Deliverable 5

Rui Nan – run7

Vulnerability 1: **Cross Site Scripting**

1. What part of the InfoSec Triad does this vulnerability attack (confidentiality, integrity, or availability)?

Confidentiality.

1. What kind of security attack can exploit this vulnerability (interruption, interception, modification, or fabrication)?

Modification, Fabrication.

1. Are attacks that exploit this vulnerability active or passive?

Active

1. What business value would be lost due to exploiting this vulnerability (data loss, unauthorized access, denial of service, etc)?

It can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. Because user will bypass the access control.

So it will cause data loss, unauthorized access.

1. What steps should the development team take to fix this vulnerability?

The simple way to fix that is to add XSS protect function. Developer may check the input contents that does not allow any JavaScript statements or HTML tags in the input box.

1. The URL of the website with the described vulnerability.

Test URL: <http://demo.testfire.net/bank/login.aspx>

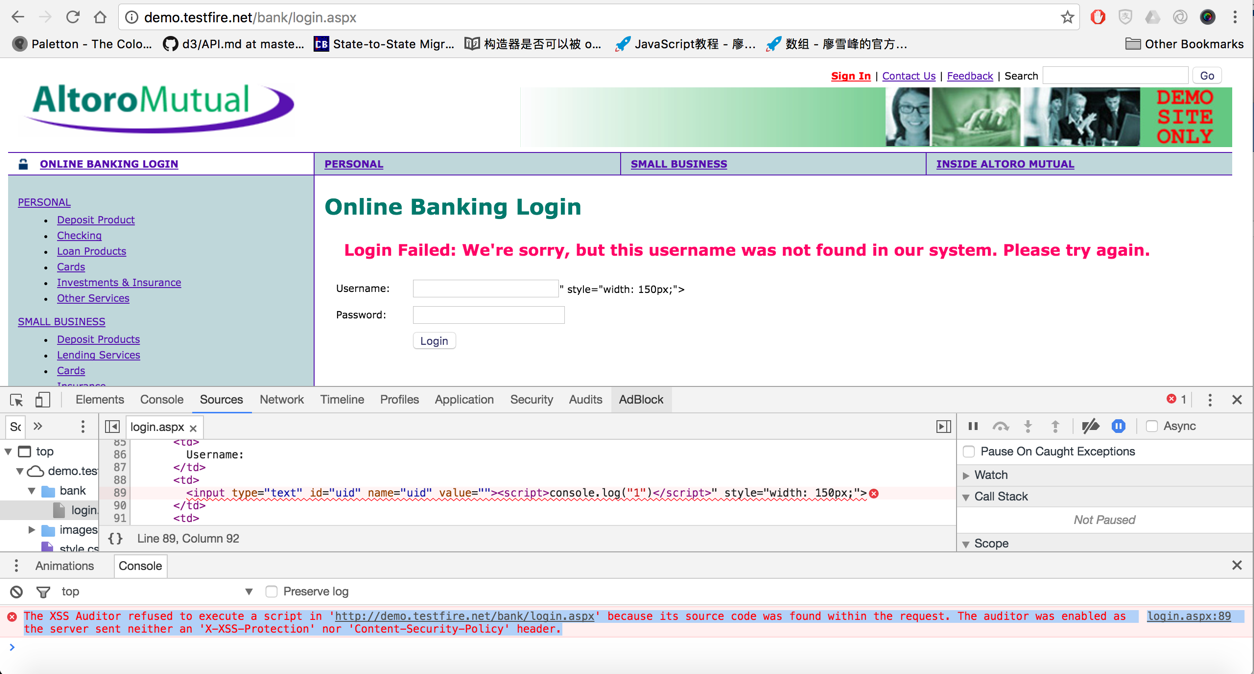
1. Steps taken to exploit the vulnerability.

First, click the ONLINE BANKING LOGIN link;

Second, add “"><script>console.log("1")</script>"” into the username input box; And add any password into password box

Third, click LOGIN button.

1. A screenshot (if applicable) of the vulnerability.



Vulnerability 2: **SQL Injection**

1. What part of the InfoSec Triad does this vulnerability attack (confidentiality, integrity, or availability)?

Availability, Integrity

1. What kind of security attack can exploit this vulnerability (interruption, interception, modification, or fabrication)?

Fabrication

1. What business value would be lost due to exploiting this vulnerability (data loss, unauthorized access, denial of service, etc)?

The unauthorized user will access administrator account. It means user will obtain some authorities that would control whole site.

1. What steps should the development team take to fix this vulnerability?

I think the way to fix the vulnerability is like the method for fixing the previous vulnerability. First, developer needs to install some checking mechanism to make sure what input is in accordance with the rules. Second, the database should set a firewall

1. The URL of the website with the described vulnerability.

Test URL: <http://demo.testfire.net/bank/login.aspx>

1. Steps taken to exploit the vulnerability.

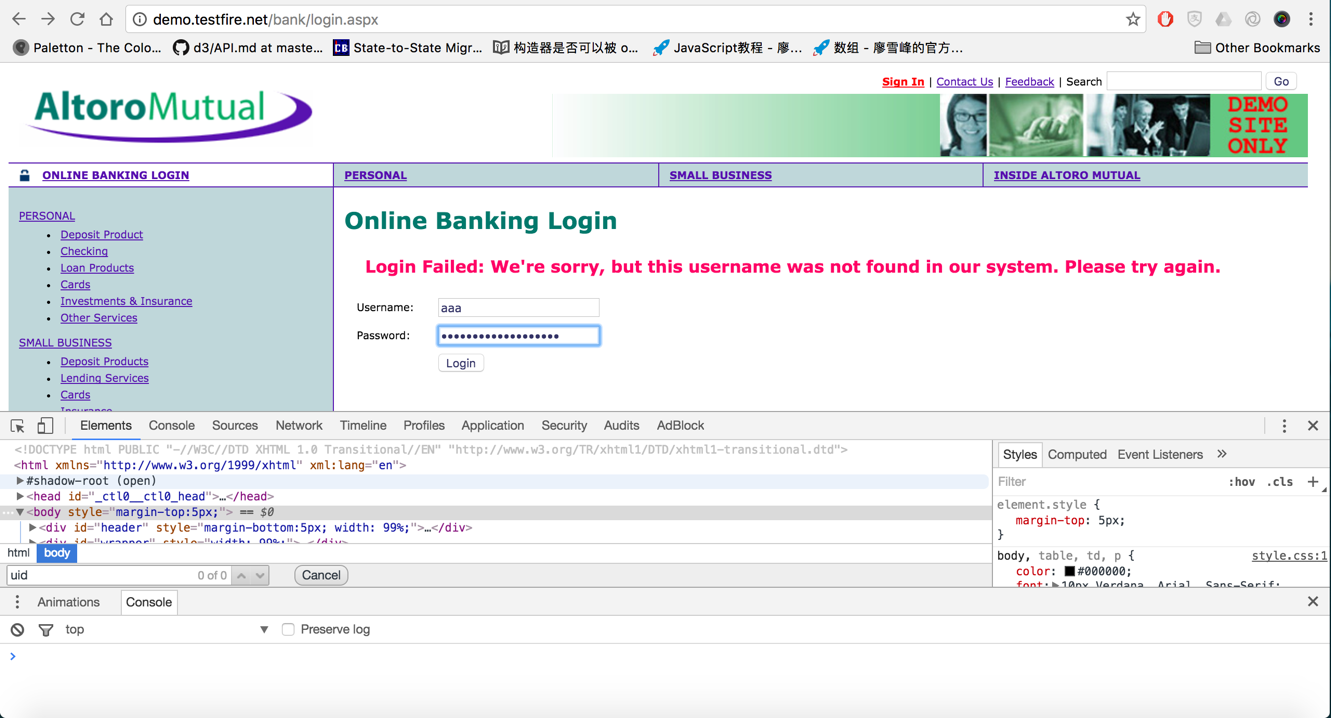
First, click the ONLINE BANKING LOGIN link;

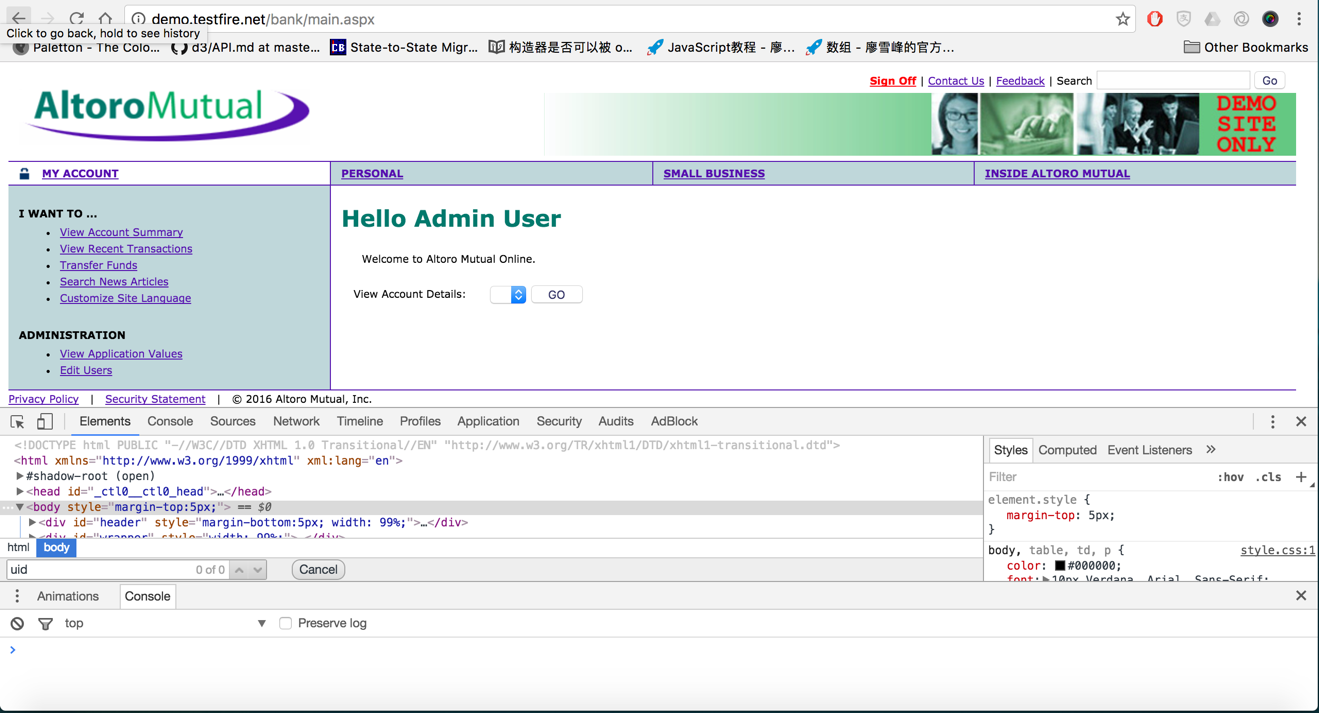
Second, input “ZAP' OR '1'='1' –“ to the password box, then type any username you want.

Third, click LOGIN button.

1. A screenshot (if applicable) of the vulnerability.

I will got the admin access.





Vulnerability 3: **Directory Browsing**

1. What part of the InfoSec Triad does this vulnerability attack (confidentiality, integrity, or availability)?

Confidentiality, Integrity

1. What kind of security attack can exploit this vulnerability (interruption, interception, modification, or fabrication)?

Modification, Fabrication

1. Are attacks that exploit this vulnerability active or passive?

Passive

1. What business value would be lost due to exploiting this vulnerability (data loss, unauthorized access, denial of service, etc)?

The whole directory exposed. So the visitor could read the source code for your website. And maybe they can upload or download files through the server. Because they already know where are the files and what are their function. So it is much easier to modify the files or insert some malicious codes in order to manipulate the website.

1. What steps should the development team take to fix this vulnerability?

The directory should be invisible for the visitor. Development team could add some statements into configure file to prevent this happen.

1. The URL of the website with the described vulnerability.

Test URL: <http://scanme.nmap.org/shared/>

1. Steps taken to exploit the vulnerability.

First, add /shared/ behind http://scanme.nmap.org

Second, click Enter, or let browser visit this site.

Third, you can visit the directory.

1. A screenshot (if applicable) of the vulnerability.

