Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

BetDSI

Type of Report – Vulnerability Assessment

December, 2023

**Table of Contents**

[Executive Summary 2](#_Toc154659109)

[Introduction 2](#_Toc154659110)

[Executive Summary 2](#_Toc154659111)

[Severity Level Details 3](#_Toc154659112)

[Scope 4](#_Toc154659113)

[Detailed External Findings 6](#_Toc154659114)

[HSTS Missing From HTTPS Server (RFC 6797) 7](#_Toc154659115)

[Host Vulnerability Tables 8](#_Toc154659116)

[Findings for www.spartansportsbook.com 8](#_Toc154659117)

[Methodology Tasks Completed 9](#_Toc154659118)

[Appendices 9](#_Toc154659119)

[Appendix A: Tools Used 9](#_Toc154659120)

# Executive Summary

## Introduction

The cybersecurity teams of a company must align with the best security practices to keep events such as attacks or information leaks to a minimum. Security Consulting Group is committed to collaborating with BetDSI to present a vulnerability analysis and a report on improvement points for information protection.

Vulnerability analyses must be carried out periodically to maintain an updated view of the equipment with vulnerabilities depending on their software, hardware, and respective end-of-support dates. The analysis also aims to discover new vulnerabilities that could be exploited by attackers and compromise the equipment, information, and reputation of the companies.

BetDSI has already conducted these exercises in the past, and as part of the cybersecurity team's effort to maintain a secure posture, this new report is being conducted.

The objective of a vulnerability analysis is to present the degree of impact or damage that the state or condition of exposed information represents in the event of exploiting identified vulnerabilities and how it can affect the company. The severity level for each vulnerability is based on the Common Vulnerability Scoring System (CVSS) standard.

The Common Vulnerability Scoring System (CVSS) provides a way to capture the main characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations assess and prioritize their vulnerability management processes.

On the other hand, it is advisable to use the information from this report in the risk analysis since it indicates the probability of exploiting these vulnerabilities.

## Executive Summary

The SCG team is pleased to present the results of the Vulnerability Assessment Report for the website www.spartnasportbook.com.

This analysis consists of an analysis of vulnerabilities that can be found with automated tools and provide recommendations.

The risk classification of the findings was assigned based on the Common Vulnerability Scoring System (CVSS), using the detailed scale in the table below. To learn more about CVSS, you can visit https://www.first.org/cvss.

CVSS is a published standard used by organizations worldwide, and the mission of SIG is to continue improving it. Refer to Table 1 for the classification and scoring of vulnerabilities.

|  |  |
| --- | --- |
| CVSS Score Range | Risk Rating |
| 9.0 to 10.0 | **Critical** |
| 7.0 to 8.9 | **High** |
| 4.0 to 6.9 | **Medium** |
| 0.1 to 3.9 | **Low** |
| n/a | **Informational** |

## Severity Level Details

Severity Level: Critical

Vulnerabilities scoring in the critical range typically exhibit most of the following characteristics:

* Exploiting the vulnerability is likely to result in a compromise at the root level of servers or infrastructure devices.
* Exploitation is usually straightforward, meaning the attacker doesn't need any special authentication credentials or knowledge about individual victims, and there's no need to persuade a target user, for example, through social engineering, to perform any special function.

For critical vulnerabilities, it is recommended to apply a patch or update as soon as possible, unless other mitigation measures are in place. For example, a mitigating factor could be that your installation is not accessible from the internet.

Severity Level: High

Vulnerabilities scoring in the high range usually exhibit some of the following characteristics:

* The vulnerability is challenging to exploit.
* Exploitation could result in elevated privileges.
* Exploitation could result in significant data loss or downtime.

Severity Level: Medium

Vulnerabilities scoring in the medium range typically exhibit some of the following characteristics:

* Vulnerabilities that require the attacker to manipulate individual victims through social engineering tactics.
* Denial-of-service vulnerabilities that are difficult to configure.
* Exploitation of vulnerabilities that require an attacker to reside in the same local network as the victim or be physically within the premises.
* Vulnerabilities where exploitation provides only very limited access.
* Vulnerabilities that require user privileges for successful exploitation.

Severity Level: Low

Vulnerabilities in the low range usually have minimal impact on an organization's business. Exploiting such vulnerabilities generally requires access to the local or physical system. Vulnerabilities in third-party code that cannot be accessed from the code can be downgraded to low severity.

Severity Level: Informational

These are not vulnerabilities in equipment or software per se but rather information that could assist attackers in gaining a better understanding of the organization or its objectives.

A total of 1 finding was identified. Of these, 0 were classified with Critical risk, 0 was classified with High risk, 1 were categorized with medium risk, and 0 was classified with Low risk.

A total of 0 findings was/were categorized as Internal, and 1 was/were categorized as External.

## Scope

The list of hosts covered by this assessment included:

* www.spartansportsbook.com

A total of 0 findings was/were categorized as Internal, and 1 was/were categorized as External.

|  |  |  |  |
| --- | --- | --- | --- |
| Finding | Risk Rating | Location | Affected Hosts |
| HSTS Missing From HTTPS Server (RFC 6797) | **Medium** | **External** | [www.spartansportsbook.com](http://www.spartansportsbook.com) |

|  |  |  |
| --- | --- | --- |
| CVSS Score Range | Risk Rating | Number of Findings |
| 9.0 to 10.0 | **Critical** | 0 |
| 7.0 to 8.9 | **High** | 0 |
| 4.0 to 6.9 | **Medium** | 1 |
| 0.1 to 3.9 | **Low** | 0 |
| n/a | **Informational** | 0 |

# Detailed External Findings

|  |  |  |
| --- | --- | --- |
| Finding | Risk Rating | Affected Hosts |
| HSTS Missing From HTTPS Server (RFC 6797) | **Medium** | [www.spartansportsbook.com](http://www.spartansportsbook.com) |

## HSTS Missing From HTTPS Server (RFC 6797)

**Rating**: Medium

**CVSS Score**: 6.5

**CVSS Vector**:

**Description**

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

**Solution**

Configure the remote web server to use HSTS.

**References**

<https://tools.ietf.org/html/rfc6797>

**Hosts affected:** [www.spartansportsbook.com](http://www.spartansportsbook.com)

**Evidence for www.spartansportsbook.com**

Location: tcp/443

The remote HTTPS server does not send the HTTP  
 "Strict-Transport-Security" header.

# Host Vulnerability Tables

## Findings for www.spartansportsbook.com

|  |  |  |
| --- | --- | --- |
| Finding | Risk Rating | CVSS Score |
| HSTS Missing From HTTPS Server (RFC 6797) | **Medium** | 6.5 |

# Methodology Tasks Completed

# Appendices

## Appendix A: Tools Used

|  |  |
| --- | --- |
| Tool | Description |
| **Dradis Framework** | Collaboration and reporting software for information security teams.  https://dradisframework.com/pro/ |
| **Nessus** | Nessus is one of the most popular and capable vulnerability scanners, particularly for UNIX systems.  http://www.tenable.com/products/nessus-vulnerability-scanner |

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

services@securitygroupcr.com