

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>

Vulnerability Descriptions:

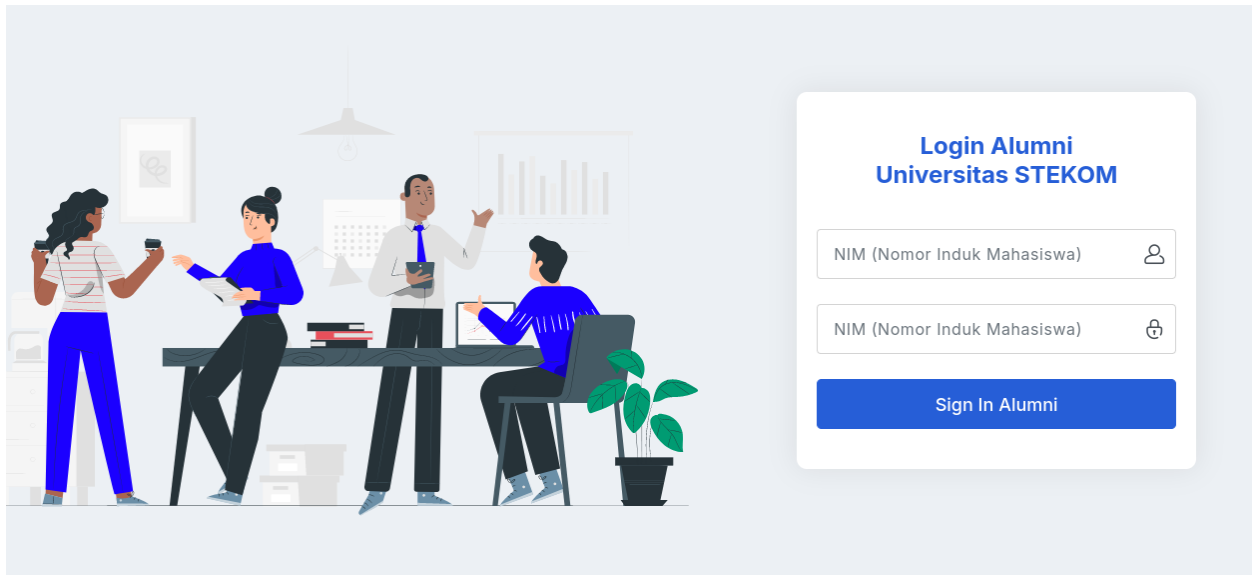
- Authentication Bypass is a critical security vulnerability that occurs when an attacker is able to gain unauthorized access to an application, system, or account by circumventing or exploiting flaws in the authentication process. This vulnerability undermines the fundamental purpose of authentication mechanisms, which is to verify the identity of users attempting to access protected resources.

Impact:

- Malicious actors can gain access to login page of the application without proper credentials(password).
- Anyone can gain access to a student's account simply by knowing the student's NIM number.

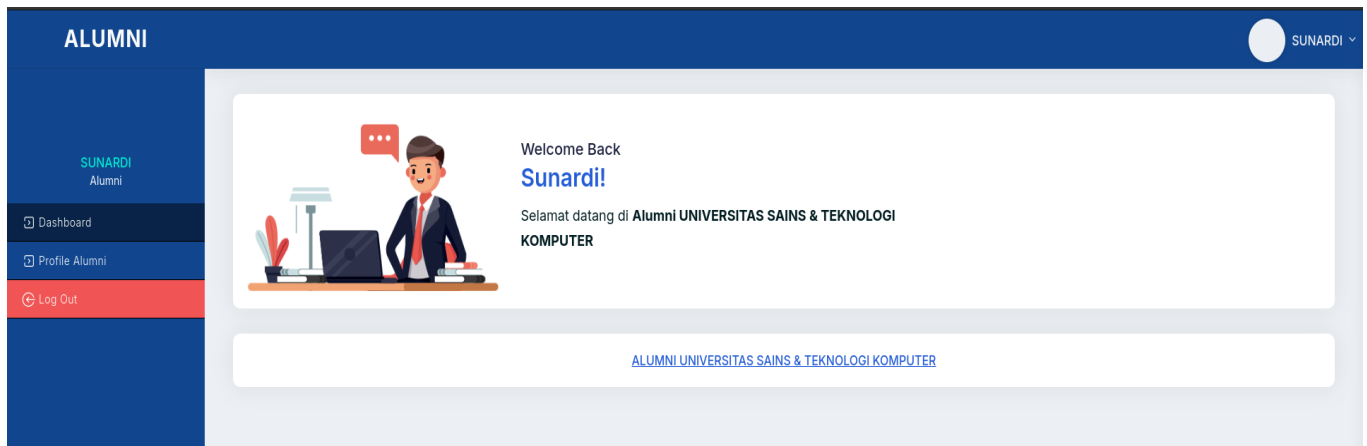
POC:

1. Access the login portal <https://alumni.stekom.ac.id/login-alumni>.



2. When logged in using only the NIM number of the student with a password.
3. By capturing the request using Burpsuite and leaving the password to be blank. The request is sent.
4. Got 200 status and logged in to the students account.

```
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 X-Powered-By: PHP/8.1.31
3 Expires: Thu, 19 Nov 1981 08:52:00 GMT
4 Cache-Control: no-store, no-cache, must-revalidate
5 Pragma: no-cache
6 Cache-Control: max-age=0
7 Content-Type: text/html; charset=UTF-8
8 Content-Length: 5217
9 Vary: Accept-Encoding
10 Date: Tue, 21 Jan 2025 08:44:02 GMT
11 Server: LiteSpeed
12
13
14 <!DOCTYPE html>
15 <html>
16 <head>
17 <!-- Basic Page Info -->
18 <meta charset="utf-8">
19 <title>
20 Login
21 </title>
22
23 <!-- Site favicon -->
24 <link rel="apple-touch-icon" sizes="180x180" href="
25 https://alumni.stekom.ac.id/assets/admin/vendors/images/apple-touch-icon.png">
```



Remediation:

- Implement a strong password policy that requires users to create and use complex passwords during login.
- Make sure that the login requires a password field.
- Ensure the backend verifies the presence and correctness of both the username and password before granting access.

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

Severity: High

Location: "<https://alumni.stekom.ac.id/manage-users/profile/ab79bc851b18231ff1d0360c00d2a5912a97ecf7>"

Vulnerability Descriptions:

- 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.

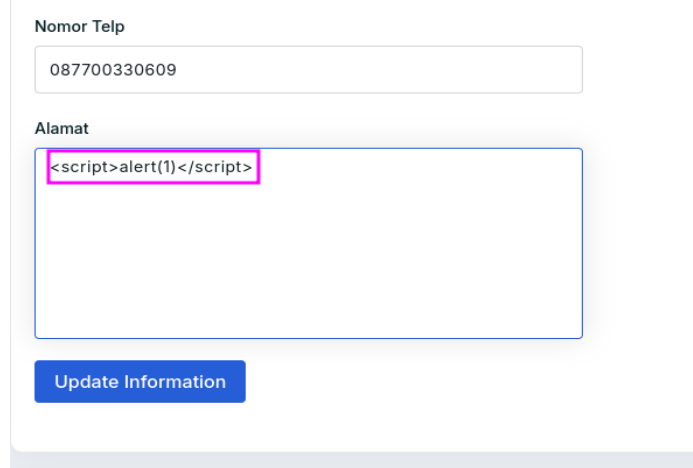
Impact:

- Attackers could steal personal information of the student's Phone number, email id, Cookies by injecting malicious scripts into student profiles or comment sections.

- Exploiting this vulnerability could lead to defacement of university pages, compromising the credibility of the institution and eroding trust among students, faculty, and staff.

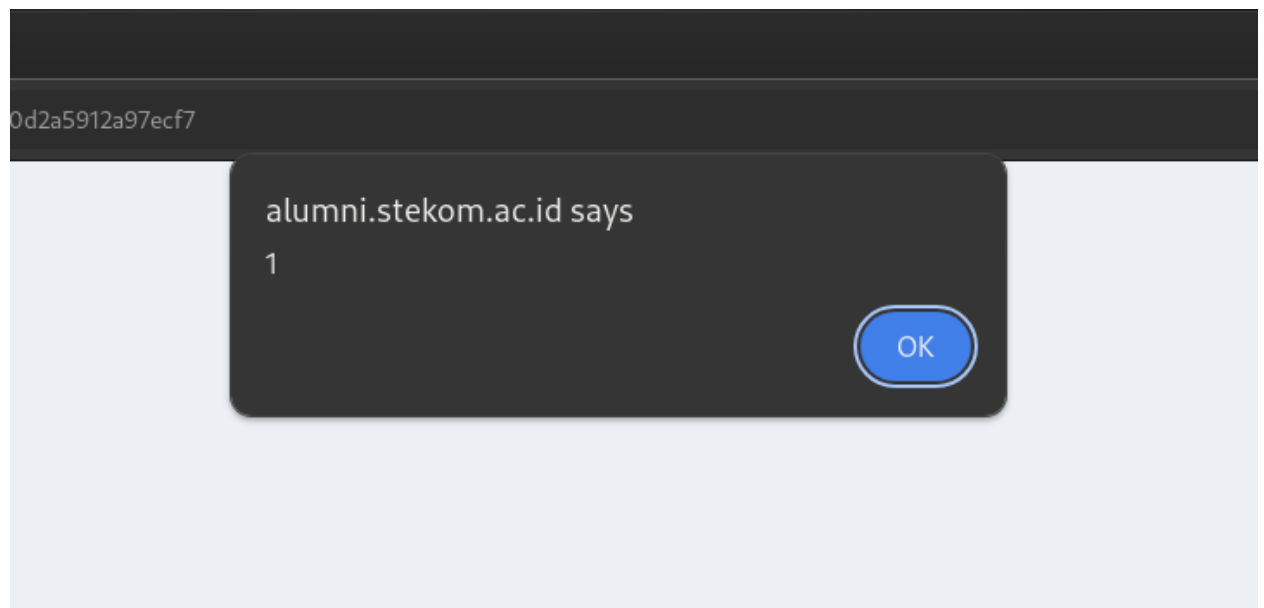
POC:

1. In the Address field of the students profile can execute malicious javascript payload, the used payload `<script>alert(1)</script>`.



The screenshot shows a web form for updating student information. It has two input fields: 'Nomor Telp' (Phone Number) with the value '087700330609' and 'Alamat' (Address). The 'Alamat' field contains the malicious payload `<script>alert(1)</script>`, which is highlighted with a pink border. Below the fields is a blue button labeled 'Update Information'.

2. And by Updating the information function the payloads gets executed to everyone who visits the site and can steal the sensitive information.



Remediation:

- Validate and sanitize all user inputs to ensure that potentially harmful characters (e.g., `<`, `>`, `"`, `'`)

- Implement a strong Content Security Policy (CSP) to restrict the sources from which scripts can be loaded.
- Encode user-generated content before displaying it in the browser, converting special characters into their HTML entity equivalents