## **Website Vulnerability Assessment Report**

**Project Name:** Website Vulnerability Scanning Report

**Date:** 23/07/2024

**Executive Summary:**

* This assessment aims to identify security vulnerabilities in websites that we conducted vulnerability assessment for
* The Overall Security Posture of the websites was Medium

**Target Information:**

* **URL 1 =** [www.itsecgames.com](http://www.itsecgames.com)
* URL 2 = [defendtheweb.net](http://defendtheweb.net)

**Assessment Methodology:**

* In this assessment we used automated vulnerability scanning tools to identify weaknesses in the websites we assessed

**Key Findings:**

* Website 1 :
  + **Vulnerability Description:** We noticed that server software and technology details are exposed, potentially helping attackers in tailoring specific exploits against identified systems and versions
  + **Impact:** It can be used by malicious actors for malicious purposes, it can lead to unauthorised access, it can leads to a data breach and results in identity theft as well
  + **Severity:** Medium

**Website 2:**

* **Vulnerability Description:** The website transmits cookies without the "HttpOnly" flag.
* **Impact:** An attacker could potentially steal a user's session cookie and gain unauthorized access to their account.
* **Severity:** Medium

**Recommendation & Mitigation Strategies:**

* Mitigation for the Vulnerability of Website 1
  + We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Mitigation for the Vulnerability of Website 2 :

* Enable the HttpOnly flag for all cookies. In this scenario (if the browser supports this flag) it means that cookies can’t be accessed using any malicious scripts and even if it has a XSS flaw then it prevents cookies info being revealed through a trick link created by attackers
* [HttpOnly | OWASP Foundation](https://owasp.org/www-community/HttpOnly)

**Next Steps:**

Here's a recommended course of action for the website owner:

* **Configure server details:** Work with your web developers to hide unnecessary information from website responses**.**
* **Review website code:** Remove any parts that reveal software details
* **(Website 2) Enable the HttpOnly flag for all cookies:** This strengthens the website's security posture by preventing malicious scripts from accessing cookies, even if an XSS vulnerability exists. (Website 2)

**Disclaimer:**

* This report is for informational purposes only and should not be considered a comprehensive security audit.