**TASK:3**

**Vulnerabilities Report**

**WEB APPLICATION SECURITY**

**TESTING WEBSITE:** [**http://testphp.vulnweb.com/**](http://testphp.vulnweb.com/)

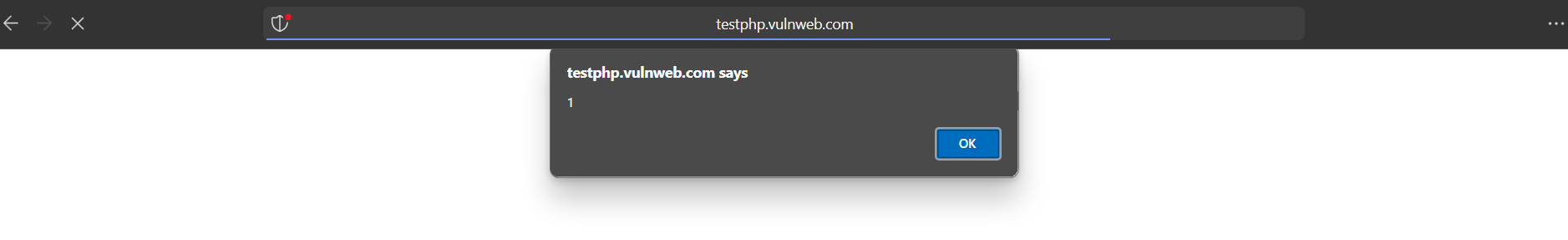
**Description:** [**http://testphp.vulnweb.com/**](http://testphp.vulnweb.com/) **is a very simple website.it is made for testing a different-different types of vulnerabilities. This website is having some different types of vulnerabilities like: XSS,CSRF,SQL injection, Session Hijacking… Let’s find**

**Vulnerability 1: XSS (cross-site scripting)**

**Description: it is the most common vulnerability names XSS an attacker inject the malicious code in a input field of any website and after the correct payload was executed and website display the given input in a pop-up window an attacker was successfully find the XSS vulnerability.**

**Payload :** <script>alert("XSS")</script>

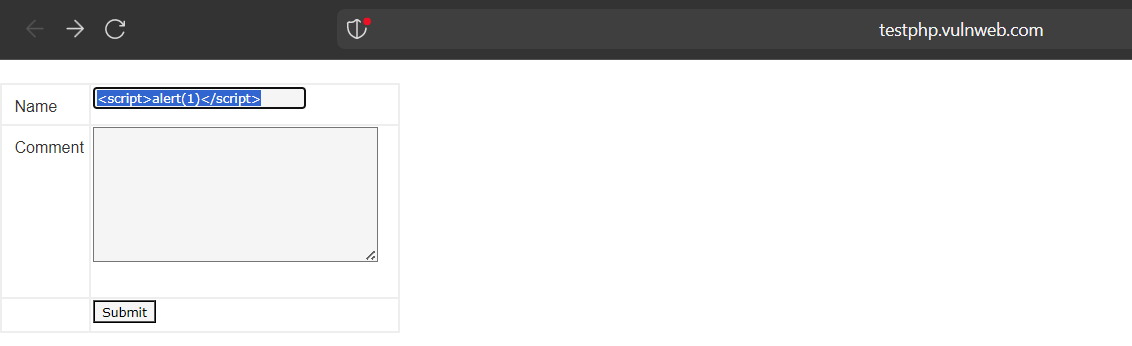
As you can see the same javascript code I was excuted in the below given image and when I was hit enter so one pop-up this was called XSS vulnerabiltity.

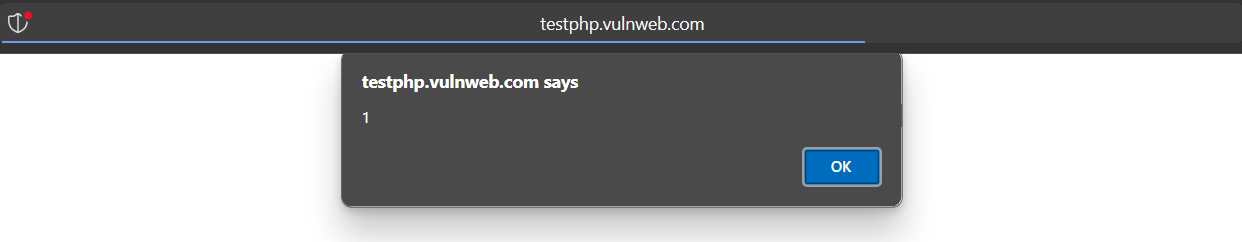
****

****

**XSS in comment box: in the website there was a comment box for end users for do some comment on posted pictures so I am entering simple javascript basic payload and after hiting enter button one pop-up window was shown.**

**Images are given below.**

****

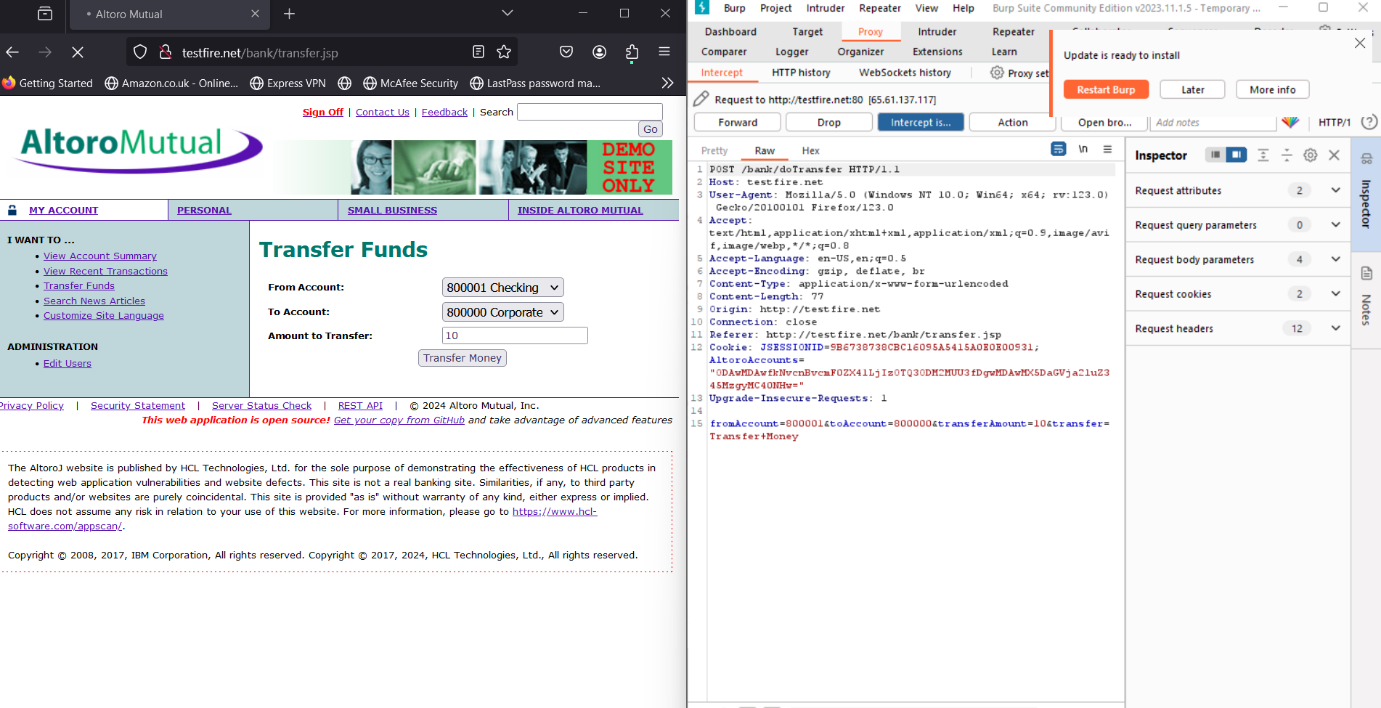
****

**Website name: Testfire.net**

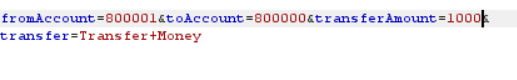
**Vulnerability 2: Request manupulation**

**In this vulnerability attacker was capturing the request is sending by user to server using burp suite and manipulate the request.**

**Ex if an user sending $10 to any account and attacker captures the request and change the amount $10 to $1000 so $1000 will be debited from users account images are given below**

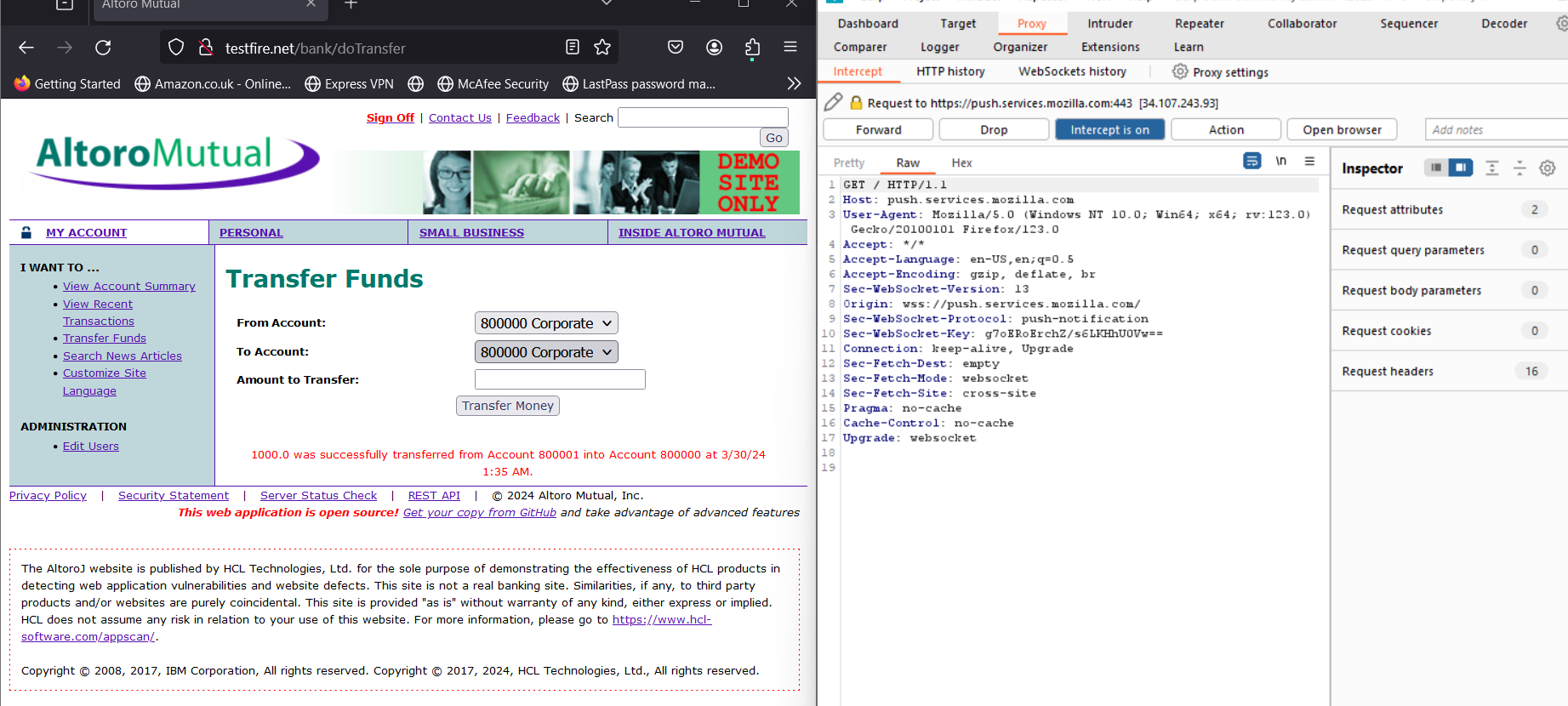
****

**In image user sending $10 and attacker caputes the request using burp suite and change the transaction amount**

****

**After changing the amount $1000 was debited from the users account**

**Image are given below.**





**In the given image we were seen the red line was highlighted that 1000$ was successfully transferred.**

**Vulnerability:3**

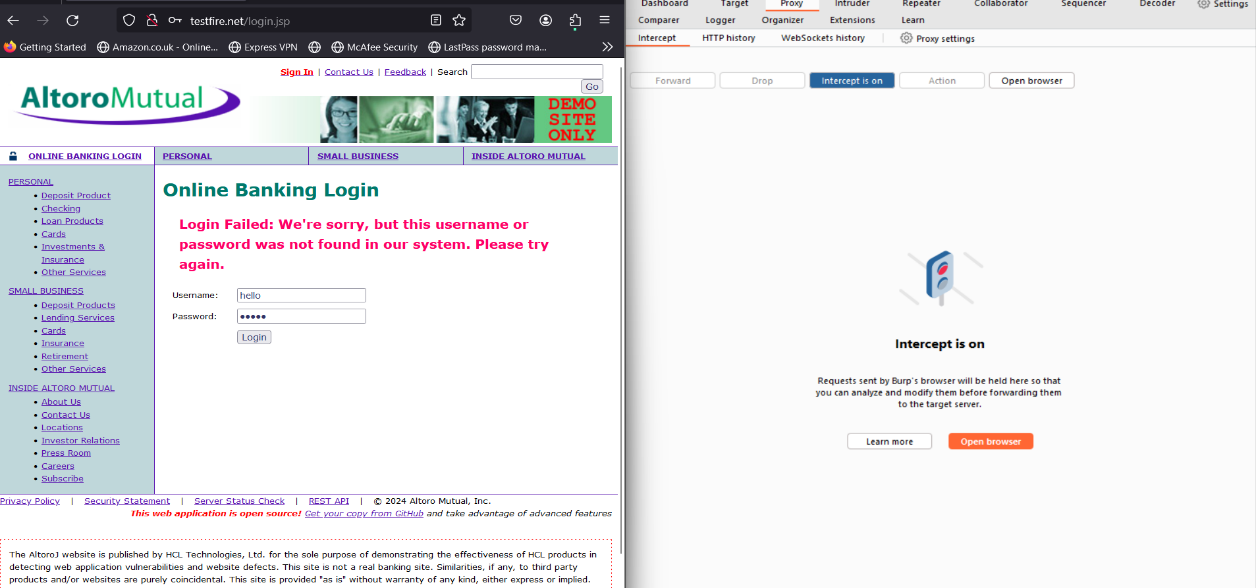
**SQL injection: it is a most common vulnerability in this attacker targets those website that are using databases like mysql,oracle. In this attacker input malicious sql code in a input field ex. Username,password field. In sql injection attacker has no need to enter username and password it will enter a malicious query in a input field and bypass login page.**

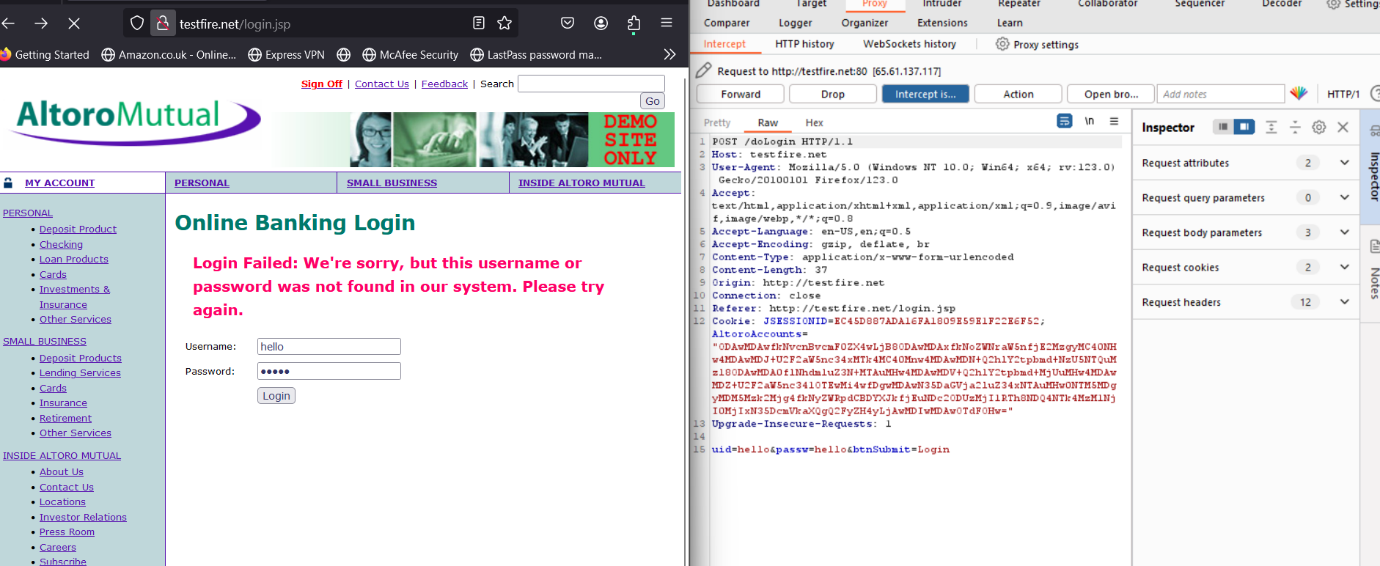
**Ex. ‘ OR 1=1—**

**Website name : testfire.net**

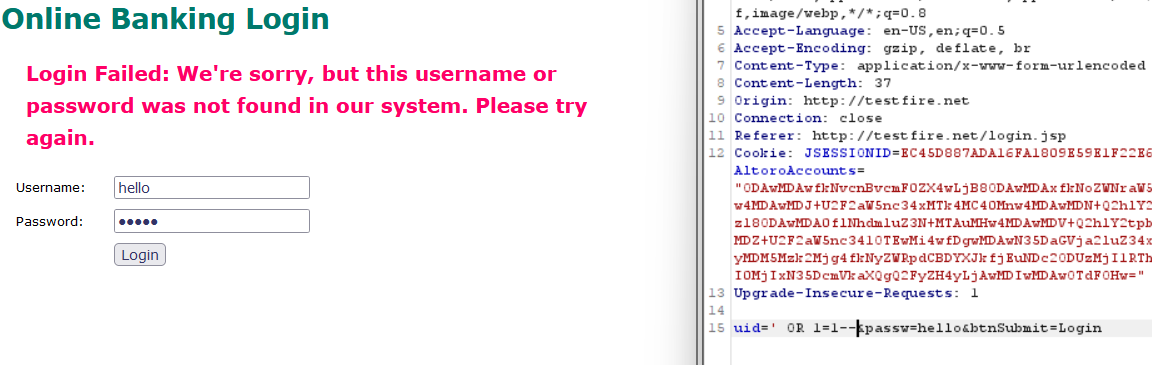
**In this website there wasa login page so in the input field attacker can enter sql query and hit enter after hitting enter if the website was vulnerable to sql injection attacker was login in the account without entering username and password**

**In the given image you can see username is hello**

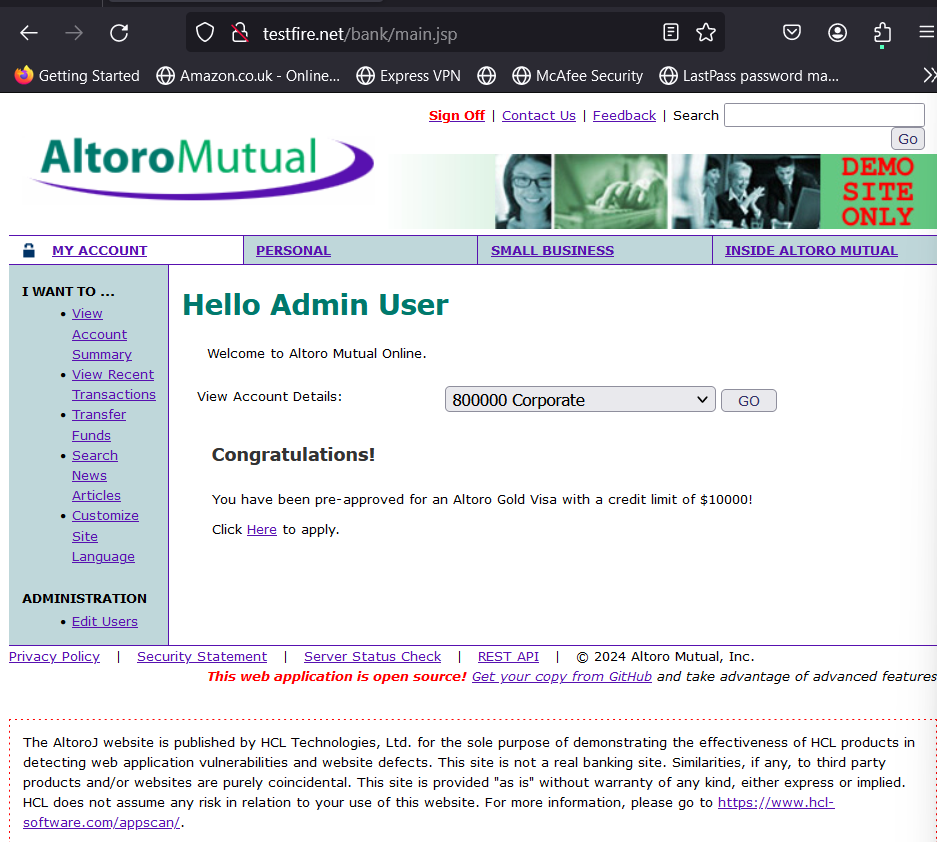
****

****

**.In this image attacker intercept the request**

****

**.in this image attacker entering malicious query**

****

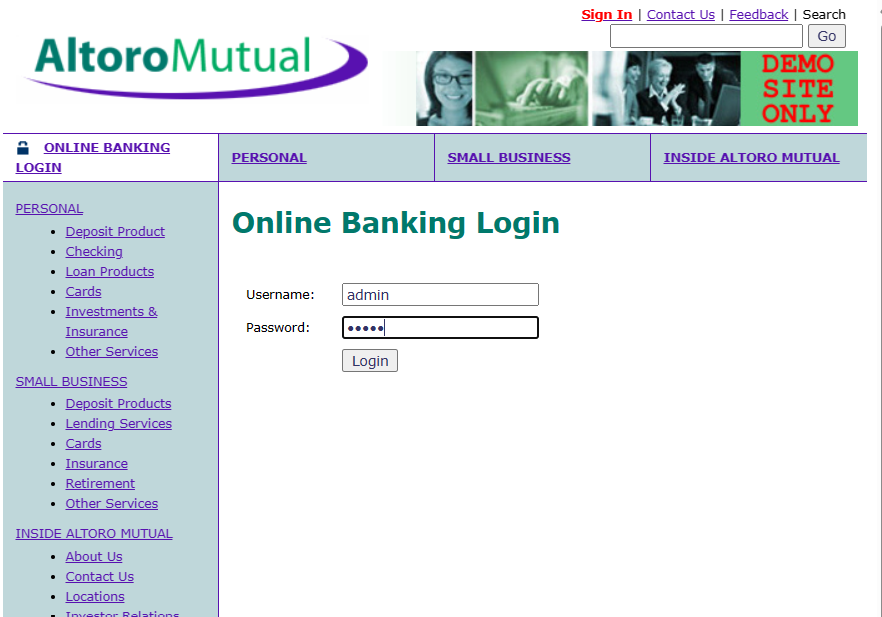
**After forwarding the request attacker succesfully login into the admin account.**

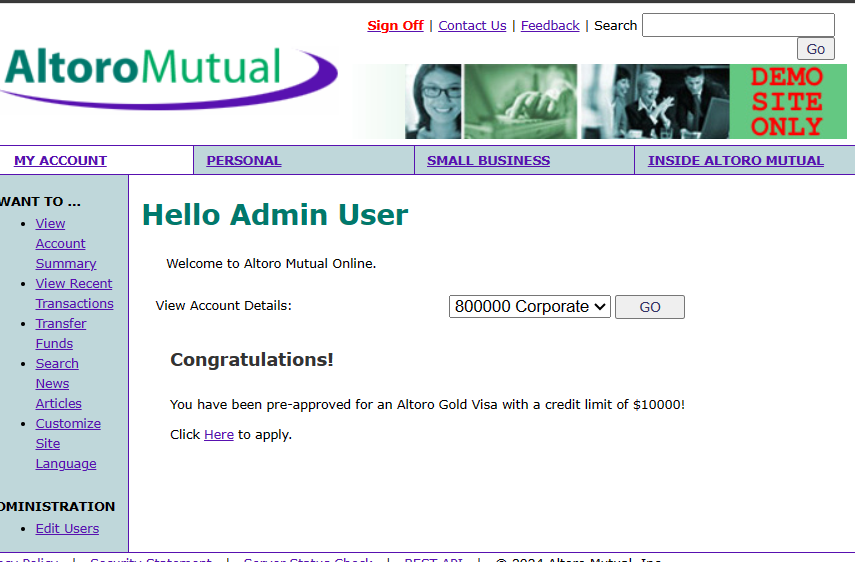
**Vulnerability:4**

**Session hijacking: In this attacker already enters in a network or in a system after that attacker monitor the outgoing and incoming traffic and captures the request and steal the user cookies and after stealing cookies attacker was no need to use credentials it was directly login to any account.**

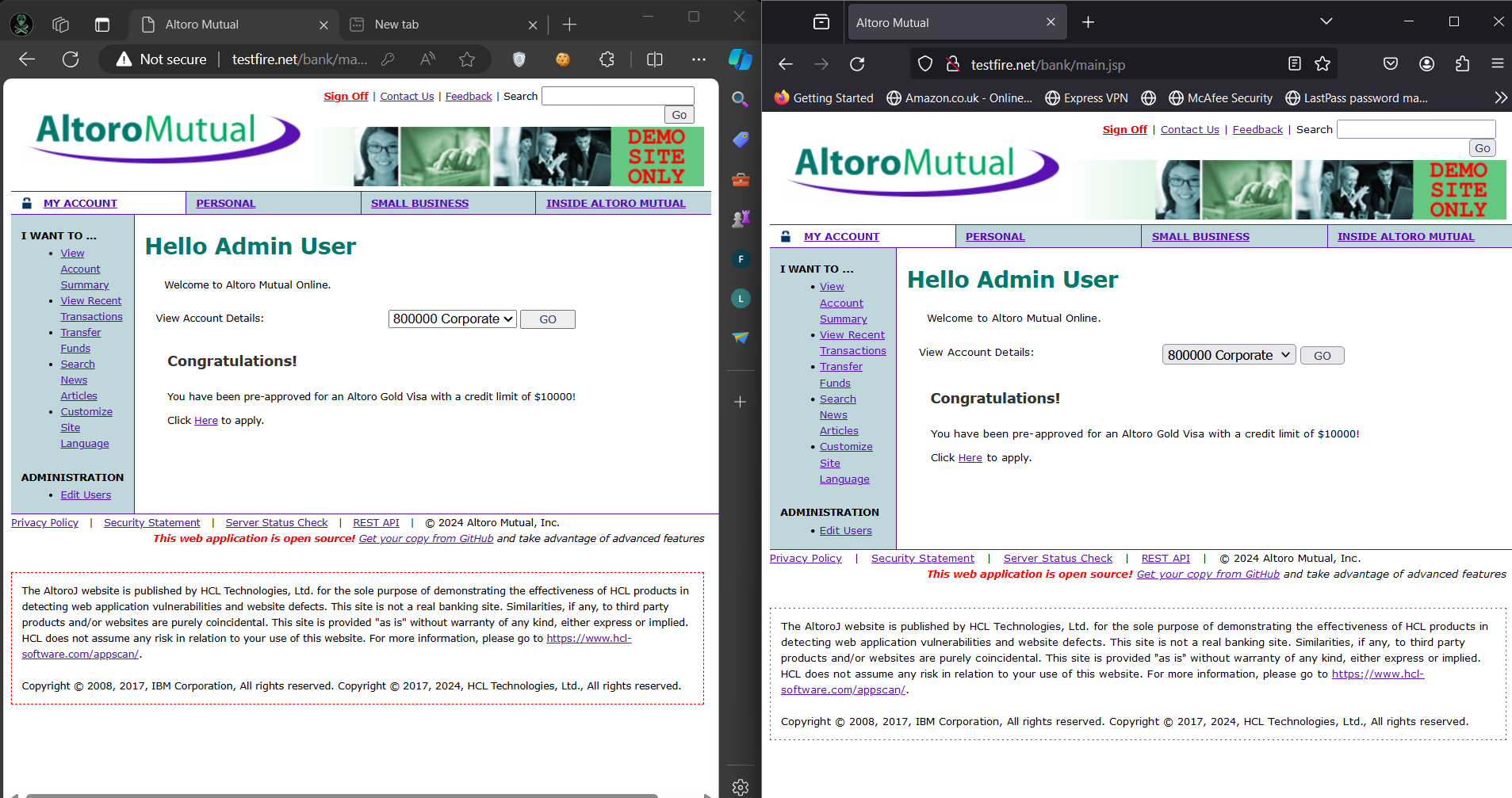
**Extension name: Cookie editor**

**This is a tool that that helps to import and export the cookies**

****

****

**I am showing you as an user I am valid login credentials but on the other hand and different browser I am import and export the cookies using cookie editor**

****

**On the other hand I am importing microsoft edge cookies to firefox and see’s the magic same account was opened without entering the credentials**