VAPT REPORT

BUSINESS CONFIDENTIAL

CONFIDENTIALITY & PROPRIETARY

This document is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this disclaimer is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this document is strictly prohibited. If you received this document in error, please notify us immediately by telephone and return the original document to us at the address below. If you have received an electronic copy of the document, please remove it immediately after reading this disclaimer.

The Company Provides no warranty that this document is Completely Error Free. The identification of the issues in the report is mainly based on the tests carried out during the limited time for conducting such an exercise. As the basis of selecting the most appropriate weaknesses / vulnerabilities is purely judgmental in view of the time available, the outcome of the analysis may not be exhaustive and representing all possibilities, though we have taken reasonable care to cover the major eventualities.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Objective:

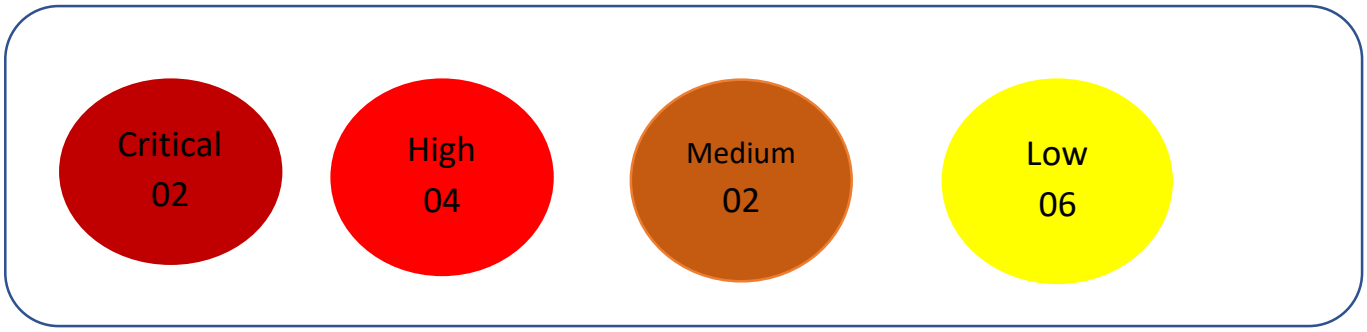
The client indicated that their objective in performing this engagement was to improve the security of their services that they provide. The testing that was conducted should focus on identifying attack vectors in addition to the vulnerabilities and risks these attack vectors may expose. Thus The Test Will Help To Improve The Security of The Digital Assets.

Background:

On January 14 2021, Client A engaged Us to perform a security assessment of their Web Application in an effort to ensure the security of their customer's personal information, which is processed and stored by the application.

Findings Summary

During the Security Testing we observed several areas of concern
that we believe could pose a significant risk to the security of the application, The Summary of Risks Identified in the Web Application is Shown Below.



The Following are Security Finding in the Web Application

RISK	DESCRIPTION	Status	ID
Critical	SQL Injection	*Fixed*	*C-01*
Critical	Probable SQL Injection	*Fixed*	*C-02*
High	Cross-site Scripting	*Fixed*	*H-01*
High	Cross-site Scripting	*Fixed*	*H-02*
High	Out-of-date Version (MySQL)	*Fixed*	*H-03*
High	Session Cookie Not Marked as Secure	Fixed	*H-04*
Medium	Source Code Disclosure	Fixed	*M-01*
Medium	Out-of-date Version (Bootstrap)	Fixed	*M-02*
Low	Cookie Not Marked as HttpOnly	*Fixed*	*L-01*

Low	Cookie Not Marked as Secure	*Fixed*	*L-02*
Low	Insecure Frame	*Pending*	*L-03*
Low	Internal Server Error	*Pending*	*L-04*
Low	User Controllable Cookie	*Pending*	*L-05*
Low	Cross-site Request Forgery	*Pending*	*L-06*

Strategic Recommendations:

- **Ensure Proper Access Control in Areas Where Data is Stored / Retrieved from the Server.**
- **Implement Rate Limiting Mechanism Such As Captcha In all Sensitive Endpoints Such As Login Page.**
- **Handle Session Properly and Destroy Session After Logout.**
- **Use CSRF Token in Request Which Process Some Sensitive Information**
- **Also Develops Should Be Trained To Follow Securing Coding Practices**

Novo Security affirms that the overall security posture of the Website lacks some important security controls and encourages Developers to fix/solve all issues reported in this document and perform further security exercises to ensure the assets stored and managed by the platform remain secure at all times.

Scope:

The Security Researcher performed a Web Application penetration Testing exercise on the following Application

https://www.speedymentors.com/

Scope Exclusion:

As Per client request testing was only done on the given application.

Client Allowance:

No Allowance Was Provided by the Client to Assist the Testing.

Process and Methodology:

The Web Application Penetration Testing was Performed on the Clients Web Application By Following The Testing Guidelines and Process based on The Web Security Testing Guide V4.1.

Also, All The Checks Were Done on Most Common Vulnerabilities based on The OWASP TOP 10 Project

OWASP TOP 10

A1:2017-Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2:2017-Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

A3:2017-Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

A4:2017-XML External Entities (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

A5:2017-Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc

A6:2017-Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

A7:2017-Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with usersupplied data using a browser API that can create HTML or JavaScript. XSS allows

attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A8:2017-Insecure Deserialization

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

A9:2017-Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

A10:2017-Insufficient Logging & Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

DETAILED FINDINGS

C-01 SQL Injection

Status: **Fixed**

URL : https://www.speedymentors.com/browsementor

Parameter Name : search

Parameter Type : POST

Attack Pattern : -1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(109)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27

Vulnerability Details

We have identified an SQL injection, which occurs when data input by a user is interpreted as an 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.

We confirmed the vulnerability by executing a test SQL query on the backend database.

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 or tables from the database
- Executing commands on the underlying operating system

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

A robust method for mitigating the threat of SQL injection-based vulnerabilities is to use 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.

C-02 Probable SQL Injection

Status: **Fixed**

URL : https://www.speedymentors.com/browsementor

Parameter Name : search

Parameter Type : POST

Attack Pattern : %27%2b+(select+convert(int%2c+cast(0x5f21403264696c656d6d61+as+varchar(8000)))+from+syscolumns)+%2b%27

Vulnerability Details

We have identified a probable SQL injection, which occurs when data input by a user is interpreted as an 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.

Even though we believe there is a SQL injection in here, it could not confirm it. There can be numerous reasons for we not being able to confirm this. We strongly recommend investigating the issue manually to ensure it is an SQL injection and that it needs to be addressed. You can also

consider sending the details of this issue to us so we can address this issue for the next time and give you a more precise result.

Impact

Depending on the backend database, 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.

Actions to Take

1. See the remedy for solution.
2. If you are not using a database access layer (DAL) within the architecture consider its benefits and implement if appropriate. As a minimum the use of s DAL will help centralize the issue and its resolution. You can also use ORM (*object relational mapping*). Most ORM systems use parameterized queries and this can solve many if not all SQL injection-based problems.
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. Monitor and review weblogs and application logs to uncover active or previous exploitation attempts.

Remedy

A very robust method for mitigating the threat of SQL injection-based vulnerabilities is to use 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 test for 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. SQL injection is one of the most common web application vulnerabilities.

H-01 Cross-site Scripting

Status: Fixed

URL : https://www.speedymentors.com/browsementor

Parameter Name : search

Parameter Type : POST

Vulnerability Details

We detected cross-site scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-Cross Site Scripting.

External References

- OWASP - Cross-site Scripting
- Cross-site Scripting Web Application Vulnerability
- XSS Shell
- XSS Tunnelling

Remedy References

- Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet
- OWASP AntiSamy Java

Proof of Concept Notes

Generated XSS exploit might not work due to browser XSS filtering. Please follow the guidelines below in order to disable XSS filtering for different browsers. Also note that;

- XSS filtering is a feature that's enabled by default in some of the modern browsers. It should only be disabled temporarily to test exploits and should be reverted back if the browser is actively used other than testing purposes.
- Even though browsers have certain checks to prevent Cross-site scripting attacks in practice there are a variety of ways to bypass this mechanism therefore a web application should not rely on this kind of client-side browser checks.

Chrome

- Open command prompt.
- Go to folder where chrome.exe is located.
- Run the command `chrome.exe --args --disable-xss-auditor`

Internet Explorer

- Click Tools->Internet Options and then navigate to the Security Tab.
- Click Custom level and scroll towards the bottom where you will find that Enable XSS filter is currently Enabled.
- Set it to disabled. Click OK.
- Click Yes to accept the warning followed by Apply.

Firefox

- Go to `about:config` in the URL address bar.
- In the search field, type *urlbar.filter* and find *browser.urlbar.filter.javascript*.
- Set its value to `false` by double clicking the row.

H-02 Cross-site Scripting

Status:
Fixed

URL : https://www.speedymentors.com/browsementor
Parameter Name : search
Parameter Type : POST

Vulnerability Details

We detected cross-site scripting, which allows an attacker to execute a dynamic script (*JavaScript, VBScript*) in the context of the application.

This allows several different attack opportunities, mostly hijacking the current session of the user or changing the look of the page by changing the HTML on the fly to steal the user's credentials. This happens because the input entered by a user has been interpreted as HTML/JavaScript/VBScript by the browser. Cross-site scripting targets the users of the application instead of the server. Although this is a limitation, since it allows attackers to hijack other users' sessions, an attacker might attack an administrator to gain full control over the application.

Impact

There are many different attacks that can be leveraged through the use of cross-site scripting, including:

- Hijacking user's active session.
- Mounting phishing attacks.
- Intercepting data and performing man-in-the-middle attacks.

Remedy

The issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, output should be encoded according to the output location and context. For example, if the output goes in to a JavaScript block within the HTML document, then output needs to be encoded accordingly. Encoding can get very complex, therefore it's strongly

recommended to use an encoding library such as OWASP ESAPI and Microsoft Anti-Cross Site Scripting.

External References

- OWASP - Cross-site Scripting
- Cross-site Scripting Web Application Vulnerability
- XSS Shell
- XSS Tunnelling

Remedy References

- Microsoft Anti-XSS Library
- OWASP XSS Prevention Cheat Sheet
- OWASP AntiSamy Java

Proof of Concept Notes

Generated XSS exploit might not work due to browser XSS filtering. Please follow the guidelines below in order to disable XSS filtering for different browsers. Also note that;

- XSS filtering is a feature that's enabled by default in some of the modern browsers. It should only be disabled temporarily to test exploits and should be reverted back if the browser is actively used other than testing purposes.
- Even though browsers have certain checks to prevent Cross-site scripting attacks in practice there are a variety of ways to bypass this mechanism therefore a web application should not rely on this kind of client-side browser checks.

Chrome

- Open command prompt.
- Go to folder where chrome.exe is located.
- Run the command `chrome.exe --args --disable-xss-auditor`

Internet Explorer

- Click Tools->Internet Options and then navigate to the Security Tab.
- Click Custom level and scroll towards the bottom where you will find that Enable XSS filter is currently Enabled.
- Set it to disabled. Click OK.
- Click Yes to accept the warning followed by Apply.

Firefox

- Go to `about:config` in the URL address bar.
- In the search field, type *urlbar.filter* and find *browser.urlbar.filter.javascript*.
- Set its value to `false` by double clicking the row.

H-03 Out-of-date Version (MySQL)

Status:
Fixed

URL	:	https://www.speedymentors.com/browsementor
Identified Version	:	5.6.38
Latest Version	:	5.6.43 (in this branch)
Vulnerability Database	:	Result is based on 03/26/2019 18:50:00 vulnerability database content.
Parameter Name	:	search
Parameter Type	:	POST

Attack Pattern : -1%27+and+6%3d3+or+1%3d1%2b(SELECT+1+and+ROW(1%2c1)%3e(SELECT+COUNT(*)%2cCONCAT(CHAR(95)%2cCHAR(33)%2cCHAR(64)%2cCHAR(52)%2cCHAR(100)%2cCHAR(105)%2cCHAR(108)%2cCHAR(101)%2cCHAR(109)%2cCHAR(109)%2cCHAR(97)%2c0x3a%2cFLOOR(RAND(0)*2))x+FROM+INFORMATION_SCHEMA.COLLATIONS+GROUP+BY+x)a)%2b%27

Vulnerability Details

We 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.

Remedy

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

Remedy References

- MySQL Downloads

Known Vulnerabilities in this Version

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.42

External References

- CVE-2019-2537

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).

Affected Versions

5.6.2 to 5.6.42

External References

- CVE-2019-2534

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13

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 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.42

External References

- CVE-2019-2531

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.42

External References

- CVE-2019-2529

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.42

External References

- CVE-2019-2507

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection Handling). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit 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 unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H).

Affected Versions

5.6.2 to 5.6.42

External References

- CVE-2019-2503

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.42

External References

- CVE-2019-2482

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.42

External References

- CVE-2019-2481

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.42

External References

- CVE-2019-2455

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Storage Engines). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 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 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.40

External References

- CVE-2018-3282

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: RBR). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 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 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.40

External References

- CVE-2018-3278

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 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 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.40

External References

- CVE-2018-3276

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.40

External References

- CVE-2018-3251

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Merge). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 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 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

Affected Versions

5.6.2 to 5.6.40

External References

- CVE-2018-3247

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes 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 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.40

External References

- CVE-2018-3174

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.40

External References

- CVE-2018-3156

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.40

External References

- CVE-2018-3143

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.40

External References

- CVE-2018-3133

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2819

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 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 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2818

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2817

MySQL Sensitive Information Disclosure Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 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 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2813

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: GIS Extension). Supported versions that are affected are 5.6.39 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2805

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2787

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2784

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2782

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 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 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2781

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 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 hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2773

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Locking). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 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 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2771

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 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 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2766

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated 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 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2761

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.39 and prior and 5.7.21 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2758

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit 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 and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2755

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.38 and prior and 5.7.20 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2703

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily

exploitable vulnerability allows unauthenticated 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 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2696

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2668

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2665

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.38 and prior and 5.7.20 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 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2647

MySQL Sensitive Information Disclosure Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.38 and prior and 5.7.20 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 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2645

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2640

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2622

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.38 and prior and 5.7.20 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 and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2612

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). Supported versions that are affected are 5.6.38 and prior and 5.7.19 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 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2591

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.38 and prior and 5.7.20 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 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2590

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Stored Procedure). Supported versions that are affected are 5.6.38 and prior and 5.7.20 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 3.0 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2583

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: GIS). Supported versions that are affected are 5.6.38 and prior and 5.7.20 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 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2573

MySQL Unspesificed Vulnerability

Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.19

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 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).

Affected Versions

5.6.2 to 5.6.38

External References

- CVE-2018-2562

H-04 Session Cookie Not Marked as Secure

URL : https://www.speedymentors.com/
Identified Cookie(s) : ci_session
Cookie Source : HTTP Header

Status: Fixed

Vulnerability Details

We identified a session cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept the traffic, following a successful man-in-the-middle attack.

It is important to note that we inferred from the its name that the cookie in question is session related.

Impact

This cookie will be transmitted over a HTTP connection, therefore an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to your website in order to steal the cookie.

Actions to Take

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

Remedy

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to understand layer 2 and have gained access to a system between the victim and the web server.

External References

- .NET Cookie.Secure Property
- How to Create Totally Secure Cookies

M-01 Source Code Discloser

URL : https://www.speedymentors.com/apply-for-mentor.html

Status:
Fixed

Vulnerability Details

We identified possible source code disclosure (ColdFusion). 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 the business logic of the 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.

Remedy

- Confirm exactly what aspects of the source code are actually disclosed; due to the limitations of these types of vulnerability, it might not be possible to confirm this in all instances. Confirm this is not an intended functionality.
- 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.
- Ensure that the server has all the current security patches applied.
- Remove all temporary and backup files from the web server.

External References

- Secureyes - Source Code Disclosure over Http

M-02 Out-of-date Version (Bootstrap)

Status: **Fixed**

URL	:	https://www.speedymentors.com/
Identified Version	:	4.1.2
Latest Version	:	4.3.1 (in this branch)
Vulnerability Database	:	Result is based on 03/26/2019 18:50:00 vulnerability database content.

Vulnerability Details

We 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.

Actions to Take

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

Known Vulnerabilities in this version

bootstrap.js Cross-Site Scripting (XSS) Vulnerability
In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.

Affected Versions
4.0.0 to 4.2.0
External References
CVE-2018-14042
bootstrap.js Cross-Site Scripting (XSS) Vulnerability
In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.

Affected Versions
4.0.0 to 4.2.0
External References

CVE-2018-14040
bootstrap.js Cross-Site Scripting (XSS) Vulnerability
In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.

Affected Versions
4.0.0 to 4.2.0
External References
CVE-2016-10735

External References

- Secureyes - Source Code Disclosure over Http

L-01 Not Marked as HttpOnly

URL : https://www.speedymentors.com/login

Identified Cookie(s) :
- remember_email
- remember_password
- remember_me

Cookie Source : HTTP Header

Status: Fixed

Vulnerability Details

We identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

Actions to Take

1. See the remedy for solution.
2. Consider marking all of the cookies used by the application as HTTPOnly. (*After these changes javascript code will not be able to read cookies.*)

Remedy

Mark the cookie as HTTPOnly. This will be an extra layer of defense against XSS. However this is not a silver bullet and will not protect the system against cross-site scripting attacks. An attacker can use a tool such as XSS Tunnel to bypass HTTPOnly protection.

External References

- OWASP HTTPOnly Cookies
- MSDN - ASP.NET HTTPOnly Cookies

L-02 Cookie Not Marked as Secure

URL : https://www.speedymentors.com/login

Identified Cookie(s) :
- `remember_email`
- `remember_password`
- `remember_me`

Status: Fixed

Cookie Source : `HTTP Header`

Vulnerability Details

We identified a cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

Impact

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (*such as a session cookie*), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

Actions to Take

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

Remedy

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To exploit this issue, the attacker needs to be able to intercept traffic. This generally requires local access to the web server or to the victim's network. Attackers need to be understood layer 2, have physical access to systems either as waypoints for the traffic, or have locally gained access to to a system between the victim and the web server.

External References

- .NET Cookie.Secure Property

- How to Create Totally Secure Cookies

L-03 Insecure Frame

URL : https://www.speedymentors.com/

Frame Name(s) : stripeXDM_default848227_provider

Parsing Source : DOM Parser

Frame Source(s) : https://js.stripe.com/v2/m/outer.html#referrer=&title=Speedy%20Mentors&url=https%3A%2F%2Fwww.speedymentors.com%2F&muid=NA&sid=NA&version=6&preview=false&

Status: Pending

Vulnerability Details

We 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.

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

L-04 Internal Server Error

URL : https://www.speedymentors.com/browsementor
Parameter Name : search
Parameter Type : POST
Attack Pattern : %27+WAITFOR+DELAY+%270%3a0%3a25%27--

Status: Pending

Vulnerability Details

We 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..

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.

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.

L-05 User Controllable Cookie

URL	:	https://www.speedymentors.com/login
Identified Cookie(s)	:	remember_email
Cookie Source	:	HTTP Header
Parameter Name	:	email
Parameter Type	:	POST
Attack Pattern	:	N3tSp4rK3R

Status:
Pending

Vulnerability Details

We identified a user controllable cookie.

Impact

Attackers can easily set an arbitrary value in the cookie and this may allow them to bypass authentication, carry out attacks such as SQL injection and cross-site scripting or modify inputs in unexpected ways.

Remedy

Add integrity checks and server-side validation to detect tampering.

L-06 Cross-site Request Forgery

URL : https://www.speedymentors.com/signup

Form Action(s) : https://www.speedymentors.com/signup

Status:
Pending

Vulnerability Details

We 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).

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

Thank You !