# **Domain:** https://alumni.stekom.ac.id/

**IP Address: 192.168.2.1**

**Year: 2025**

## **1. Bug Name: Authentication Bypass**

**Severity: High**

**CVSS Score: 9**

**Location:** <https://alumni.stekom.ac.id/login-alumni>

**Description:**

• - Authentication Bypass is a critical security vulnerability that occurs when an attacker is

• able to gain unauthorized access to an application, system, or account by circumventing

• or exploiting flaws in the authentication process. This vulnerability undermines the

• fundamental purpose of authentication mechanisms, which is to verify the identity of

• users attempting to access protected resources.

**Impact:**

**Proof of Concept:**

**Remediation:**

## **2. Bug Name: Cross-site Scripting (Stored XSS)**

**Severity: High**

**CVSS Score: N/A**

**Location:**

**Description:**

• - Stored Cross-Site Scripting (XSS) is a security vulnerability that occurs when an attacker

• is able to inject malicious JavaScript code into a web application, and the injected script is

• stored on the server. This script is then executed automatically every time a legitimate

• user accesses the affected page or resource, without their knowledge or consent.

**Impact:**

**Proof of Concept:**

**Remediation:**