**Assignment 4**

**What is burp suite?**

Burp Suite is a graphical integrated development environment (IDE) used for web application penetration testing. It is developed by PortSwigger and is the most widely used web application security testing software. Burp Suite provides a suite of tools that can be used to manually or automatically test web applications for security vulnerabilities.

Burp Suite works by intercepting and analyzing all HTTP traffic between the web browser and the web server. This allows the user to see and modify the contents of requests and responses, as well as to send requests to other tools in Burp Suite for further analysis.

Burp Suite includes a variety of tools for performing different types of security testing, such as:

* **Proxy:** The proxy tool allows the user to intercept and analyze all HTTP traffic between the web browser and the web server.
* **Scanner:** The scanner tool automatically scans web applications for common security vulnerabilities.
* **Intruder:** The intruder tool allows the user to perform automated attacks against web applications.
* **Repeater**: The repeater tool allows the user to repeat HTTP requests with different parameters.
* **Sequencer:** The sequencer tool allows the user to analyze the sequence of HTTP requests and responses.
* **Decoder:** The decoder tool allows the user to decode and encode different types of data.

Burp Suite is a powerful tool that can be used to perform comprehensive security testing of web applications. It is used by security professionals, penetration testers, and web developers worldwide.

Here are some of the functions of Burp Suite:

* **Web application scanning:** Burp Suite's scanner tool can be used to automatically scan web applications for common security vulnerabilities.
* **Vulnerability identification:** Burp Suite's proxy and intruder tools can be used to manually identify vulnerabilities in web applications.
* **Vulnerability exploitation:** Burp Suite's intruder tool can be used to exploit vulnerabilities in web applications.
* **Web application security testing:** Burp Suite can be used to perform comprehensive security testing of web applications, including manual and automated testing.

**Why burp suite?**

Burp Suite is a popular web application security testing (WAST) tool used by security professionals, penetration testers, and web developers worldwide. It is a powerful tool that can be used to perform comprehensive security testing of web applications, including manual and automated testing.

Here are some of the reasons why you should use Burp Suite:

* **It is comprehensive.** Burp Suite provides a wide range of tools for performing different types of security testing, such as proxy, scanner, intruder, repeater, sequencer, and decoder.
* **It is easy to use.** Burp Suite has a user-friendly interface that makes it easy to learn and use.
* **It is powerful.** Burp Suite's tools are very powerful and can be used to identify and exploit a wide range of vulnerabilities in web applications.
* **It is versatile.** Burp Suite can be used to test a variety of web applications, including those that use different programming languages and frameworks.
* **It is supported by a large community.** Burp Suite has a large and active community of users and developers who provide support and contribute to the development of the tool.

Overall, Burp Suite is a powerful and versatile WAST tool that can be used to perform comprehensive security testing of web applications. It is a good choice for security professionals, penetration testers, and web developers who are looking for a comprehensive and easy-to-use WAST tool.

Here are some specific examples of how Burp Suite can be used to improve the security of web applications:

* **Identifying vulnerabilities:** Burp Suite's scanner tool can be used to automatically scan web applications for common security vulnerabilities. This can help to identify vulnerabilities that may not be easily detected by manual testing.
* **Exploiting vulnerabilities:** Burp Suite's intruder tool can be used to exploit vulnerabilities in web applications. This can be used to test the severity of vulnerabilities and to develop patches or workarounds.
* **Performing penetration testing:** Burp Suite can be used to perform penetration testing of web applications. This involves using Burp Suite's tools to identify and exploit vulnerabilities in web applications in order to assess the security of the applications.
* **Developing secure web applications:** Burp Suite can be used to develop secure web applications by identifying and fixing vulnerabilities before they are deployed to production.

**What are the features of burp suite?**

Burp Suite is a comprehensive web application security testing (WAST) tool that provides a wide range of features for both manual and automated testing. Here is a summary of the key features of Burp Suite:

* **Proxy**: The proxy tool allows you to intercept and analyze all HTTP traffic between your browser and the target web application. This allows you to view and modify the contents of requests and responses, as well as to send requests to other tools in Burp Suite for further analysis.
* **Scanner**: The scanner tool automatically scans web applications for common security vulnerabilities. It uses a variety of techniques, such as fuzzing and crawling, to identify potential vulnerabilities.
* **Intruder**: The intruder tool allows you to perform automated attacks against web applications. This can be used to test the security of web applications against common attack vectors, such as SQL injection and cross-site scripting.
* **Repeater**: The repeater tool allows you to repeat HTTP requests with different parameters. This can be used to test the behavior of web applications under different conditions.
* **Sequencer**: The sequencer tool allows you to analyze the sequence of HTTP requests and responses. This can be used to understand the logic of web applications and to identify potential vulnerabilities.
* **Decoder**: The decoder tool allows you to decode and encode different types of data, such as HTML, URL, and Base64. This can be useful for analyzing the contents of HTTP requests and responses.

In addition to these core features, Burp Suite also provides a variety of other features, such as:

* **Support for multiple programming languages and frameworks:** Burp Suite can be used to test web applications written in a variety of programming languages and frameworks, including Java, PHP, Python, and Ruby on Rails.
* **Extensibility:** Burp Suite can be extended with custom extensions, which can be used to add new features or to automate specific tasks.
* **Collaboration tools:** Burp Suite provides a variety of collaboration tools, such as project sharing and team annotation, which can help teams to work together more effectively.

Burp Suite is a powerful and versatile WAST tool that can be used to perform comprehensive security testing of web applications. It is a good choice for security professionals, penetration testers, and web developers who are looking for a comprehensive and easy-to-use WAST tool.

**Test the vulnerabilities of testfire.net**

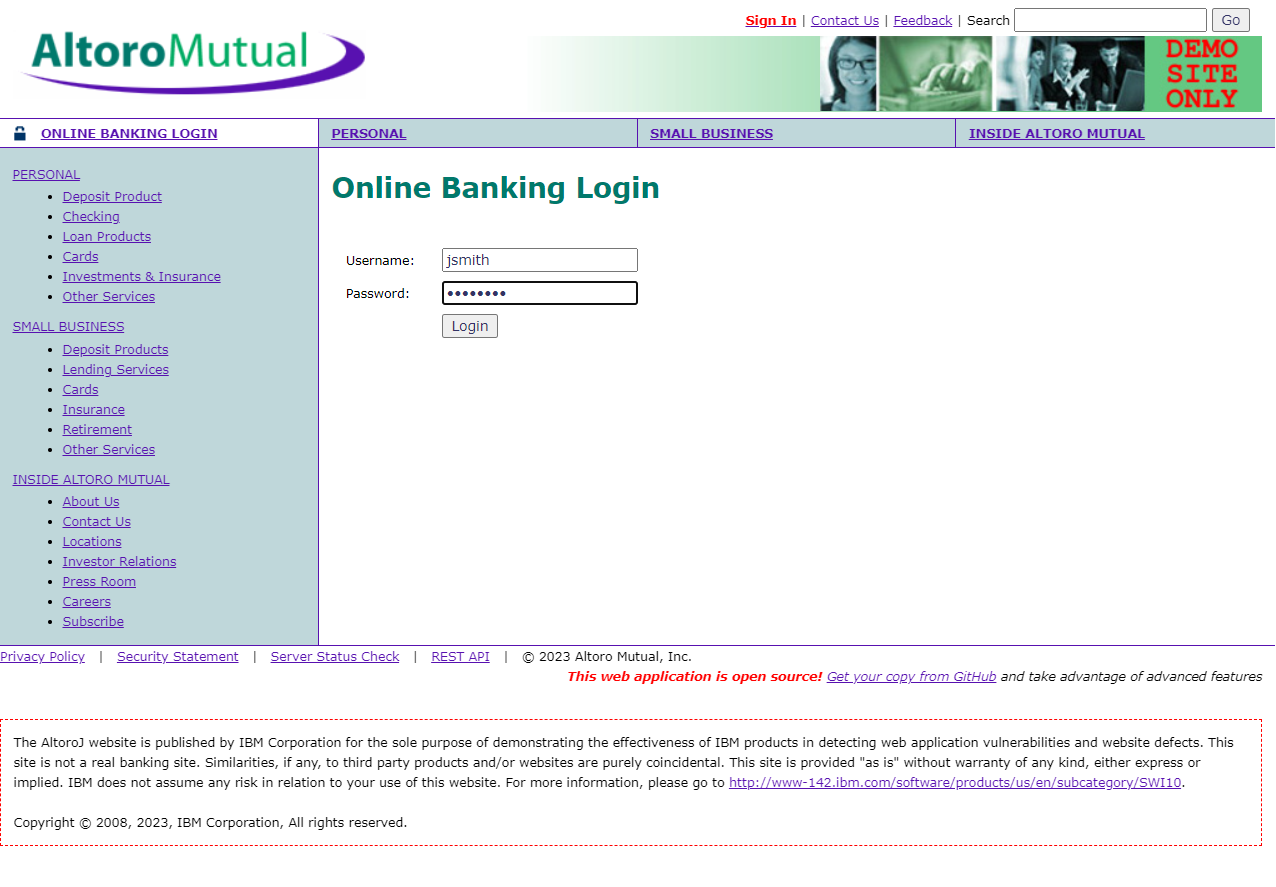
<http://testfire.net>

First and foremost, I used the login account as jsmith and used its password to access the account

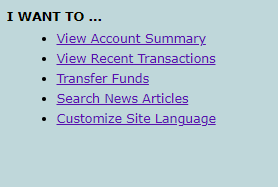
**Checking for IDOR(Insecure Direct Object References)**

Procedure

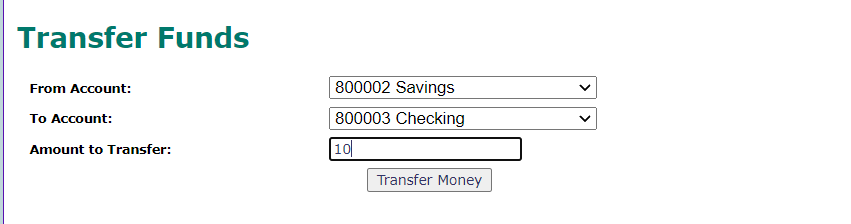
* Sign in using the credentials



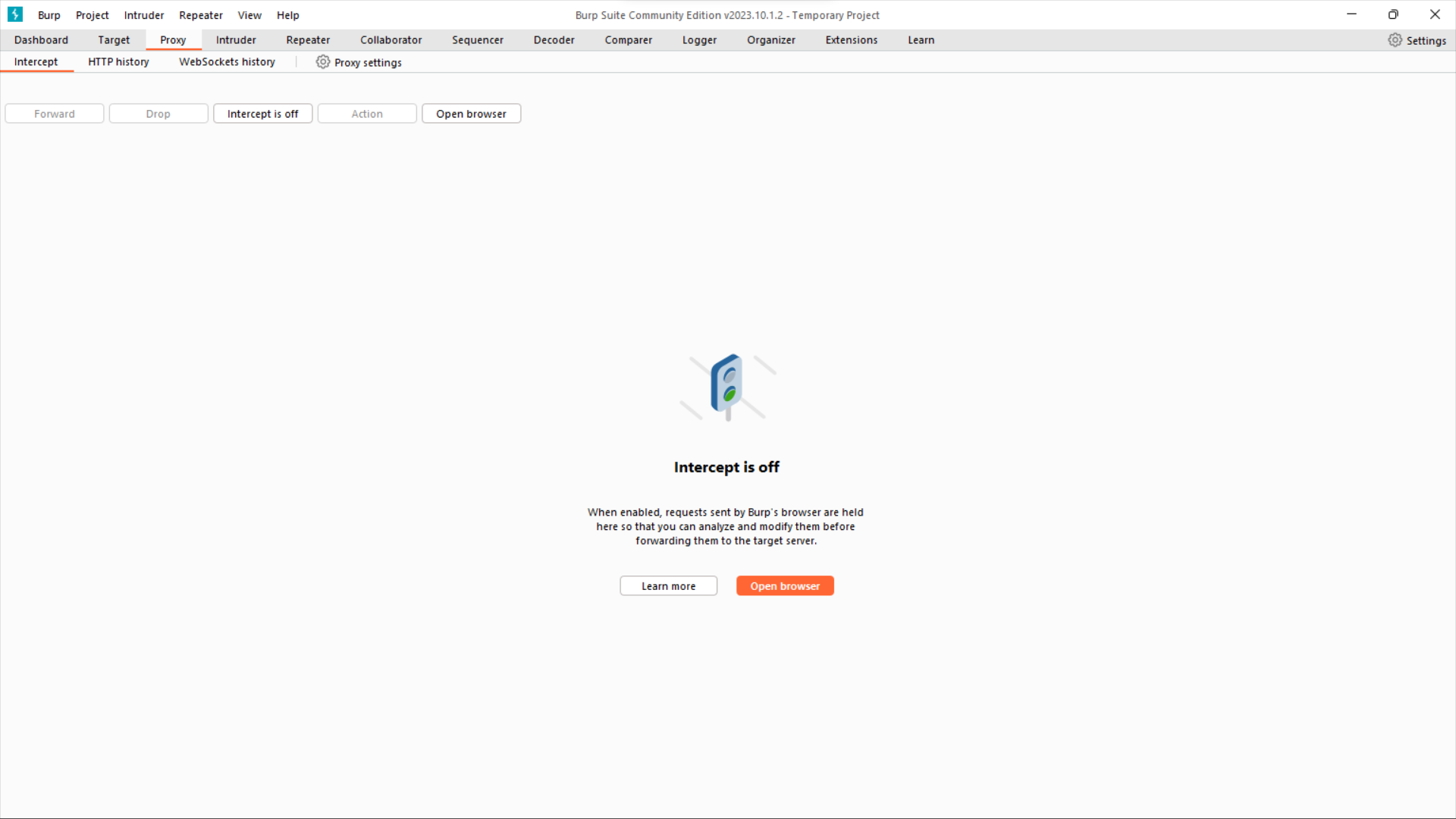
* Go to transfer funds



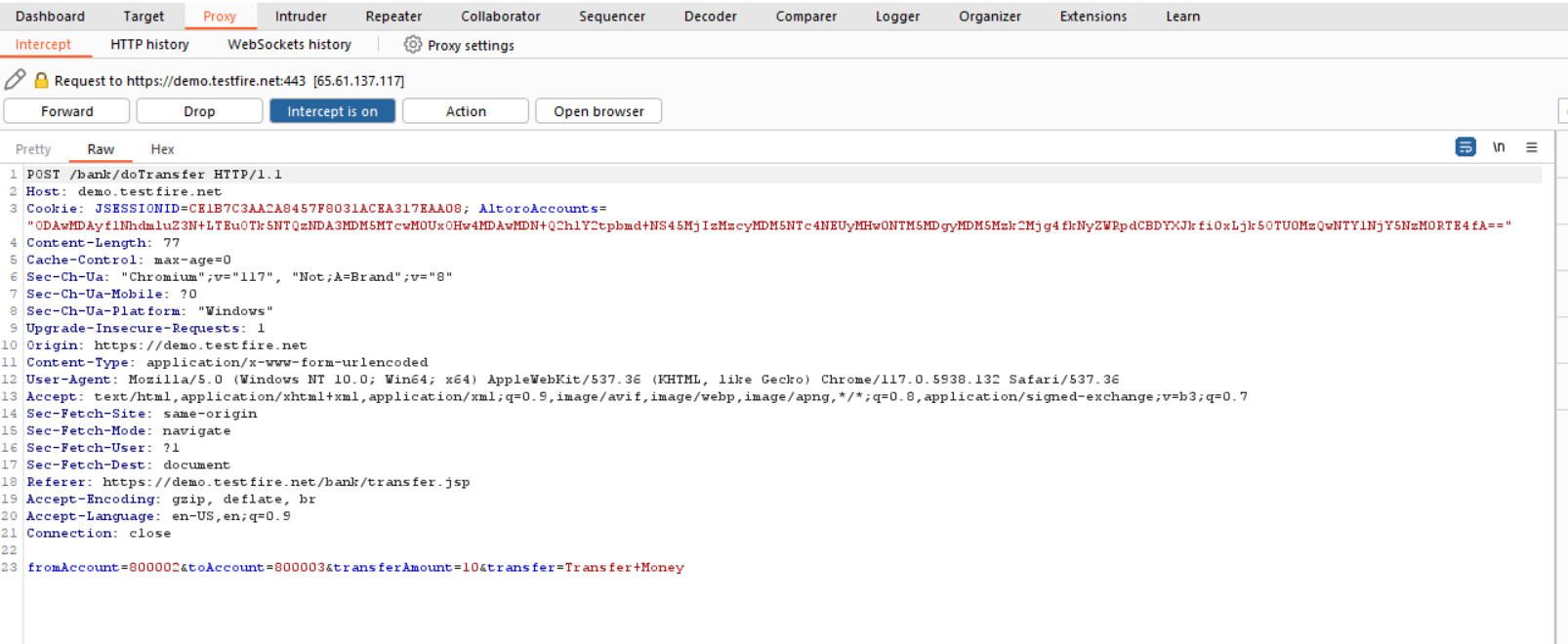
* Put the money from saving account to checking account and put the amount as 10.



* Go to your burp suite and turn on intercept from the proxy section



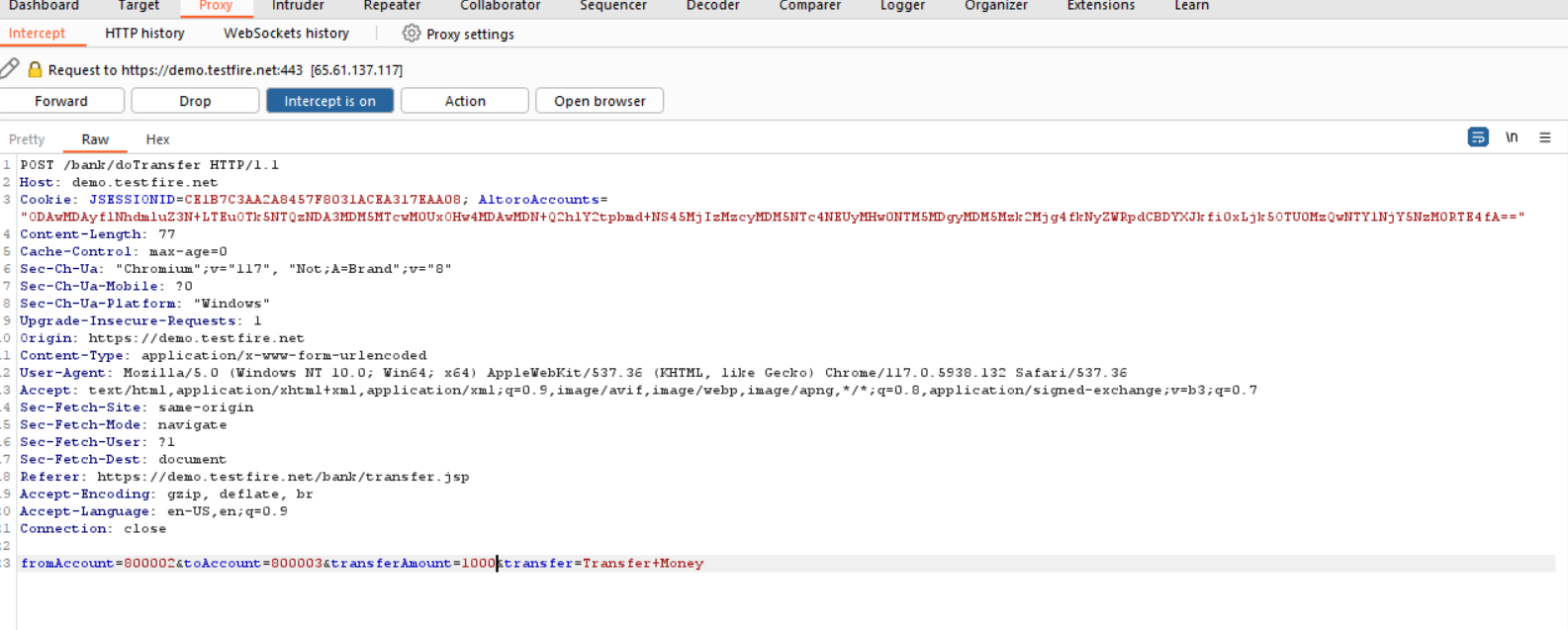
* Now go back to the browser and click on transfer money. The request will get intercepted and will be shown in intercept section of the burp suite.





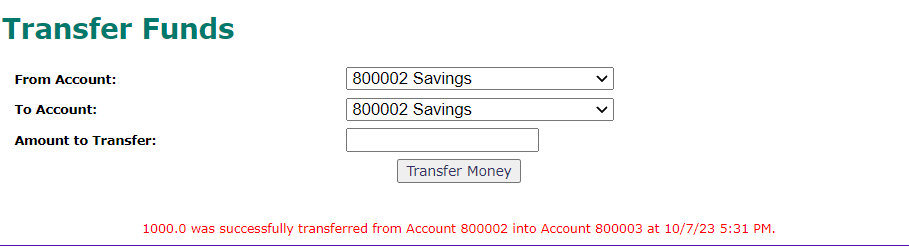
* Here you can edit the request from 10$ to any amount you require. Lets say 1000$ in this case.



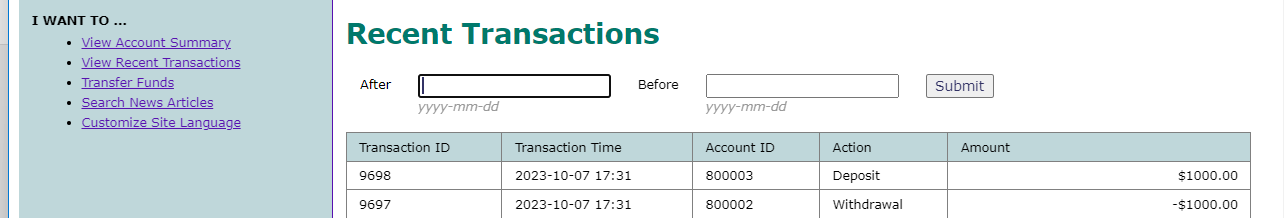




* Now forward the reqeuest.



* As you can see in the above message that is shown, 1000$ has been transferred although the request was of 10$.



This proves that there in IDOR vulnerability.