Pentesting BlackBoard

Bram ter Borch - Auke Zwaan



# Subject

The goal of this project is to expose vulnerabilities, if any, of the application Blackboard (blackboard.uva.nl) and report these issues to the application owner within the University of Amsterdam (UvA). We will perform this penetration test 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. Besides this, 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. Since this application is used by all UvA students and personal information is stored within the application, the project is relevant as tens of thousands of people might be affected in case of a cyber incident. The results will be addressed and improvements are suggested to the owner of the application.

# Conditions

To perform the test, we need to get into contact with the functional owner of the Blackboard application. Since Bram is an employee of the UvA he is able to get into contact with the application owner and deal with the ethical issues concerning the attack from the university’s side.

The UvA’s implementation of the Blackboard application, according to the application owner, is never audited this way. Therefore, we believe, the chances of finding at least some minor issues are relatively high. The big task will be to deal with the complexity of the system and to define and follow a structured approach.

# Aproach

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. This includes the IP range from which the attack will be performed. 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. During these tests, we will start writing the report and have to figure out how to use the data and come up with ways of improving the system.

This project is of an academic level due to the approach. We will try to get data out of the system without the risks for other users and without the possibility of bringing the system to its knees. All the information retrieved will be kept secure and will be destroyed after the research. Since we look into the black-box and grey-box approach the research gets its depth. This means we will come up with an approach first and then we will try to use this approach to ‘attack’ the system. The real ‘intelligent’ part of the test will be the recommendations. One can never assume a system to be fully secure since there will likely be factors that limit some security measures (budget, compatibility, etc.). Taking these factors into account, we will try to come up with reasonable countermeasures that can be implemented by the application owner not only in theory, but in practice as well. All vulnerabilities will be given a rating based on their likelihood and impact.

# Ethics

To make this project work we will take care of the necessary ethical measures. The students need to sign a document stating that they will not keep the data found during the test and will not get more data then necessary for the project, the report will not be publicly available and that some parts may have to be altered after inspection by the security officer. A daily reports needs to be send to the system owner containing the security threads found so far. The system owner will receive possible improvements for the system. The results will be presented for the system and application owner.

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 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 the attack is clearly visible at all times, a clear scope is strictly defined in the signed letter of consent. This means the IP addresses of both the attackers and the systems to be attacked are known. In case a real attack is done by a third party during the tests, it can still be identified as such by filtering out these 'trusted' IP addresses.

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.

# Limitations

Because blackboard is one of the critical applications within the UvA not every all attacks are allowed during the blackbox tests. Because the goal is to see what a regular student can do to the system using “hacking” tools. The blackbox tests will be performed on the live system.

The brute force attacks and attacks on the operating system can only be performed on the test environment.