hardsecure

CASE STUDY

PENTEST

WHAT IS THE IMPACT ON YOUR BUSINESS?

R. Acácio de Paiva nº 16, 1ºdir,
1700-006 Lisbon, Portugal

www.hardsecure.com
geral@hardsecure.com

INDEX

OBJECTIVE

The purpose of this document is to provide an overview of a vulnerability found in a pentest performed in a Hardsecure customer, addressing, where necessary, more technical aspects of the tests performed, but focusing on a clear and concise presentation that allows someone not versed in technical details to understand the impact of what was found, what contribution the carrying out of a pentest can have to the business activity, either by what it reveals about the real protection of the data targeted by client applications, or by the mitigation of vulnerabilities and consequent reduction of the attack surface, and the potential damage that exploiting them could cause to an institution (financial, reputational, among others).

FRAMEWORK

Hardsecure was requested to perform a Pentest in a web application that serves as a portal for employees and associates of the specific customer.
After authentication, internal users of the entity have accounts with roles (hereinafter referred to as roles) appropriate to the role they perform in it (e.g. Financial Department, IT Department, Administration, among others), and there are also accounts for partners of the entity, with very limited access and limited permissions compared to the actions they can perform.
Authentication in this application is made by a third party entity, which after inserting the correct credentials by the user, directs him towards the homepage of the platform appropriate to the role of the user has on it.
Once inside the platform, depending on the user's role, it is possible to configure the allocation of financial funds, change business priorities previously defined for the several departments, or create new ones, modifying project deadlines, managing the platform itself (create, update, read or delete entities of the platform, whether these entities are users, their permissions, documents, among others), or, for accounts with lower privileges, simply viewing information that users with permissions to create, edit and remove content on the platform makes available.

WHAT WAS THE CUSTOMER´S INTENT BY REQUIRING THE PENTEST

In a pre-pentest phase, it was understood what would be the customer's priority, i.e., given the features provided by the platform and the business concerns, what type of vulnerabilities they would consider more pressing, and to what would be more useful to spend larger blocks of time during the tests, given the time window agreed to perform them.

The intent at this stage was very clear: to understand, given the time constraints for engagement, what the client was concerned about, and what is considered to be a priority in a pipeline of intrusion tests.

Given that this was a platform with a panoply of roles and information that had to be fairly well segmented among all the departments represented on it, the client made it clear during this process that it was crucial to ensure that access to a department's data was contained to that department, and the restriction of access to data outside the scope of a particular role was ensured, especially since some of the visible and editable data on the platform targeted information with some relevance for the business.

On top of all this lateral segmentation, in the sense of users with more or fewer permissions, but without a direct hierarchy between them, the platform's administration section would also have to be very well protected, apart from any of the others, since compromising it would jeopardize the compromise of all the sections.

It was therefore clear that, given the role that the platform represented to the customer and the various types of users that interacted with it daily, one of the focuses of the pentest would be to understand if there was any type of Broken Access Control, i.e., if unauthorized users were somehow able to access or change information outside of what, at the outset, would be their scope of action, given the assigned role. As an example, if someone as a common user, without major privileges, would be able to access the administration panel (having reached during the pentest the conclusion that yes, they would).

REQUIREMENTS

To test this particular vulnerability, the customer was required to provide user accounts that in their view, warranted more exhaustive testing.

FINDINGS

During the execution of the tests, it was possible to notice that a partner account, which at the beginning should only have read permissions of what was made available to it by roles with greater authority on the platform, able to access the financial management panels of the company. Although some actions of the Financial area could not be directly executed with this minor account, through the code analysis present in several pages it was possible not only to identify functions that executed certain actions of the department, and call them with the appropriate parameters according to the intention, but also to identify functionalities hidden only by styles (CSS), in the pages. Thorough inspection and alteration of code in the browser itself, client-side, it was then possible to reveal a series of hidden panels, but still present in the platform, visible to someone with the disposition to look at its code and understand the totality of what it contained.

Later was verified the possibility of exfiltration of access logs, reports, and alteration of contents related to the Financial area by this account with minor privileges, of partner.

Eventually, still with the same account, it was possible to access the administration panel of the platform, where, among other actions, it could be performed the elevation of this particular partner account to an administrator account, or, as an example, a total deconfiguration of the platform, from placing all the administrators of the same with fewer privileges than any partner account to the complete removal of permissions (not only their allocation or not to certain roles, but even making the non-existent rule), changing the platform filters, which would make more private information available to users who should not have permission to access it, among others.

These last actions listed would easily draw the attention of those responsible for the platform, and since they are not the least bit silent, one would quickly realize that there was something wrong, or that someone was interacting in a destructive way with the platform.

Even so, all these actions were a possibility and explored in a more furtive and measured way, during a long period of time, would certainly cause more than ephemeral damage to the entity, without immediately sounding so many noisy alarms.

Hardsecure noted the possibility of this scenario and made an attempt to deregulate the platform, restricting itself to gathering evidence that proved the possibility of the actions in question. At no time was the normal functioning of the platform disturbed.

Through the analysis of the code provided by the browser (function names present in files, parameters, etc...) it was also possible to understand the nomenclature predominantly used by the platform developers, to access particular pages/paths/files of the platform, given the nature of the business, and from there to other areas whose existence was initially veiled to any of the past accounts, but which were still present on the platform.

The impact of such a finding - an account without major privileges reaching the administration of a platform - is serious, given the data the platform handles and the actions it allows. Moreover, during the pentest, a considerable number of user accounts were found in data breaches, with the entity's domain, having, after accessing the administrator panel, verified the presence of these same accounts on the platform, by listing all the users of the same.

Depending on the client's remaining care regarding the platform's security, peripherally to this isolated pentest, someone malicious could have had access to this data, to admin panels, funds, among others, for a potentially unlimited time.

The mitigation of this particular vulnerability, by correctly segmenting the access of users to the areas relevant to their role, allows the creation of concrete barriers between the different types of actions that may be performed on the platform, limiting them to those who legitimately have permission to perform them.

Imagining that someone, just by having an account on a site/platform, would be able to access its administration panels, eventually configure it as they wish, view information from other users without major restrictions, among other powers that the role of an administrator entails, it is clear then, without much room for doubt, the value adds to a business, gaining visibility of this fact and ensuring something that from the outset is taken for granted by most users with an account on any site: The segmentation of the actions of your account compared to others.

CONCLUSION

Other vulnerabilities were found during this test, but since this document is a very particular analysis of only one vulnerability of an engagement, the intention is to try to demonstrate how far only one vulnerability can go.

The purpose against this specific vulnerability was to give visibility to the client of gaps in basic elements of a platform that incorporates the concepts of user accounts and roles associated with them, elements that, precisely because they are basic, are practically taken for granted by any user of a platform of the same type. Namely, we refer to the segmentation between your account, what it can do, what it can access and modify, and the other accounts on the platform. It would be a clear blow to the trust and credibility of an entity, if eventual exploitation of this vulnerability with purposes other than testing, hence the importance of a Pentest, and the visibility it gives.