.13.3' /* caseIgnoreOrderingMatch */],
                ['attr' => 'cn',  'oid' => '2.5.13.3' /* caseIgnoreOrderingMatch */]
            ]
        ],
        [
            'oid'          => LDAP_CONTROL_VLVREQUEST,
            'iscritical'   => TRUE,
            'value' => [
                'before'  => 0, // Return 0 entry before target
                'after'   => 1, // Return 1 entry after target
                'offset'  => 2, // Target entry is the second one
                'count'   => 0, // We have no idea how many entries there are
            ]
        ]
    ]
);
```

Maintaining and extending PHP-LDAP

Futur development for PHP-LDAP:

- Encoding help for more controls
- Encoding help for EXOPs?
- Documentation
- Your suggestion goes here

Maintaining and extending PHP-LDAP

Thank you for your attention

Links:
https://bugs.php.net
https://www.fusiondirectory.org

Contact:
come@opensides.be
mcmic@php.net
irc.freenode.net: #php, #php-ldap, #fusiondirectory