**Desktop Cloud Technology's smart online campus system has ultra vires, leading to serious information leakage**

**Vulnerability Introduction:**

**Because the system interface is not authenticated, data packets can be constructed to arbitrarily view the information of teachers and students in the school, and the data is extremely detailed, including the names, ID cards, and photos of all teachers and students (including graduates) of the school where the system is located. , address, mobile phone number, address, college class, student number and other information.**

**Vulnerability hazards:**

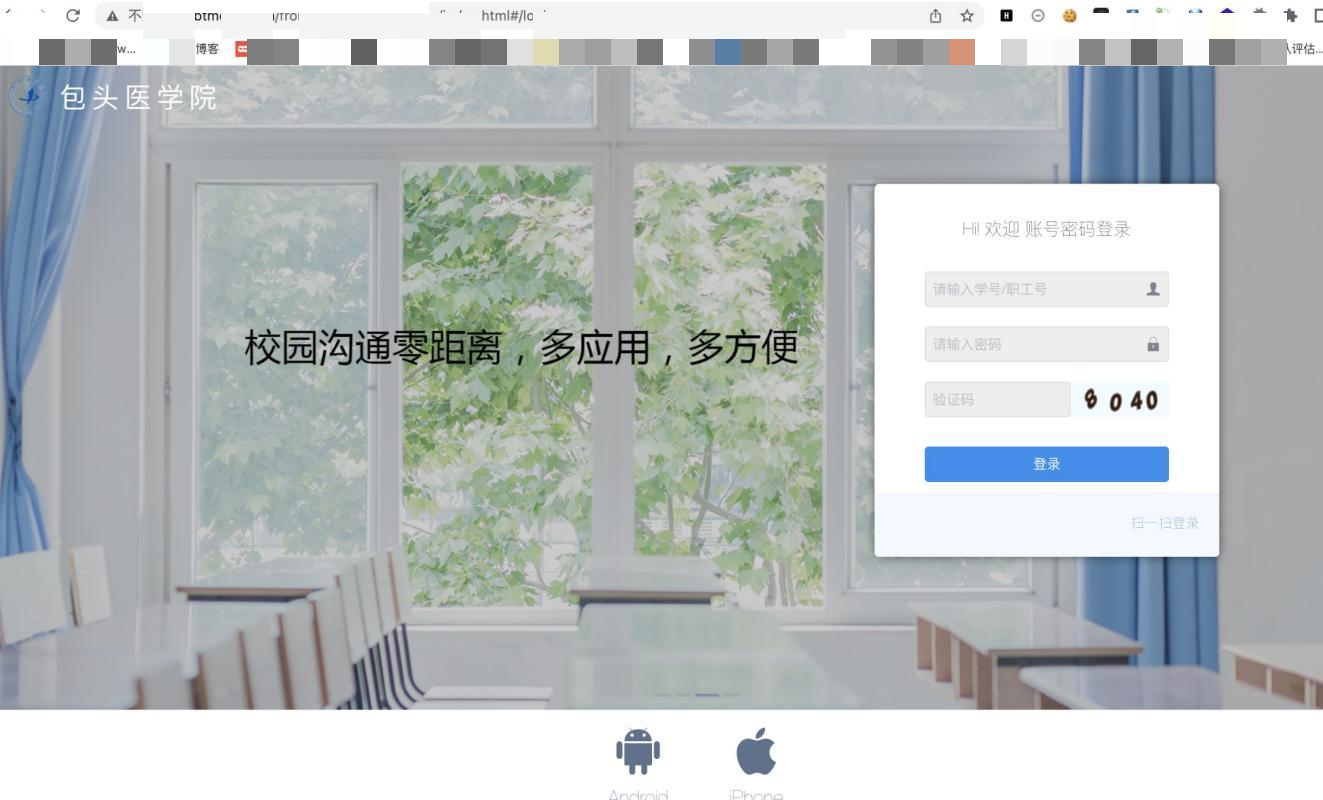
**It leaked tens of thousands of extremely detailed data of each school that used this system, including the names, ID cards, photos, addresses, mobile phone numbers, residential addresses, college classes, student numbers and other information of teachers and students (including those who have graduated) . It may lead to telecommunication fraud, account theft and other events that seriously endanger people's safety.**

**Coverage:**

**The data on its official website as of 2018 shows that less than 40 schools in China use this risk component, but the actual test shows that it is far more than that. There are some schools with loopholes that are not on its display interface, and incomplete statistics have been carried out. , more than ten colleges and universities in China's Inner Mongolia region have used it and reproduced it in six colleges and universities, all of which have this problem.**

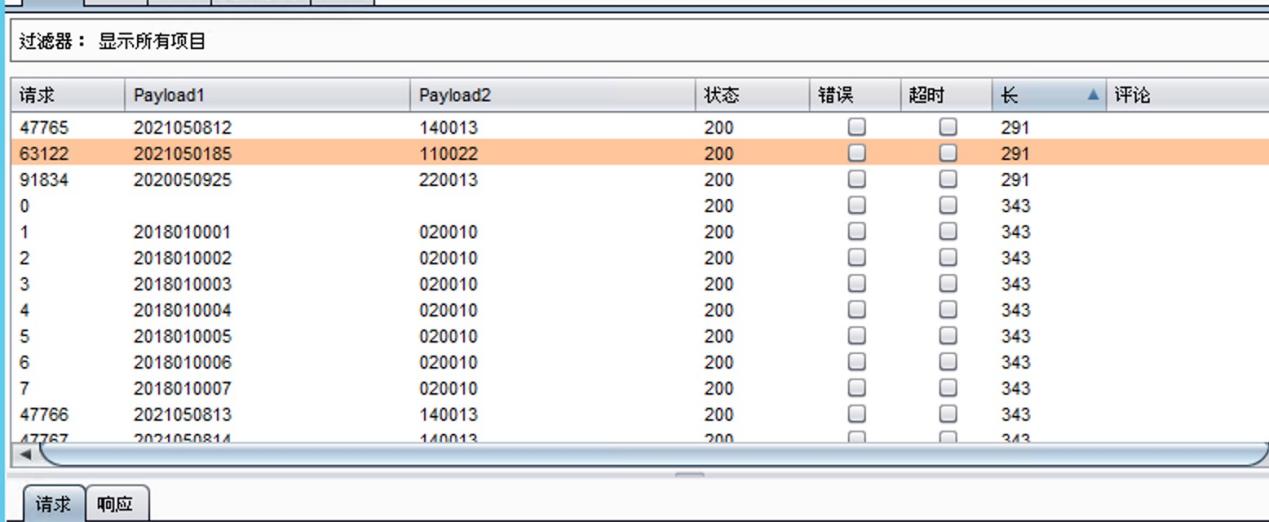
**Exploit Difficulty: Easy**

**Vulnerability Exploitation Process:**

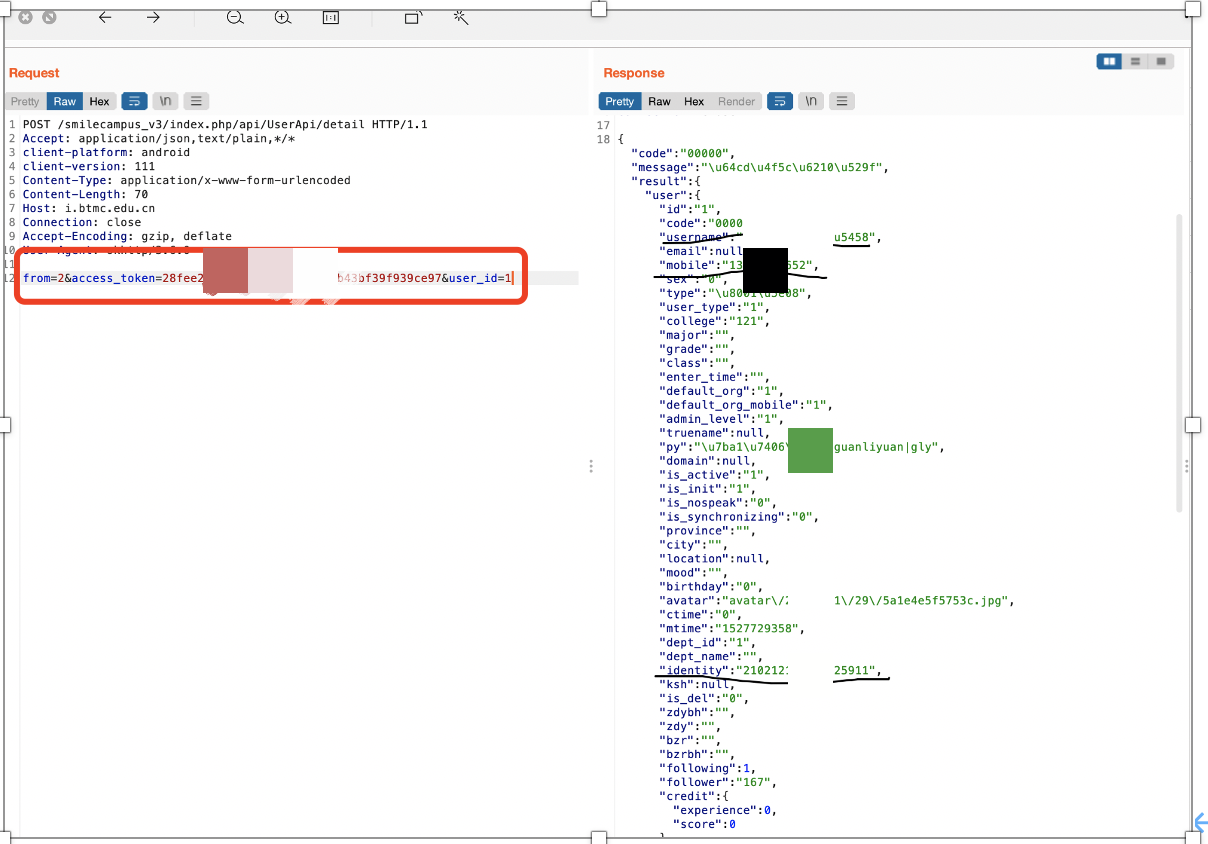


**Log in and blast this system, or social workers can obtain account passwords, because the users of this system are all students and teachers, and the database of each system has about 10,000 users, and according to my observation, the default password is The last six digits of the ID card, so it is very simple to blast out the password. I obtained the account passwords of the students of the six schools in less than half an hour through the blasting method, and successfully completed the vulnerability verification of these six schools. Because of the huge number of users, it can even be obtained through "friends".**

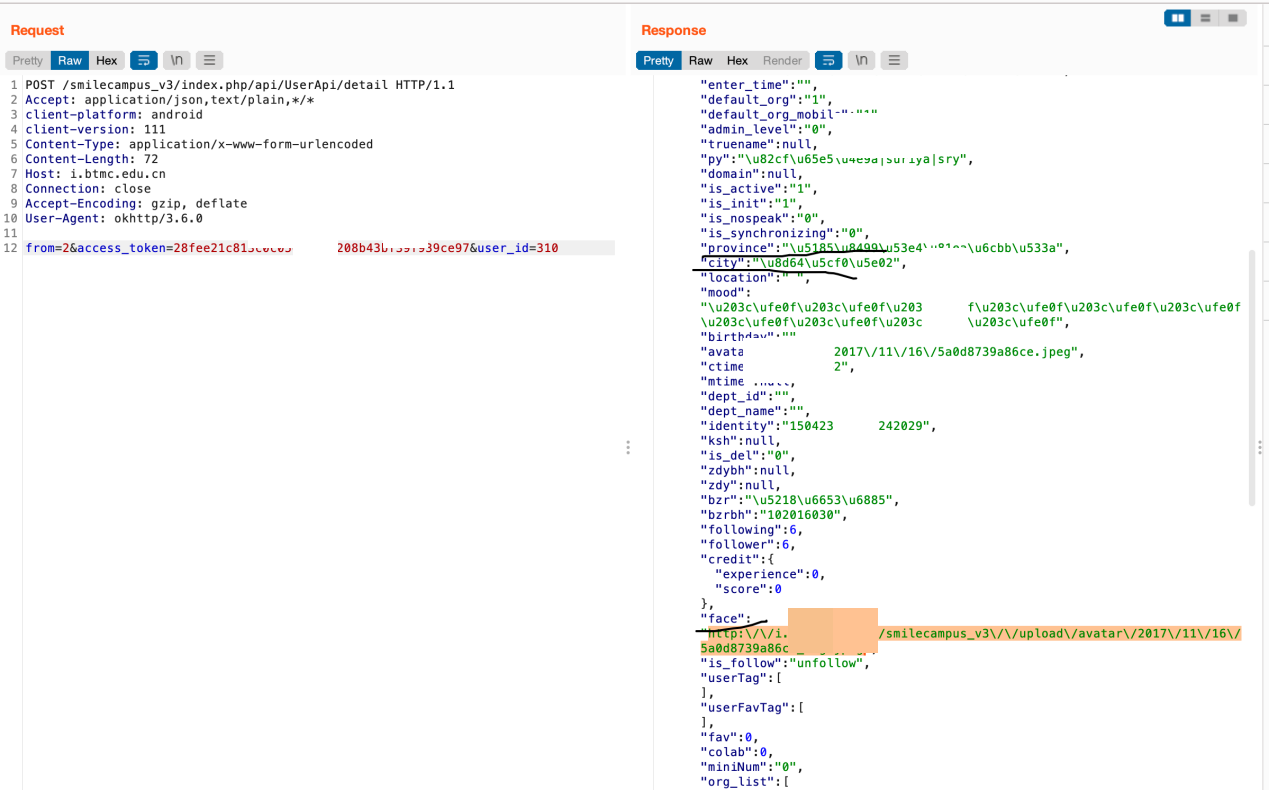
**Like a screenshot of my blasting success**

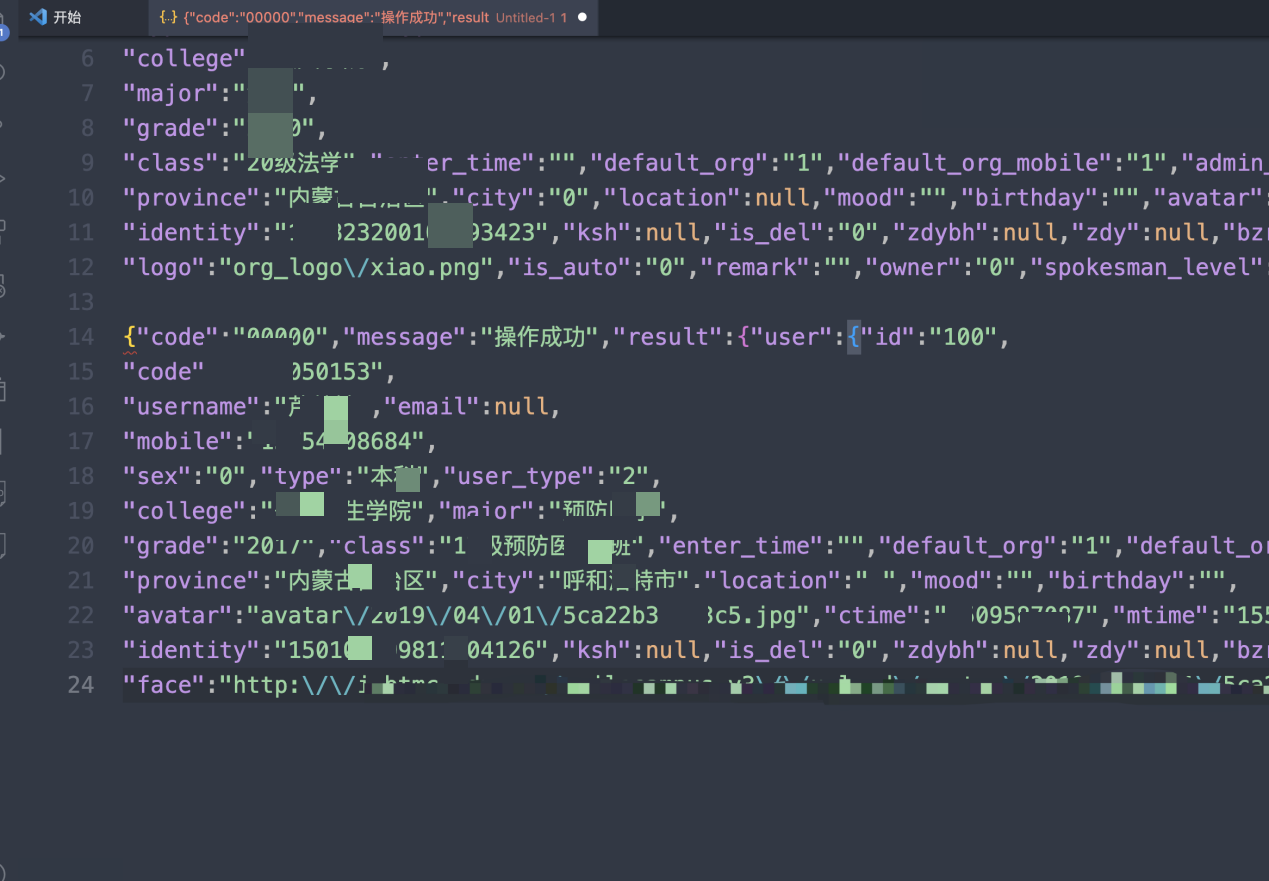
****

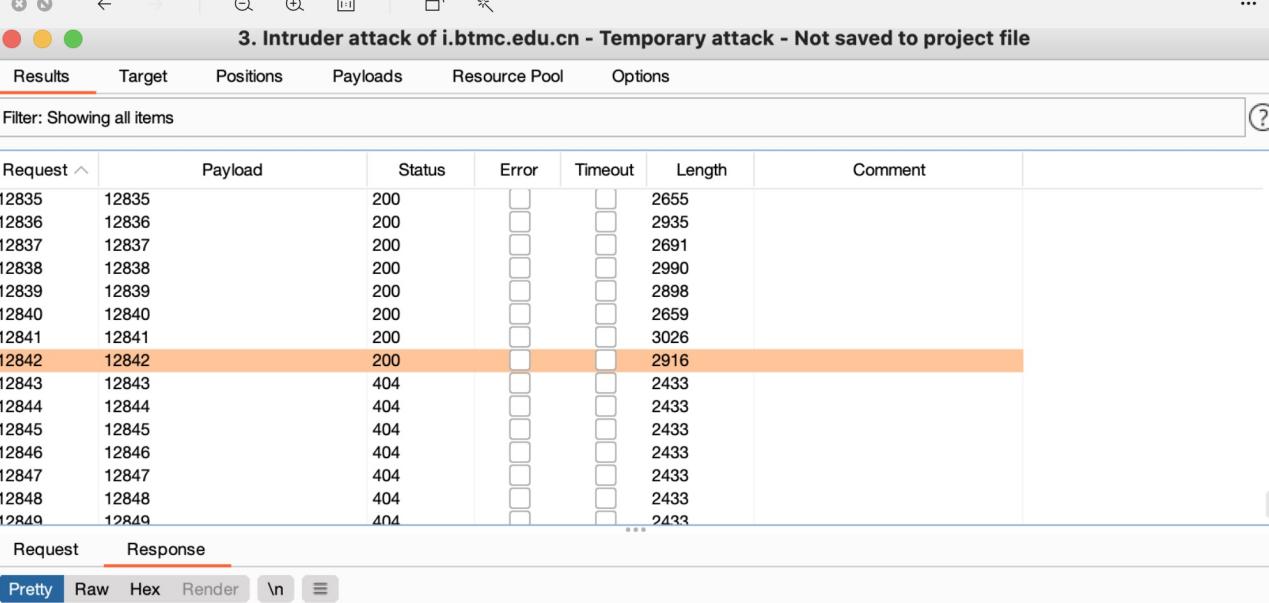
**After we log in with the account password, we will get a token, just replace the obtained token with the token in the red box in the figure below**

****

**As shown in the figure above, a page of data is successfully obtained. We change the id, and we can see that a different page of data is successfully obtained:**

****

**We can take a random page and decode it. As shown in the figure, we can get the name, ID card, photo, address, mobile phone number, address, college class, student number, gender xw and other information, and display any decoded data. Photo:**

**By traversing the id parameter, we can find that the school has a total of 12,842 pages, with more than one piece of data per page, so tens of thousands of pieces of data have been leaked, including the names, ID cards, photos, addresses, and mobile phone numbers of all teachers and students in the school (including those who have graduated). , address, college class, student number and other information:**

**Schools with successful vulnerability verification:**

**In order to prove that this loophole is a general loophole, a total of six schools, including Baotou Medical College, Baotou Normal School, Baotou Iron and Steel, Jining Normal School, Ordos Institute of Applied Technology, and Ordos Vocational College that have used this system, have been tested. Verification succeeded.**