



8.08.2022 12:33:59 (UTC+03:00)

## Detailed Scan Report

<https://yazilimmuhendisim.com/>

Scan Time : 8.08.2022 02:46:02 (UTC+03:00)  
Scan Duration : 00:09:39:37  
Total Requests : 124.675  
Average Speed : 3,6r/s

Risk Level:  
**CRITICAL**

**44**  
IDENTIFIED

**11**  
CONFIRMED

**2**  
CRITICAL

**2**  
HIGH

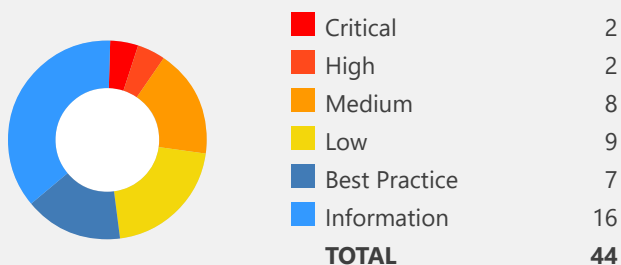
**8**  
MEDIUM

**9**  
LOW

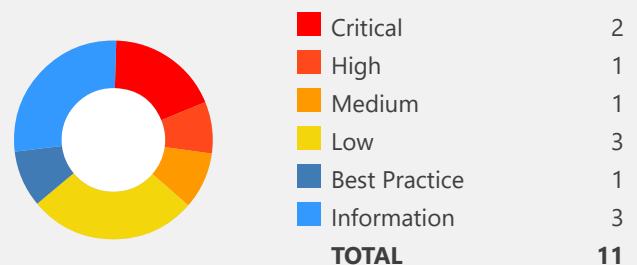
**7**  
BEST PRACTICE

**16**  
INFORMATION
































### Identified Vulnerabilities





























































### Confirmed Vulnerabilities





# Vulnerability Summary

| CONFIRM   | VULNERABILITY  | METHOD | URL  | PARAMETER   |
|---|--|--------|--|---|
|       | <a href="#">Boolean Based SQL Injection</a>                              | GET    | https://yazilimmuhendisim.com/portfolio-details.php?p=12%20OR%2017-7%3d10                                    |  |
|       | <a href="#">Out-of-date Version (MySQL)</a>                              | GET    | https://yazilimmuhendisim.com/portfolio-details.php?p=12%20OR%2017-7%3d10                                    |  |
|       | <a href="#">Out-of-date Version (jQuery Validation)</a>                  | GET    | https://yazilimmuhendisim.com/phpmyadmin/js/vendor/jquery/jquery.validate.js                                 |   |
|       | <a href="#">Database User Has Admin Privileges</a>                       | GET    | https://yazilimmuhendisim.com/portfolio-details.php?p=12%20OR%2017-7%3d10                                    |  |
|       | <a href="#">[Possible] BREACH Attack Detected</a>                        | GET    | https://yazilimmuhendisim.com/phpmyadmin/index.php?db=&lang=sq&table=&token=3950577b52347032265556636f583530 |   |
|       | <a href="#">[Possible] Source Code Disclosure (PHP)</a>                  | GET    | https://yazilimmuhendisim.com/assets/img/portfolio/mtnanny/1.webp  |   |
|   | <a href="#">HTTP Strict Transport Security (HSTS) Policy Not Enabled</a> | GET    | https://yazilimmuhendisim.com/   |   |
|   | <a href="#">Out-of-date Version (jQuery UI Autocomplete)</a>             | GET    | https://yazilimmuhendisim.com/phpmyadmin/  |   |
|   | <a href="#">Out-of-date Version (jQuery UI Dialog)</a>                   | GET    | https://yazilimmuhendisim.com/phpmyadmin/  |   |
|   | <a href="#">Out-of-date Version (jQuery UI Tooltip)</a>                  | GET    | https://yazilimmuhendisim.com/phpmyadmin/  |   |
|   | <a href="#">Out-of-date Version (jQuery)</a>                             | GET    | https://yazilimmuhendisim.com/phpmyadmin/  |   |
|   | <a href="#">Weak Ciphers Enabled</a>                                     | GET    | https://yazilimmuhendisim.com/   |   |
|   | <a href="#">[Possible] Backup File Disclosure</a>                        | GET    | https://yazilimmuhendisim.com/index.php/etc/index.php~   |   |
|   | <a href="#">[Possible] Cross-site Request Forgery</a>                    | GET    | https://yazilimmuhendisim.com/   |   |

| CONFIRM   | VULNERABILITY   | METHOD | URL  | PARAMETER              |
|---|---|--------|--|------------------------|
|       | <a href="#">[Possible] Internal IP Address Disclosure</a>                     | GET    | https://yazilimmuhendisim.com/phpmyadmin/doc/html/setup.html   |                        |
|       | <a href="#">[Possible] Phishing by Navigating Browser Tabs</a>                | GET    | https://yazilimmuhendisim.com/   |                        |
|       | <a href="#">Missing Content-Type Header</a>                                   | GET    | https://yazilimmuhendisim.com/assets/img/portfolio/mettrainigclubv2/1.webp   |                        |
|       | <a href="#">Missing X-Frame-Options Header</a>                                | GET    | https://yazilimmuhendisim.com/   |                        |
|       | <a href="#">Insecure Frame (External)</a>                                     | GET    | https://yazilimmuhendisim.com/   |                        |
|       | <a href="#">Insecure Transportation Security Protocol Supported (TLS 1.0)</a> | GET    | https://yazilimmuhendisim.com/   |                        |
|       | <a href="#">Internal Server Error</a>   | GET    | https://yazilimmuhendisim.com/forms/mail/lib/SendGrid.php  |                        |
|     | <a href="#">Content Security Policy (CSP) Not Implemented</a>                 | GET    | https://yazilimmuhendisim.com/   |                        |
|   | <a href="#">Expect-CT Not Enabled</a>   | GET    | https://yazilimmuhendisim.com/cdn-cgi/l/email-protection#ea938b908386838789f828f848e83998387aa8d878b8386c4898587                 |                        |
|   | <a href="#">Missing X-XSS-Protection Header</a>                               | GET    | https://yazilimmuhendisim.com/   |                        |
|   | <a href="#">Referrer-Policy Not Implemented</a>                               | GET    | https://yazilimmuhendisim.com/   |                        |
|   | <a href="#">SameSite Cookie Not Implemented</a>                               | GET    | https://yazilimmuhendisim.com/phpmyadmin/js/whitelist.php?v=5.0.3  |                        |
|   | <a href="#">Subresource Integrity (SRI) Not Implemented</a>                   | GET    | https://yazilimmuhendisim.com/   |                        |
|   | <a href="#">Insecure Transportation Security Protocol Supported (TLS 1.1)</a> | GET    | https://yazilimmuhendisim.com/   |                        |
|   | <a href="#">[Possible] Administration Page Detected</a>                       | GET    | https://yazilimmuhendisim.com/phpmyadmin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00DD5C)%3C/scRipt%3E | <a href="#">nsextt</a> |

| CONFIRM   | VULNERABILITY  | METHOD | URL   | PARAMETER              |
|---|--|--------|---|------------------------|
|       | <a href="#">[Possible] Internal Path Disclosure (*nix)</a>                                     | GET    | https://yazilimmuhendisim.com/phpmyadmin/doc/html/setup.html  |                        |
|       | <a href="#">[Possible] Internal Path Disclosure (Windows)</a>                                  | GET    | https://yazilimmuhendisim.com/assets/img/portfolio/multi/1.webp?nsextt=%0d%0ans%3anetsparker056650%3dvuln   | <a href="#">nsextt</a> |
|       | <a href="#">[Possible] Login Page Identified</a>   | GET    | https://yazilimmuhendisim.com/phpmyadmin/db_structure.php   |                        |
|       | <a href="#">An Unsafe Content Security Policy (CSP) Directive in Use</a>                       | GET    | https://yazilimmuhendisim.com/phpmyadmin/   |                        |
|       | <a href="#">data: Used in a Content Security Policy (CSP) Directive</a>                        | GET    | https://yazilimmuhendisim.com/phpmyadmin/   |                        |
|       | <a href="#">default-src Used in Content Security Policy (CSP)</a>                              | GET    | https://yazilimmuhendisim.com/phpmyadmin/   |                        |
|     | <a href="#">Directory Listing (Apache)</a>   | GET    | https://yazilimmuhendisim.com/assets/vendor/bootstrap/  |                        |
|   | <a href="#">Email Address Disclosure</a>   | GET    | https://yazilimmuhendisim.com/phpmyadmin/js/vendor/jquery/jquery.debounce-1.0.5.js  |                        |
|   | <a href="#">Expect-CT in Report Only Mode</a>  | GET    | https://yazilimmuhendisim.com/  |                        |
|   | <a href="#">Multiple Content Security Policy (CSP) Implementation Detected</a>                 | GET    | https://yazilimmuhendisim.com/phpmyadmin/   |                        |
|   | <a href="#">Out-of-date Version (Bootstrap)</a>  | GET    | https://yazilimmuhendisim.com/assets/vendor/bootstrap/js/bootstrap.bundle.min.js  |                        |
|   | <a href="#">Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive</a> | GET    | https://yazilimmuhendisim.com/phpmyadmin/   |                        |
|   | <a href="#">Database Detected (MySQL)</a>  | GET    | https://yazilimmuhendisim.com/portfolio-details.php?p=12%27OR%201%3d1%20AND%20IFNULL(ASCII(SUBSTRING((SELECT%200x4E4554535041524B4552)%2c9%2c1))%2c0)%3d82--%20 | <a href="#">p</a>      |
|   | <a href="#">Forbidden Resource</a>   | GET    | https://yazilimmuhendisim.com/cdn-cgi/scripts/  |                        |

| CONFIRM  | VULNERABILITY                          | METHOD  | URL                                   | PARAMETER |
|--|--|---------|---------------------------------------|-----------|
|   | <a href="#">OPTIONS Method Enabled</a> | OPTIONS | https://yazilimmuhendisim.com/assets/ |           |

# 1. Boolean Based SQL Injection

CRITICAL



1

CONFIRMED



1

Netsparker identified a Boolean-Based SQL Injection, which occurs when data input by a user is interpreted as a SQL command rather than as normal data by the backend database.

This is an extremely common vulnerability and its successful exploitation can have critical implications.

Netsparker **confirmed** the vulnerability by executing a test SQL query on the backend database. In these tests, SQL injection was not obvious, but the different responses from the page based on the injection test allowed Netsparker to identify and confirm the SQL injection.

## Impact

Depending on the backend database, the database connection settings and the operating system, an attacker can mount one or more of the following type of attacks successfully:

- Reading, updating and deleting arbitrary data/tables from the database
- Executing commands on the underlying operating system

## Vulnerabilities

1.1. <https://yazilimmuhendisim.com/portfolio-details.php?p=12%20OR%2017-7%3d10>

**CONFIRMED**

| Method | Parameter | Value         |
|--------|-----------|---------------|
| GET    | p         | 12 OR 17-7=10 |

## Proof of Exploit

### Identified Database Version

8.0.21-0ubuntu0.20.04.4

### Identified Database User

alper@yazilimmuhendisim.com

## Identified Database Name

yazilimmuhendisim

### Request

GET /portfolio-details.php?p=12%200R%2017-7%3d10 HTTP/1.1  
Host: yazilimmuhendisim.com  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Referer: https://yazilimmuhendisim.com/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

## Response

Response Time (ms) : 121,613    Total Bytes Received : 5184    Body Length : 4436    Is Compressed : No

HTTP/1.1 200 OK  
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 7373f1117a6f5a25-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=Z0EodCw3bJKqNxWWADgP57Z7PS94xKQ0x4Qz3uxyGdQT1ju407JvcEtJwrfgwTXrRUKjoUeOIZCvzBWqBOZYQZnuRm1Ydw7KPj8ZKwvZueXmvp14JE93uCzz6Ii1EyrR9GwUoswHA%3D"}], "group": "cf-nel", "max\_age": 604800}  
NEL: {"success\_fraction": 0, "report\_to": "cf-nel", "max\_age": 604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Sun, 07 Aug 2022 23:55:10 GMT  
Vary: Accept-Encoding

```
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<title>Me Training Club v2 Mobil Uygulaması</title>
<meta content="" name="description">
<meta content="" name="keywords">

<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">

<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">

<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vendor/bootstrap-icons/bootstrap-icons.css" rel="stylesheet">
<link href="assets/vendor/boxicons/css/boxicons.min.css" rel="stylesheet">
<link href="assets/vendor/glightbox/css/glightbox.min.css" rel="stylesheet">
<link href="assets/vendor/remixicon/remixicon.css" rel="stylesheet">
<link href="assets/vendor/swiper/swiper-bundle.min.css" rel="stylesheet">
<link href="assets/css/style.css" rel="stylesheet">
</head>
<body>

<header id="header" class="fixed-top header-inner-pages">
<div class="container d-flex align-items-center justify-content-between">
<h1 clas
```



...

## Actions to Take

1. See the remedy for solution.
2. If you are not using a database access layer (DAL), consider using one. This will help you centralize the issue. You can also use ORM (*object relational mapping*). Most of the ORM systems use only parameterized queries and this can solve the whole SQL injection problem.
3. Locate all of the dynamically generated SQL queries and convert them to parameterized queries. (*If you decide to use a DAL/ORM, change all legacy code to use these new libraries.*)
4. Use your weblogs and application logs to see if there were any previous but undetected attacks to this resource.

## Remedy

The best way to protect your code against SQL injections is using parameterized queries (*prepared statements*). Almost all modern languages provide built-in libraries for this. Wherever possible, do not create dynamic SQL queries or SQL queries with string concatenation.

## Required Skills for Successful Exploitation

There are numerous freely available tools to exploit SQL injection vulnerabilities. This is a complex area with many dependencies; however, it should be noted that the numerous resources available in this area have raised both attacker awareness of the issues and their ability to discover and leverage them.

## External References

- [OWASP SQL injection](#)
- [SQL Injection Cheat Sheet](#)
- [SQL Injection Vulnerability](#)

## Remedy References

- [SQL injection Prevention Cheat Sheet](#)
- [A guide to preventing SQL injection](#)



## CLASSIFICATION

|              |  |
|--------------|--|
| PCI DSS v3.2 | <a href="#">6.5.1</a>                  |
| OWASP 2013   | <a href="#">A1</a>                     |
| OWASP 2017   | <a href="#">A1</a>                     |
| SANS Top 25  | <a href="#">89</a>                     |
| CAPEC        | <a href="#">66</a>                     |
| WASC         | <a href="#">19</a>                     |
| HIPAA        | <a href="#">164.306(A), 164.308(A)</a> |
| ISO27001     | <a href="#">A.14.2.5</a>               |

## CVSS 3.0 SCORE

|               |               |
|---------------|---------------|
| Base          | 10 (Critical) |
| Temporal      | 10 (Critical) |
| Environmental | 10 (Critical) |

## CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

## CVSS 3.1 SCORE

|               |               |
|---------------|---------------|
| Base          | 10 (Critical) |
| Temporal      | 10 (Critical) |
| Environmental | 10 (Critical) |

**CVSS Vector String**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

## 2. Out-of-date Version (MySQL)

CRITICAL



1

CONFIRMED



1

Netsparker identified you are using an out-of-date version of MySQL.

### Impact

Since this is an old version of the software, it may be vulnerable to attacks.

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35608](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35607](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35602](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21245](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21264](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 3.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21265](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21270](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.25

#### **External References**

- [CVE-2021-2339](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Memcached). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).

#### **Affected Versions**

8.0.0 to 8.0.25

#### **External References**

- [CVE-2021-2340](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.25

#### **External References**

- [CVE-2021-2352](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Federated). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.25

## External References

- [CVE-2021-2354](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H).

## Affected Versions

8.0.0 to 8.0.25

## External References

- [CVE-2021-2356](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.25

## External References

- [CVE-2021-2357](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21284](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35643](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35646](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35645](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35644](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:



(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35647](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35648](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35640](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35641](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human

interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 1.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35618](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35630](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.25

### External References

- [CVE-2021-35629](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35628](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35633](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Data Dictionary). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35632](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35636](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35635](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.26

#### **External References**

- [CVE-2021-35634](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.26

#### **External References**

- [CVE-2021-35638](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.26

#### **External References**

- [CVE-2021-35637](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.26

#### **External References**

- [CVE-2021-35622](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.33 and prior, 7.5.23 and prior, 7.6.19 and prior and 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

#### **Affected Versions**

8.0.0 to 8.0.26

#### **External References**

- [CVE-2021-35621](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.26

#### **External References**

- [CVE-2021-35642](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: GIS). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.26

#### **External References**

- [CVE-2021-35631](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.26

## External References

- [CVE-2021-35591](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Error Handling). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35596](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35612](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35610](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35597](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-2481](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-2479](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-2478](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL

Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35625](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 5.7.35 and prior and 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35624](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35626](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.25 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35537](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected



are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35623](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35546](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Connectors accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. CVSS 3.1 Base Score 5.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-2471](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 1.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2021-35618](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.26

#### **External References**

- [CVE-2021-35627](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21285](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.28

#### **External References**

- [CVE-2022-21454](#)

### **MySQL Uncontrolled Resource Consumption Vulnerability**

In nghttp2 before version 1.41.0, the overly large HTTP/2 SETTINGS frame payload causes denial of service. The proof of concept attack involves a malicious client constructing a SETTINGS frame with a length of 14,400 bytes (2400 individual settings entries) over and over again. The attack causes the CPU to spike at 100%. nghttp2 v1.41.0 fixes this vulnerability. There is a workaround to this vulnerability. Implement nghttp2\_on\_frame\_rcv\_callback callback, and if received frame is SETTINGS frame and the number of settings entries are large (e.g., > 32), then drop the connection.

#### **Affected Versions**

8.0.0 to 8.0.21

## External References

- [CVE-2020-11080](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.28

## External References

- [CVE-2022-21444](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

## Affected Versions

8.0.0 to 8.0.28

## External References

- [CVE-2022-21478](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

## Affected Versions

8.0.0 to 8.0.28

## External References

- [CVE-2022-21425](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).

## Affected Versions

8.0.0 to 8.0.28

## External References

- [CVE-2022-21460](#)

### MySQL Use After Free Vulnerability

png\_image\_free in png.c in libpng 1.6.x before 1.6.37 has a use-after-free because png\_image\_free\_function is called under png\_safe\_execute.

## Affected Versions

1.5.1 to 8.0.22

## External References

- [CVE-2019-7317](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.28

## External References

- [CVE-2022-21417](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.28

## External References

- [CVE-2022-21412](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via MySQL Protocol to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35577](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2021-35575](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.28

## External References

- [CVE-2022-21489](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.28

## External References

- [CVE-2022-21427](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.28

## External References

- [CVE-2022-21451](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.28 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server and unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.28

## External References

- [CVE-2022-21479](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.28

## External References

- [CVE-2022-21482](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.28

## External References

- [CVE-2022-21483](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker

with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

### Affected Versions

8.0.0 to 8.0.28

### External References

- [CVE-2022-21484](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

### Affected Versions

8.0.0 to 8.0.28

### External References

- [CVE-2022-21485](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

### Affected Versions

8.0.0 to 8.0.28

### External References

- [CVE-2022-21486](#)

#### MySQL Use After Free Vulnerability

png\_image\_free in png.c in libpng 1.6.x before 1.6.37 has a use-after-free because png\_image\_free\_function is called under png\_safe\_execute.

### Affected Versions

1.5.1 to 8.0.23

### External References

- [CVE-2019-7317](#)

#### **MySQL NULL Pointer Dereference Vulnerability**

Nullptr dereference when a null char is present in a proto symbol. The symbol is parsed incorrectly, leading to an unchecked call into the proto file's name during generation of the resulting error message. Since the symbol is incorrectly parsed, the file is nullptr. We recommend upgrading to version 3.15.0 or greater.

#### **Affected Versions**

8.0 to 8.0.28

#### **External References**

- [CVE-2021-22570](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21324](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21320](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).



## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21319](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21318](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21317](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21316](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker

with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21315](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21325](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21308](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

### Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21326](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21330](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21329](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21310](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS

Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21309](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21328](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21327](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21314](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21313](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21312](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21311](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21303](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21307](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21322](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21323](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are

7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21321](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21378](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 4.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21368](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21374](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21372](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Compiling). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21367](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21256](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).



## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21253](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21249](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21286](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21287](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently

repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21370](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21289](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21290](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.26

### External References

- [CVE-2022-21297](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21301](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21302](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21304](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21254](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21288](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/J). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21363](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21362](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21358](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21334](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21333](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

#### **Affected Versions**

8.0.0 to 8.0.27

#### **External References**

- [CVE-2022-21335](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21332](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.26 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2022-21278](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21279](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L)

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21331](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21336](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21357](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21356](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 2.9 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21355](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.36 and prior and 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21344](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.27

## External References

- [CVE-2022-21342](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.26 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H).

## Affected Versions

8.0.0 to 8.0.26

## External References

- [CVE-2022-21352](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server



accessible data. CVSS 3.1 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21351](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21348](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.27 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21339](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.4.34 and prior, 7.5.24 and prior, 7.6.20 and prior and 8.0.27 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Cluster executes to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Cluster. CVSS 3.1 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).

### Affected Versions

8.0.0 to 8.0.27

### External References

- [CVE-2022-21337](#)



#### MySQL Use After Free Vulnerability

In SQLite through 3.31.1, the ALTER TABLE implementation has a use-after-free, as demonstrated by an ORDER BY clause that belongs to a compound SELECT statement.

## Affected Versions

8.0.0 to 8.0.22

## External References

- [CVE-2020-11656](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

## Affected Versions

8.0.0 to 8.0.23

## External References

- [CVE-2021-2304](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.23

## External References

- [CVE-2021-2305](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).

## Affected Versions

8.0 to 8.0.23

## External References

- [CVE-2021-2307](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

### Affected Versions

8.0.0 to 8.0.23

### External References

- [CVE-2021-2308](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

### Affected Versions

8.0.0 to 8.0.23

### External References

- [CVE-2021-2301](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.23

### External References

- [CVE-2021-2300](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.23

### External References

- [CVE-2021-2299](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.23

#### **External References**

- [CVE-2021-2298](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0 to 8.0.22

#### **External References**

- [CVE-2021-2178](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0 to 8.0.23

#### **External References**

- [CVE-2021-2179](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0 to 8.0.23

#### **External References**

- [CVE-2021-2180](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.23

#### **External References**

- [CVE-2021-2193](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0 to 8.0.23

#### **External References**

- [CVE-2021-2194](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.23

#### **External References**

- [CVE-2021-2196](#)

#### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.23

## External References

- [CVE-2021-2201](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0 to 8.0.22

## External References

- [CVE-2021-2202](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Partition). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.23

## External References

- [CVE-2021-2208](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.23

## External References

- [CVE-2021-2212](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.22

## External References

- [CVE-2021-2213](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.23

## External References

- [CVE-2021-2215](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.23

## External References

- [CVE-2021-2217](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).

## Affected Versions

8.0 to 8.0.23

## External References

- [CVE-2021-2226](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.23

## External References

- [CVE-2021-2230](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 1.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).

## Affected Versions

8.0.0 to 8.0.23

## External References

- [CVE-2021-2232](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.23

## External References

- [CVE-2021-2278](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.23

## External References

- [CVE-2021-2293](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:



(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.23

## External References

- [CVE-2021-2203](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector:

(CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0 to 8.0.23

## External References

- [CVE-2021-2174](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector:

(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.23

## External References

- [CVE-2021-2172](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:

(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0 to 8.0.23

## External References

- [CVE-2021-2146](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple

protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

### Affected Versions

8.0 to 8.0.23

### External References

- [CVE-2021-2162](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.23

### External References

- [CVE-2021-2164](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0 to 8.0.23

### External References

- [CVE-2021-2166](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0 to 8.0.23

### External References

- [CVE-2021-2169](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.23 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.23

### External References

- [CVE-2021-2170](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0 to 8.0.23

### External References

- [CVE-2021-2171](#)

#### MySQL NULL Pointer Dereference Vulnerability

The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL\_NAME\_cmp which compares different instances of a GENERAL\_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL\_NAMES contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL\_NAME\_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS\_RESP\_verify\_response and TS\_RESP\_verify\_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s\_server, s\_client and verify tools have support for the "-crl\_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).

### Affected Versions

8.0 to 8.0.22

### External References

- [CVE-2020-1971](#)

#### MySQL Improper Initialization Vulnerability

SQLite through 3.31.1 allows attackers to cause a denial of service (segmentation fault) via a malformed window-function query

because the AggInfo object's initialization is mishandled.

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2020-11655](#)



#### MySQL Out-of-bounds Write Vulnerability

In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transitive properties for constant propagation.

### Affected Versions

8.0 to 8.0.22

### External References

- [CVE-2020-15358](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2122](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2088](#)



#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.22

## External References

- [CVE-2021-2087](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2021-2028](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2021-2030](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.22

## External References

- [CVE-2021-2031](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Information Schema). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector:

(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).

## Affected Versions

8.0.0 to 8.0.22

## External References

- [CVE-2021-2032](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.22

## External References

- [CVE-2021-2036](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.22

## External References

- [CVE-2021-2038](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2021-2042](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products.

Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2046](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2048](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.21

### External References

- [CVE-2021-2055](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2058](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are

5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2060](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2061](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2065](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2070](#)

#### MySQL Insufficient Information Vulnerability



Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2072](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2076](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2081](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.22

### External References

- [CVE-2021-2056](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.22

#### **External References**

- [CVE-2021-2024](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.22

#### **External References**

- [CVE-2021-2002](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Client accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Client. CVSS 3.1 Base Score 4.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:L).

#### **Affected Versions**

8.0.0 to 8.0.22

#### **External References**

- [CVE-2021-2010](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.22

## External References

- [CVE-2021-2011](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.22

## External References

- [CVE-2021-2021](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.22

## External References

- [CVE-2021-2022](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0 to 8.0.21

## External References

- [CVE-2020-14866](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14867](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0 to 8.0.21

## External References

- [CVE-2020-14868](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).

## Affected Versions

8.0 to 8.0.21

## External References

- [CVE-2020-14860](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0 to 8.0.21

## External References

- [CVE-2020-14861](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14869](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: X Plugin). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0 to 8.0.21

## External References

- [CVE-2020-14870](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0 to 8.0.21

## External References

- [CVE-2020-14873](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).

## Affected Versions

8.0 to 8.0.21

## External References

- [CVE-2020-14878](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector:

(CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14888](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0 to 8.0.21

## External References

- [CVE-2020-14891](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0 to 8.0.21

## External References

- [CVE-2020-14893](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0 to 8.0.21

## External References

- [CVE-2020-14829](#)



### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to

compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0 to 8.0.21

### External References

- [CVE-2020-14830](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).

### Affected Versions

8.0 to 8.0.21

### External References

- [CVE-2020-14828](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.21

### External References

- [CVE-2020-14812](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0 to 8.0.21

### External References

- [CVE-2020-14814](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and

prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.21

### External References

- [CVE-2020-14821](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).

### Affected Versions

8.0.0 to 8.0.21

### External References

- [CVE-2020-14827](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0 to 8.0.21

### External References

- [CVE-2020-14846](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.21

### External References

- [CVE-2020-14848](#)

#### MySQL Insufficient Information Vulnerability



Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0 to 8.0.21

### External References

- [CVE-2020-14852](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0 to 8.0.21

### External References

- [CVE-2020-14845](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.21

### External References

- [CVE-2020-14844](#)

#### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

### Affected Versions

8.0.0 to 8.0.21

### External References

- [CVE-2020-14836](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0 to 8.0.21

#### **External References**

- [CVE-2020-14837](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).

#### **Affected Versions**

8.0.0 to 8.0.21

#### **External References**

- [CVE-2020-14838](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0 to 8.0.21

#### **External References**

- [CVE-2020-14839](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.21

#### **External References**

- [CVE-2020-14776](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.21

#### **External References**

- [CVE-2020-14777](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.21

#### **External References**

- [CVE-2020-14785](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.21

#### **External References**

- [CVE-2020-14786](#)

### **MySQL Insufficient Information Vulnerability**

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

#### **Affected Versions**

8.0.0 to 8.0.21

## External References

- [CVE-2020-14789](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14790](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14791](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14793](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14794](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14800](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14804](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0 to 8.0.21

## External References

- [CVE-2020-14809](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14775](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14773](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14765](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

## Affected Versions

8.0.0 to 8.0.21

## External References

- [CVE-2020-14769](#)

### MySQL Insufficient Information Vulnerability

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).

Affected Versions

8.0.0 to 8.0.21

External References

- [CVE-2020-14771](#)

Vulnerabilities

2.1. <https://yazilimmuhendisim.com/portfolio-details.php?p=12%20OR%2017-7%3d10>  
**CONFIRMED**

| Method | Parameter | Value         |
|--------|-----------|---------------|
| GET    | p         | 12 OR 17-7=10 |

Identified Version

- 8.0.21

Latest Version

- 8.0.29 (in this branch)

Vulnerability Database

- Result is based on 08/05/2022 18:00:00 vulnerability database content.

**Request**

```
GET /portfolio-details.php?p=12%20OR%2017-7%3d10 HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://yazilimmuhendisim.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 121,613    Total Bytes Received : 5184    Body Length : 4436    Is Compressed : No

HTTP/1.1 200 OK  
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 7373f1117a6f5a25-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=Z0EodCw3bJYKqNxWWADgP57Z7PS94xKQ0x4Qz3uxyGdQT1ju407JvcEtJwrfgwTXrRUKjoUeOIZCvzBWqBOZYQZnuRm1Ydw7KPj8ZKwvZueXmvp14JE93uCzz6Ii1EyrR9GwUoswHA%3D"}],"group":"cf-nel","max\_age":604800}  
NEL: {"success\_fraction":0,"report\_to":"cf-nel","max\_age":604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Sun, 07 Aug 2022 23:55:10 GMT  
Vary: Accept-Encoding

```
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<title>Me Training Club v2 Mobil Uygulaması</title>
<meta content="" name="description">
<meta content="" name="keywords">

<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">

<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">

<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vendor/bootstrap-icons/bootstrap-icons.css" rel="stylesheet">
<link href="assets/vendor/boxicons/css/boxicons.min.css" rel="stylesheet">
<link href="assets/vendor/glightbox/css/glightbox.min.css" rel="stylesheet">
<link href="assets/vendor/remixicon/remixicon.css" rel="stylesheet">
<link href="assets/vendor/swiper/swiper-bundle.min.css" rel="stylesheet">
<link href="assets/css/style.css" rel="stylesheet">
</head>
<body>

<header id="header" class="fixed-top header-inner-pages">
<div class="container d-flex align-items-center justify-content-between">
<h1 clas
```



...

Remedy

Please upgrade your installation of MySQL to the latest stable version.

Remedy References

- [MySQL Downloads](#)

|   |                                  |
|---|----------------------------------|
|  <b>CLASSIFICATION</b> |                                  |
| PCI DSS v3.2  | <a href="#">6.2</a>              |
| OWASP 2013  | <a href="#">A9</a>               |
| OWASP 2017  | <a href="#">A9</a>               |
| SANS Top 25   | <a href="#">829</a>              |
| CAPEC   | <a href="#">310</a>              |
| HIPAA   | <a href="#">164.308(A)(1)(I)</a> |
| ISO27001  | <a href="#">A.14.1.2</a>         |

# 3. Database User Has Admin Privileges

HIGH

1

CONFIRMED

1

Netsparker detected the Database User Has Admin Privileges.

This issue has been **confirmed** by checking the connection privileges via an identified SQL injection vulnerability in the application.

## Impact

This can allow an attacker to gain extra privileges via SQL injection attacks. Here is the list of attacks that the attacker might carry out:

- Gain full access to the database server.
- Gain a reverse shell to the database server and execute commands on the underlying operating system.
- Access the database with full permissions, where it may be possible to read, update or delete arbitrary data from the database.
- Depending on the platform and the database system user, an attacker might carry out a privilege escalation attack to gain administrator access to the target system.

## Vulnerabilities

3.1. <https://yazilimmuhendisim.com/portfolio-details.php?p=12%20OR%2017-7%3d10>

CONFIRMED

| Method | Parameter | Value         |
|--------|-----------|---------------|
| GET    | p         | 12 OR 17-7=10 |

Request

GET /portfolio-details.php?p=12%20OR%2017-7%3d10 HTTP/1.1  
Host: yazilimmuhendisim.com  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Referer: https://yazilimmuhendisim.com/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

## Response

Response Time (ms) : 121,613    Total Bytes Received : 5184    Body Length : 4436    Is Compressed : No

HTTP/1.1 200 OK  
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 7373f1117a6f5a25-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=Z0EodCw3bJKqNxWWADgP57Z7PS94xKQ0x4Qz3uxyGdQT1ju407JvcEtJwrfgwTXrRUKjoUeOIZCvzBWqBOZYQZnuRm1Ydw7KPj8ZKwvZueXmvp14JE93uCzz6Ii1EyrR9GwUoswHA%3D"}], "group": "cf-nel", "max\_age": 604800}  
NEL: {"success\_fraction": 0, "report\_to": "cf-nel", "max\_age": 604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Sun, 07 Aug 2022 23:55:10 GMT  
Vary: Accept-Encoding

```
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<title>Me Training Club v2 Mobil Uygulaması</title>
<meta content="" name="description">
<meta content="" name="keywords">

<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">

<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">

<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vendor/bootstrap-icons/bootstrap-icons.css" rel="stylesheet">
<link href="assets/vendor/boxicons/css/boxicons.min.css" rel="stylesheet">
<link href="assets/vendor/glightbox/css/glightbox.min.css" rel="stylesheet">
<link href="assets/vendor/remixicon/remixicon.css" rel="stylesheet">
<link href="assets/vendor/swiper/swiper-bundle.min.css" rel="stylesheet">
<link href="assets/css/style.css" rel="stylesheet">
</head>
<body>

<header id="header" class="fixed-top header-inner-pages">
<div class="container d-flex align-items-center justify-content-between">
<h1 clas
```

...

### Remedy

Create a database user with the least possible permissions for your application and connect to the database with that user. Always follow the principle of providing the least privileges for all users and applications.

### External References

- [Authorization and Permissions in SQL Server \(ADO.NET\)](#)
- [Wikipedia - Principle of Least Privilege](#)
- [How to Use MySQL GRANT to Grant Privileges to Account](#)



## CLASSIFICATION

|              |                         |
|--------------|-------------------------|
| PCI DSS v3.2 | <a href="#">6.5.6</a>   |
| OWASP 2013   | <a href="#">A5</a>      |
| OWASP 2017   | <a href="#">A6</a>      |
| SANS Top 25  | <a href="#">267</a>     |
| WASC         | <a href="#">14</a>      |
| ISO27001     | <a href="#">A.9.2.2</a> |

## CVSS 3.0 SCORE

|               |              |
|---------------|--------------|
| Base          | 9 (Critical) |
| Temporal      | 9 (Critical) |
| Environmental | 9 (Critical) |

## CVSS Vector String

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

## CVSS 3.1 SCORE

|               |                |
|---------------|----------------|
| Base          | 9 (Critical)   |
| Temporal      | 9 (Critical)   |
| Environmental | 9,1 (Critical) |

**CVSS Vector String**

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

# 4. Out-of-date Version (jQuery Validation)

HIGH



1

Netsparker identified that the target web site is using jQuery Validation and detected that it is out of date.

## Impact

Since this is an old version of the software, it may be vulnerable to attacks.

### jQuery Validation Other Vulnerability

The jQuery Validation Plugin (jquery-validation) provides drop-in validation for forms. Versions of jquery-validation prior to 1.19.5 are vulnerable to regular expression denial of service (ReDoS) when an attacker is able to supply arbitrary input to the url2 method. This is due to an incomplete fix for CVE-2021-43306. Users should upgrade to version 1.19.5 to receive a patch.

## Affected Versions

1.6.0 to 1.19.3

## External References

- [CVE-2022-31147](#)

### jQuery Validation Other Vulnerability

An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the jquery-validation npm package, when an attacker is able to supply arbitrary input to the url2 method

## Affected Versions

1.6.0 to 1.19.3

## External References

- [CVE-2021-43306](#)

### jQuery Validation Uncontrolled Resource Consumption Vulnerability

The jQuery Validation Plugin provides drop-in validation for your existing forms. It is published as an npm package &quot;jquery-validation&quot;. jquery-validation before version 1.19.3 contains one or more regular expressions that are vulnerable to ReDoS (Regular Expression Denial of Service). This is fixed in 1.19.3.

## Affected Versions

1.6.0 to 1.19.2

## External References

- [CVE-2021-21252](#)

## Vulnerabilities

4.1. <https://yazilimmuhendisim.com/phpmyadmin/js/vendor/jquery/jquery.validate.js>

## Identified Version

- 1.19.1

#### Latest Version

- 1.19.5 (in this branch)

#### Vulnerability Database

- Result is based on 08/05/2022 18:00:00 vulnerability database content.

#### Certainty



#### Request

```
GET /phpmyadmin/js/vendor/jquery/jquery.validate.js HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=en; phpMyAdmin_https=1i97aaqc0qga5desacbt2brl1tc
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```



## Response

Response Time (ms) : 146,0412    Total Bytes Received : 51567    Body Length : 50690    Is Compressed : No

```
HTTP/1.1 200 OK
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Cache-Control: max-age=14400
ETag: "c602-5b14883c46080-gzip"
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=FcL4JKZqAmUaH3SatuCcVGTSa
a5yMEQKVJYV7aQImS7F8gZIkqFJHdd6JHwXS0tKR6x%2FQSAkNZha5%2Bwkbu1GAlqRgR7FgKblzqA%2Fh85M9btpC5QoSMxavykNus
mHP%2B6qQTITasfOI1k%3D"}], "group":"cf-nel", "max_age":604800}
CF-RAY: 7373f5848f010f86-MXP
Server: cloudflare
CF-Cache-Status: MISS
Accept-Ranges: bytes
Connection: keep-alive
Vary: Accept-Encoding
Content-Length: 13531
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sat, 10 Oct 2020 03:18:10 GMT
Content-Type: application/javascript
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Date: Sun, 07 Aug 2022 23:58:13 GMT
Con
...
at, 10 Oct 2020 03:18:10 GMT
Content-Type: application/javascript
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Date: Sun, 07 Aug 2022 23:58:13 GMT
Content-Encoding:

/*!
* jQuery Validation Plugin v1.19.1
*
* https://jqueryvalidation.org/
*
* Copyright (c) 2019 Jörn Zaefferer
* Released under the MIT license
*/
(function( factory ) {
if ( typeof define === "function" && define.amd ) {
...

```

## Remedy

Please upgrade your installation of jQuery Validation to the latest stable version.

Remedy References

- [Downloading jQuery Validation](#)



CLASSIFICATION

|                          |                                  |
|--------------------------|----------------------------------|
| PCI DSS v3.2             | <a href="#">6.2</a>              |
| OWASP 2013               | <a href="#">A9</a>               |
| OWASP 2017               | <a href="#">A9</a>               |
| SANS Top 25              | <a href="#">829</a>              |
| CAPEC                    | <a href="#">310</a>              |
| HIPAA                    | <a href="#">164.308(A)(1)(I)</a> |
| OWASP Proactive Controls | <a href="#">C1</a>               |
| ISO27001                 | <a href="#">A.14.1.2</a>         |

# 5. [Possible] BREACH Attack Detected

MEDIUM 

1

Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.

Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

## Impact

Even if you use an SSL/TLS protected connection, an attacker can still view the victim’s encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

- Inject partial plaintext they have uncovered into a victim's requests
- Measure the size of encrypted traffic

## Vulnerabilities

5.1. <https://yazilimmuhendisim.com/phpmyadmin/index.php?db=&lang=sq&table=&token=3950577b52347032265556636f583530>

| Method | Parameter | Value                            |
|--------|-----------|----------------------------------|
| GET    | db        |                                  |
| GET    | token     | 3950577b52347032265556636f583530 |
| GET    | table     |                                  |
| GET    | lang      | sq                               |

Reflected Parameter(s)

- db,table

Sensitive Keyword(s)

- token

## Certainty



## Request

```
GET /phpmyadmin/index.php?db=&lang=sq&table=&token=3950577b52347032265556636f583530 HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=en; phpMyAdmin_https=ep821a37h9nhji20ke8b8b0eos
Referer: https://yazilimmuhendisim.com/phpmyadmin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 168,781    Total Bytes Received : 15542    Body Length : 13281    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373f89e1d245a37-MXP
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
CF-Cache-Status: DYNAMIC
X-Robots-Tag: noindex, nofollow
Set-Cookie: phpMyAdmin_https=ep82la37h9nhji20ke8b8b0eos; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: pma_lang_https=sq; expires=Wed, 07-Sep-2022 00:00:20 GMT; Max-Age=2592000; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: phpMyAdmin_https=d3gvq211fbvdqlk0ugvhu19h5e; path=/phpmyadmin/; secure; HttpOnly
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=4cuMRtNHyLsvBYOMPzaur6oqlyr25YicGu1Khv%2F0xpA3x3ykIs1DX3jfxNV2%2FtwATfEGyXuVYqN%2FEja2%2FGeBHMmg1iGcOwIWZHE6rkJ2CX3s2M6PN1EhubcmvOedD4HWVxtFuoa1j7g%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Pragma: no-cache
Server: cloudflare
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Expires: Mon, 08 Aug 2022 00:00:20 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Mon, 08 Aug 2022 00:00:20 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies:
...
```

## Remedy

Netsparker reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:

- Served from a server that uses HTTP-level compression (ie. gzip)

- Reflects user-input in the HTTP response bodies
- Contains sensitive information (such as a CSRF token) in HTTP response bodies

To mitigate the issue, we recommend the following solutions:

1. If possible, disable HTTP level compression
2. Separate sensitive information from user input
3. Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
4. Hide the length of the traffic by adding a random number of bytes to the responses.
5. Add in a rate limit, so that the page maximum is reached five times per minute.

#### External References

- [Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext](#)
  - [Using the Same-Site Cookie Attribute to Prevent CSRF Attacks](#)
-



## CLASSIFICATION

|             |                     |
|-------------|---------------------|
| OWASP 2013  | <a href="#">A9</a>  |
| OWASP 2017  | <a href="#">A9</a>  |
| SANS Top 25 | <a href="#">310</a> |

### CVSS 3.0 SCORE

|               |              |
|---------------|--------------|
| Base          | 6,5 (Medium) |
| Temporal      | 6,5 (Medium) |
| Environmental | 6,5 (Medium) |

### CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

### CVSS 3.1 SCORE

|               |              |
|---------------|--------------|
| Base          | 6,5 (Medium) |
| Temporal      | 6,5 (Medium) |
| Environmental | 6,5 (Medium) |

### CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

# 6. [Possible] Source Code Disclosure (PHP)

MEDIUM



1

Netsparker identified a possible source code disclosure (PHP).

An attacker can obtain server-side source code of the web application, which can contain sensitive data - such as database connection strings, usernames and passwords - along with the technical and business logic of the application.

## Impact

Depending on the source code, database connection strings, username, and passwords, the internal workings and business logic of application might be revealed. With such information, an attacker can mount the following types of attacks:

- Access the database or other data resources. Depending on the privileges of the account obtained from the source code, it may be possible to read, update or delete arbitrary data from the database.
- Gain access to password protected administrative mechanisms such as dashboards, management consoles and admin panels, hence gaining full control of the application.
- Develop further attacks by investigating the source code for input validation errors and logic vulnerabilities.

## Vulnerabilities

### 6.1. <https://yazilimmuhendisim.com/assets/img/portfolio/mtnanny/1.webp>

## Identified Source Code

```
<?      ?!q3^"??U??gd?.ut{G~??A0[?x\zK?v???b?V?? SdG?w?k?H6,?i?Q(k???&C?? ?BR?
i1o>h?5A3Q?????'?|??PK?_i??+???t??s+?x?□???YP*3?□□?g??□u<%cJy???@?δ~\?(???=wT?n{??o?y???/???
j?(1?s?5?n!]?@? □(?
R????□?0'1????*?möcK[V?g??B???□???:□?9B??~zW□g??d`?p□??□□?,?"?p?□? ??□□3?$?(?!6?sU0b□V□□ ?s~?I?
R?□?Y9o'□?C??Y';??f??-.?`d/??□???C?6?□???JRb3%???□???u7?Y?,?□?xx}?□???□2i?c+;?!□q□???□?w?O?
1y>o-□x?\O?□??,g?o?{#□?θuj???q4?\M>W□O???q4~???k?n·?a??&??□=F?□9?U5??`□~Iq???C?4??&)?
?UN??e||\?.7?8a?pm?CG?,5□???I?拊|Fv?□???z?#??H?J??□???@?W7?????}f$ ?[?>
...
<? ????□?A?A,□???|?' .
L ?h?□At???□A□t7!????□m\??m?Y□?K□?^*?"□?C?□z□H]Ka??□□?□&□n?□s??(□□w?b
?mq_?9???Z73U□□??7?□M@z?4VpS□ ??<ym V
???ZTh?[?^???!□~□?8?Z)y1??□?(?j?M?[□?h??^?} ?ûj??@|#,7z???T
LB□??}y?
P??}<?T??t?~?R□ ?□??□□??□y???vk4?□□?r??□(?□体??U□??C?=LV?9?$??□_??c??j,□??;???u???|?>
...
<?□r???~□p□?E?){□??B(??E)&,?d??□V^?□3...

```

## Certainty





## Request

```
GET /assets/img/portfolio/mtnanny/1.webp HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://yazilimmuhendisim.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 335,0862    Total Bytes Received : 422408    Body Length : 421581    Is Compressed : No

```

HTTP/1.1 200 OK
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: HIT
CF-RAY: 7373e674ec8283b4-MXP
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=kIntNt%2BLDDK1Enhb4raWD6u
j%2Bt1Q4FrF1W%2F4xP4wj%2FfM%2B5oZqxVAD0sQE8cvjZ0sjVRh7ePVeH4IO17h4nGpL9Ds5ehFKivBRtKLoKH41TqMVCkyeGilZP
uPwnJOIHxRf6YTM7145nU%3D"}], "group": "cf-nel", "max_age": 604800}
Content-Length: 429600
Last-Modified: Fri, 28 Jan 2022 19:33:23 GMT
Accept-Ranges: bytes
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Vary: Accept-Encoding
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Age: 294
Date: Sun, 07 Aug 2022 23:47:56 GMT
ETag: "68e20-5d6a9821590c6"
Cache-Control:
...
[]wč[]i?, ??_[]8??T()q????p|[]0??n?=G?<[]5W????[]?_?d^#)0q?i??N[ü[]?N?U. ?F??C?????[]?[]?鐸M????N??` ???
>??q??[]?}1??
x? !????|C+??[]?>?d?[]0????q4?\M>W[]0??q?qZX??[]?????
EZ?[]??Ä[]?~xD[]????6
?N?e?
`????z{<?C?L<? ?!q3^"?U??gd?.ut[]{G~??A0[[]?x\zK[]v?????[]b?V??[] SdG?w?k?[]H6,?i?Q[](k[]????&C??
?BR?i1[]>h?5A3Q?????[]' ?|??PK?_i??[]+????t??s+?x?[]????YP*3?[]??g??[]?u<%cJy?????@?đ~\?(???=wT?n?
{???o?y????/???j?(1?s?5?n!)]?@? []?(?
R????[]?0'1'????*?möcE[V?g??B????[]??:[]?9B??~zW[]g??d`?p[]??[]?[],?"?p?[]? ??[]?3?$(?!6?sU0b[]?[]?[] ?s~?I?
R?[]?Y9o'[]?C??Y';??f??-.'`d/?[]?[]?C?6?[]?[]?JRb3%??[]?[]?u7?Y?,[]?xx?[]?[]?[]?2j?c+;?![]q[]?[]?[]?w?Q?1y>o
-[]x?\0[]?[]?,g?o?{#[]?[]?[]?[]?[]?q4?\M>W[]0????q4?~???k??n·?a??&??[]=?F?[]9?U5??`?[]~Iq??[]C?4??&)?
?UN?[]?e[]\?.7?8a?pm?CG?,5[]?[]?I?[]Fv?[]?z?#?[]?H?J?[]?[]?@[]?W7?????)f$ ?[?>[]5?t[] `H[]?vM[]x[]~?[]?[]?[]?V
w? []?T?[]n@8t?[]U??m?[]?~h??[]Z?[]R??Z2?;{[],?a??[]?[]_WmgN?[]6?[]4ds??[]?[] ?[]7-?[]n:1[](\?aM4??9B;$6k??h
|???[]?[]u??p??A?/[]a?!6c\#?J.p[]!/?-w?H????3?X[]0????[]?|???[]?E?17QP??VMS[]G?G?a[]?0?
...
?[]Z?t?f?[]s?0-(?O????g?v$[]?[]?O[]?d?1[]?[]?[]總?[??>?[]?[])????k8??mh?5[]?[]n?, ???>?[]?[]?r=~>????[_D*?=
(.k???b×?/?V???'[]\hR????q ? ?<?a??/?Q[]/9?45v?[]?[]?[]?<[]?[]?Q5??q4?\M>W[]0????q4?\M>W[]Y&4M>
$[]E??s??8?Z<? ?????[]?A?A, ?????|?'` .
L ?_h?[]?At????[]?A?t7?!????m[]?m?Y[]?K[]?^*"?[]?C?[]z[]H]Ka??[]?[]?[]?&[]?n?[]s??([]?w?b
?mq_??9??Z73U[]?[]?[]?M@z?4VpS[] ??<ym V
???ZTh?[?^?![]~[]?8%Z)y1??[]?(?j?M?[[]?[]?^?) ?üj??@|#,7z??T
LB[]??}y?
P??><T?[]?~?R[] ?[]?[]?[]?[]?[]y????yK4?[]?[]?r??[]?([]?体??U[]?[]?C?=LV?9?$??[]_??c??j,[]??;???u??|?>.g
+%????[]?[]?[]?N[]?[]?OQ??K?O????R4????[]?{[]?[]?Z?q4?\M>W[]0????q4?*??[]?[]?K[]?}' []B[]\ic[]?[]?[]?{???!xo ?L?S??c
yYS??J????I????Q????55?[??[]@Mq?uj?[]B[]?[] 3?fd?*??[]?[]?0P?~?[]?1
"
?[]?&sdV)??z??=????C?\

```

99 / 243

4??/?a<??1?QA□□u??□?c?R?E! ?Z□y??W8?| ?&?+????i?| ?&?+????i?| ?&?+????i?| ?&?+????i?| ?&?+????i?  
i?| ?&?+????i?| ?&?+????{??(????@f.8? (□□□□□b^??s@?D8Y7Jd??□;Θuj????q4? \M>W□O????q4? \M>W□O????q4? \M>  
W□O????q4? \M>W□O????q4? \M>W□O????q4? \M>W□O????q4? \M>W□O????q4? \M>W□O????q4? \M>W□O????q4? \M>W□O????q4? \M>  
4? \M>W□O????q4? \M>W□O????... ?d?□O????q4? \M>W□O????q4? \M>W□O????q4? \M>W□O????q4? \M>W□O????q4? \M>  
W□O????q4? \M>W□O????q4? \M>W□O????TR?□L??F?□b?hκ??B.□?B;??  
?□??1?n^?"???z>j□□□□S□??□???4? \M>W□O????q4? \M>W□O????q4? \M>W□O????q4? \M>W□O????q4? \M>  
...  
???>Ueh□X?????Q????1Mf?q3I?v???  
□=?6????□Vp"Y?K□\$\*a????=jZ9z?w?^X?A?`?)?1?Ri?({}8Ž ?dB~0\_.?h????□KtF1s?□'ϕ?X??tX>a?□R□?□T  
v ????=?□□??\*!i5?.??□?Z??f1??□E??N\*#q3?C2?□????1?N+k?3A?iW □L??□ÓP((□t□G?])?□#<? 3E|?□?□?□?□□.?  
s???T?□?;?eV?j??m?V?□?&\*7N`??□?Jw  
%□??Nk?g\???8I□?rk?J?m?K??zC□□□θ□s?+□W ?□?Qk9+:?□I/G??□?□4??□N□?d□Q'  
(?1??^M?□C□N□??g?:□□□:??r???yM?????N7+)????J?□?□?PQd??K?P□w`□\$?□□??[? X□\$??N`????;?□???1b  
6/!??SUV?WD}:?□????□b\$????□□□□□□□□□□?Q?|h □?`!??□□d?>s??d??□\$m??□h??□?崙□'????[p???X?@  
foPx`\$?k?%□?P?S□?""?X?=??^□A?6?θ??Bq?B?b7  
...  
?fV?}?□%?B□Aj\$(o?4?oV?□??'ϕg?Q□#?.?f?rG?I□k?F??Sn?O□@o?1:~h?`^Z~???x  
y□  
C□n?D??1?J?4????□□E?%?θ=?j□O??□?□3□#?Q?□□\*?CP&?}?yZp??=?□?k?□v?□  
?□??(??B?k?+1/??-0?1|B'□?θ7%????8?9□?1?|□□E6?+??j@n?<?1fj?-m??A?{?c?□?+%□?□Q?□?□r??D?JF?  
g\*?D+□??□%□7:????b□?□zn?貳/2s\_?□@□?'?T????{?~?  
??B□?s?{?b□?2?5?j8?!□kw?~?  
?:?6□===?????□Wup??  
B???yG?Y?V?Ke\_□??□□=??□g?□(λj?z\$????□?V?Pda;?8?A?w-P□????T??v??j!??C. ??X□j□|b\*????□?□9?□  
?□#  
□n□.?ge\_Uj□□??b□?  
-M?□)^?#E□Q□?m\$?d?\_?^m?n??K?<??  
?,??]  
?□2t??□?Rz□□/h??□□?78{L?"?+??og□\*?P□W□?<?Y□?#??u?□??g????R?{??j?|z??  
1??□/□?O?.9?□?□?Gi□ uEAb?w\*Qg?K???5?□?□p?[GM□□p'?w E□??S??R`???□?  
3?x??jI?&?□□□??□?e(??/□#?+?□f?□□?7?g/□\_?|Q□x□r"??□?k?\$?pc□???□□`????,?/□□Q"??O?k□?m?r□?b?3  
□?????<Kq?E??5Lz^O?;C?y?ni?E (kF\y?{#?I?\_A1?1:%□r??!h3?j□Y9dI?□Zy□8??□?u?□q?? ?/A?;□??N□牒d;  
B?????-0?62?□-?}??~#?□□C]??4I??□v?□□~T??M?□□3□??□<?□?eg□d#?fF?\_M?buW?sFD\_□?□□Y??-???t?  
=□□???1?4m□□eo?m[Y?□?tE?{"~??&->D?i??□?□8o?/P  
mg;???5?□?"??#?□.??&6?n□?c?D□%??+?8□s??; ;?□?%:□?W?G?□?□???d□?□?□!??H4nG???&sF??~□t?o□g\$?□/??7oj??  
HUK  
...  
aG&??□?t??□#|?n^??□?t□' ?8?G??tV7□?3???□?Aj?H??|x?;?Ya.??□?I??r&?&????/vQC?□\_?7?□Ho]□??g?  
H?□???□?C?3□?S??,????[??a?T?□?  
\?0X???? +G@.W??α?L&??????□a??;x??  
□?Mo?:U?jE????| }o??(J□??????Z??Qg?d?<? -???Tn??'□??Kg□? ?<???T?????o??U7?%?  
??!/H\_????□Cm□□,?□??ML?z ???□□?(&t"?"/F1□????(??m?□J????□h□?y?/]□`???Lu?□[Fs□b?b????q-????kb?□□QC  
o□□T□9?m□wy□□???□???  
□?cUaL???DBK??[?u9Q?QP-??□?u??'??ov?f ?K1□M?7?T[??.?□□c?□□?'??\□  
y?u□□?%NZ?fh??? Ftn?□□□□□□□□□568?U?□V?□□L???~□□□?x□n?Z?\_????&□A?<T□?M???□K□?|MI  
|8□??"?;?;O??□?z? ?????hofO?+L'□6?k???XA?&s&□?□?□1????>#rJ??\*N?8:~p`\$q?Tp?rO??%wb?□?t?;=□  
\vw??'?F??□v?a?iR□%??#X??nP?6\*  
yw□□□??8?W??}??V3□??W?□O}□X3p@5?□?□??□  
h□?D??謫\*W,?)=o??n?/?|k???yJu?□?d□????~?\_f?□□□□?K????\$?/H□??\*:□□G?1[s??  
??Em8??v=?□□??  
...  
[???□???]?□E?3;ca8S\$?t? 猫?韜J'???"?{\$a??V□E????d??□?r??"Lr??□???W? ??c? ?J?|?v?□(?1?f  
8??D□??c□???□I?;

I??/q&0`?.???`>q?       ?%?□??□8  
?????□3□<1?8?{??&>?g?<iK? ???u?-??qL?G□方U?X~=????~□8?m??|J?+??2??<?  
#m?□?  
6d?zIk???"X□)?□3R@y!]????;??K?□?I?8?□r(??□?□\$□q?DT8?0?f.□?□G??h?I?%>SR?g?B??□□|??K?□\*}|PD-\W□}?w?  
(□?□/B□6??w?L?3(??#??E????)?□H?%?'??□?(?U?□1?pB6□g□??<□3??\sm?]?>?D□□□□9□??r?L????Ms?&ZyÖ??  
p??□+?K□M? ???6@D??       □?n?□Cb[/%?[Y□??VVP□□??ib?\????v□p'??□?□?]?{?q??f|)!□yL?\E'?a?□?□?L?□?f  
s??8□?+□?w□??A?□?□rI□□?□Q□M(□|V0?t?`?4#????\>-\$eOv3??e?□vⅢ,}  
???□?T?□<?37□  
...  
GX6.{□□?[!o\?"?%psZ????t"4??n]□?sY<LT/`?n?????□       \$?[Q□1?NI□?>???:?  
?A?1;?(?F?12-?8{!0???2??□2□?□?b#?D? ?????□!?(r=???Z□\??ETO□}?q??(? (M?1???0?A>y?□□. ?{V□□?gS□?9  
dtLP?□???□□a????□m?□:??\*?t?I???□p<?   ???"?Lo□??Je?@?a?□N?GrbP?)?|???R?{???'?F?I□d□FkX4?: :I7p???&??  
D??#LK?□!{??%?r?T#□????/?|????f□SMN????r□?A4?[<?:?-□???&□□p)xp,I?  
Ä??□?#??vß???C?□?\_?□???#4?□?VU? ???□, E????G?□?D□  
?r□?□#?□?|□???□X?  
????t?@?>tBv?b□???; Lk\*?0□=????□???□%"?kI?+□-b 7'h?m? ?????1[?k2-?????#□?9?????.?A?Mu?w?a? ?0q???T?+?=  
5□??W}?9?????&=□□?□~□???18????□f□\$@?????f???????f?8X?^□\_?s-??f1??□□9?A1u|?TkK?[?âq□  
é??B?rkk?□V??6pEe^??□p  
...  
@?w>n? ?6]n;??P??:pW?□S?~\??OY?ko1?g#?c?9?τ?ε-H?1?-?n%1}?□??□R?h?XS□e??f???o?□?@n????ç1□??I??□  
       □V?0!xSS/  
ImK?7??&?`?0??□□       L?Y?□?@?a? ?uD3???cUw>?□f?□  
?????w,?'??~#c?y{?DJ?xN?□□?!g???\b<kw□r?x??s?±?è?<?   ?@J?=+=+□  
?A}?y□?X?V??       I1??/?3??9? \? ?□?)??r|QEc□?h???????z.????W`??□G???0,?□p10?b?□-□?V??E-D□?TRw??Zf?L  
8?□?8?"?C       ?Û?"5□?v1?□up????+□?o1`?Q6z88o??□jty`?□Z9       ??ε?^Sv???VD?□?c^??□o?a?`???b□>Km  
2??□B?E.f□?&□?-?□?ry□??i□~?\□=S??□??)?□<□\*? \9"  
????kag?{?r?bbR?□+???<\$?9?=?\*?]?a□?F□?IY□???d???Y□|j=?J??□;?[?□=???Yyh  
?0?<??a{??muL?□??@??□Dp?□?@?0?v;?<?"??K□?c?k'?E???????9?□y?fDψ??□?8?q^       f??\*???B??□>?\_?  
[????:??□S  
,q??□??G\??□?oL?e{?K?0q=□????□v?□??#□?□?C?pf?6?<?G]□M???□,[?e)?1?U ?..??H?mr□??□R?□?8□????-?  
W???:□4?/??E%o?U?□&□s`?????C?U??`?□?4?hQ??□X?M1????|s? ]I/Xv?V?□?D?(? ?L=□□???.C611-?M/□~J)J□?@?□?□?  
^□JP?J?□□?+?QI???a?]????x       \s□??□  
?O□\*n?1?\_&??AP?-?       ?:r?5W?L?????A????p????B?A□~{?Oq□? ?1uuaa+????f???       ???T?  
??&??K?HÖ2~v?1Ud?B?kk[?"00? [cvb;?\_ 艸?s???qS?:L???|o????O? \$?pRz?1?o??-hd?:□□□y<??{□??>BbдE□dFT□??  
□?□?;f |çR?1????k?tn□2? \$???d□???z?ev?T□<cB  
WX??7??x'?□)~□3Q?[????□?+x(□□  
?1?       ?□?)□?qRqf□!□□????S?□??T?(□?1□;?□?F???>f????c??□?'??□????? O?6????7?????洩□Xu?&i'm뽕+???kq:u??  
#?P?□??7?E?□?  
...  
?□y{□□□-Pn????□\6??□B□K?m?g??wD??□?X???w??^???!S?????□9i?w□v0?u??]□bz?  
?b?a?&?%?a#??L?Ç?0)?□???□?<?>?t\?[??Zt?Z??<?BFj|\$???:+?□9S???????;a&=□†+□\$1?/z=□??6?i?'??  
?□  
?□R□□2?d?^????D? ???N?t([?□: ?n□t??□skx<??x?%??L`0~T??       □?N?6??-g??  
??????m?"□?□?□□????□??饋?]?  
|?v?+??????`E????□{???G{x9zT???Z?e?s  
RG?7Mi?u?|/wU?□?4a  
?r?K□□"???5??□□?5ysk?<???%?y?^□?|`?/z????□?8'?3??□?a??@1□?@JW?G??□Z?□5??\_o?JU?????□/G?□9□??n??  
b?□?□□??洪>}'□???'O?□?□#??gLU?Y?H?y??i□□?v?□?R???7?#?/□?0□\*□??v□E??~??r\$?U????\_\\_□X       □?k  
6□????>??Hum□I□?P?□?qLd?□%h{R?P??□?w?0#???^T??h???d□? \$I□□..□?????s?/~?s??t□p.1`D?j?□□□f0?BY?  
r????#  
?????]??I□K?!?#□LQ??f?   ??(fg\*?□?  
+-{Xi;□?ǔ?□v?+(       D?ice??K;A???d???!????CÁ?躡N??c0??\_ε]/`□?f□1?#???Q??□/□K?U□??D□B뽕?t;U\???'g  
P??}H?V?:r?70□s?□E??Lv?Z/?□□????□(y;[t?□?x^??□?m[????□?(</p></div>
</p>
</div>
<div data-bbox="884 960 951 973" data-label="Page-Footer">
101 / 243
</div>

D?□?k b? s? u? □M??=(□f s r j? b? ? s n? m p V 2? ? \_? x k? Q? ? ? ? ? ? ~ 3 □ { 3? < ? ? t □? | ? ? { ' ? P □ \$ F t? □? V? +? ` 1? ? A? ? : □? ? □ □ p C? K? Z □ E  
@? O c □ ' ? ? ? - □ \? ? \*? 3 G? 0 s w? # a? ? ? ? 1 L? ?  
S? @? ? m S R? ? P C? ? □ □? O o? □ u X □ O 3 k 9? ? | J 9? Y? □ R □ □ X m? ' V? ? □ t? s? } w? v □ U #? . \$? ? ? ? ? } F □? s? m? y? ? ? ? \ □? m? 6 7 [ < ? ' ? ] k? ~ ? )  
W? ? ? 2 #? ? " ? ? ? □? 1 A 1? ? □ y? 1? { ? } □? ? Z? ? F? ? 4 s? ] 2? □? ? ? □? ? □ W? h % V? ? T ^ □ □ , P? ? \$? ? ? □ r < C? " ? w? J □ S { □ □? ? □? || t y e □ l s P  
H j? ? \$ H? g? Z b u? ? C? = G? w? G h? ? ? □ : M? ? ? □ □ □? ? x? ? □ Y? ? ? ? --? ? ? o? 5 x? ]? ? A? Z F □ d? ? ? F? + □ □ ^? ? ? ? i Y H' j? w  
? ? ? \?  
...  
~? d? ? r? B m? ? ? ? □? ? \*? ? ? j? ? ? □? . ? ? □ V 5 K o z? 0 □? ? #? F = ? ? = □ □ ? ? ? ? h y 2? / ? " M? ~ p? D? ? ? ? L \_? & ? M? ? A? □? □? ? & m □ H S? □? ? 5 □? ? R □ 6? ? ?  
S? 6? 1 c? v X? ? ? X I? ? ? ? ? ? ? ? H - H? ? ' ? m M : : □? ? ? ? ? \? < ? t #? □ □ ? ? ? □ □ Q I? i? ? ? α? W? □? ? V? Z? ? ' ? P X 9? □ n? ? p □? □? ? e r? ? ? ? ? " 1 . ? □ O? L? f  
~ < ? ' ? O @? m? ? ? e? ? [ □ | ? ? L? ? ? p □ V? ? } □ F \$ □ □ □? q? ? ? ? ? □? > ' ? C? ? □ 1 ! ? X? □? ? @? ? 5 □ N? ? E N? ? p? □? H O N? " ? ? ? T? □? ? z? □ [ ? ] o □ v O  
u? ^? ? ? □? < z? \ U C? ? d? ? B? ? | T? i 5 j ? O? X? ? ? 0? } S? } □ k k? ? ? 3 k? ? □ y L? ? R? G? ? f  
? ? )? ? □? ? s g n 0? ! z? □ , ? ? ? \_? l n B m? ? ? ? \_? ? ? ? □ 7 ] 9? X E? ? g? ? - □ t? □ 3 H? 3 A? □ k T □? ? @ < ? P < Φ? ? D } u? 8? ?  
...  
b? ? □?  
K □ g? ? ? 2? ? G? G? □ & K 1? ? v H 1 B? 9? ? ? ? ? ? ? 3 □? ? E C e? ? ? □ 1 p? 8 & ? ? y 0  
U \_ O? ? ? o? V? □ x □? t ) ]? ? □ 9? □ h 0? k 0 0? □? ? 8? ? ? d □? \_ f? " ? S? { - ? G □ e? □? ? n? 4 □? < ? ? ? s + ? \$ □? p x q? æ 1? { > ?  
L □ { ? ? ? □ s? ? □ ' k? - ? ? ? □? ? □ i C? □ b i P? H h? u? □? □ J? □? ? ? □ □ J? ? u H 6 0? < ? □ □? / ? s? 1 □ I 1? o? ? p? ? " S R & □? I @ □ r? ? ? ? ? #?  
r? ? ? □? ? n" □ p? ~ ? U A k? ? z? ? ? Y? ? ? ũ? - ? ? ? □ j y \ ? @? ? e )? ? C > ? p . ? ? ? □ ^? □? ' ? p? ? z? □? x □ B F > ? ? S T ~ ? , □? ? ? / B k R? A ( □ r : W A E? ?  
Y □? )? ? \*? ? ? . z B e 1? W T? , □ Q? s □? e e? E? k m J 2 v □ p ; ( ? V? h c ' ? A . ? I? ]? Y? ? ? y ? ? x ' ? ? ? S? 5 □ J S □ □ 9 ~ u 7 δ □? ? ? ? % 7 □ " ? □ O □?  
\ z? ' 3? } ? ( X G? G? J? d? □? R? ! ð z? ? □ □ □? W O □? ]? ? ? r \_? % M □  
? S? \*? ? ? A? ? > ? ? @? ? ? ? B? 8 □ G? □? ? ? □ □ 8? ? ? □ i? , ? ? ? , □? ? ? ? ? ? □? ? O e? ? Y? ? 8 ^? ? ? ? > K? ? ? ' o? ? w? ? n? ? D? ? ? ? ? ? \$ 6 | ? - ? } u? ? ?  
x □? ?  
? G B 2? □? □ N? u □ < ? ? □ M 1 L? X e? ? ? v 4 ( L? z? k? , f W A T ) 5? □? 8 □ □? , ? ? E? 1 J? ? ? e . n 7 b?  
? ? ? C ( ? M? #? ]? 7 R? □? ? ? Z o □? □ V? k? = T? C T □? c? 8 □? ?  
...  
\*? ? □? v □ c H? ? ? ? ? E □? = < ( A? ? ? ? q? ? □? ? ? ? ? ? ? a ^ □ | ? □ □ \*? n? □ □ p? ? □ □ w? ^? e □? [ ? ? ? □ - ? b Q Y " ? \*? v I? ? ? e )? ? ? ? □? 7 w? + ? ? ? P T  
2? H % \$ ? \* q L? / ? □? 8 ^? ? 7? □? = ? ? 9? ? ? □ ~? ? ? ? & ? p g ` V? ? P 1? ] ? ? ? w 4 8? > q < ? ? c? @? ]? ? K? □ □ Ō c □? O? ? ? ? dt? U? □ + D □ □? \_ + I? ? □? ? m? ? ' e  
u < ? a? P R V w - )? ? ? R? B 6? ? ? . ? ? 2? ? ? □ w? ? □ □ < < ? ? ? } ? ? ^? ? d ; ? □? ? ? □? ? ? 1? ? ? ' = \$ ?  
? P ! ? 2 = ? | ? g? w ? d? ? k? ? ? ? ? ? ? ? ? ? R f R? ? 4? ? N? d? ? ? ? ? 0 V □ v 5 8 □ 9? N? w 9? ' ? □? ? ? □? ? ? ? ? ? t? } □? " ? b? ? ? ' ? o e? ? } □? ? ? ? v ^?  
A □? ~ □? □ \_ ? □ T V? ? 鏞? } ? 1? □? □? U? ! N? ? ? ) ; \* 9 H [ , □ F y j P? q? ? ? u T \*? x? ? o < ? ? g s 1 □? ? ? [ m & ~  
? ? O [ ? □ q? ? ? ? < ? 1? B? A? ? ; ? □ { ? x U 9? ? 0 0? ? e □? ? ? ; ~ 9 W? k? p □? □ " / - ' ? ? ? ? ? @ 2? □? ? ! E q V ` = □ □ □? ? A m π @ □ □? ? ? @ : ? ? □? [ ? ? □? ; k?  
i? c? ^? ? ~ ? ? ? □? = : ? = ( ? □ □? ? T? ? ? )? ? ? K / h  
? 3 5? ? ( □? ? \*? . c X ~ ? q? ? P? ? f? ? ? □? ? ? 4 ^? c □ [ j g ? ? ? ? E c Ĭ | ? ? ; Z \* G? t 8 %? □? 5 / ? R? ? ? ? ? 6? □? ? + ? □ % □? □ y r □? / ? Z? ? & ? ? ? ? H % □? ?  
Y } ? ? . □? ? □? q □? □? Y? ? \$? ? m @ \_? ? 0? r? [ □? ? q □? ? ? ? ? z [ c - Ĭ = ? ? \ N? ? ? □? [ □? ]? ? ? o □ Z? } ? z □ h #? ( ? ? ? W? ? ? □ □ □? ? □ □ A □? ? □?  
v? L 2 ? e 1 ? ? ? ? ? □ D? ? r q □ □ ]? □? G 6 N @ 4 ? ? ? ? 9 & ? s 썰 R? ? ? ? ? q? □? 8? . ? □ 1? ; □? ? ? u Z % □ ^? %? ? \_ | B h? B 5? ? X? ? ? ? ? W □ K? d A? v? ? Y? ?  
w? ? V 1? 6? ? B □? ? ? □? ; ? ? ? ? 8? ? ? K? ? □? ? □ \_ a? ? H Y? D? n? M? ? ? ? r? ? ? ? ? u? ? ? U □ □ S □? B L? q? ? 𐄂 o \ { ? ? □? > P " □ | ? - H m ; □? ? ; ?  
u? ? Q C ] E? ? E? ? w o u? ? V □? ? ? ? i □ ) □? \_ J □ □ □? □? ? ? ? h? 0? □ S? ? ? 3? 8 q u? ? 5  
? ? □ = ? ? ? ? f? □ A? ? ? i Z % 4 i? ? □? □? ? ? ? ? □ □ E A □ & ? □ K? ? e ' @ m □ j \_ a □? ? ? 吓? ? ? ? ? K? ? ? | - ? ? P □ V 2? ? ? ? ? □? } ? 2 A? o? ^? ? + h O □? ? ? ? < ?  
E  
烁? A? □ Q? T? ? T? 0 □ ; X , t? □ )? ? □ Ĭ □ □ \ 菴 v +  
...  
? □? %? v? ? ? = & ? ? ? G □ □ ? ? . ! ? c? Z? @? ? ? k □? w □ Q 8 > ? ? ? ? P k? ? ? □ v? ? 0 □ \_? ? ? ? □? □ β? p ŭ? ? □? \*? )? ? 1? - Y? U? 9? ? ? □? □? 4? e J T? ? 4?  
y? ? \_ ? □ F? ? ? ? □ ; ? □? ? N d? ? ? ? 5 □? ? j? ? ? K? ; ? g = ? ? / a? ? ? d G Y? ? ? ? ? ? ? v? ? r? ? 6 q? ? 4? ; H B m = ? ? x? B T k ^ 4 T E? ? c □ 4? □ □ □? ? a? ? □ □? \? ? z? 8  
> ? ? < ?  
| ? > 5 □ L A A h? G n □ b  
L? ? ? □? I? ? ? ? : W  
□? #? ? ? i | J □? □? q? ? 1? ? V? 2? G? s ` y | O? t ' ? ? H? □ M X ` ? N □? ? R  
? + ? w? ? g □? @ □ & ? e □? B \*? ? ? ? 8 A? ? O? K? ? ? H [ ( □ ` ? ? ~ ? □? ) B 2? □? y ! ? @? □? ? ! q K? □ 1? ? ? ? ? L? □ □? o? ? ? 3 □? □? ~ ? ? ? c z w? □? □ & v?  
Q? s \*? ' ? ? \* F? r □ i 0 e □ ' ? 3 o? □?  
...  
? S? | ? ? y? L? 錐 □? T □ □? ? ?  
g? ? w? 掣 1? ? f? □ o? ? 0 2 k n? □? > y? c \$? ? g u? ? \* \$ 7 a m? ) T 2 6 ©? r o? N \$? 1 2? P B? % U / ' v 0 8? " ? □ d? 7? ? %? □ □? #? ? ? ? M? F? ? B? ? F ( r t?

?甯~?;??^□?2S?`??Gc??? Q#=????□?^???IK:???2?□?G???Z□1?ksd□=?3~?□?s?????t□□  
□R{??<? jk??,01?□????<?C?9?&tu□□I□□?x??□?B?□%□4-?1?□"?V?#H\*e?□????G□ZYō?c□□?+w+CS  
F????n8?[p-??  
^#ihmJiS?D??v?!?b□1~??\????9ū????J: \_????□WY?xtz??~4□s???0%?Y□????uI?wU?? @]□Fj?I?IS;?M?□?? ?&?e??  
r????]□L<?□V????□~?????n□?  
?[~?,  
??st□?M?????Tη???v\$R?□□G?□?6ij??N2YAUt\$??'b%p□□#f?fh??u?□Q????□10??f??W□?F□?}u?????)??!JZ??s?????  
(??N??□XI□??6?E□|η??□İ?영1?aØ□?<n?G? □?}?!□η;B?\$□JT- ?□??□□□???'????□o?  
s?□??Lrr??ka□勑t4??tK?  
?v2??3?  
£@?k??□?□?□?□?HV?□???~□?7c?Y?r3?1/□ i?□-Cm?□□??□?□?□?□?  
??V??□~?□?-??□?+&BXi\_M?????T□??|□?}?5□????6?a?dY?R?I?N??1g?□1?W??A??G??kby?????□c(M?\*?  
n????□O??□?□h?' □???□\$□□1??I□=6????a□?k??eg??Txk□?□UP?URT%~>@B□r?□?□y?89????□TK?□?□S?j^a?T□?  
I□?□=□□□C?:=?□??>i□□?u?E??s?□???Æ????>□□????y5Z?%Af?????"?u?pTs?,???hp?W?????□?1?2?hX??□???bl?)?8  
-?????&?□?'?c?X??;??□M???8?]□D??□□□aK□?aKo□.□c?\$?9(???{?K??s/□6??r????!□□?Y?p□?Q?U?, :g#□??x0  
Č???□o????|?□?9?h?  
□  
...  
SJ|??9?□ ?  
??g??{□s~??O,Y?  
?Bb??2?□Hbx+□#?L]5□`B??0f1?!!!!Ä?/\??□????□y□?□?<??f??□p?□5c?9□M??R????G?J?(S?T□□ω&???  
~,???□\_??c□a??7□????Yv??□?i=?r J??]□Wj?? ?X?gP?yf?&?□?"?y□z  
?Ngc\*%???□?:??□??<? ?;?K??□g+E+???□?]□vE□?□□.□K??g?hVU?????<□?a□□^??Iz?|w???\_q?□????□?P?G  
n?]□'=t??□NmBKl□□??2T????□??□@□????□□??%???g?? 1?  
??□?!???□2'S?V?I  
<?-]NPrS?T?L???1??Iq?ks?□m3??? ?rKtb??N?□?E?Xb□□K-t□?□gh}B3??□?c9b?A?□????k[K?oq????□lo????□  
y?]|?b□□????^□?O?Ŵ???|□\$?? ?'N\? wx?V ??□?r?m?M?`??`?u□??;????(S?Sgi3????3?( &?p□SA5?F????j<?~X|{!n?  
k??^~??□?"??dtTi?)□□|,?B????M?îd(???os-3?\?b?<????□5□??}?w??[?囁V?Y?@?1"m????□??5□□□O?`□戎  
¿????□?□f?3u[q?□1^??`??□□e□□??+Dh}?F?&□□□??Z???Y□□kw?M\_?"  
M?N?S???N?e??<K?A?Y7á???  
?□I!□?|J? 5??K??W□v??α??~nU??#1k?&??{+?R,???dX?¿?b□2?!b????□□t??□?B>?XaH?A'?b????]n?¿!|□hub??qI>X??o  
6?¿<,A?T□????i{???X?□??□5□????`?□"????I?□?0B?1?Fh?~1?□?K□k?□?-□Y??□?□[?I□?????+`???frz?□?|?2??,?  
5!□□□j?\_□{=????DV?  
?\$?t??□?□y??QQ  
`??□/wBQD□3Z??□?□□□1L?d?K?□E?|m뽰\*?[7\_□O??□>??a?(+)!?v??B2B□???.?  
?/????□?□\_?;YF□H?9L?w?n??□h?□?E\?c?□??□□t?□?(□??□??d2??1□?"???r#P???□□?g????S? ,C?}?□4#La?  
n?;?□[?X????D??p?8,¿J??n□????  
"yC????????J?w????(a??D□?B#□'ò□T??3???□'Mq?□□P??m??{?đ?&...?  
c?□?z??Rt?O??□!????□3□??9□??~?{□jY6??S????H □2S??aR????< □N^??)?WT?7?U5?y □?s?□□mA□t?  
@□?G#v(\$?\* ?□S□n#□□n02?□x'□.???S???Z\_?í?G?\_?????#?□=8□(?=□□□O{67 ?48????z?@???4t?}]1~yb  
@□?yh??□S??T??EE?<Y  
#  
...  
qd??;?□????1+?)\$Z?C???Cr□? ????K???????□7'□?□q□G???E??□???Y?□???R?M?□3| ????[??  
h?□T???□[□k\*□/F???Q??□3???u?□:X\?뵆???Wz??□y?V)□B)□□???ŵ7:??□>W□??,??&Kq?%??□3???'???i?pc}?f^\*  
3?????@?θ?□?@?f?T?y? □<? J?P□vJ?z?E?π  
? ,□□□?bJ?e\$T??&?hVt□?? á????□?f?□?e]?□!p?u?B\_ ????;b?□?V^?A?o□WJV□?□□)□?o????□?□?  
\*?"\_□????x?B}?RO?d.??+?u????oz□?+????Rh??A?□?T????'a??'???]□T?R□?w????Z?b?ýL□????θ?□N!-?'?<□?□?  
`??θ?????k.?G:9?□e?^?□?M?□b\$□?□□S?'?□□?¿?□Jd{?+?□?Kϥhwn~{A???/M?□□??+y?&□|X?q□□9?□0?Dí????'Z\*??>?  
(??9???rE8}?`??uC??f?s  
?□??\$?□????□]&□>□??}???)>g<s???□??m3????;  
;?'BJ¿B????□?□>?8??o?d??□q????χ□?]?@?7' (??X??□???S□???1????□/□c??□b?}kU?e???8J?k????□?  
í?T??□?j??□B??,{?4~?\*<E;???7□i□qF?\_???L□?cE/Z?□

```
...
??K?#?aT?I?-?1??q??□?□???j?δl?|`??_XB?□???P-?躡6R7z□      ?3?Q6
□?□?T2?;!??□oI?□?q?qw□s?□?□?p□z?6S9□?QE??+□6<=?7w□?d_}[?C?□IS??z?k□      ?$□□?&.□r□i5?%????~?
::????□?X□□??????}l?K{F?(?□6?'(□?H^C?Qo?D;???iM<?□%?□@□???□?S?,?Ÿ?□?R□????□?D4S?9?!Cz?_??~□?7?Y?*
&P5□?3???tWc□,?*?Y?{?&|?Y*M?B?□O?MqS?G?ur□?AvR?n??^
@?????^???<?;Á?Б?us??{??????e??????o?J???3?□□?#?A]?a???q???!??5?|Xh2????;z?V?>i?QP?U??x????□?s??
z?@????□?fbY□????a??^k??      ?|?fv??@?U

?Oo*ZA%d?□??(??^?K??□?zJ?□?K3?k#dp]?□A???□sU□?9???"
?s??_?e]?□"???□=???{?#1XU?3???N?*□□?|??`?qya;?t??l?A"??g?b□□?_#?w?g??□□???□?*??c□?2}??X
...
```

**Actions to Take**

- 1. Confirm exactly what aspects of the source code are actually disclosed; due to the limitations of this type of vulnerability, it might not be possible to confirm this in all instances. Confirm this is not an intended functionality.
- 2. If it is a file required by the application, change its permissions to prevent public users from accessing it. If it is not, then remove it from the web server.
- 3. Ensure that the server has all the current security patches applied.
- 4. Remove all temporary and backup files from the web server.

**Required Skills for Successful Exploitation**

This is dependent on the information obtained from the source code. Uncovering these forms of vulnerabilities does not require high levels of skills. However, a highly skilled attacker could leverage this form of vulnerability to obtain account information from databases or administrative panels, ultimately leading to the control of the application or even the host the application resides on.

**External References**

- [Source Code Disclosure over HTTP - SecurEyes](#)





## CLASSIFICATION

|             |  |
|-------------|--|
| OWASP 2013  | <a href="#">A5</a>                     |
| OWASP 2017  | <a href="#">A3</a>                     |
| SANS Top 25 | <a href="#">540</a>                    |
| CAPEC       | <a href="#">118</a>                    |
| WASC        | <a href="#">13</a>                     |
| HIPAA       | <a href="#">164.306(A), 164.308(A)</a> |
| ISO27001    | <a href="#">A.9.4.5</a>                |

## CVSS 3.0 SCORE

|               |              |
|---------------|--------------|
| Base          | 5,3 (Medium) |
| Temporal      | 5,3 (Medium) |
| Environmental | 5,3 (Medium) |

## CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

## CVSS 3.1 SCORE

|               |              |
|---------------|--------------|
| Base          | 5,3 (Medium) |
| Temporal      | 5,3 (Medium) |
| Environmental | 5,3 (Medium) |

**CVSS Vector String**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

# 7. HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM



1

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, <http://example.com/some/page/> will be modified to <https://example.com/some/page/> before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

## Vulnerabilities

### 7.1. <https://yazilimmuhendisim.com/>

## Certainty



### Request

```
GET / HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 129,2203    Total Bytes Received : 19554    Body Length : 18800    Is Compressed : No

HTTP/1.1 200 OK  
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 7373e528fe6983b8-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=jClu9YeeEwaJVij14N5%2Fr4LIeokEeJ8CWC0tu49cFc6LjopR45%2FC8wEJk0orak97LmXPZdrYpjUZFlQw7aVxtBGkimS7YVvhe8Fslf%2FIxKW1zJzx1FmZKyKDQ82cJZZVNwyMtFn2pto%3D"}],"group":"cf-nel","max\_age":604800}  
NEL: {"success\_fraction":0,"report\_to":"cf-nel","max\_age":604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Sun, 07 Aug 2022 23:47:03 GMT  
Vary: Accept-Encoding

```
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<title>Yazılım Mühendisim - Profesyonel Yazılım Çözümleri</title>
<meta content="Biz güncel teknolojileri kullanarak mobil, masaüstü ve web uygulamaları geliştiriyoruz.
Teklif almak için bizimle iletişime geçebilirsiniz." name="description">
<meta content="yazılım,
yazılım mühendisi,
yazılım mühendisim,
android uygulama,
ios uygulama,
mobil uygulamalar,
mobil uygulama geliştirme,
mobil uygulama fiyatları,
mobil uygulama yapmak,
mobil uygulama kodlama,
mobil uygulama yapma,
mobil uygulama ajansı,
web sitesi,
web sitesi geliştirme,
masaüstü uygulama,
masaüstü uygulama geliştirme,
kendini keşfet ve geliştir" name="keywords">

<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
```

```
<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">

<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vend
...

```

## Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
    ServerAlias *
    RewriteEngine On
    RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
    # Use HTTP Strict Transport Security to force client to use secure connections only
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

    # Further Configuration goes here
    [...]
</VirtualHost>

```

## External References

- [Wikipedia - HTTP Strict Transport Security](#)
- [Configure HSTS \(HTTP Strict Transport Security\) for Apache/Nginx](#)
- [HTTP Strict Transport Security \(HSTS\) HTTP Header](#)
- [Mozilla SSL Configuration Generator](#)



## CLASSIFICATION

|             |                          |
|-------------|--------------------------|
| OWASP 2013  | <a href="#">A6</a>       |
| OWASP 2017  | <a href="#">A3</a>       |
| SANS Top 25 | <a href="#">523</a>      |
| CAPEC       | <a href="#">217</a>      |
| WASC        | <a href="#">4</a>        |
| ISO27001    | <a href="#">A.14.1.2</a> |

# 8. Out-of-date Version (jQuery UI Autocomplete)

MEDIUM



1

Netsparker identified the target web site is using jQuery UI Autocomplete and detected that it is out of date.

## Impact

Since this is an old version of the software, it may be vulnerable to attacks.

### jQuery UI Autocomplete Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

## Affected Versions

1.12.0 to 1.12.1

## External References

- [CVE-2021-41182](#)

### jQuery UI Autocomplete Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `\*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `\*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `\*Text` options from untrusted sources.

## Affected Versions

1.12.0 to 1.12.1

## External References

- [CVE-2021-41183](#)

### jQuery UI Autocomplete Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

## Affected Versions

1.12.0 to 1.12.1

## External References

- [CVE-2021-41184](#)

## Vulnerabilities

### 8.1. <https://yazilimmuhendisim.com/phpmyadmin/>

#### Identified Version

- 1.12.1

#### Latest Version

- 1.12.1 (in this branch)

#### Vulnerability Database

- Result is based on 08/05/2022 18:00:00 vulnerability database content.

#### Certainty



#### Request

```
GET /phpmyadmin/ HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=en; phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9
Referer: https://yazilimmuhendisim.com/phpmyadmin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```



## Response

Response Time (ms) : 156,2569    Total Bytes Received : 15357    Body Length : 13222    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373e7b8bc5b3761-MXP
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
CF-Cache-Status: DYNAMIC
X-Robots-Tag: noindex, nofollow
Set-Cookie: phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: phpMyAdmin_https=8ar344b5guktllesql197use6f; path=/phpmyadmin/; secure; HttpOnly
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=tghJz4Xi4XgKoQdwe666VWNTcThD0dyQUBdmyRtty3z2Mt65G5bG9zd6nF95clYXZUwzmebsiP%2FHj7B6EjbM49h4XZT3LqJ1%2FQj1Yjy0ZqratV57unAdoY%2FI5tW1rMmLULwR229P9zM%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Pragma: no-cache
Server: cloudflare
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Expires: Sun, 07 Aug 2022 23:48:48 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-
...
```

## Remedy

Please upgrade your installation of jQuery UI Autocomplete to the latest stable version.

## Remedy References

- [Downloading jQuery UI Autocomplete](#)



**CLASSIFICATION**

|                          |                                  |
|--------------------------|----------------------------------|
| PCI DSS v3.2             | <a href="#">6.2</a>              |
| OWASP 2013               | <a href="#">A9</a>               |
| OWASP 2017               | <a href="#">A9</a>               |
| SANS Top 25              | <a href="#">829</a>              |
| CAPEC                    | <a href="#">310</a>              |
| HIPAA                    | <a href="#">164.308(A)(1)(I)</a> |
| OWASP Proactive Controls | <a href="#">C1</a>               |
| ISO27001                 | <a href="#">A.14.1.2</a>         |

# 9. Out-of-date Version (jQuery UI Dialog)

MEDIUM



1

Netsparker identified the target web site is using jQuery UI Dialog and detected that it is out of date.

## Impact

Since this is an old version of the software, it may be vulnerable to attacks.

### 🚩 jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

## Affected Versions

1.12.0 to 1.12.1

## External References

- [CVE-2021-41184](#)

### 🚩 jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `\*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `\*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `\*Text` options from untrusted sources.

## Affected Versions

1.12.0 to 1.12.1

## External References

- [CVE-2021-41183](#)

### 🚩 jQuery UI Dialog Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

## Affected Versions

1.12.0 to 1.12.1

## External References

- [CVE-2021-41182](#)

## Vulnerabilities

## 9.1. https://yazilimmuhendisim.com/phpmyadmin/

### Identified Version

- 1.12.1

### Latest Version

- 1.12.1 (in this branch)

### Vulnerability Database

- Result is based on 08/05/2022 18:00:00 vulnerability database content.

### Certainty



### Request

```
GET /phpmyadmin/ HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=en; phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9
Referer: https://yazilimmuhendisim.com/phpmyadmin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 156,2569    Total Bytes Received : 15357    Body Length : 13222    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373e7b8bc5b3761-MXP
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
CF-Cache-Status: DYNAMIC
X-Robots-Tag: noindex, nofollow
Set-Cookie: phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: phpMyAdmin_https=8ar344b5guktllesql197use6f; path=/phpmyadmin/; secure; HttpOnly
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=tghJz4Xi4XgKoQdwe666VWNTcThD0dyQUBdmyRtty3z2Mt65G5bG9zd6nF95clYXZUwzmebsiP%2FHj7B6EjbM49h4XZT3LqJ1%2FQj1Yjy0ZqratV57unAdoY%2FI5tW1rMmLULwR229P9zM%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Pragma: no-cache
Server: cloudflare
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Expires: Sun, 07 Aug 2022 23:48:48 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-
...
```

## Remedy

Please upgrade your installation of jQuery UI Dialog to the latest stable version.

## Remedy References

- [Downloading jQuery UI Dialog](#)



**CLASSIFICATION**

|                          |                                  |
|--------------------------|----------------------------------|
| PCI DSS v3.2             | <a href="#">6.2</a>              |
| OWASP 2013               | <a href="#">A9</a>               |
| OWASP 2017               | <a href="#">A9</a>               |
| SANS Top 25              | <a href="#">829</a>              |
| CAPEC                    | <a href="#">310</a>              |
| HIPAA                    | <a href="#">164.308(A)(1)(I)</a> |
| OWASP Proactive Controls | <a href="#">C1</a>               |
| ISO27001                 | <a href="#">A.14.1.2</a>         |

# 10. Out-of-date Version (jQuery UI Tooltip)

MEDIUM 

1

Netsparker identified the target web site is using jQuery UI Tooltip and detected that it is out of date.

## Impact

Since this is an old version of the software, it may be vulnerable to attacks.

### jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.

## Affected Versions

1.12.0 to 1.12.1

## External References

- [CVE-2021-41182](#)

### jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.

## Affected Versions

1.12.0 to 1.12.1

## External References

- [CVE-2021-41184](#)

### jQuery UI Tooltip Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `\*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. The values passed to various `\*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `\*Text` options from untrusted sources.

## Affected Versions

1.12.0 to 1.12.1

## External References

- [CVE-2021-41183](#)

## Vulnerabilities

## 10.1. <https://yazilimmuhendisim.com/phpmyadmin/>

### Identified Version

- 1.12.1

### Latest Version

- 1.12.1 (in this branch)

### Vulnerability Database

- Result is based on 08/05/2022 18:00:00 vulnerability database content.

### Certainty



#### Request

```
GET /phpmyadmin/ HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=en; phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9
Referer: https://yazilimmuhendisim.com/phpmyadmin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```



## Response

Response Time (ms) : 156,2569    Total Bytes Received : 15357    Body Length : 13222    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373e7b8bc5b3761-MXP
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
CF-Cache-Status: DYNAMIC
X-Robots-Tag: noindex, nofollow
Set-Cookie: phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: phpMyAdmin_https=8ar344b5guktllesql197use6f; path=/phpmyadmin/; secure; HttpOnly
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=tghJz4Xi4XgKoQdwe666VWNTcThD0dyQUBdmyRtty3z2Mt65G5bG9zd6nF95clYXZUwzmebsiP%2FHj7B6EjbM49h4XZT3LqJ1%2FQj1Yjy0ZqratV57unAdoY%2FI5tW1rMmLULwR229P9zM%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Pragma: no-cache
Server: cloudflare
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Expires: Sun, 07 Aug 2022 23:48:48 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-
...
```

## Remedy

Please upgrade your installation of jQuery UI Tooltip to the latest stable version.

## Remedy References

- [Downloading jQuery UI Tooltip](#)



**CLASSIFICATION**

|                          |                                  |
|--------------------------|----------------------------------|
| PCI DSS v3.2             | <a href="#">6.2</a>              |
| OWASP 2013               | <a href="#">A9</a>               |
| OWASP 2017               | <a href="#">A9</a>               |
| SANS Top 25              | <a href="#">829</a>              |
| CAPEC                    | <a href="#">310</a>              |
| HIPAA                    | <a href="#">164.308(A)(1)(I)</a> |
| OWASP Proactive Controls | <a href="#">C1</a>               |
| ISO27001                 | <a href="#">A.14.1.2</a>         |

# 11. Out-of-date Version (jQuery)

MEDIUM



1

Netsparker identified the target web site is using jQuery and detected that it is out of date.

## Impact

Since this is an old version of the software, it may be vulnerable to attacks.

### 🚩 jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

## Affected Versions

1.9.0 to 3.4.1

## External References

- [CVE-2020-11022](#)

### 🚩 jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing `<option>` elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

## Affected Versions

1.9.0 to 3.4.1

## External References

- [CVE-2020-11023](#)

## Vulnerabilities

11.1. <https://yazilimmuhendisim.com/phpmyadmin/>

### Identified Version

- 3.4.1

### Latest Version

- 3.6.0 (in this branch)

### Vulnerability Database

- Result is based on 08/05/2022 18:00:00 vulnerability database content.

## Certainty



## Request

GET /phpmyadmin/ HTTP/1.1  
Host: yazilimmuhendisim.com  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: pma\_lang\_https=en; phpMyAdmin\_https=ipkpi80pqsrulbro0eolhrr0t9  
Referer: https://yazilimmuhendisim.com/phpmyadmin/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

## Response

Response Time (ms) : 156,2569    Total Bytes Received : 15357    Body Length : 13222    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373e7b8bc5b3761-MXP
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
CF-Cache-Status: DYNAMIC
X-Robots-Tag: noindex, nofollow
Set-Cookie: phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: phpMyAdmin_https=8ar344b5guktllesql197use6f; path=/phpmyadmin/; secure; HttpOnly
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=tghJz4Xi4XgKoQdwe666VWNTcThD0dyQUBdmyRtty3z2Mt65G5bG9zd6nF95clYXZUwzmebsiP%2FHj7B6EjbM49h4XZT3LqJ1%2FQj1Yjy0ZqratV57unAdoY%2FI5tW1rMmLULwR229P9zM%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Pragma: no-cache
Server: cloudflare
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Expires: Sun, 07 Aug 2022 23:48:48 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-
...
```

## Remedy

Please upgrade your installation of jQuery to the latest stable version.

## Remedy References

- [Downloading jQuery.](#)



## CLASSIFICATION

|                          |                                  |
|--------------------------|----------------------------------|
| PCI DSS v3.2             | <a href="#">6.2</a>              |
| OWASP 2013               | <a href="#">A9</a>               |
| OWASP 2017               | <a href="#">A9</a>               |
| SANS Top 25              | <a href="#">829</a>              |
| CAPEC                    | <a href="#">310</a>              |
| HIPAA                    | <a href="#">164.308(A)(1)(I)</a> |
| OWASP Proactive Controls | <a href="#">C1</a>               |
| ISO27001                 | <a href="#">A.14.1.2</a>         |

# 12. Weak Ciphers Enabled

MEDIUM



1

CONFIRMED



1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

## Impact

Attackers might decrypt SSL traffic between your server and your visitors.

## Vulnerabilities

12.1. <https://yazilimmuhendisim.com/>

**CONFIRMED**

### List of Supported Weak Ciphers

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA (0xC009)
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xC00A)
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 (0xC023)
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 (0xC024)

### Request

[NETSPARKER] SSL Connection

### Response

Response Time (ms) : 1    Total Bytes Received : 27    Body Length : 0    Is Compressed : No

[NETSPARKER] SSL Connection

## Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"  
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type regedt32 or type regedit, and then click OK.

b. In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56  
SCHANNEL\Ciphers\RC4 64/128  
SCHANNEL\Ciphers\RC4 40/128  
SCHANNEL\Ciphers\RC2 56/128  
SCHANNEL\Ciphers\RC2 40/128  
SCHANNEL\Ciphers\NULL  
SCHANNEL\Hashes\MD5
```

## Remedy

Configure your web server to disallow using weak ciphers.

## External References

- [OWASP - Insecure Configuration Management](#)
- [OWASP Top 10-2017 A3-Sensitive Data Exposure](#)
- [Zombie Poodle - Golden Doodle \(CBC\)](#)
- [Mozilla SSL Configuration Generator](#)
- [Strong Ciphers for Apache, Nginx and Lighttpd](#)





## CLASSIFICATION

|              |                          |
|--------------|--------------------------|
| PCI DSS v3.2 | <a href="#">6.5.4</a>    |
| OWASP 2013   | <a href="#">A6</a>       |
| OWASP 2017   | <a href="#">A3</a>       |
| SANS Top 25  | <a href="#">327</a>      |
| CAPEC        | <a href="#">217</a>      |
| WASC         | <a href="#">4</a>        |
| ISO27001     | <a href="#">A.14.1.3</a> |

## CVSS 3.0 SCORE

|               |              |
|---------------|--------------|
| Base          | 6,8 (Medium) |
| Temporal      | 6,8 (Medium) |
| Environmental | 6,8 (Medium) |

## CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

## CVSS 3.1 SCORE

|               |              |
|---------------|--------------|
| Base          | 6,8 (Medium) |
| Temporal      | 6,8 (Medium) |
| Environmental | 6,8 (Medium) |

**CVSS Vector String**

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

# 13. [Possible] Backup File Disclosure

LOW



1

Netsparker identified a possible backup file disclosure on the web server.

## Impact

Backup files can contain old or current versions of a file on the web server. This could include sensitive data such as password files or even the application's source code. This form of issue normally leads to further vulnerabilities or, at worst, sensitive information disclosure.

## Vulnerabilities

13.1. <https://yazilimmuhendisim.com/index.php/etc/index.php~>

## Certainty



### Request

```
GET /index.php/etc/index.php~ HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://yazilimmuhendisim.com/index.php/etc/index.php~
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 533,8397    Total Bytes Received : 19550    Body Length : 18798    Is Compressed : No

HTTP/1.1 200 OK  
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 7376200d2cc50f66-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=1q1Bj9aIpHNEw2xxv%2FN6jPwOVTLTW3inS1VxFSyC3QhHhN7kF8q8AP687P94V%2FVt4iJ0xUUFypn91MhyeLHvQiTiXNi3t8xSMayjwmVw9GhIbVoY4IDTKlA8rUvac5dQ20SMnXI0fYk%3D"}],"group":"cf-nel","max\_age":604800}  
NEL: {"success\_fraction":0,"report\_to":"cf-nel","max\_age":604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Mon, 08 Aug 2022 06:16:46 GMT  
Vary: Accept-Encoding

```
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<title>Yazılım Mühendisim - Profesyonel Yazılım Çözümleri</title>
<meta content="Biz güncel teknolojileri kullanarak mobil, masaüstü ve web uygulamaları geliştiriyoruz.
Teklif almak için bizimle iletişime geçebilirsiniz." name="description">
<meta content="yazılım,
yazılım mühendisi,
yazılım mühendisim,
android uygulama,
ios uygulama,
mobil uygulamalar,
mobil uygulama geliştirme,
mobil uygulama fiyatları,
mobil uygulama yapmak,
mobil uygulama kodlama,
mobil uygulama yapma,
mobil uygulama ajansı,
web sitesi,
web sitesi geliştirme,
masaüstü uygulama,
masaüstü uygulama geliştirme,
kendini keşfet ve geliştir" name="keywords">

<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
```


```
<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">

<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vendor
...

```

Remedy

Do not store backup files on production servers.

|   |  |
|---|--|
|  <b>CLASSIFICATION</b> |  |
| PCI DSS v3.2  | <a href="#">6.5.8</a>                  |
| OWASP 2013  | <a href="#">A7</a>                     |
| OWASP 2017  | <a href="#">A5</a>                     |
| SANS Top 25   | <a href="#">530</a>                    |
| CAPEC   | <a href="#">87</a>                     |
| WASC  | <a href="#">34</a>                     |
| HIPAA   | <a href="#">164.306(A), 164.308(A)</a> |
| ISO27001  | <a href="#">A.18.1.3</a>               |

# 14. [Possible] Cross-site Request Forgery

LOW



1

Netsparker identified a possible Cross-Site Request Forgery.

CSRF is a very common vulnerability. It's an attack which forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

## Impact

Depending on the application, an attacker can mount any of the actions that can be done by the user such as adding a user, modifying content, deleting data. All the functionality that's available to the victim can be used by the attacker. Only exception to this rule is a page that requires extra information that only the legitimate user can know (such as user's password).

## Vulnerabilities

### 14.1. <https://yazilimmuhendisim.com/>

#### Form Name(s)

- sentMessage

#### Certainty



#### Request

```
GET / HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1776,6294    Total Bytes Received : 19552    Body Length : 18798    Is Compressed : No

```
HTTP/1.1 200 OK
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
CF-RAY: 7373e3cb98dc83a9-MXP
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=zZ2ugAm3Cut09L1wv5cQk28lJW4%2BEm60PuhB4lQAVduIh2gGdjha003TfBu9MFxyPw0KTQar4g1iJNzEBFI%2FYcbu3v1Gjj73PtMXUoPLOXE%2BvfGcEsqS0f2nUVwjY00FNDF1UGhcc10%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Sun, 07 Aug 2022 23:46:07 GMT
Vary:
...
/a>
<a href="tel:+905070249033"><div class="phone">
<i class="bi bi-phone"></i>
<h4>Telefon Numarası:</h4>
<p>+90 507 024 90 33</p>
</div>
</a>
</div>
</div>
<div class="col-lg-8 mt-5 mt-lg-0">
<form name="sendMessage" id="contactForm" method="post" action="forms/mail/contact.php">
<div class="row">
<div class="col-md-6 form-group">
<input type="text" class="form-control" name="name" placeholder="Ad ve Soyad" requi
...
```

## Remedy

- Send additional information in each HTTP request that can be used to determine whether the request came from an authorized source. This "validation token" should be hard to guess for attacker who does not already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should reject the request.
- If you are posting form in ajax request, custom HTTP headers can be used to prevent CSRF because the browser prevents sites from sending custom HTTP headers to another site but allows sites to send custom HTTP headers to themselves using XMLHttpRequest.
  - For native XMLHttpRequest (XHR) object in JavaScript;

```
xhr = new XMLHttpRequest();  
xhr.setRequestHeader('custom-header', 'valueNULL');
```

For JQuery, if you want to add a custom header (or set of headers) to

a. **individual request**

```
$.ajax({  
  url: 'foo/bar',  
  headers: { 'x-my-custom-header': 'some value' }  
});
```

b. **every request**

```
$.ajaxSetup({  
  headers: { 'x-my-custom-header': 'some value' }  
});  
OR  
$.ajaxSetup({  
  beforeSend: function(xhr) {  
    xhr.setRequestHeader('x-my-custom-header', 'some value');  
  }  
});
```

#### External References

- [OWASP Cross-Site Request Forgery \(CSRF\)](#)

#### Remedy References

- [OWASP Cross-Site Request Forgery \(CSRF\) Prevention Cheat Sheet](#)





## CLASSIFICATION

|              |                            |
|--------------|----------------------------|
| PCI DSS v3.2 | <a href="#">6.5.9</a>      |
| OWASP 2013   | <a href="#">A8</a>         |
| OWASP 2017   | <a href="#">A5</a>         |
| SANS Top 25  | <a href="#">352</a>        |
| CAPEC        | <a href="#">62</a>         |
| WASC         | <a href="#">9</a>          |
| HIPAA        | <a href="#">164.306(A)</a> |
| ISO27001     | <a href="#">A.14.2.5</a>   |

# 15. [Possible] Internal IP Address Disclosure

LOW



1

Netsparker identified a Possible Internal IP Address Disclosure in the page.

It was not determined if the IP address was that of the system itself or that of an internal network.

## Impact

There is no direct impact; however, this information can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.

## Vulnerabilities

15.1. <https://yazilimmuhendisim.com/phpmyadmin/doc/html/setup.html>

### Extracted IP Address(es)

- 10.0.0.0
- 192.168.0.0
- 172.16.0.0
- 172.30.21.21
- 172.26.36.7
- 172.26.36.8
- 172.26.36.9
- 172.26.36.10

### Extracted IP Addresses

- 10.0.0.0
- 192.168.0.0
- 172.16.0.0
- 172.30.21.21
- 172.26.36.7
- 172.26.36.8
- 172.26.36.9
- 172.26.36.10

## Certainty



## Request

```
GET /phpmyadmin/doc/html/setup.html HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=hy; phpMyAdmin_https=ofkno9c3qlv9ebmnfq1av3ogt4
Referer: https://yazilimmuhendisim.com/phpmyadmin/doc/html/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 134,0336    Total Bytes Received : 129776    Body Length : 128993    Is Compressed : No

```
HTTP/1.1 200 OK
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
CF-RAY: 73744910bdcbbac9-MXP
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=IQ%2FDUN151C5kZpwX1%2Bgndr2FZAIKJFE6NE4PuaVFVuPWEKsfW3taXMPYvxiCpZJ0qKgoPQ57L9EokZmAohl8mBYugOMZevE9999HWieHdETXE5uUcUbZXjJTsjmg1DGPxiAhThauDc%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Last-Modified: Sat, 10 Oct 2020 03:18:10 GMT
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Content-Type: text/html
Transfer-Encoding: chunked
Content-Encoding:
Date: Mon, 08 Aug 2022 00:55:15 GMT
Vary:
...
"highlight-text notranslate"><div class="highlight"><pre><span></span>frontend http
bind *:80
option forwardfor
option http-server-close

### NETWORK restriction
acl LOCALNET src 10.0.0.0/8 192.168.0.0/16 172.16.0.0/12

# /phpmyadmin
acl phpmyadmin path_dir /phpmyadmin
use_backend phpmyadmin if phpmyadmin LOCALNET

backend phpmyadmin
mode http


requirep ^(GET|POST|HEAD)\ /phpmyadmin/(.*) \1 \2

# phpMyAdmin container IP
server localhost 172.30.21.21:80
</pre></div>
</div>
<p>When using traefik, something like following should work:</p>
<div class="highlight-text notranslate"><div class="highlight"><pre><span></span>defaultEntryPoints =
[&quot;ht
...
"l l-Scalar l-Scalar-Plain">8000:80</span>
<span class="nt">environment</span><span class="p">:</span></span>
<span class="p p-Indicator"></span> <span class="l l-Scalar l-Scalar-Plain">PMA_HOSTS=172.26.36.7,172.
26.36.8,172.26.36.9,172.26.36.10</span></span>
```

```
<span class="p p-Indicator">-</span> <span class="l l-Scalar l-Scalar-Plain">PMA_VERBOSE=production-db
1,production-db2,dev-db1,dev-db2</span>
<span class="p p-Indicator">-</span>
...
```

**Remedy**

First, ensure this is not a false positive. Due to the nature of the issue, Netsparker could not confirm that this IP address was actually the real internal IP address of the target web server or internal network. If it is, consider removing it.

|   |                          |
|---|--------------------------|
|  <b>CLASSIFICATION</b> |                          |
| OWASP 2013  | <a href="#">A6</a>       |
| OWASP 2017  | <a href="#">A3</a>       |
| SANS Top 25   | <a href="#">200</a>      |
| ISO27001  | <a href="#">A.18.1.4</a> |

# 16. [Possible] Phishing by Navigating Browser Tabs

LOW



1

Netsparker identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"` can modify `window.opener.location` and replace the parent webpage with something else, even on a different origin.

## Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"` attribute, a third party site can change the URL of the source tab using `window.opener.location.assign` and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

## Vulnerabilities

### 16.1. <https://yazilimmuhendisim.com/>

#### External Links

- <https://www.linkedin.com/in/alperragib/>
- <https://bionluk.com/yazilimmuhendisim>
- <https://www.facebook.com/yazilimmuhendisim/>
- <https://www.instagram.com/yazilimmuhendisim/>
- <https://www.linkedin.com/company/yazilimmuhendisim>

## Certainty

### Request

```
GET / HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1776,6294    Total Bytes Received : 19552    Body Length : 18798    Is Compressed : No

```
HTTP/1.1 200 OK
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
CF-RAY: 7373e3cb98dc83a9-MXP
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=zZ2ugAm3Cut09L1wv5cQk281jW4%2BE60PuhB4lQAVduIh2gGdjha003TfBu9MFxyPw0KTQar4g1iJNzEBFI%2FYcbu3v1Gjj73PtMXUoPLOXE%2BvfGcEsqS0f2nUVwjY00FNDF1UGhcc10%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Sun, 07 Aug 2022 23:46:07 GMT
Vary:
...
mdir</h3>
<p>Yazılım Mühendisim, tecrübeli ekibiyle profesyonel yazılım çözümleri üreten bir kuruluştur. </p>
</div>
<div class="row content">
<div class="col-lg-6">
<p>
Yazılım Mühendisim, <a href="https://www.linkedin.com/in/alperragib/" target="_blank">Alper Ragıb</a> t
arafından Ocak 2019 tarihinde kurulmuştur. Yazılım Mühendisim'in en önemli ilkeleri aşağıda listelenmiş
tir.
</p>
<ul>
<li><i class="ri-check-double-line"></i> Projey
...
ydınlatma Metni</a>
<div class="copyright">
&copy; Copyright <strong><span>Yazılım Mühendisim</span></strong>.
</div>
</div>
<div class="social-links text-center text-md-right pt-3 pt-md-0">
<a href="https://bionluk.com/yazilimmuhendisim" target="_blank" class="twitter"><i><b>bi</b></i></a>
<a href="https://www.facebook.com/yazilimmuhendisim/" target="_blank" class="facebook"><i class="bx bxl
-facebook"></i></a>
<a href="https://www.instagram.com/yazilimmuhendisim/" target="_blank" class="instagram"><i class="bx b
xl-instagram"></i></a>
<a href="https://www.linkedin.com/company/yazilimmuhendisim" target="_blank" class="linkedin"><i class
="bx bxl-linkedin"></i></a>
</div>
</div>
</footer>
<a href="#" class="back-to-top d-flex align-items-center justify-content-center"><i class="bi bi-arrow-
```

up  
...


Remedy

- Add rel=noopener to the linksto prevent pages from abusing window.opener. This ensures that the page cannot access the window.openerproperty in Chrome and Opera browsers.
- For older browsers and in Firefox, you can add rel=noreferrerwhich additionally disables the Referer header.

```
<a href="..." target="_blank" rel="noopener noreferrer">...</a>
```

External References

- [Reverse Tabnabbing](#)
- [Blankshield & Reverse Tabnabbing Attacks](#)
- [Target=" blank" - the most underestimated vulnerability ever](#)

|  |                          |
|--|--------------------------|
|  <b>CLASSIFICATION</b> |                          |
| OWASP 2013   | <a href="#">A5</a>       |
| OWASP 2017   | <a href="#">A6</a>       |
| SANS Top 25  | <a href="#">16</a>       |
| WASC   | <a href="#">15</a>       |
| ISO27001   | <a href="#">A.14.1.2</a> |



# 17. Insecure Frame (External)

LOW



1

CONFIRMED



1

Netsparker identified an external insecure or misconfigured iframe.

## Impact

IFrame sandboxing enables a set of additional restrictions for the content within a frame in order to restrict its potentially malicious code from causing harm to the web page that embeds it.

The Same Origin Policy (SOP) will prevent JavaScript code from one origin from accessing properties and functions - as well as HTTP responses - of different origins. The access is only allowed if the protocol, port and also the domain match exactly.

Here is an example, the URLs below all belong to the same origin as *http://site.com*:

*http://site.com*  
*http://site.com/*  
*http://site.com/my/page.html*

Whereas the URLs mentioned below aren't from the same origin as *http://site.com*:

*http://www.site.com* (a sub domain)  
*http://site.org* (different top level domain)  
*https://site.com* (different protocol)  
*http://site.com:8080* (different port)

When the `sandbox` attribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
- Forms are disabled. The hosted content is not allowed to make forms post back to any target.
- Scripts are disabled. JavaScript is disabled and will not execute.
- Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
- Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the `sandbox` attribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

- It might trick the user into supplying a username and password to the site loaded inside the iframe.
- It might navigate the parent window to a phishing page.
- It might execute untrusted code.
- It could show a popup, appearing to come from the parent site.

Sandbox containing a value of :

- allow-same-origin will not treat it as a unique origin.
- allow-top-navigation will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.
- allow-forms will allow form submissions from inside the iframe.
- allow-popups will allow popups.
- allow-scripts will allow malicious script execution however it won't allow to create popups.

## Vulnerabilities

### 17.1. <https://yazilimmuhendisim.com/>

#### CONFIRMED

#### Frame Source(s)

- <https://newassets.hcaptcha.com/captcha/v1/750f21b/static/hcaptcha.html#frame=checkbox&id=06emps6ugze&host=yazilimmuhendisim.com/f71a-4baf-8518-b36d4fce129e&theme=light>
- <https://newassets.hcaptcha.com/captcha/v1/750f21b/static/hcaptcha.html#frame=challenge&id=06emps6ugze&host=yazilimmuhendisim.com/f71a-4baf-8518-b36d4fce129e&theme=light>

#### Parsing Source

- DOM Parser

#### Request

```
GET / HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1776,6294    Total Bytes Received : 19552    Body Length : 18798    Is Compressed : No

HTTP/1.1 200 OK  
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 7373e3cb98dc83a9-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=zZ2ugAm3Cut09L1wv5cQk281jW4%2BEm60PuhB4lQAVduIh2gGdjha003TFBu9MFxyPw0KTQar4g1iJNzEBFI%2FYcbu3v1Gjj73PtMXUoPLOXE%2BvfGcEsqS0f2nUVwjY00FNDFlUGhcc10%3D"}],"group":"cf-nel","max\_age":604800}  
NEL: {"success\_fraction":0,"report\_to":"cf-nel","max\_age":604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Sun, 07 Aug 2022 23:46:07 GMT  
Vary: Accept-Encoding

```
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<title>Yazılım Mühendisim - Profesyonel Yazılım Çözümleri</title>
<meta content="Biz güncel teknolojileri kullanarak mobil, masaüstü ve web uygulamaları geliştiriyoruz.
Teklif almak için bizimle iletişime geçebilirsiniz." name="description">
<meta content="yazılım,
yazılım mühendisi,
yazılım mühendisim,
android uygulama,
ios uygulama,
mobil uygulamalar,
mobil uygulama geliştirme,
mobil uygulama fiyatları,
mobil uygulama yapmak,
mobil uygulama kodlama,
mobil uygulama yapma,
mobil uygulama ajansı,
web sitesi,
web sitesi geliştirme,
masaüstü uygulama,
masaüstü uygulama geliştirme,
kendini keşfet ve geliştir" name="keywords">

<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
```

```
<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">

<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vend
...

```

## Remedy

- Apply sandboxing in inline frame

```
<iframe sandbox src="framed-page-url"></iframe>
```

- For untrusted content, avoid the usage of seamless attribute and allow-top-navigation, allow-popups and allow-scripts in sandbox attribute.

## External References

- [HTML5 Security Cheat Sheet](#)

## Remedy References

- [How to Safeguard your Site with HTML5 Sandbox](#)
- [Play safely in sandboxed IFrames](#)



### CLASSIFICATION

|             |                          |
|-------------|--------------------------|
| OWASP 2017  | <a href="#">A6</a>       |
| SANS Top 25 | <a href="#">16</a>       |
| WASC        | <a href="#">15</a>       |
| ISO27001    | <a href="#">A.14.1.2</a> |

# 18. Insecure Transportation Security Protocol Supported (TLS 1.0)

LOW



1

CONFIRMED



1

Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 are considered non-compliant by PCI since 30 June 2018.

## Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

## Vulnerabilities

18.1. <https://yazilimmuhendisim.com/>

CONFIRMED

Request

[NETSPARKER] SSL Connection

Response

Response Time (ms) : 1    Total Bytes Received : 27    Body Length : 0    Is Compressed : No

[NETSPARKER] SSL Connection

## Actions to Take

We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

## Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod\_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive `ssl_protocols` in the `nginx.conf` file and remove TLSv1.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
  1. Click on Start and then Run, type `regedt32` or `regedit`, and then click OK.
  2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\
```

3. Locate a key named `Server` or create if it doesn't exist.
  4. Under the `Server` key, locate a `DWORD` value named `Enabled` or create if it doesn't exist and set its value to "0".
- For `lighttpd`, put the following lines in your configuration file:

```
ssl.use-ssl2 = "disable"  
ssl.use-ssl3 = "disable"  
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up  
ssl.ec-curve = "secp384r1"
```

## External References

- [How to Disable TLS v1.0](#)
- [OWASP - Insecure Configuration Management](#)
- [OWASP Top 10 - 2017 A3 - Sensitive Data Exposure](#)
- [How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services](#)
- [IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012](#)
- [Date Change for Migrating from SSL and Early TLS](#)
- [Browser Exploit Against SSL/TLS Attack \(BEAST\)](#)
- [Are You Ready for 30 June 2018? Saying Goodbye to SSL/early TLS](#)



## CLASSIFICATION

|              |                          |
|--------------|--------------------------|
| PCI DSS v3.2 | <a href="#">6.5.4</a>    |
| OWASP 2013   | <a href="#">A6</a>       |
| OWASP 2017   | <a href="#">A3</a>       |
| SANS Top 25  | <a href="#">326</a>      |
| CAPEC        | <a href="#">217</a>      |
| WASC         | <a href="#">4</a>        |
| HIPAA        | <a href="#">164.306</a>  |
| ISO27001     | <a href="#">A.14.1.3</a> |

# 19. Internal Server Error

LOW



1

CONFIRMED



1

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

## Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

## Vulnerabilities

### 19.1. <https://yazilimmuhendisim.com/forms/mail/lib/SendGrid.php>

**CONFIRMED**

#### Request

```
GET /forms/mail/lib/SendGrid.php HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://yazilimmuhendisim.com/forms/mail/lib/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```



## Response

Response Time (ms) : 233,582    Total Bytes Received : 734    Body Length : 0    Is Compressed : No

### HTTP/1.1 500 Internal Server Error

alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 737433b7ed54e8eb-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=gvF3ASi64lSEntw2hGJ%2FyXngBQkeAGfDnXIzdjtyStEFhuUzhJv09fWDP7NMcuSQ%2F4e9TLG6hzoBn2THTu%2FVhC6JtIbilk10I%2BfLI1jqIyS3%2FeiZKbWkGylDEWKGJ770Qx08c5Tnmc%3D"}], "group": "cf-nel", "max\_age": 604800}  
NEL: {"success\_fraction": 0, "report\_to": "cf-nel", "max\_age": 604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Date: Mon, 08 Aug 2022 00:40:40 GMT

## Remedy

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.



### CLASSIFICATION

SANS Top 25

[550](#)

WASC

[13](#)

ISO27001

[A.14.1.2](#)

# 20. Missing Content-Type Header

LOW



1

Netsparker detected a missing Content-Typeheader which means that this website could be at risk of a MIME-sniffing attacks.

## Impact

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.

This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.

The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.

## Vulnerabilities

20.1. <https://yazilimmuhendisim.com/assets/img/portfolio/mettrainigclubv2/1.webp>

## Certainty



Request

GET /assets/img/portfolio/mettrainigclubv2/1.webp HTTP/1.1  
Host: yazilimmuhendisim.com  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Referer: https://yazilimmuhendisim.com/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

Response

Response Time (ms) : 4463,1863    Total Bytes Received : 1357    Body Length : 528    Is Compressed : No

Binary response detected, response has not saved.

Remedy

- 1. When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served. For example, if you are serving an HTML page, you should send the HTTP header:

Content-Type: text/html

- 2. Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.

X-Content-Type-Options: nosniff

External References

- [MIME Sniffing: feature or vulnerability?](#)
- [X-Content-Type-Options HTTP Header](#)



CLASSIFICATION

|             |                          |
|-------------|--------------------------|
| OWASP 2013  | <a href="#">A5</a>       |
| OWASP 2017  | <a href="#">A6</a>       |
| SANS Top 25 | <a href="#">16</a>       |
| WASC        | <a href="#">15</a>       |
| ISO27001    | <a href="#">A.14.1.2</a> |

# 21. Missing X-Frame-Options Header

LOW



1

Netsparker detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

## Impact

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

## Vulnerabilities

21.1. <https://yazilimmuhendisim.com/>

## Certainty



### Request

```
GET / HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1776,6294    Total Bytes Received : 19552    Body Length : 18798    Is Compressed : No

HTTP/1.1 200 OK  
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 7373e3cb98dc83a9-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=zZ2ugAm3Cut09L1wv5cQk281jW4%2BEm60PuhB4lQAVduIh2gGdjha003TFBu9MFxyPw0KTQar4g1iJNzEBFI%2FYcbu3v1Gjj73PtMXUoPLOXE%2BvfGcEsqS0f2nUVwjY00FNDFlUGhcc10%3D"}],"group":"cf-nel","max\_age":604800}  
NEL: {"success\_fraction":0,"report\_to":"cf-nel","max\_age":604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Sun, 07 Aug 2022 23:46:07 GMT  
Vary: Accept-Encoding

```
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<title>Yazılım Mühendisim - Profesyonel Yazılım Çözümleri</title>
<meta content="Biz güncel teknolojileri kullanarak mobil, masaüstü ve web uygulamaları geliştiriyoruz.
Teklif almak için bizimle iletişime geçebilirsiniz." name="description">
<meta content="yazılım,
yazılım mühendisi,
yazılım mühendisim,
android uygulama,
ios uygulama,
mobil uygulamalar,
mobil uygulama geliştirme,
mobil uygulama fiyatları,
mobil uygulama yapmak,
mobil uygulama kodlama,
mobil uygulama yapma,
mobil uygulama ajansı,
web sitesi,
web sitesi geliştirme,
masaüstü uygulama,
masaüstü uygulama geliştirme,
kendini keşfet ve geliştir" name="keywords">

<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
```

```
<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">

<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vend
...

```

## Remedy

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
  - X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.
  - X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.
  - X-Frame-Options: ALLOW-FROM *URL* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

## External References

- [Clickjacking](#)
- [Can I Use X-Frame-Options](#)
- [X-Frame-Options HTTP Header](#)

## Remedy References

- [Clickjacking Defense Cheat Sheet](#)



### CLASSIFICATION

|             |                          |
|-------------|--------------------------|
| OWASP 2013  | <a href="#">A5</a>       |
| OWASP 2017  | <a href="#">A6</a>       |
| SANS Top 25 | <a href="#">693</a>      |
| CAPEC       | <a href="#">103</a>      |
| ISO27001    | <a href="#">A.14.2.5</a> |

# 22. Content Security Policy (CSP) Not Implemented

## BEST PRACTICE

1

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src**: Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the `unsafe-eval` and `unsafe-inline` keywords.
- **base-uri**: Base element is used to resolve relative URL to absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to `base-href` attribute of the document.
- **frame-ancestors**: It is very similar to `X-Frame-Options` HTTP header. It defines the URLs by which the page can be loaded in an `iframe`.
- **frame-src / child-src**: `frame-src` is the deprecated version of `child-src`. Both define the sources that can be loaded by `iframe` in the page. (Please note that `frame-src` was brought back in CSP 3)
- **object-src**: Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for `XMLHttpRequest` and `WebSocket` objects.
- **default-src**: It is a fallback for the directives that mostly ends with `-src` suffix. When the directives below are not defined, the value set to `default-src` will be used instead:
  - `child-src`
  - `connect-src`
  - `font-src`
  - `img-src`
  - `manifest-src`
  - `media-src`
  - `object-src`
  - `script-src`
  - `style-src`

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self**: Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as `eval()`.

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://\*.example.com;
```

```
Content-Security-Policy: script-src https://example.com:\*;
```

```
Content-Security-Policy: script-src https;;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

**Impact**

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out this extra layer of security.

**Vulnerabilities**

22.1. <https://yazilimmuhendisim.com/>

**Certainty**



**Request**

GET / HTTP/1.1  
Host: yazilimmuhendisim.com  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker



## Response

Response Time (ms) : 1776,6294    Total Bytes Received : 19552    Body Length : 18798    Is Compressed : No

HTTP/1.1 200 OK  
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 7373e3cb98dc83a9-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=zZ2ugAm3Cut09L1wv5cQk281jW4%2BEm60PuhB4lQAVduIh2gGdjha003TfBu9MFxyPw0KTQar4g1iJNzEBFI%2FYcbu3v1Gjj73PtMXUoPLOXE%2BvfGcEsqS0f2nUVwjY00FNDFlUGhcc10%3D"}],"group":"cf-nel","max\_age":604800}  
NEL: {"success\_fraction":0,"report\_to":"cf-nel","max\_age":604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Sun, 07 Aug 2022 23:46:07 GMT  
Vary: Accept-Encoding

```
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<title>Yazılım Mühendisim - Profesyonel Yazılım Çözümleri</title>
<meta content="Biz güncel teknolojileri kullanarak mobil, masaüstü ve web uygulamaları geliştiriyoruz.
Teklif almak için bizimle iletişime geçebilirsiniz." name="description">
<meta content="yazılım,
yazılım mühendisi,
yazılım mühendisim,
android uygulama,
ios uygulama,
mobil uygulamalar,
mobil uygulama geliştirme,
mobil uygulama fiyatları,
mobil uygulama yapmak,
mobil uygulama kodlama,
mobil uygulama yapma,
mobil uygulama ajansı,
web sitesi,
web sitesi geliştirme,
masaüstü uygulama,
masaüstü uygulama geliştirme,
kendini keşfet ve geliştir" name="keywords">

<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
```

```
<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">

<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vend
...

```

Actions to Take


- Enable CSP on your website by sending the Content-Security-Policyin HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Netsparker identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the Content-Security-Policyin HTTP response headers that instruct the browser to apply the policies you specified.

External References

- [An Introduction to Content Security Policy](#).
- [Content Security Policy \(CSP\) HTTP Header](#)
- [Content Security Policy \(CSP\)](#).

|   |                          |
|---|--------------------------|
|  <b>CLASSIFICATION</b> |                          |
| SANS Top 25   | <a href="#">16</a>       |
| WASC  | <a href="#">15</a>       |
| ISO27001  | <a href="#">A.14.2.5</a> |

# 23. Expect-CT Not Enabled

BEST PRACTICE



1

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissued certificates to be used.

## Vulnerabilities

23.1. <https://yazilimmuhendisim.com/cdn-cgi/l/email-protection#ea938b9083868387879f828f848e83998387aa8d878b8386c4898587>

## Certainty



### Request

```
GET /cdn-cgi/l/email-protection#ea938b9083868387879f828f848e83998387aa8d878b8386c4898587 HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://yazilimmuhendisim.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 93,764    Total Bytes Received : 4972    Body Length : 4698    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Type-Options: nosniff
Server: cloudflare
CF-RAY: 7373e739981f59e3-MXP
Connection: keep-alive
X-Frame-Options: DENY
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Sun, 07 Aug 2022 23:48:27 GMT

<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Email Protection | Cloudflare</title>
<meta charset="UTF-8" />
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<meta http-equiv="X-UA-Compatible" content="IE=Edge" />
<meta name="robots" content="noindex, nofollow" />
<meta name="viewport" content="width=device-width,initial-scale=1" />
<link rel="stylesheet" id="cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" />
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/cf.errors.ie.css" />
<![endif]-->
<style>body{margin:0;padding:0}</style>

<!--[if gte IE 10]><!-->
<script>
if (!navigator.cookieEnabled) {
window.addEventListener('DOMContentLoaded', function () {
var cookieEl = document.getElementById('cookie-alert');
cookieEl.style.display = 'block';
})
}
</script>
<!--<![endif]-->

</head>
<body>
<div id="cf-wrapper">
<div class="cf-alert cf-alert-error cf-cookie-error" id="cookie-alert" data-translate="enable_cookies">
Please enable cookies.</div>
<div id="cf-error-details" class="cf-error-details-wrapper">
```

```

<div class="cf-wrapper cf-header cf-error-overview">
<h1 data-translate="block_headline">Email Protection</h1>
<h2 class="cf-subheadline"><span data-translate="unable_to_access">You are unable to access this email
  address</span> yazilimmuhendisim.com</h2>
</div><!-- /.header -->

<div class="cf-sect
...

```

## Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode** first. If everything goes well and your certificate is ready, go with the Expect-CT enforce mode. To use **report-only mode** first, omit **enforce** flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

## External References

- [Expect-CT Extension for HTTP](#)
- [Expect-CT HTTP Header](#)
- [Expect-CT Header](#)



### CLASSIFICATION

SANS Top 25

[16](#)

WASC

[15](#)

ISO27001

[A.14.1.2](#)

# 24. Insecure Transportation Security Protocol Supported (TLS 1.1)

BEST PRACTICE

1

CONFIRMED

1

Netsparker detected that a deprecated, insecure transportation security protocol (TLS 1.1) is supported by your web server.

TLS 1.1 will be considered as deprecated by major web browsers (i.e. Chrome, Firefox, Safari, Edge, Internet Explorer) starting in 2020.

### Impact

Your website will be inaccessible due to web browser deprecation.

### Vulnerabilities

24.1. <https://yazilimmuhendisim.com/>

CONFIRMED

Request

[NETSPARKER] SSL Connection

Response

Response Time (ms) : 1    Total Bytes Received : 27    Body Length : 0    Is Compressed : No

[NETSPARKER] SSL Connection

### Actions to Take

We recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher. See Remedy section for more details.

### Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod\_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```

- For Nginx, locate any use of the directive ssl\_protocols in the nginx.conf file and remove TLSv1.1.

```
ssl_protocols TLSv1.2;
```

- For Microsoft IIS, you should make some changes on the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**
  1. Click on Start and then Run, type regedt32 or regedit, and then click OK.
  2. In Registry Editor, locate the following registry key or create if it does not exist:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\
```

3. Locate a key named Server or create if it doesn't exist.
  4. Under the Server key, locate a DWORD value named Enabled or create if it doesn't exist and set its value to "0".
- For lighttpd, put the following lines in your configuration file:

```
ssl.use-ssl2 = "disable"  
ssl.use-ssl3 = "disable"  
ssl.openssl.ssl-conf-cmd = ("Protocol" => "-TLSv1.1, -TLSv1, -SSLv3") # v1.4.48 or up  
ssl.ec-curve = "secp384r1"
```

## External References

- [Deprecating TLSv1.0 and TLSv1.1 draft-ietf-tls-oldversions-deprecate-00](#)
- [Google Security Blog: Modernizing Transport Security](#)
- [OWASP - Insecure Configuration Management](#)
- [OWASP Top 10 - 2017 A3 - Sensitive Data Exposure](#)
- [IIS Crypto is a free tool that gives administrators the ability to enable or disable protocols, ciphers, hashes and key exchange algorithms on Windows Server 2003, 2008 and 2012](#)
- [Date Change for Migrating from SSL and Early TLS](#)



## CLASSIFICATION

|              |                          |
|--------------|--------------------------|
| PCI DSS v3.2 | <a href="#">6.5.4</a>    |
| OWASP 2013   | <a href="#">A6</a>       |
| OWASP 2017   | <a href="#">A3</a>       |
| SANS Top 25  | <a href="#">326</a>      |
| CAPEC        | <a href="#">217</a>      |
| WASC         | <a href="#">4</a>        |
| HIPAA        | <a href="#">164.306</a>  |
| ISO27001     | <a href="#">A.14.1.3</a> |



# 25. Missing X-XSS-Protection Header

BEST PRACTICE



1

Netsparker detected a missing X-XSS-Protectionheader which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

### Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

### Vulnerabilities

25.1. <https://yazilimmuhendisim.com/>

### Certainty



**Request**  
GET / HTTP/1.1  
Host: yazilimmuhendisim.com  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

## Response

Response Time (ms) : 1776,6294    Total Bytes Received : 19552    Body Length : 18798    Is Compressed : No

HTTP/1.1 200 OK  
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 7373e3cb98dc83a9-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=zZ2ugAm3Cut09L1wv5cQk281jW4%2BEm60PuhB4lQAVduIh2gGdjha003TFBu9MFxyPw0KTQar4g1iJNzEBFI%2FYcbu3v1Gjj73PtMXUoPLOXE%2BvfGcEsqS0f2nUVwjY00FNDFlUGhcc10%3D"}], "group": "cf-nel", "max\_age": 604800}  
NEL: {"success\_fraction": 0, "report\_to": "cf-nel", "max\_age": 604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Sun, 07 Aug 2022 23:46:07 GMT  
Vary: Accept-Encoding

```
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<title>Yazılım Mühendisim - Profesyonel Yazılım Çözümleri</title>
<meta content="Biz güncel teknolojileri kullanarak mobil, masaüstü ve web uygulamaları geliştiriyoruz.
Teklif almak için bizimle iletişime geçebilirsiniz." name="description">
<meta content="yazılım,
yazılım mühendisi,
yazılım mühendisim,
android uygulama,
ios uygulama,
mobil uygulamalar,
mobil uygulama geliştirme,
mobil uygulama fiyatları,
mobil uygulama yapmak,
mobil uygulama kodlama,
mobil uygulama yapma,
mobil uygulama ajansı,
web sitesi,
web sitesi geliştirme,
masaüstü uygulama,
masaüstü uygulama geliştirme,
kendini keşfet ve geliştir" name="keywords">

<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
```

```
<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">

<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vend
...

```

Remedy

Add the X-XSS-Protection header with a value of "1; mode= block".

- X-XSS-Protection: 1; mode=block

External References

- [Internet Explorer 8 Security Features - MSDN](#)
- [X-XSS-Protection HTTP Header](#)
- [Internet Explorer 8 XSS Filter](#)



CLASSIFICATION

|             |                            |
|-------------|----------------------------|
| SANS Top 25 | <a href="#">16</a>         |
| WASC        | <a href="#">15</a>         |
| HIPAA       | <a href="#">164.308(A)</a> |
| ISO27001    | <a href="#">A.14.2.5</a>   |

# 26. Referrer-Policy Not Implemented

BEST PRACTICE



1

Netsparker detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

## Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

## Vulnerabilities

26.1. <https://yazilimmuhendisim.com/>

## Certainty



### Request

```
GET / HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 1776,6294    Total Bytes Received : 19552    Body Length : 18798    Is Compressed : No

HTTP/1.1 200 OK  
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 7373e3cb98dc83a9-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=zZ2ugAm3Cut09L1wv5cQk281jW4%2BEm60PuhB4lQAVduIh2gGdjha003TfBu9MFxyPw0KTQar4g1iJNzEBFI%2FYcbu3v1Gjj73PtMXUoPLOXE%2BvfGcEsqS0f2nUVwjY00FNDF1UGhcc10%3D"}], "group": "cf-nel", "max\_age": 604800}  
NEL: {"success\_fraction": 0, "report\_to": "cf-nel", "max\_age": 604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Sun, 07 Aug 2022 23:46:07 GMT  
Vary: Accept-Encoding

```
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<title>Yazılım Mühendisim - Profesyonel Yazılım Çözümleri</title>
<meta content="Biz güncel teknolojileri kullanarak mobil, masaüstü ve web uygulamaları geliştiriyoruz.
Teklif almak için bizimle iletişime geçebilirsiniz." name="description">
<meta content="yazılım,
yazılım mühendisi,
yazılım mühendisim,
android uygulama,
ios uygulama,
mobil uygulamalar,
mobil uygulama geliştirme,
mobil uygulama fiyatları,
mobil uygulama yapmak,
mobil uygulama kodlama,
mobil uygulama yapma,
mobil uygulama ajansı,
web sitesi,
web sitesi geliştirme,
masaüstü uygulama,
masaüstü uygulama geliştirme,
kendini keşfet ve geliştir" name="keywords">

<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
```

```
<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">

<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vend
...
```

## Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading"></a>
```

## Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the rel attribute.

## External References

- [Referrer Policy](#)
- [Referrer Policy - MDN](#)
- [Referrer Policy HTTP Header](#)
- [A New Security Header: Referrer Policy](#)
- [Can I Use Referrer-Policy](#)



## CLASSIFICATION

|             |                                 |
|-------------|---------------------------------|
| OWASP 2013  | <a href="#"><u>A6</u></a>       |
| OWASP 2017  | <a href="#"><u>A3</u></a>       |
| SANS Top 25 | <a href="#"><u>200</u></a>      |
| ISO27001    | <a href="#"><u>A.14.2.5</u></a> |

# 27. SameSite Cookie Not Implemented

BEST PRACTICE

💡

1

Cookies are typically sent to third parties in cross origin requests. This can be abused to do CSRF attacks. Recently a new cookie attribute named *SameSite* was proposed to disable third-party usage for some cookies, to prevent CSRF attacks.

Same-site cookies allow servers to mitigate the risk of CSRF and information leakage attacks by asserting that a particular cookie should only be sent with requests initiated from the same registrable domain.

## Vulnerabilities

### 27.1. <https://yazilimmuhendisim.com/phpmyadmin/js/whitelist.php?v=5.0.3>

| Method | Parameter | Value |
|--------|-----------|-------|
| GET    | v         | 5.0.3 |

#### Identified Cookie(s)

- phpMyAdmin\_https

#### Cookie Source

- HTTP Header

#### Certainty



Request

GET /phpmyadmin/js/whitelist.php?v=5.0.3 HTTP/1.1  
Host: yazilimmuhendisim.com  
Accept: /\*/\*  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5,en-US,en;q=0.9  
Cache-Control: no-cache  
Cookie: pma\_lang\_https=en; phpMyAdmin\_https=8ar344b5guktl1lesql197use6f  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker



## Response

Response Time (ms) : 156,1274    Total Bytes Received : 3204    Body Length : 2000    Is Compressed : No

```
HTTP/1.1 200 OK
X-ob_mode: 1
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Cache-Control: private, max-age=10800
Set-Cookie: phpMyAdmin_https=8ar344b5guktl1lesql197use6f; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
CF-RAY: 7373ea91aadb5a43-MXP
Server: cloudflare
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=FBPVjPA011POU7zZcfvROMcAMZjfPkgKJXhQoi12WSSiv774jefQIHZyqkxyzJ%2BA91TnRmT%2BwonQc%2BTazUAPs7GtHfwxFGkbn8GgQnRhQ0yzy13UNMeAqEUVQ4MGIVm31ugUwMZtxkU%3D"}],"group":"cf-nel","max_age":604800}
Connection: keep-alive
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Vary: Accept-Encoding
Content-Length: 478
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sat, 10 Oct 2020 03:18:10 GMT
Content-Type: text/javascript; charset=UTF-8
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Date: Sun, 07 HTTP/1.1 200 OK
X-ob_mode: 1
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Cache-Control: private, max-age=10800
Set-Cookie: phpMyAdmin_https=8ar344b5guktl1lesql197use6f; path=/phpmyadmin/; secure; HttpOnly

Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/ph
...
```

## Remedy

The server can set a same-site cookie by adding the `SameSite=...` attribute to the `Set-Cookie` header. There are three possible values for the `SameSite` attribute:

- **Lax:** In this mode, the cookie will only be sent with a top-level get request.

```
Set-Cookie: key=value; SameSite=Lax
```

- Strict: In this mode, the cookie will not be sent with any cross-site usage even if the user follows a link to another website.

```
Set-Cookie: key=value; SameSite=Strict
```

- None: In this mode, the cookie will be sent with the cross-site requests. Cookies with SameSite=None must also specify the Secure attribute to transfer them via a secure context. Setting a SameSite=None cookie without the Secure attribute will be rejected by the browsers.

```
Set-Cookie: key=value; SameSite=None; Secure
```

**External References**

- [Security Cookies - SameSite Attribute - Netsparker](#)
- [Using the Same-Site Cookies Attribute to Prevent CSRF Attacks](#)
- [Same-site Cookies](#)
- [Preventing CSRF with the same-site cookie attribute](#)
- [SameSite cookies explained](#)
- [Get Ready for New SameSite=None; Secure Cookie Settings](#)



**CLASSIFICATION**

|             |                          |
|-------------|--------------------------|
| SANS Top 25 | <a href="#">16</a>       |
| WASC        | <a href="#">15</a>       |
| ISO27001    | <a href="#">A.14.2.5</a> |

# 28. Subresource Integrity (SRI) Not Implemented

BEST PRACTICE

!

1

Subresource Integrity (SRI) provides a mechanism to check integrity of the resource hosted by third parties like Content Delivery Networks (CDNs) and verifies that the fetched resource has been delivered without unexpected manipulation.

SRI does this using hash comparison mechanism. In this way, hash value declared in HTML elements (for now only script and link elements are supported) will be compared with the hash value of the resource hosted by third party.

Use of SRI is recommended as a best-practice, whenever libraries are loaded from a third-party source.

## Vulnerabilities

### 28.1. <https://yazilimmuhendisim.com/>

#### Identified Sub Resource(s)

- https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i
- https://hcaptcha.com/1/api.js

#### Certainty



Request

GET / HTTP/1.1  
Host: yazilimmuhendisim.com  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

## Response

Response Time (ms) : 1776,6294    Total Bytes Received : 19552    Body Length : 18798    Is Compressed : No

```
HTTP/1.1 200 OK
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
CF-RAY: 7373e3cb98dc83a9-MXP
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=zZ2ugAm3Cut09L1wv5cQk281JW4%2BEm60PuhB4lQAVduIh2gGdjha003TfBu9MFxyPw0KTQar4g1iJNzEBFI%2FYcbu3v1Gjj73PtMXUoPLOXE%2BvfGcEsqS0f2nUVwjY00FNDF1UGhcc10%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Sun, 07 Aug 2022 23:46:07 GMT
Vary:
...
```

```
masaüstü uygulama geliştirme,
kendini keşfet ve geliştir" name="keywords">
```

```
<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
```

```
<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">
```

```
<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vendor/bootstrap-icons/bootstrap-icons.css" rel="stylesheet">
<link href="assets/vendor/boxicons/css/b
```

...

```
t">
```

```
<link href="assets/vendor/remixicon/remixicon.css" rel="stylesheet">
<link href="assets/vendor/swiper/swiper-bundle.min.css" rel="stylesheet">
```

```
<link href="assets/css/style.css" rel="stylesheet">
<script src="https://hcaptcha.com/1/api.js" async defer></script>
</head>
<body>
```

```
<header id="header" class="fixed-top ">
<div class="container d-flex align-items-center justify-content-between">
<h1 class="logo"><a href="index.php">Yazılım Mühendisim</a></h1>
<nav id="n
```

...

Remedy


Using Subresource Integrity is simply to add *integrity* attribute to the *script* tag along with a base64 encoded cryptographic hash value.

```
<script src="https://code.jquery.com/jquery-2.1.4.min.js" integrity="sha384-
R4/ztc4Z1RqWjqIuvf6RX5yb/v90qNGx6fS48N0tRxiGkqveZETq72KgDVJCp2TC" crossorigin="anonymous"></script>
```

The hash algorithm must be one of **sha256**, **sha384** or **sha512**, followed by a '-' character.

External References

- [Subresource Integrity](#)
- [Do not let your CDN betray you: Use Subresource Integrity](#)
- [Web Application Security with Subresource Integrity](#)
- [SRI Hash Generator](#)

|   |                          |
|---|--------------------------|
|  | CLASSIFICATION           |
| SANS Top 25   | <a href="#">16</a>       |
| WASC  | <a href="#">15</a>       |
| ISO27001  | <a href="#">A.14.2.5</a> |

# 29. [Possible] Administration Page Detected

INFORMATION ⓘ

1

Netsparker detected a possible administration page.

### Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

### Vulnerabilities

29.1. [https://yazilimmuhendisim.com/phpmyadmin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker\(0x00DD5C\)%3C/scRipt%3E](https://yazilimmuhendisim.com/phpmyadmin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00DD5C)%3C/scRipt%3E)

| Method | Parameter | Value   |
|--------|-----------|---|
| GET    | nsextt    | '"--></style></scRipt><scRipt>netsparker(0x00DD5C)</scRipt> |

### Certainty



Request

GET /phpmyadmin/?nsextt='%22--%3E%3C/style%3E%3C/scRipt%3E%3CscRipt%3Enetsparker(0x00DD5C)%3C/scRipt%3E HTTP/1.1  
Host: yazilimmuhendisim.com  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Cookie: pma\_lang\_https=en; phpMyAdmin\_https=k434t33aadu3tr3n8ej8hk5n8p  
Referer: https://yazilimmuhendisim.com/phpmyadmin/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

## Response

Response Time (ms) : 139,8205    Total Bytes Received : 15359    Body Length : 13222    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373f7da7c78f937-MXP
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
CF-Cache-Status: DYNAMIC
X-Robots-Tag: noindex, nofollow
Set-Cookie: phpMyAdmin_https=k434t33aadu3tr3n8ej8hk5n8p; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: phpMyAdmin_https=30mmavqkjvodphe7ur7hcgh7em; path=/phpmyadmin/; secure; HttpOnly
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=FN69sfnl1Lky28vF%2FQ4nHQVMN4xeoymwG%2BuA93iY0i5FeczZn05U75FAA6jEDTv8hF8BAvYi8SsZ%2BG03TRTTQYqaotazhqt1QnVKbZGiBdKuGnS9GrVplwf8%2BaBIKTbH4HSUBR7kvjk%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Pragma: no-cache
Server: cloudflare
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Expires: Sun, 07 Aug 2022 23:59:48 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:59:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
D
...
name">Username:</label>
<input type="text" name="pma_username" id="input_username" value="" size="24" class="textfield">
</div>
<div class="item">
<label for="input_password">Password:</label>
<input type="password" name="pma_password" id="input_password" value="" size="24" class="textfield">
</div> <input type="hidden" name="server" value="1"></fieldset><fieldset class="tblFooters"><input class="btn btn-primary
```

...

### Remedy

You should manually investigate the found URL.

---





## CLASSIFICATION

|                          |  |
|--------------------------|--|
| PCI DSS v3.2             | <a href="#">6.5.8</a>                  |
| OWASP 2013               | <a href="#">A7</a>                     |
| OWASP 2017               | <a href="#">A5</a>                     |
| SANS Top 25              | <a href="#">425</a>                    |
| CAPEC                    | <a href="#">87</a>                     |
| WASC                     | <a href="#">34</a>                     |
| HIPAA                    | <a href="#">164.306(A), 164.308(A)</a> |
| OWASP Proactive Controls | <a href="#">C6</a>                     |
| ISO27001                 | <a href="#">A.9.4.1</a>                |

## CVSS 3.0 SCORE

|               |              |
|---------------|--------------|
| Base          | 5,3 (Medium) |
| Temporal      | 5,3 (Medium) |
| Environmental | 5,3 (Medium) |

## CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

## CVSS 3.1 SCORE

|          |              |
|----------|--------------|
| Base     | 5,3 (Medium) |
| Temporal | 5,3 (Medium) |

**CVSS 3.1 SCORE**

|               |              |
|---------------|--------------|
| Environmental | 5,3 (Medium) |
|---------------|--------------|

**CVSS Vector String**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

# 30. [Possible] Internal Path Disclosure (\*nix)

INFORMATION ⓘ

1

Netsparker identified a Possible Internal Path Disclosure (\*nix) in the document.

## Impact

There is no direct impact; however, this information can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.

## Vulnerabilities

### 30.1. <https://yazilimmuhendisim.com/phpmyadmin/doc/html/setup.html>

#### Identified Internal Path(s)

- /etc/phpmyadmin
- /usr/share/doc/phmyadmin/README.Debian
- /etc/phpMyAdmin/
- /etc/phpmyadmin/config.user.inc.php
- /usr/sbin/pma-configure
- /usr/sbin/pma-secure
- /usr/share/phpmyadmin/passwd

#### IdentifiedInternalPaths

- /etc/phpmyadmin
- /usr/share/doc/phmyadmin/README.Debian
- /etc/phpMyAdmin/
- /etc/phpmyadmin/config.user.inc.php
- /usr/sbin/pma-configure
- /usr/sbin/pma-secure
- /usr/share/phpmyadmin/passwd

## Certainty



## Request

```
GET /phpmyadmin/doc/html/setup.html HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=hy; phpMyAdmin_https=ofkno9c3qlv9ebmnfq1av3ogt4
Referer: https://yazilimmuhendisim.com/phpmyadmin/doc/html/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 134,0336    Total Bytes Received : 129776    Body Length : 128993    Is Compressed : No

```
HTTP/1.1 200 OK
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
CF-RAY: 73744910bdcbbac9-MXP
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=IQ%2FDUN151C5kZpwX1%2Bgndr2FZAIKJFE6NE4PuaVFVuPWEKsfW3taXMPYvxiCpZJ0qKgoPQ57L9EokZmAohl8mBYugOMZevE9999HWieHdETXE5uUcUbZXjJTsjmg1DGPxiAhThauDc%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Last-Modified: Sat, 10 Oct 2020 03:18:10 GMT
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Content-Type: text/html
Transfer-Encoding: chunked
Content-Encoding:
Date: Mon, 08 Aug 2022 00:55:15 GMT
Vary:
...
dline">¶</a></h3>
<p>Debian's package repositories include a phpMyAdmin package, but be aware that
the configuration file is maintained in <code class="docutils literal notranslate"><span class="pre">/etc/phpmyadmin</span></code> and may differ in
some ways from the official phpMyAdmin documentation. Specifically, it does:</p>
<ul class="simple">
<li>Configuration of a web server (works for Apache and lighttpd).
...
al" href="https://salsa.debian.org/phpmyadmin-team/phpmyadmin/blob/master/debian/README.Debian">README.
Debian</a>
(it is installed as <code class="file docutils literal notranslate"><span class="pre">/usr/share/doc/phpmyadmin/README.Debian</span></code> with the package).</p>
</div>
</div>
<div class="section" id="opensuse">
<h3>OpenSUSE<a class="headerlink" href="#opensuse" title="Permalink to this headline">¶</a></h3>
<p>OpenSUSE alr
...
="Permalink to this headline">¶</a></h3>
<p>Fedora ships the phpMyAdmin package, but be aware that the configuration file
is maintained in <code class="docutils literal notranslate"><span class="pre">/etc/phpMyAdmin/</span></code> and may differ in some ways from the
official phpMyAdmin documentation.</p>
</div>
<div class="section" id="red-hat-enterprise-linux">
<h3>Red Hat Enterprise Linux<a class="headerlink"
...
e external" href="https://fedoraproject.org/wiki/EPEL/FAQ#howtouse">enabled</a>.
But be aware that the configuration file is maintained in
```

```

<code class="docutils literal notranslate"><span class="pre">/etc/phpMyAdmin/
```

 and may dif
fer in some ways from the
official phpMyAdmin documentation.</p>
</div>
</div>
<div class="section" id="installing-on-windows">
<h2>Installing on Windows<a class="headerlink"
...
link" href="#customizing-configuration" title="Permalink to this headline">¶</a></h3>
<p>Additionally configuration can be tweaked by <code class="file docutils literal notranslate"><span c
lass="pre">/etc/phpmyadmin/config.user.inc.php</span></code>. If
this file exists, it will be loaded after configuration is generated from above
environment variables, so you can override any configuration variable. This
configuration can be added as a volume when invoking docker using
<code>-v /some/local/directory/config.user.inc.php:/etc/phpmyadmin/config.user.inc.php</code> parameter
s.</p>
<p>Note that the supplied configuration file is applied after <a class="reference internal" href="#dock
er-vars"><span class="std std-ref">Docker environment variables</span></a>
...
ocker-volumes" title="Permalink to this headline">¶</a></h3>
<p>You can use the following volumes to customize image behavior:</p>
<p><code class="file docutils literal notranslate"><span class="pre">/etc/phpmyadmin/config.user.inc.ph
p</span></code></p>
<blockquote>
<div>Can be used for additional settings, see the previous chapter for more details.</div></blockquote>
<p><code class="file docutils literal notranslate"><span class="
...
light-sh notranslate"><div class="highlight"><pre><span></span>docker run --name phpmyadmin -d --link m
ysql\_db\_server:db -p <span class="m">8080</span>:80 -v /some/local/directory/config.user.inc.php:/etc/p
hpmyadmin/config.user.inc.phpphpmyadmin/phpmyadmin
</pre></div>
</div>
<p>Running with additional themes:</p>
<div class="highlight-sh notranslate"><div class="highlight"><pre><span></span>docker run --name phpmya
dmin -d --link
...
-Indicator">-</span> <span class="l l-Scalar l-Scalar-Plain">/sessions</span>
<span class="p p-Indicator">-</span> <span class="l l-Scalar l-Scalar-Plain">~/docker/phpmyadmin/confi
g.user.inc.php:/etc/phpmyadmin/config.user.inc.php</span>
<span class="p p-Indicator">-</span> <span class="l l-Scalar l-Scalar-Plain">/custom/phpmyadmin/them
e/:/www/themes/theme/</span>
</pre></div>
</div>
<div class="admonition seealso">
<p>cl
...
, in a way
that single command has to be executed for either of these.</p>
<p>To allow editing configuration invoke:</p>
<div class="highlight-sh notranslate"><div class="highlight"><pre><span></span>/usr/sbin/pma-configure
</pre></div>
</div>
<p>To block editing configuration invoke:</p>

```

<div class="highlight-sh notranslate"><div class="highlight"><pre><span></span>/usr/sbin/pma-secure
</pre></div>
</div>
</div>
<div class="section" id="setup-script-on-opensuse">
<h4>Setup script on openSUSE<a class="headerlink" href="#setup-script-on-opensuse" title="Permalink to
this headline">¶<
...
"><pre><span></span><span class="nb">AuthType</span> Basic
<span class="nb">AuthName</span> <span class="s2">"Restricted Access"</span>
<span class="nb">AuthUserFile</span> <span class="sx">/usr/share/phpmyadmin/passwd</span>
<span class="nb">Require</span> valid-user
</pre></div>
</div>
<p>Once you have changed the configuration, you need to create a list of users which
can authenticate. This can be done using the <strong class="program">htpasswd</strong> utility:</p>
<div class="highlight-sh notranslate"><div class="highlight"><pre><span></span>htpasswd -c /usr/share/p
hpmyadmin/passwdusername
</pre></div>
</div>
</li>
<li><p class="first">If you are afraid of automated attacks, enabling Captcha by
<span class="target" id="index-40"></span><a class="reference internal" href="confi
...

```

## External References

- [OWASP - Full Path Disclosure](#)



## CLASSIFICATION

|                          |  |
|--------------------------|--|
| OWASP 2017               | <a href="#">A6</a>                     |
| SANS Top 25              | <a href="#">200</a>                    |
| CAPEC                    | <a href="#">118</a>                    |
| WASC                     | <a href="#">13</a>                     |
| HIPAA                    | <a href="#">164.306(A), 164.308(A)</a> |
| OWASP Proactive Controls | <a href="#">C7</a>                     |
| ISO27001                 | <a href="#">A.9.4.1</a>                |



# 31. [Possible] Internal Path Disclosure (Windows)

INFORMATION ⓘ

1

Netsparker identified a possible Internal Path Disclosure (Windows) in the document.

### Impact

There is no direct impact, however this information can help an attacker identify other vulnerabilities or help during the exploitation of other identified vulnerabilities.

### Vulnerabilities

31.1. <https://yazilimmuhendisim.com/assets/img/portfolio/multi/1.webp?nsextt=%0d%0ans%3anetsparker056650%3dvuln>

| Method | Parameter | Value                    |
|--------|-----------|--------------------------|
| GET    | nsextt    | ns:netsparker056650=vuln |

### Identified Internal Path(s)

- f:/E□

### Certainty



Request

GET /assets/img/portfolio/multi/1.webp?nsextt=%0d%0ans%3anetsparker056650%3dvuln HTTP/1.1  
Host: yazilimmuhendisim.com  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
Referer: https://yazilimmuhendisim.com/  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

## Response

Response Time (ms) : 231,9094    Total Bytes Received : 152733    Body Length : 151921    Is Compressed : No

```
HTTP/1.1 200 OK
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: MISS
CF-RAY: 7373eb9659635a31-MXP
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=tWFTz8mjys1lH0pefoXpGulsc
0yrQgYwHbeLuZZnX4AstnffkX6GLCiMQN4e9W51X71wPaYrL8S5ayvVvKKhpwV%2Bpueug5c4JhToqW25L%2FuN31w7qVXPQBvbgK5pO
aJLfS4SKfIgaITo%3D"}],"group":"cf-nel","max_age":604800}
Content-Length: 154618
Last-Modified: Fri, 28 Jan 2022 19:33:25 GMT
Accept-Ranges: bytes
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Vary: Accept-Encoding
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Date: Sun, 07 Aug 2022 23:51:26 GMT
ETag: "25bfa-5d6a9822a8fdb"
Cache-Control
...
??h?
?|?u+?n?G?8?!!?fw?F?B??L6?'bAm??\?4?|.??~??F??zve?????Et"c?Fv,????btg??B?~n??t?40?+???7r`??
g???/?????B??ü?+?n?n??.??e?!!?C?-f??/?V?K??)??N<?????R??c?>??|q???.?u???'s?n?????+c??^
Q?`f:/E???`???????9?? ?H??F??jL6{?n1?p???.wF4??4cis?p1'I?aU?;3"???,??TWa???4JX+?-?,?SS
â~D~?/????ZC?5J0y?D?uUM?o?3?@1Q?r?"??Q?|?c?????u?d?9??7N??*,??Q?TL?W?{2??i?U:?
D?gK?[??^?F
...
```

## Remedy

Ensure this is not a false positive. Due to the nature of the issue, Netsparker could not confirm that this file path was actually the real file path of the target web server.

- Error messages should be disabled.
- Remove this kind of sensitive data from the output.

## External References

- [OWASP - Full Path Disclosure](#)



## CLASSIFICATION

|                          |   |
|--------------------------|---|
| SANS Top 25              | <a href="#"><u>200</u></a>                    |
| CAPEC                    | <a href="#"><u>118</u></a>                    |
| WASC                     | <a href="#"><u>13</u></a>                     |
| HIPAA                    | <a href="#"><u>164.306(A), 164.308(A)</u></a> |
| OWASP Proactive Controls | <a href="#"><u>C7</u></a>                     |
| ISO27001                 | <a href="#"><u>A.8.1.1</u></a>                |

# 32. [Possible] Login Page Identified

INFORMATION ⓘ

1

Netsparker identified a login page on the target website.

### Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

### Vulnerabilities

#### 32.1. [https://yazilimmuhendisim.com/phpmyadmin/db\\_structure.php](https://yazilimmuhendisim.com/phpmyadmin/db_structure.php)

##### form.id

- login\_form

##### input.id

- input\_username

### Certainty



#### Request

```
GET /phpmyadmin/db_structure.php HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=en; phpMyAdmin_https=1i97aaqc0qga5desacbt2brl1tc
Referer: https://yazilimmuhendisim.com/phpmyadmin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 153,0429    Total Bytes Received : 15366    Body Length : 13229    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373f6d03d213752-MXP
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
CF-Cache-Status: DYNAMIC
X-Robots-Tag: noindex, nofollow
Set-Cookie: phpMyAdmin_https=1i97aaqc0qga5desacbt2brltc; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: phpMyAdmin_https=n1lo7sia7f9c9dkr90tvjtfvab; path=/phpmyadmin/; secure; HttpOnly
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=XfMPbmgkFd17wxUu8pX6ce4pVMhAjsj5LORWY6JKzslp17B83k1%2F3yPkEabWRI56lykeWp2Th67%2B3Gg1df79TZeZY3uDhBANLha3HSPrKbdsY%2FJ72IFnUTyuQw4yM20%2FXHwgfICR9A%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Pragma: no-cache
Server: cloudflare
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Expires: Sun, 07 Aug 2022 23:59:06 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:59:06 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
D
...
icated on the server and client. This can lead to a non working phpMyAdmin or a security risk. Please fix your server configuration to indicate HTTPS properly.</div>
</div>
<div class='hide js-show'> <form method="get" action="index.php" class="disableAjax">
<input type="hidden" name="db" value=""><input type="hidden" name="table" value=""><input type="hidden" name="token" value="3c3a5c4b552569405b6d2479593a5979">
<fieldset>
<legend lang="en" dir="ltr">L
```

```

...
lue="uk">
&#1059;&#1082;&#1088;&#1072;&#1111;&#1085;&#1089;&#1100;&#1082;&#1072; - Ukrainian
</option>
<option value="vi">
Tiếng Việt - Vietnamese
</option>
</select>
</fieldset>
</form>
</div>
<br>

<form method="post" id="login_form" action="index.php" name="login_form" autocomplete="off" class="disa
bleAjax hide login js-show"><form method="post" id="login_form" action="index.php" name="login_form" au
tocomplete="off" class="disableAjax hide login js-show"><form method="post" id="login_form" action="ind
ex.php" name="login_form" autocomplete="off" class="disableAjax hide login js-show">
<fieldset>
<legend><input type="hidden" name="set_session" value="n1lo7sia7f9c9dkr90tvjtfvab">Log in<a href="doc/h
tml/index.html" target="documentation">

#### Unsafe Directive Used In Csp

- unsafe-inline

## Certainty



### Request

```
GET /phpmyadmin/ HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=en; phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9
Referer: https://yazilimmuhendisim.com/phpmyadmin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 156,2569    Total Bytes Received : 15357    Body Length : 13222    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373e7b8bc5b3761-MXP
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
CF-Cache-Status: DYNAMIC
X-Robots-Tag: noindex, nofollow
Set-Cookie: phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: phpMyAdmin_https=8ar344b5guktllesql197use6f; path=/phpmyadmin/; secure; HttpOnly
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=tghJz4Xi4XgKoQdwe666VWNTcThD0DYQUBdmyRtty3z2Mt65G5bG9zd6nF95clYXZUwzmebsiP%2FHj7B6EjbM49h4XT3LqJ1%2FQj1Yjy0ZqratV57unAdoY%2FI5tW1rMmLULwR229P9zM%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Pragma: no-cache
Server: cloudflare
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Expires: Sun, 07 Aug 2022 23:48:48 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
D
...
no-referrer
X-Frame-Options: DENY
Expires: Sun, 07 Aug 2022 23:48:48 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
```



```
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src
'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Date: Sun, 07 Aug 2022 23:48:48 GMT
Content-Encoding:

<!doctype html>
<html lang="en" dir="ltr">
<head>
<meta charset="utf-8"
...
```

## Remedy

If possible remove `unsafe-eval` and `unsafe-inline` from your CSP directives.

## External References

- [An Introduction to Content Security Policy](#)
- [Content Security Policy \(CSP\) HTTP Header](#)
- [Content Security Policy \(CSP\)](#)



## CLASSIFICATION

|             |                          |
|-------------|--------------------------|
| SANS Top 25 | <a href="#">16</a>       |
| WASC        | <a href="#">15</a>       |
| ISO27001    | <a href="#">A.14.2.5</a> |

# 34. data: Used in a Content Security Policy (CSP) Directive

INFORMATION ⓘ

1

Netsparker detected data: use in a CSP directive.

## Impact

An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully by using data:protocol.

## Vulnerabilities

34.1. <https://yazilimmuhendisim.com/phpmyadmin/>

### Data Directive Used

- data:

## Certainty



### Request

```
GET /phpmyadmin/ HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=en; phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9
Referer: https://yazilimmuhendisim.com/phpmyadmin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 156,2569    Total Bytes Received : 15357    Body Length : 13222    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373e7b8bc5b3761-MXP
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
CF-Cache-Status: DYNAMIC
X-Robots-Tag: noindex, nofollow
Set-Cookie: phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: phpMyAdmin_https=8ar344b5guktllesql197use6f; path=/phpmyadmin/; secure; HttpOnly
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=tghJz4Xi4XgKoQdwe666VWNTcThD0DYQUBdmyRtty3z2Mt65G5bG9zd6nF95clYXZUwzmebsiP%2FHj7B6EjbM49h4XZT3LqJ1%2FQj1Yjy0ZqratV57unAdoY%2FI5tW1rMmLULwR229P9zM%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Pragma: no-cache
Server: cloudflare
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Expires: Sun, 07 Aug 2022 23:48:48 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
DHTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373e7b8bc5b3761-MXP
...
ion":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer
```

```
r;style-src 'self' 'unsafe-inline' ;img-src 'self' data:*.tile.openstreetmap.org;object-src 'none';
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src
'self' 'unsafe-inline' ;img-src 'self' data:*.tile.openstreetmap.org;object-src 'none';
Date: Sun, 07 Aug 2022 23:48:48 GMT
Content-Encoding:

<!doctype html>
<html lang="en" dir="ltr">
<head>
<meta charset="utf-8">
<meta name="viewport"
...
```

## Remedy

Remove data:sources from your CSP directives.

## External References

- [An Introduction to Content Security Policy](#)
- [Content Security Policy \(CSP\)](#)
- [Content Security Policy \(CSP\) HTTP Header](#)



## CLASSIFICATION

ISO27001

[A.14.2.5](#)

# 35. Database Detected (MySQL)

INFORMATION

1

CONFIRMED

1

Netsparker detected the target website is using MySQL as its backend database.

This is generally not a security issue and is reported here for informational purposes only.

## Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

## Vulnerabilities

35.1. [https://yazilimmuhendisim.com/portfolio-details.php?p=12%27OR%201%3d1%20AND%20IFNULL\(ASCII\(SUBSTRING\(\(SELECT%200x4E4554535041524B4552\)%2c9%2c1\)\)%2c0\)%3d82--%20](https://yazilimmuhendisim.com/portfolio-details.php?p=12%27OR%201%3d1%20AND%20IFNULL(ASCII(SUBSTRING((SELECT%200x4E4554535041524B4552)%2c9%2c1))%2c0)%3d82--%20)

CONFIRMED

| Method | Parameter    | Value                                                                              |
|--------|--------------|------------------------------------------------------------------------------------|
| GET    | <div>p</div> | 12'OR 1=1 AND IFNULL(ASCII(SUBSTRING((SELECT 0x4E4554535041524B4552),9,1)),0)=82-- |

Request

GET /portfolio-details.php?p=12%27OR%201%3d1%20AND%20IFNULL(ASCII(SUBSTRING((SELECT%200x4E4554535041524B4552)%2c9%2c1))%2c0)%3d82--%20 HTTP/1.1

Host: yazilimmuhendisim.com

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8

Accept-Encoding: gzip, deflate

Accept-Language: en-us,en;q=0.5

Cache-Control: no-cache

Referer: https://yazilimmuhendisim.com/

User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36

X-Scanner: Netsparker

## Response

Response Time (ms) : 120,9748    Total Bytes Received : 5206    Body Length : 4436    Is Compressed : No

HTTP/1.1 200 OK  
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 7373f38ccaf90e26-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=Njmwm1c%2BbNG%2FGD%2BUV1EajWK9ZI%2BVN%2Bd8TY%2B0x9SqcfyXz2h0cijkfaI0zSd472aKew1g09QGsz56jqeJjb2%2B%2FNjw%2FjreVLGBM%2BE%2BYwFT7iE8UjpEos8qIM2NswH8fcqjGZiAhlifBSQ%3D"}],"group":"cf-nel","max\_age":604800}  
NEL: {"success\_fraction":0,"report\_to":"cf-nel","max\_age":604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Sun, 07 Aug 2022 23:56:52 GMT  
Vary: Accept-Encoding

```
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<title>Me Training Club v2 Mobil Uygulaması</title>
<meta content="" name="description">
<meta content="" name="keywords">

<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">

<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunito:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="stylesheet">

<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vendor/bootstrap-icons/bootstrap-icons.css" rel="stylesheet">
<link href="assets/vendor/boxicons/css/boxicons.min.css" rel="stylesheet">
<link href="assets/vendor/glightbox/css/glightbox.min.css" rel="stylesheet">
<link href="assets/vendor/remixicon/remixicon.css" rel="stylesheet">
<link href="assets/vendor/swiper/swiper-bundle.min.css" rel="stylesheet">
<link href="assets/css/style.css" rel="stylesheet">
</head>
<body>

<header id="header" class="fixed-top header-inner-pages">
<div class="container d-flex align-items-center justify-content-center">
...
```





## CLASSIFICATION

|             |                         |
|-------------|-------------------------|
| SANS Top 25 | <a href="#">200</a>     |
| WASC        | <a href="#">13</a>      |
| ISO27001    | <a href="#">A.8.1.1</a> |

### CVSS 3.0 SCORE

|               |            |
|---------------|------------|
| Base          | 4 (Medium) |
| Temporal      | 4 (Medium) |
| Environmental | 4 (Medium) |

### CVSS Vector String

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N

### CVSS 3.1 SCORE

|               |            |
|---------------|------------|
| Base          | 4 (Medium) |
| Temporal      | 4 (Medium) |
| Environmental | 4 (Medium) |

### CVSS Vector String

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N



# 36. default-src Used in Content Security Policy (CSP)

INFORMATION ⓘ

1

Netsparker detected that you used *default-src* in CSP directive. It is important to know that *default-src* cannot be used as a fallback for the functions below:

base-uri

form-action

frame-ancestors

plugin-types

report-uri

sandbox

## Vulnerabilities

36.1. <https://yazilimmuhendisim.com/phpmyadmin/>

## Certainty

### Request

```
GET /phpmyadmin/ HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=en; phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9
Referer: https://yazilimmuhendisim.com/phpmyadmin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 156,2569    Total Bytes Received : 15357    Body Length : 13222    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373e7b8bc5b3761-MXP
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
CF-Cache-Status: DYNAMIC
X-Robots-Tag: noindex, nofollow
Set-Cookie: phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: phpMyAdmin_https=8ar344b5guktllesql197use6f; path=/phpmyadmin/; secure; HttpOnly
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=tghJz4Xi4XgKoQdwe666VWNTcThD0DYQUBdmyRtty3z2Mt65G5bG9zd6nF95clYXZUwzmebsiP%2FHj7B6EjbM49h4XZT3LqJ1%2FQj1Yjy0ZqratV57unAdoY%2FI5tW1rMmLULwR229P9zM%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Pragma: no-cache
Server: cloudflare
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Expires: Sun, 07 Aug 2022 23:48:48 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
DHTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://
...
ep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
```

```
Expires: Sun, 07 Aug 2022 23:48:48 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;
style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src
'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Date: Sun, 07 Aug 2022 23:48:48 GMT
Cont
...
```

## External References

- [An Introduction to Content Security Policy](#)
- [Content Security Policy \(CSP\)](#)
- [Content Security Policy \(CSP\) HTTP Header](#)



## CLASSIFICATION

OWASP Proactive Controls

[C9](#)

ISO27001

[A.14.2.5](#)

# 37. Directory Listing (Apache)

INFORMATION ⓘ

1

Netsparker identified a Directory Listing (Apache).

The web server responded with a list of files located in the target directory.

## Impact

An attacker can see the files located in the directory and could potentially access files which disclose sensitive information.

## Vulnerabilities

37.1. <https://yazilimmuhendisim.com/assets/vendor/bootstrap/>

## Certainty



### Request

```
GET /assets/vendor/bootstrap/ HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 468,7546    Total Bytes Received : 1904    Body Length : 1151    Is Compressed : No

```
HTTP/1.1 200 OK
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
CF-RAY: 7373e55dcdf5a37-MXP
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=bUqK6NQUGC8ttECh90ud7qHkh1LUNitArAa8CTd02NVjeiMwpvsoUC%2Fc99%2B1ydhcOirdMse9fwjkToRcXlpEDb7UelCQCYsHaXKwEyWWEKw%2BnNsDJLroiISWyJxkbzQNMNG3uubmvo%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Sun, 07 Aug 2022 23:47:11 GMT
Vary: Accept-Encoding
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /assets/vendor/bootstrap</title>
</head>
<body>
<h1>Index of /assets/vendor/bootstrap</h1>
<table>
<tr><th valign="top"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr>
<tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"></td><td><a href="/assets/vendor/">Parent Directory</a></td><td>&nbsp;</td><td align="right"> - </td><td>&nbsp;</td></tr>
<tr><td valign="top"></td><td><a href="css/">css</a></td><td align="right">2021-12-23 19:42 </td><td align="right"> - </td><td>&nbsp;</td></tr>
<tr><td valign="top"></td><td><a href="js/">js</a></td><td align="right">2021-12-23 19:42 </td><td align="right"> - </td><td>&nbsp;</td></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.4.41 (Ubuntu) Server at yazilimmuhendisim.com Port 80</address>
</body></html>
```

## Actions to Take

1. Change your server configuration file. A recommended configuration for the requested directory should be in the following format:

```
<Directory /{YOUR DIRECTORY}>  
    Options FollowSymLinks  
</Directory>
```

Remove the *Indexes* option from configuration. Do not forget to remove *MultiViews* as well.

2. Configure the web server to disallow directory listing requests.
3. Ensure that the latest security patches have been applied to the web server and the current stable version of the software is in use.

#### External References

- [WASC - Directory Indexing](#)
- [NVD - Apache Directory Indexing](#)



## CLASSIFICATION

|                          |                         |
|--------------------------|-------------------------|
| OWASP 2013               | <a href="#">A5</a>      |
| OWASP 2017               | <a href="#">A6</a>      |
| SANS Top 25              | <a href="#">548</a>     |
| CAPEC                    | <a href="#">127</a>     |
| WASC                     | <a href="#">16</a>      |
| OWASP Proactive Controls | <a href="#">C6</a>      |
| ISO27001                 | <a href="#">A.9.4.1</a> |

## CVSS 3.0 SCORE

|               |              |
|---------------|--------------|
| Base          | 5,3 (Medium) |
| Temporal      | 5,1 (Medium) |
| Environmental | 5,1 (Medium) |

## CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

## CVSS 3.1 SCORE

|               |              |
|---------------|--------------|
| Base          | 5,3 (Medium) |
| Temporal      | 5,1 (Medium) |
| Environmental | 5,1 (Medium) |

### CVSS Vector String

---

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

---



# 38. Email Address Disclosure

INFORMATION ⓘ

1

Netsparker identified an Email Address Disclosure.

## Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

## Vulnerabilities

38.1. <https://yazilimmuhendisim.com/phpmyadmin/js/vendor/jquery/jquery.debounce-1.0.5.js>

### Email Address(es)

- alpha@zforms.ru

## Certainty



### Request

```
GET /phpmyadmin/js/vendor/jquery/jquery.debounce-1.0.5.js HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=en; phpMyAdmin_https=1i97aaqc0qga5desacbt2brltc
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 131,0331    Total Bytes Received : 2041    Body Length : 1169    Is Compressed : No

```
HTTP/1.1 200 OK
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Cache-Control: max-age=14400
ETag: "491-5b14883c46080-gzip"
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=iz4zx3Np65F3CdVbgN7vq87M5tKzMR2msRG4GfIwTpM4YorbS2h2BPzzP36nFsST09D06jTLTx9WxWuf%2FNWjuTf%2FISDRB6ns%2BnhUR5f5nRmhdPbixhNd5XjLYcdBE313pKbDonDdF3Y%3D"}],"group":"cf-nel","max_age":604800}
CF-RAY: 7373f5b3d903ba97-MXP
Server: cloudflare
CF-Cache-Status: MISS
Accept-Ranges: bytes
Connection: keep-alive
Vary: Accept-Encoding
Content-Length: 529
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sat, 10 Oct 2020 03:18:10 GMT
Content-Type: application/javascript
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Date: Sun, 07 Aug 2022 23:58:20 GMT
Con
...
port_to":"cf-nel","max_age":604800}
Date: Sun, 07 Aug 2022 23:58:20 GMT
Content-Encoding:

/**
 * Debounce and throttle function's decorator plugin 1.0.5
 *
 * Copyright (c) 2009 Filatov Dmitry (alpha@zforms.ru)
 * Dual licensed under the MIT and GPL licenses:
 * http://www.opensource.org/licenses/mit-license.php
 * http://www.gnu.org/licenses/gpl.html
 */

(function($) {

$.extend({

debounce : functio
...

```

## Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

**External References**

- [Wikipedia - Email Spam](#)



## CLASSIFICATION

|                          |                         |
|--------------------------|-------------------------|
| SANS Top 25              | <a href="#">200</a>     |
| CAPEC                    | <a href="#">118</a>     |
| WASC                     | <a href="#">13</a>      |
| OWASP Proactive Controls | <a href="#">C7</a>      |
| ISO27001                 | <a href="#">A.9.4.1</a> |

### CVSS 3.0 SCORE

|               |              |
|---------------|--------------|
| Base          | 5,3 (Medium) |
| Temporal      | 5,3 (Medium) |
| Environmental | 5,3 (Medium) |

### CVSS Vector String

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

### CVSS 3.1 SCORE

|               |              |
|---------------|--------------|
| Base          | 5,3 (Medium) |
| Temporal      | 5,3 (Medium) |
| Environmental | 5,3 (Medium) |

### CVSS Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N



# 39. Expect-CT in Report Only Mode

INFORMATION ⓘ

1

Netsparker identified that Expect-CT is in **report only mode**. The optional **enforced** directive controls whether the browser should drop the connection when the policy is violated.

## Impact

When Expect-CT policy is deployed in **report only mode** and the user agent does not receive a valid Certificate Transparency Log, rather than dropping the connection it will simply send a report to the specified endpoint which is set with **report-uri** directive.

## Vulnerabilities

39.1. <https://yazilimmuhendisim.com/>

## Certainty



Request

GET / HTTP/1.1  
Host: yazilimmuhendisim.com  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

## Response

Response Time (ms) : 1776,6294    Total Bytes Received : 19552    Body Length : 18798    Is Compressed : No

HTTP/1.1 200 OK  
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400  
CF-Cache-Status: DYNAMIC  
CF-RAY: 7373e3cb98dc83a9-MXP  
Server: cloudflare  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=zZ2ugAm3Cut09L1wv5cQk281JW4%2BEm60PuhB4lQAVduIh2gGdjha003TFBu9MFxyPw0KTQar4g1iJNzEBFI%2FYcbu3v1Gjj73PtMXUoPLOXE%2BvfGcEsqS0f2nUVwjY00FNDFlUGhcc10%3D"}], "group": "cf-nel", "max\_age": 604800}  
NEL: {"success\_fraction": 0, "report\_to": "cf-nel", "max\_age": 604800}  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Sun, 07 Aug 2022 23:46:07 GMT  
Vary: Accept-Encoding

```
<!DOCTYPE html>
<html lang="tr">
<head>
<meta charset="utf-8">
<meta content="width=device-width, initial-scale=1.0" name="viewport">
<title>Yazılım Mühendisim - Profesyonel Yazılım Çözümleri</title>
<meta content="Biz güncel teknolojileri kullanarak mobil, masaüstü ve web uygulamaları geliştiriyoruz.
Teklif almak için bizimle iletişime geçebilirsiniz." name="description">
<meta content="yazılım,
yazılım mühendisi,
yazılım mühendisim,
android uygulama,
ios uygulama,
mobil uygulamalar,
mobil uygulama geliştirme,
mobil uygulama fiyatları,
mobil uygulama yapmak,
mobil uygulama kodlama,
mobil uygulama yapma,
mobil uygulama ajansı,
web sitesi,
web sitesi geliştirme,
masaüstü uygulama,
masaüstü uygulama geliştirme,
kendini keşfet ve geliştir" name="keywords">

<link href="assets/img/favicon.png" rel="icon">
<link href="assets/img/apple-touch-icon.png" rel="apple-touch-icon">
```

```
<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Nunit
o:300,300i,400,400i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i" rel="styles
heet">

<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vend
...

```


Remedy

Use enforce flag in definition of Expect-CT.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL "
```

External References

- [Expect-CT Extension for HTTP](#)
- [Expect-CT HTTP Header](#)
- [Expect-CT Header](#)

|                                                                                     |                          |
|-------------------------------------------------------------------------------------|--------------------------|
|  | CLASSIFICATION           |
| OWASP Proactive Controls                                                            | <a href="#">C9</a>       |
| ISO27001                                                                            | <a href="#">A.14.1.2</a> |



# 40. Forbidden Resource

INFORMATION

1

CONFIRMED

1

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

## Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

## Vulnerabilities

### 40.1. <https://yazilimmuhendisim.com/cdn-cgi/scripts/>

CONFIRMED

**Request**

GET /cdn-cgi/scripts/ HTTP/1.1  
Host: yazilimmuhendisim.com  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate  
Accept-Language: en-us,en;q=0.5  
Cache-Control: no-cache  
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36  
X-Scanner: Netsparker

## Response

Response Time (ms) : 109,3737    Total Bytes Received : 1287    Body Length : 553    Is Compressed : No

### HTTP/1.1 403 Forbidden

X-Content-Type-Options: nosniff  
Server: cloudflare  
CF-RAY: 7373e55b8e360e06-MXP  
Connection: keep-alive  
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=jsTKvBSJlbcHud4BDsdIm33REe0B3%2FZ%2FGbau7oqkT2gdVWY7N0aq3HeUa%2BarNh4m6jTpjR1bKGGJsM4fJOAjf16%2F3W8X0%2BQh73GwuF1lp%2BKehF1H50%2BCTR3%2B6KE4L6dMC%2BIUD10vSWQ%3D"}], "group": "cf-nel", "max\_age": 604800}  
NEL: {"success\_fraction": 0, "report\_to": "cf-nel", "max\_age": 604800}  
X-Frame-Options: DENY  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Content-Type: text/html  
Transfer-Encoding: chunked  
Content-Encoding:  
Date: Sun, 07 Aug 2022 23:47:11 GMT  
Vary: Accept-Encoding

```
<html>
<head><title>403 Forbidden</title></head>
<body>
<center><h1>403 Forbidden</h1></center>
<hr><center>cloudflare</center>
</body>
</html>

<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```



## CLASSIFICATION

OWASP Proactive Controls

[C8](#)

ISO27001

[A.8.1.1](#)



# 41. Multiple Content Security Policy (CSP) Implementation Detected

INFORMATION ⓘ

1

Netsparker detected that multiple CSP declaration types were implemented in the page for backward compatibility.

### Impact

Using multiple CSP implementations together might cause CSP directives to not work as intended.

### Vulnerabilities

41.1. <https://yazilimmuhendisim.com/phpmyadmin/>

#### Deprecated CSP Header

- X-Content-Security-Policy

### Certainty



#### Request

```
GET /phpmyadmin/ HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=en; phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9
Referer: https://yazilimmuhendisim.com/phpmyadmin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 156,2569    Total Bytes Received : 15357    Body Length : 13222    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373e7b8bc5b3761-MXP
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
CF-Cache-Status: DYNAMIC
X-Robots-Tag: noindex, nofollow
Set-Cookie: phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: phpMyAdmin_https=8ar344b5guktllesql197use6f; path=/phpmyadmin/; secure; HttpOnly
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=tghJz4Xi4XgKoQdwe666VWNTcThD0dyQUBdmyRtty3z2Mt65G5bG9zd6nF95clYXZUwzmebsiP%2FHj7B6EjbM49h4XZT3LqJ1%2FQj1Yjy0ZqratV57unAdoY%2FI5tW1rMmLULwR229P9zM%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Pragma: no-cache
Server: cloudflare
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Expires: Sun, 07 Aug 2022 23:48:48 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
DHTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report
```

Remedy

Remove these deprecated implementations:

- X-Content-Security-Policy
- X-Webkit-CSP

External References

- [An Introduction to Content Security Policy](#)
- [Content Security Policy \(CSP\)](#)
- [Content Security Policy \(CSP\) HTTP Header](#)



CLASSIFICATION

|                          |                          |
|--------------------------|--------------------------|
| SANS Top 25              | <a href="#">16</a>       |
| WASC                     | <a href="#">15</a>       |
| OWASP Proactive Controls | <a href="#">C9</a>       |
| ISO27001                 | <a href="#">A.14.2.5</a> |

## 42. OPTIONS Method Enabled

INFORMATION ⓘ

1

CONFIRMED ⓘ

1

Netsparker detected that OPTIONSmethod is allowed. This issue is reported as extra information.

### Impact

Information disclosed from this page can be used to gain additional information about the target system.

### Vulnerabilities

42.1. <https://yazilimmuhendisim.com/assets/>

**CONFIRMED**

#### Allowed methods

- POST,OPTIONS,HEAD,GET

#### Request

```
OPTIONS /assets/ HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 116,0423    Total Bytes Received : 730    Body Length : 0    Is Compressed : No

```
HTTP/1.1 200 OK
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
CF-RAY: 7373e6f6c8d7e8ff-MXP
Server: cloudflare
Connection: keep-alive
Allow: POST,OPTIONS,HEAD,GET
Content-Length: 0
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=p1Lqt1DUajgVK%2FuAMUmlWqMd%2BWEv9%2FOHDScy20LxgRP9EHpaTBeFsrw6fdJsHj3Bw0inlvdZdv6yhRb9IyhZ6H4E03jPoNiLXMKCi36RCQ0z8mvmpJpU41V64iV%2B5mppDpqdNBylEeE%3D"}], "group": "cf-nel", "max_age": 604800}
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Content-Type: httpd/unix-directory
NEL: {"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800}
Date: Sun, 07 Aug 2022 23:48:17 GMT
```

## Remedy

Disable OPTIONS method in all production systems.

## External References

- [Testing for HTTP Methods and XST \(OWASP-CM-008\)](#)
- [HTTP/1.1: Method Definitions](#)





## CLASSIFICATION

|             |                          |
|-------------|--------------------------|
| OWASP 2013  | <a href="#">A5</a>       |
| OWASP 2017  | <a href="#">A6</a>       |
| SANS Top 25 | <a href="#">16</a>       |
| CAPEC       | <a href="#">107</a>      |
| WASC        | <a href="#">14</a>       |
| ISO27001    | <a href="#">A.14.1.2</a> |

# 43. Out-of-date Version (Bootstrap)

INFORMATION ⓘ

1

Netsparker identified that the target web site is using Bootstrap and detected that it is out of date.

## Impact

Since this is an old version of the software, it may be vulnerable to attacks.

## Vulnerabilities

### 43.1. <https://yazilimmuhendisim.com/assets/vendor/bootstrap/js/bootstrap.bundle.min.js>

#### Identified Version

- 5.1.3

#### Latest Version

- 5.2.0 (in this branch)

#### Vulnerability Database

- Result is based on 08/05/2022 18:00:00 vulnerability database content.

## Certainty



#### Request

```
GET /assets/vendor/bootstrap/js/bootstrap.bundle.min.js HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://yazilimmuhendisim.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 468,7546    Total Bytes Received : 79008    Body Length : 78129    Is Compressed : No

```
HTTP/1.1 200 OK
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Cache-Control: max-age=14400
ETag: "13131-5d3d56f0ef320-gzip"
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=K0FofZrsheAdlDJwc%2Fnsjqs6i4IbN4TZEsp71rjuZcHSqZe%2BABJJUKdfTgSpgedrJbxYd4n%2BpV7oDeXvhXPrP5m5fkK8scRKu9z0d4wrJChr%2Buk4U5BQGYfQIQ5DqmdWAb04QX%2BHMbo%3D"}],"group":"cf-nel","max_age":604800}
CF-RAY: 7373e55db9660f72-MXP
Server: cloudflare
CF-Cache-Status: HIT
Accept-Ranges: bytes
Connection: keep-alive
Vary: Accept-Encoding
Content-Length: 23053
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Thu, 23 Dec 2021 19:42:08 GMT
Content-Type: application/javascript
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Date: Sun, 07 Aug 2022 23:47:11 GMT
Con
...
hu, 23 Dec 2021 19:42:08 GMT
Content-Type: application/javascript
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Date: Sun, 07 Aug 2022 23:47:11 GMT
Content-Encoding:

/*!
* Bootstrap v5.1.3(https://getbootstrap.com/)
* Copyright 2011-2021 The Bootstrap Authors (https://github.com/twbs/bootstrap/graphs/contributors)
* Licensed under MIT (https://github.com/twbs/bootstrap/blob/main/L
...
```

## Remedy

Please upgrade your installation of Bootstrap to the latest stable version.

## Remedy References

- [Downloading Bootstrap](#)



## CLASSIFICATION

|                          |                                  |
|--------------------------|----------------------------------|
| PCI DSS v3.2             | <a href="#">6.2</a>              |
| OWASP 2013               | <a href="#">A9</a>               |
| OWASP 2017               | <a href="#">A9</a>               |
| SANS Top 25              | <a href="#">829</a>              |
| CAPEC                    | <a href="#">310</a>              |
| HIPAA                    | <a href="#">164.308(A)(1)(I)</a> |
| OWASP Proactive Controls | <a href="#">C1</a>               |
| ISO27001                 | <a href="#">A.14.1.2</a>         |

# 44. Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive

INFORMATION ⓘ

1

Netsparker detected that wildcard was used in domain portion of a CSP directive.

### Impact

This means you trust all of the subdomains of this domain, if this is the case there is no impact.

### Vulnerabilities

44.1. <https://yazilimmuhendisim.com/phpmyadmin/>

#### Wildcard Detected In Domain

- \*.tile.openstreetmap.org

### Certainty



#### Request

```
GET /phpmyadmin/ HTTP/1.1
Host: yazilimmuhendisim.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: pma_lang_https=en; phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9
Referer: https://yazilimmuhendisim.com/phpmyadmin/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
X-Scanner: Netsparker
```

## Response

Response Time (ms) : 156,2569    Total Bytes Received : 15357    Body Length : 13222    Is Compressed : No

```
HTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373e7b8bc5b3761-MXP
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
CF-Cache-Status: DYNAMIC
X-Robots-Tag: noindex, nofollow
Set-Cookie: phpMyAdmin_https=ipkpi80pqsrulbro0eolhrr0t9; path=/phpmyadmin/; secure; HttpOnly
Set-Cookie: goto_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: back_https=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/phpmyadmin/; secure
Set-Cookie: phpMyAdmin_https=8ar344b5guktllesql197use6f; path=/phpmyadmin/; secure; HttpOnly
Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=tghJz4Xi4XgKoQdwe666VWNTcThD0DYQUBdmyRtty3z2Mt65G5bG9zd6nF95clYXZUwzmebsiP%2FHj7B6EjbM49h4XZT3LqJ1%2FQj1Yjy0ZqratV57unAdoY%2FI5tW1rMmLULwR229P9zM%3D"}],"group":"cf-nel","max_age":604800}
Transfer-Encoding: chunked
Pragma: no-cache
Server: cloudflare
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: keep-alive
X-ob_mode: 1
Referrer-Policy: no-referrer
X-Frame-Options: DENY
Expires: Sun, 07 Aug 2022 23:48:48 +0000
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
DHTTP/1.1 200 OK
X-Content-Security-Policy: default-src 'self' ;options inline-script eval-script;referrer no-referrer;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Vary: Accept-Encoding
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
CF-RAY: 7373e7b8bc5b3761-MXP
Cache-Control: no-store, n
...
"report_to":"cf-nel","max_age":604800}
X-WebKit-CSP: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';referrer no-referrer
```

```
r;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Sun, 07 Aug 2022 23:48:48 +0000
Content-Type: text/html; charset=utf-8
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src
'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org;object-src 'none';
Date: Sun, 07 Aug 2022 23:48:48 GMT
Content-Encoding:

<!doctype html>
<html lang="en" dir="ltr">
<head>
<meta charset="utf-8">
<meta name="viewport" content="width=device-wid
...
```

## Remedy

If you trust all of the subdomains and if this is necessary then you do not need to take any actions. However if this is not the case replace the wildcard with the only subdomain that you trust.

## External References

- [An Introduction to Content Security Policy](#)
- [Content Security Policy \(CSP\)](#)
- [Content Security Policy \(CSP\) HTTP Header](#)



## CLASSIFICATION

ISO27001

[A.14.2.5](#)

## Show Scan Detail

### Enabled Security Checks

: Apache Struts S2-045 RCE,  
Apache Struts S2-046 RCE,  
BREACH Attack,  
Code Evaluation,  
Code Evaluation (Out of Band),  
Command Injection,  
Command Injection (Blind),

Content Security Policy,  
Content-Type Sniffing,  
Cookie,  
Cross Frame Options Security,  
Cross-Origin Resource Sharing (CORS),  
Cross-Site Request Forgery,  
Cross-site Scripting,  
Cross-site Scripting (Blind),  
Custom Script Checks (Active),  
Custom Script Checks (Passive),  
Custom Script Checks (Per Directory),  
Custom Script Checks (Singular),  
Drupal Remote Code Execution,  
Expect Certificate Transparency (Expect-CT),  
Expression Language Injection,  
File Upload,  
Header Analyzer,  
Heartbleed,  
HSTS,  
HTML Content,  
HTTP Header Injection,  
HTTP Methods,  
HTTP Status,  
HTTP.sys (CVE-2015-1635),  
IFrame Security,  
Insecure JSONP Endpoint,  
Insecure Reflected Content,  
JavaScript Libraries,  
Local File Inclusion,  
Login Page Identifier,  
Mixed Content,  
Open Redirection,  
Referrer Policy,  
Reflected File Download,  
Remote File Inclusion,  
Remote File Inclusion (Out of Band),  
Reverse Proxy Detection,  
RoR Code Execution,  
Server-Side Request Forgery (DNS),  
Server-Side Request Forgery (Pattern Based),  
Server-Side Template Injection,  
Signatures,  
SQL Injection (Blind),  
SQL Injection (Boolean),  
SQL Injection (Error Based),  
SQL Injection (Out of Band),  
SSL,  
Static Resources (All Paths),  
Static Resources (Only Root Path),  
Unicode Transformation (Best-Fit Mapping),  
WAF Identifier,  
Web App Fingerprint,  
Web Cache Deception,



WebDAV,  
Windows Short Filename,  
XML External Entity,  
XML External Entity (Out of Band)

**URL Rewrite Mode** : Heuristic

**Detected URL Rewrite Rule(s)** : /index.php/etc/assets/{param1}/{param2}/assets,  
/index.php/etc/assets/{param1}/{param2}/assets/css,  
/index.php/etc/assets/{param1}/{param2}/assets/img,  
/index.php/etc/assets/{param1}/{param2}/assets/js,  
/index.php/etc/assets/{param1}/{param2}/assets/vendor,  
/index.php/etc/assets/{param1}/{param2}/assets/vendor/bootstrap,  
/index.php/etc/assets/{param1}/{param2}/assets/vendor/bootstrap-icons,  
/index.php/etc/assets/{param1}/{param2}/assets/vendor/boxicons,  
/index.php/etc/assets/{param1}/{param2}/assets/vendor/glightbox,  
/index.php/etc/assets/{param1}/{param2}/assets/vendor/isotope-layout,  
/index.php/etc/assets/{param1}/{param2}/assets/vendor/php-email-form,  
/index.php/etc/assets/{param1}/{param2}/assets/vendor/remixicon,  
/index.php/etc/assets/{param1}/{param2}/assets/vendor/swiper,  
/index.php/etc/assets/{param1}/{param2}/forms,  
/index.php/etc/assets/{param1}/{param2}/forms/mail,  
/index.php/etc/assets/{param1}/assets/{param2}/assets,  
/index.php/etc/assets/{param1}/assets/{param2}/assets/css,  
/index.php/etc/assets/{param1}/assets/{param2}/assets/img,  
/index.php/etc/assets/{param1}/assets/{param2}/assets/js,  
/index.php/etc/assets/{param1}/assets/{param2}/assets/vendor,  
/index.php/etc/assets/{param1}/assets/{param2}/forms,  
/index.php/etc/assets/{param1}/assets/{param2}/forms/mail,  
/index.php/etc/assets/{param1}/assets/vendor/{param2},  
/index.php/etc/assets/{param1}/assets/vendor/assets/css,  
/index.php/etc/assets/{param1}/assets/vendor/assets/js,  
/index.php/etc/assets/assets/{param1}/{param2},  
/index.php/etc/assets/assets/{param1}/assets/css,  
/index.php/etc/assets/assets/{param1}/assets/vendor/bootstrap/css,  
/index.php/etc/assets/assets/{param1}/assets/vendor/bootstrap/js,  
/index.php/etc/assets/assets/{param1}/assets/vendor/glightbox/css,  
/index.php/etc/assets/assets/{param1}/assets/vendor/glightbox/js,  
/index.php/etc/assets/assets/vendor/{param1}/assets/css,  
/index.php/etc/assets/assets/vendor/{param1}/assets/js,  
/index.php/etc/assets/assets/vendor/{param1}/assets/vendor/bootstrap/css,  
/index.php/etc/assets/assets/vendor/{param1}/assets/vendor/bootstrap/js,  
/index.php/etc/assets/assets/vendor/{param1}/assets/vendor/glightbox/css,  
/index.php/etc/assets/assets/vendor/{param1}/assets/vendor/glightbox/js,  
/index.php/etc/assets/vendor/{param1}/{param2}/assets,  
/index.php/etc/assets/vendor/{param1}/{param2}/assets/css,  
/index.php/etc/assets/vendor/{param1}/{param2}/assets/img,  
/index.php/etc/assets/vendor/{param1}/{param2}/assets/js,  
/index.php/etc/assets/vendor/{param1}/{param2}/assets/vendor,  
/index.php/etc/assets/vendor/{param1}/{param2}/assets/vendor/bootstrap,  
/index.php/etc/assets/vendor/{param1}/{param2}/assets/vendor/bootstrap-icons,  
/index.php/etc/assets/vendor/{param1}/{param2}/assets/vendor/boxicons,  
/index.php/etc/assets/vendor/{param1}/{param2}/assets/vendor/glightbox,

/index.php/etc/assets/vendor/{param1}/{param2}/assets/vendor/isotope-layout,  
/index.php/etc/assets/vendor/{param1}/{param2}/assets/vendor/php-email-form,  
/index.php/etc/assets/vendor/{param1}/{param2}/assets/vendor/remixicon,  
/index.php/etc/assets/vendor/{param1}/{param2}/assets/vendor/swiper,  
/index.php/etc/assets/vendor/{param1}/{param2}/forms,  
/index.php/etc/assets/vendor/{param1}/assets/{param2}/{param3},  
/index.php/etc/assets/vendor/{param1}/assets/{param2}/assets/css,  
/index.php/etc/assets/vendor/{param1}/assets/{param2}/assets/img,  
/index.php/etc/assets/vendor/{param1}/assets/{param2}/assets/js,  
/index.php/etc/assets/vendor/{param1}/assets/{param2}/assets/vendor,  
/index.php/etc/assets/vendor/{param1}/assets/{param2}/forms/mail,  
/index.php/etc/assets/vendor/{param1}/assets/vendor/bootstrap/css,  
/index.php/etc/assets/vendor/{param1}/assets/vendor/bootstrap/js,  
/index.php/etc/assets/vendor/{param1}/assets/vendor/glightbox/css,  
/index.php/etc/assets/vendor/{param1}/assets/vendor/glightbox/js,  
/index.php/etc/assets/vendor/assets/{param1}/assets/vendor/bootstrap/css,  
/index.php/etc/assets/vendor/assets/{param1}/assets/vendor/bootstrap/js,  
/index.php/etc/assets/vendor/assets/{param1}/assets/vendor/glightbox/css,  
/index.php/etc/assets/vendor/assets/{param1}/assets/vendor/glightbox/js,  
/index.php/etc/assets/vendor/assets/vendor/{param1}/assets/css,  
/index.php/etc/assets/vendor/assets/vendor/{param1}/assets/js,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/assets/css,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/assets/img,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/assets/js,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/assets/vendor,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/assets/vendor/bootstrap,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/assets/vendor/bootstrap-icons,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/assets/vendor/boxicons,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/assets/vendor/glightbox,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/assets/vendor/isotope-layout,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/assets/vendor/php-email-form,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/assets/vendor/remixicon,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/assets/vendor/swiper,  
/index.php/etc/assets/vendor/bootstrap/{param1}/{param2}/forms/mail,  
/index.php/etc/assets/vendor/bootstrap/{param1}/assets/vendor/{param2},  
/index.php/etc/assets/vendor/glightbox/assets/{param1}/assets/vendor/bootstrap/css,  
/index.php/etc/assets/vendor/glightbox/assets/{param1}/assets/vendor/bootstrap/js,  
/index.php/etc/assets/vendor/glightbox/assets/{param1}/assets/vendor/glightbox/css,  
/index.php/etc/assets/vendor/glightbox/assets/{param1}/assets/vendor/glightbox/js

|                              |                                                                                                  |
|------------------------------|--------------------------------------------------------------------------------------------------|
| <b>Excluded URL Patterns</b> | : (log sign)\-?(out off)<br>exit<br>endsession<br>gtm\.<br>WebResource\axd<br>ScriptResource\axd |
|------------------------------|--------------------------------------------------------------------------------------------------|

|                       |        |
|-----------------------|--------|
| <b>Authentication</b> | : None |
|-----------------------|--------|

|                  |      |
|------------------|------|
| <b>Scheduled</b> | : No |
|------------------|------|

|                              |                                                                                     |
|------------------------------|-------------------------------------------------------------------------------------|
| <b>Additional Website(s)</b> | : <a href="https://www.yazilimuhendisim.com/">https://www.yazilimuhendisim.com/</a> |
|------------------------------|-------------------------------------------------------------------------------------|

This report created with 5.8.1.28119-master-bca4e4e

<https://www.netsparker.com>