Security evaluation BlackBoard environment UvA

Bram ter Borch - Auke Zwaan



# Subject

BlackBoard is a virtual learning environment and course management system developed by Blackboard Inc. The University of Amsterdam (UvA) uses a BlackBoard environment for all students, blackboard.uva.nl. The goal of this project is to perform a security evaluation of the UvA BlackBoard environment.

# Conditions

* The application owner need to approve the test.
* Requirements of the OS3 ethics committee need to be met.

# Approach

Within the first two days, we will read into ways of attacking a webpage. This includes setting up an attack environment and communicating the details to the application owner. Then, a clear scope (including our goals) will be defined, after which we will spend around 3 or 4 full days purely on penetration testing. We will perform this security evaluation with two different approaches. First, we want to do a black-box analysis to see what a student is able to do when logged in to the system. Second, we are interested in a grey-box analysis. By doing so, we want to examine where and how passwords are stored, what encryption techniques are used and what mechanisms are in place to provide security in different ways. The blackbox tests and the greybox tests will be performed on the test environment as it is practically the same as the production environment. Therefore, the production production system will not be disturbed.

During the tests, we will start writing the report, including recommendations. All vulnerabilities will be given a rating based on their likelihood and impact. For the recommendation we will focus on countermeasures that can be implemented by the application owner not only in theory, but in practice as well.

# Ethics

In the Dutch law, the 'Wet Computercriminaliteit' applies directly to this research. Without written consent of an authorized person, we are not allowed to do any security tests on Blackboard. Therefore, this consent was provided by the application owner. The signed letter of consent is attached to this proposal.

The application owner requested us to also attend a meeting to present the plan of approach so both the application and the system owner can verify the methods and know what is coming during the security tests.

To make sure that our activity can be identified at all times, a clear and strict scope defined in the letter of consent. This includes the IP addresses of both the attackers and the target systems.

We will not collect more data than strictly necessary for the security evaluation. All data will be stored on secure systems. All data will be securely removed after finishing the project.

OS3 has strict guidelines on responsible disclosure of any issues. These guidelines are described in the Responsible Disclosure Procedure of the Ethics Committee OS3 (ECOS3) and can be found at the following link: <https://www.os3.nl/_media/2014-2015/info/ecos3-procedure.pdf>. The members of ECOS3 will, at all times, lead the communication for the disclosure process if vulnerabilities are found.

Publication of the report is in collaboration with the system owner, in June a new version of the BlackBoard application will be going live and after this implementation the report can be published.