**⚠️VULNERABILITY REPORT⚠️**

**TARGET**

<https://demo.amarhms.com/arch/index.php?page=dashboard>

**Executive Summary:**

This vulnerability assessment report aims to outline a critical security vulnerability discovered on the website hosted at "***https://demo.amarhms.com/arch/index.php?page=PAYLOAD***". The identified vulnerability involves SQL injection, which allows attackers to manipulate database queries, potentially leading to unauthorized access and disclosure of sensitive data.

**Vulnerability Details:**

Vulnerability Type: SQL Injection

Vulnerable URL: "https://demo.amarhms.com/arch/index.php?page=PAYLOAD"

Affected Parameter: page (GET)

**Payloads Used:**

a. Boolean-based blind:

- Payload: page=-6483' OR 6800=6800-- YVJL

- Vector: OR [INFERENCE]

b. Error-based:

- Payload: page=dashboard' AND GTID\_SUBSET(CONCAT(0x71766b7a71,(SELECT (ELT(6432=6432,1))),0x71766b7871),6432)-- sXup

- Vector: AND GTID\_SUBSET(CONCAT('[DELIMITER\_START]',([QUERY]),'[DELIMITER\_STOP]'),[RANDNUM])

c. Time-based blind:

- Payload: page=dashboard' AND (SELECT 7214 FROM (SELECT(SLEEP(12)))zmTb)-- cixu

- Vector: AND (SELECT [RANDNUM] FROM (SELECT(SLEEP([SLEEPTIME]-(IF([INFERENCE],0,[SLEEPTIME])))))[RANDSTR])

d. Union query:

- Payload: page=-8155' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x71766b7a71,0x6a725041646978424f584558674d4e4f45494c6a654473434a6647676f646d7347615350506c486d,0x71766b7871),NULL-- -

- Vector: UNION ALL SELECT NULL,NULL,NULL,[QUERY],NULL-- -

**Proof**

**A screen shot of a computer

Description automatically generated**

**Impact**

Exploiting this vulnerability allows attackers to manipulate database queries, potentially leading to unauthorized access, data disclosure, and the ability to execute malicious commands within the database.

**Vulnerability Recommendation**

* To mitigate the SQL injection vulnerability, the following recommendations are advised:
* Parameterized Queries: Implement parameterized queries or prepared statements to ensure proper separation of SQL code and user input.
* Input Validation: Implement strict input validation to filter out malicious characters and patterns.
* Principle of Least Privilege: Apply the principle of least privilege to database accounts, granting only necessary permissions for accessing data.
* Block ip if there is too many responses from a single ip address.

**Risk Assessment**

Considering the severity of the SQL injection vulnerability, it is classified as high risk. Immediate action is recommended to address and remediate this vulnerability to prevent unauthorized access and protect the integrity and confidentiality of the website's data.

**Executive Summary:**

This vulnerability assessment report aims to highlight a critical security issue discovered on the website hosted at "***https://demo.amarhms.com/arch/index.php?page=dashboard***". The identified vulnerability involves Cross-Site Scripting (XSS), which allows attackers to inject malicious code into the website, potentially compromising its integrity and user data.

**Vulnerability Details:**

Vulnerability Type: **Cross-Site Scripting (XSS)**

Vulnerable URL: "**https://demo.amarhms.com/arch/index.php?page=PAYLOAD**"

Payload Used: "**dashboard'%20-->'>'"**"

**Proof**

**A screenshot of a computer

Description automatically generated**

**Impact**

Exploiting this vulnerability enables attackers to inject and execute harmful scripts on the website. It poses risks such as unauthorized access to user information, session hijacking, defacement of the website, and further exploitation.

**Vulnerability Recommendation:**

To mitigate the XSS vulnerability, the following recommendations are advised:

* Input Validation and Sanitization: Implement robust validation and sanitization mechanisms for user input fields to prevent the execution of malicious scripts.
* Output Encoding: Apply proper encoding techniques to ensure that user-supplied data is correctly displayed without executing as code.
* Content Security Policy (CSP): Enforce a Content Security Policy to restrict the execution of scripts from unauthorized sources.

**Risk Assessment:**

Given the criticality of the XSS vulnerability, it is classified as high risk. Immediate action is recommended to address and remediate this vulnerability, preventing potential exploitation and safeguarding the website and its users.