



## **Penetration Testing Report**

**Issue date: 4th November 2023**

## Administrative information

### Confidentiality Statement

This document has been created only for use by Harrow. As a result, disclosing anything inside this document is not allowed other than authorized individuals inside the business. Furthermore, no portion of this work may be copied or otherwise communicated. Distribution list below showcases the permissions that is granted.

### Distribution List

	To take action	Reviewed prior to release	For information
Jacob Johnson <b>Chief Security Officer</b> Harrow AS	✓	✓	
Anita Erasmus <b>Senior Risk Manager</b> Harrow AS			✓
Joshua Vieira <b>Head: IT</b> Harrow AS			✓
Felisha Stokkeland <b>Head: Internal Audit</b> Harrow AS			✓

## Contact

<b>Jacob Johnson</b>	Chief Security Officer	JJohnson@harrow.no
<b>Anita Erasmus</b>	Senior Risk Manager	AErasmus@harrow.no
<b>Joshua Viera</b>	Head: IT	JSolomon@harrow.no
<b>Felisha Stokkeland</b>	Head: Internal Audit	FDelange@harrow.no

## Version Control

<b>Revised on</b>	<b>Version</b>	<b>Description</b>	<b>Approved by</b>
16 November 2023	<b>V0.1</b>	Template Created	Jebril PentaserJ
30 November 2023	<b>V0.5</b>	Added findings, screenshots, missing fields	Jebril PentaserJ
4 November 2023	<b>V1.0</b>	The final product	Jebril PentaserJ

# Table of Content

<b>Administrative information .....</b>	<b>2</b>
Confidentiality Statement .....	2
Distribution List .....	2
Contact.....	3
Version Control.....	3
<b>Table of Content .....</b>	<b>4</b>
<b>Executive Summary .....</b>	<b>5</b>
Introduction.....	5
Objectives and Scope.....	6
Summary of findings.....	7
SQL Injection in Login Page.....	7
Unauthorized Data Access via Parameter Manipulation (IDOR) .....	7
Stored Cross Site Scripting (XSS) via Guestbook Field .....	7
Unauthorized File Download via Source Code Exposure .....	7
Time-Based Discount Code Bypass .....	7
Reflected Cross Site Scripting (XSS) within input fields.....	7
Disclaimer.....	8
Strengths .....	8
Appreciation.....	8
<b>Methodology .....</b>	<b>8</b>
<b>Detail Finding.....</b>	<b>9</b>
SQL Injection in Login Page .....	9
<b>Appendices .....</b>	<b>11</b>
Severity framework.....	11
Detailed outputs.....	12
Engagement Letter and Authorization Letter: .....	12

# Executive Summary

## Introduction

During the time frame of 30 November 2023 from 10:00 to 14:00 of the same day, Jebril conducted a vulnerability test on the domain Harrow AS. He discovered various vulnerabilities during the course of this time that Jebril would like to report. The goal of the vulnerability assessment is to find and categorize weaknesses in the web application in the given domain and to recommend solutions and countermeasures to close the gaps. Jebril discovered a total of 6 flaws, which are graded from 1 to 10 by severity.

Severity	Base Score Range V4
Informational	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

The vulnerabilities in this assessment do not disclose all the vulnerabilities present on the web application. SQL Injection, Stored XSS, Reflected XSS, Insecure Access Control, Business logic and Broken Access Control, were discovered in the web application. Some of these findings are very common and have simple fixes; if you want more information about the vulnerabilities, see Detail Finding and Appendix. If these flaws are not addressed, the consequences might be severe and damaging. The repercussions include data breaches, financial loss, reputational harm, regulatory compliance violations, long-term effects, and more. Harrow AS should pay close attention to these vulnerabilities and resolve them as soon as possible. Harrow must address and rectify vulnerabilities with a proactive and systemic approach to cybersecurity. It is critical to do frequent security assessments, patches, coding practices, and employees awareness training.

## Objectives and Scope

The primary goals, as approved with management, were to find any exploitable holes in the Harrow AS environment that would provide someone access to the system and data without authorization. It was approved for testing to occur between the hours of 10:00 on November 30, 2023, to 14:00 the same day. The main goal is to locate and exploit potential security vulnerabilities in the Harrow AS infrastructure that do not compromise the availability or integrity of live systems. To accomplish this, a scope will be established, thus it's critical to stay inside of it.

### Scope

**The scope of this penetration testing was limited to a penetration test of the Harrow web application, and included the following:**

- The web application and any utilized web application framework (including webserver and back-end database).
- You may conduct testing at any time within the scheduled period.
- You are authorized to elevate privileges on the application.
- While the system source code and database schema are not explicitly provided, should you obtain this, you may use it to further enhance your report. The primary focus of the penetration test is on the security of Internet facing services, rather than access via the system console.

**The scope of our engagement specifically excluded the following activities:**

- The host operating system (and by extension the system platform as a whole). As such you are not expected to elevate privileges on the operating system.
- HTTP(S) configuration is strictly out of scope since testing targets the homologation environment.
- No external systems other than the target may be considered.
- This is a purely technical engagement. There is to be no phishing or social engineering of staff or vendors. Denial of Service is also not in scope.
- You should minimize the use of any automated testing tools as there are concerns as to the fragile state of the web framework.
- We are not interested in the following already mapped vulnerabilities: clickjacking, cross-site request forgery, cookie attributes, logout functionality, brute force against the login page, ID enumeration, and open redirection.

## Summary of findings

The following findings were made during the assessment.

Number	Finding	Risk Score	Risk
1	<i>SQL Injection in Login Page</i>	9.3	Critical
2	<i>Unauthorized Data Access via Parameter Manipulation (IDOR)</i>	8.7	High
3	<i>Stored Cross Site Scripting (XSS) via Guestbook Field</i>	8.5	High
4	<i>Unauthorized File Download via Source Code Exposure</i>	7.1	High
5	<i>Time-Based Discount Code Bypass</i>	6.9	Medium
6	<i>Reflected Cross Site Scripting (XSS) within input fields</i>	5.1	Medium

## Disclaimer

The vulnerabilities in this assessment do not disclose all the vulnerabilities present on the web application. These findings are the findings Jebril was able to find, there could be more. As a result, it's critical to consider if there are any new vulnerabilities, or if Jebril missed any. No application, no matter how thoroughly tested, can ever be 100% safe. This report is only designed to provide verification that Harrow has remedied all of the issues in this report.

## Strengths

The listed results demonstrate a dedication to cybersecurity best practices and offer a strong basis for security enhancements. During the evaluation, Jebril made an effort to detect infiltration and employed best practices to strengthen the system.

## Appreciation

We would like to thank the business's personnel and management for their support and cooperation during the external penetration test. We would not have gotten very far without them. We would also like to thank Harrow AS for giving us a chance to test our skills and advance to the next level.

## Methodology

*Reconnaissance, Mapping, Discovery, and Exploitation* were the four main processes under the *Authorization and Scoping* component. During the reconnaissance we tried to gather information about Harrow's network systems. On this phase port scanning, enumeration and other methods was used to gather all the information about the asset on the target. After the reconnaissance, all the other phases are cycled. While doing so mapping plays a big role since there is a lot of information that needs to be organized. During the mapping phase it's recommended to use a mind map. After mapping comes the discovery phase, here is where the finding of vulnerabilities takes place. This stage is typically where a lot of "clicking every place" on the web application comes in. When having a clue of what can be exploited, we move onto the exploitation phase and try different payloads. Tools that were used in reconnaissance are nmap, and dirb. During all these phases Jebril gathered evidence of the vulnerabilities. The Figure below shows how the methodology is built up.



## Detail Finding

### SQL Injection in Login Page

Number	Finding	Risk Score	Risk
1	SQL Injection in Login Page	9.3	Critical

**Vector:** CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

SQL Injection is a type of attack that employs malicious SQL queries to access the backend database. If done successfully and the application is vulnerable, it can access unauthorized information that was not intended to be displayed. The information might change based on the database and the type of statements performed.

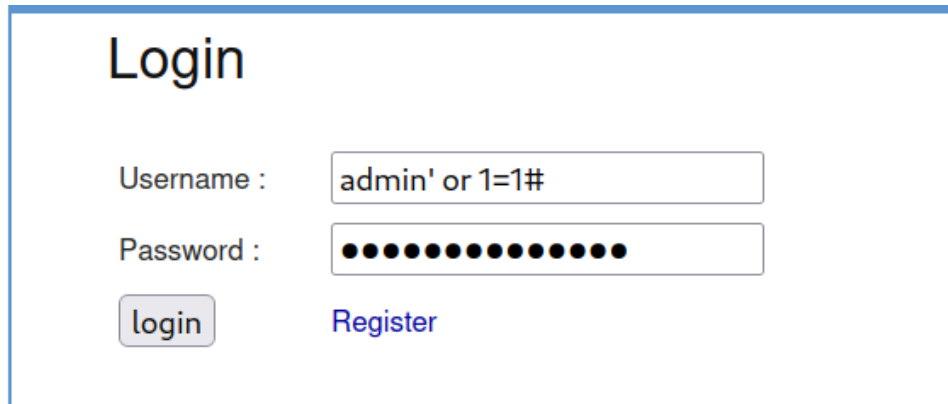
### Exploit Detail

SQL Injection vulnerabilities may be exploited by injecting SQL statements to test how the system responds. By inspecting the responses, you will receive feedback from the backend along with an error indicating what went wrong. In this instance, the web application is vulnerable. After testing the login and password fields of the most tested statement Admin ' or 1=1#, Jebril received an error message indicating that the web application is insecure. Figure below shows what kind of payload was used to detect the vulnerability.

### Potential Impact

SQL injection may result in data disclosure, financial loss, reputational damage, privilege escalation, authentication bypass, and other repercussions. The consequences might be severe, long-lasting, and even damaging to individuals whose data got exploited.

## Evidence



The screenshot shows a web application interface with a blue header bar. Below the header, the word "Login" is displayed in a large, bold, black font. Underneath, there are two input fields: "Username :" and "Password :". The "Username" field contains the text "admin' or 1=1#". The "Password" field is filled with 15 black dots. Below the "Username" field is a button labeled "login" in a grey box. To the right of the "login" button is a link labeled "Register" in blue text.

By trying payloads, Jebril managed to try admin' or 1=1#. By using ' we are trying to trick the database into thinking that we are closing the statement within the database. Since the statement is closed in the backend database, we can now try to use our own statement. Or 1=1#, makes it that if Admin is False then look if 1=1 is True (which is True) and we comment out the rest with the "#". The payload was passed on both Username and Password since both or only one can be vulnerable.

**flag:0a32b9973c104c04263beed280d34522**

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 1

## Remediation

To be secure of these kinds of vulnerabilities it's important to have good coding practice. A web application firewall (WAF) can protect a web application against injections. When setting database access, the web application should follow the concept of least privilege to reduce and defend against SQLi. Special characters should be escaped to prevent them from being recognized as SQL syntax. Employees should attend Security Awareness Training to verify that they are following best practices and mitigating risks. Error Handling should be implemented, and if an error occurs, sufficient error handling should be done to avoid disclosing critical database information. Finally, input validation and sanitization should be used. The web application validates and sanitizes all user input before utilizing it as SQL queries and does not allow assertions that might cause harm.

# Appendices

## Severity framework

The table below shows how the degree of severity is evaluated, as well as what these severity ratings indicate in more detail. This range of scores is utilized throughout the assessment report.

Severity	Base Score Range V4.0	Description
Informational	0.0	There is no vulnerability. Further information on things discovered during testing, tight controls, and additional documentation is supplied.
Low	0.1-3.9	Vulnerabilities cannot be exploited, but they do decrease an organization's attack surface. It is recommended that you devise a plan of action and patch during the next maintenance window.
Medium	4.0-6.9	Vulnerabilities exist, although they are not exploitable or need further actions, such as social engineering. It is recommended to develop a strategy and patch when high-priority issues have been handled.
High	7.0-8.9	Exploitation is more difficult, but it might result in higher privileges and even data loss or disruption. It is recommended to devise a strategy and patch as soon as feasible.
Critical	9.0-10.0	Exploitation is simple and frequently leads in system compromise. It is recommended to devise a strategy and fix promptly.

There are five categories for the vulnerabilities: **Informational**, **Low**, **Medium**, **High** and **Critical**. Critical is the most severe category, with Informational being the least harmful. In order to guarantee data confidentiality, integrity, and availability, flaws in the Critical section should receive your complete attention. Security remediations should be implemented as described in the security assessment findings. These ratings are graded according to CVSS 4.0 rating calculation. CVSS categories the severity and metrics in 3 sections being the base score which represents the intrinsic characteristics of a vulnerability which are constant over time and across user environments. And the other 2 sections are Temporal and Environmental. These calculations can be put into a vector score which you will see within this assessment report. Keep in mind that the fundamental framework for vulnerabilities based on defined sets of metrics is provided by CVSS. Businesses must complete this baseline score with a risk assessment that is appropriate to their situation. The company has to perform an internal risk analysis to determine how the risk is present in their business environment.

### Detailed outputs

Number	Finding	Risk Score	Risk
2	Unauthorized Data Access via Parameter Manipulation (IDOR)	8.7	High

**Vector:** CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Number	Finding	Risk Score	Risk
3	Stored Cross Site Scripting (XSS) via Guestbook Field	8.5	High

**Vector:** CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Number	Finding	Risk Score	Risk
4	Unauthorized File Download via Source Code Exposure	7.1	High

**Vector:** CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

Number	Finding	Risk Score	Risk
5	Time-Based Discount Code Bypass	6.9	Medium

**Vector:** CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:L/SA:L

Number	Finding	Risk Score	Risk
6	Reflected Cross Site Scripting (XSS) within input fields	5.1	Medium

**Vector:** CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N

**Engagement Letter and Authorization Letter:**



Harrow AS  
Tordenskjoldsgate 9, 4612, Kristiansand  
410 00 000  
info@harrow.no  
www.harrow.no

To: Lead Penetration Tester,

This letter serves as the engagement letter between Harrow AS (henceforth referred to as Harrow) and your consultancy, confirming the agreed terms for security testing services requested by Harrow at a meeting held on 14 November 2023.

Per the discussions, Harrow AS has recently acquired a new web property as part of a larger acquisition of security assets. We recognize that this system seems to have been sorely neglected by its previous owners and administrators and is likely a serious security risk to our organization. As mentioned during the preliminary discussions with your pre-engagement team, “we don’t want to be the next Sony”. As such the acquired host has been completely isolated from the rest of our systems and from the internet at large. We would however like to return this site to a ‘live’ status as soon as possible.

Per our agreement, you have been commissioned to conduct a penetration test on the system in question at very short notice. Your engagement is scheduled for 30 November 2023 and runs from 10:00 to 14:00 of the same day. Our management team is required to present your report at a board meeting the subsequent week. Your report should be addressed to Harrow AS, since complete rebranding of the newly acquired web property has not yet occurred.

The key contacts and recipients from Harrow include:

Jacob Johnson	Chief Security Officer	<a href="mailto:JJohnson@harrow.no">JJohnson@harrow.no</a>
Anita Erasmus	Senior Risk Manager	<a href="mailto:AErasmus@harrow.no">AErasmus@harrow.no</a>
Joshua Vieira	Head: IT	<a href="mailto:JSolomon@harrow.no">JSolomon@harrow.no</a>
Felisha Stokkeland	Head: Internal Audit	<a href="mailto:FDelange@harrow.no">FDelange@harrow.no</a>

The following have been defined as part of the engagement as 'in scope':

- The web application and any utilized web application framework (including webserver and back-end database).
- You may conduct testing at any time within the scheduled period.
- You are authorized to elevate privileges on the application.
- While the system source code and database schema are not explicitly provided, should you obtain this, you may use it to further enhance your report. The primary focus of the penetration test is on the security of Internet facing services, rather than access via the system console.

The non-scope of the engagement is described next:

- The host operating system (and by extension the system platform as a whole). As such you are not expected to elevate privileges on the operating system.
- HTTP(S) configuration is strictly out of scope since testing targets the homologation environment.
- No external systems other than the target may be considered.
- This is a purely technical engagement. There is to be no phishing or social engineering of staff or vendors. Denial of Service is also not in scope.
- You should minimize the use of any automated testing tools as there are concerns as to the fragile state of the web framework.
- We are not interested in the following already mapped vulnerabilities: clickjacking, cross-site request forgery, cookie attributes, logout functionality, brute force against the login page, ID enumeration, and open redirection.

You are required to undertake a Penetration Test on this target, paying attention to all the items in scope. You should specifically focus on the web application with a secondary focus on any other services on the host that are exposed to the network and the underlying host platform and any supporting software/application frameworks.

This letter also serves as authorization to perform testing within the stipulated scope.

Warm regards,

A handwritten signature in blue ink, appearing to read 'Jacob Johnson', with a stylized, flowing script.

Jacob Johnson  
CSO – Harrow AS