# Lab: Developing a custom gadget chain for java deserialization.

1. Get request got pass the cookie session which can be injection/altered. Get the generated session cookie.

Java program: <https://github.com/wongyaochang-123/UsefulExploits>

Sample Cookie as shown below.

Graphical user interface, text, application, email

Description automatically generated

2. Using a serialized object and base64 encode it.

Find the java codes through the requests and replace the original cookie with the cookie as shown above. The cookie will change the original SQL query and make it into a query which steals the password from the database (blind SQL injection). Then send the compiled java in compiled byte code version and replace the user session's java original byte code version.

Graphical user interface, text, application

Description automatically generated

3. Then the system is flawed and cant detect its an SQL injection and sends to the server and puts out the results of the SQL injection

Graphical user interface, text, application, email

Description automatically generated

Step3: take action, e.g. delete user

Graphical user interface, text, application, email, website

Description automatically generated