APPLICATION SECURITY ASSESSMENT REPORT

for

DEMO BANKING APPLICATION

Client Logo

Version 1.0

Feb 6, 2006

Guide to the Report

The **Certification Status** on page 4 shows how the application meets or fails the Plynt certification criteria. Wherever the application does not meet the criteria, a page reference is given for relavant findings and the mitigation details.

The **Threat Profile** on page 6 lists the threats identified for the application, and how the application defends against these threats. Wherever a threat could be exploited, a page reference is given for the relavant finding and its mitigation details. The Plynt certification requires that the application protect against all the threats in its threat profile.

The **Findings and Action Items Summary** on page 7 lists all the findings identified in the application, gives a short summary of the action to be taken to mitigate the corresponding finding. All the findings have a page reference for detailed finding and the mitigation details.

The **Findings section** on page 8 gives detailed description of all the findings with screenshots to show the exploit process, its relavance to the certification criteria and the threat profile. Also a risk rating is assigned to individual findings based on the ease of exploitation and the corresponding business impact.

The **Mitigation Tracker** on page 23 is a table listing the actions to be taken in order to mitigate the identified findings. The action items have a page reference for detailed finding and the mitigation details.

Scope of certification project

Name of organization	Demo Bank
Application Name	Vulnerable Application
Version details	1.0
IP Address	127.0.0.1
URL	http://localhost:8080/VulnerableApplication
Duration of test	Feb 1, 2006 to Feb 5, 2006
Short description of application	Internet banking application providing customers with facility to perform online transactions and also to view account summary rendered via pdf document.

Contact Details

Author contact

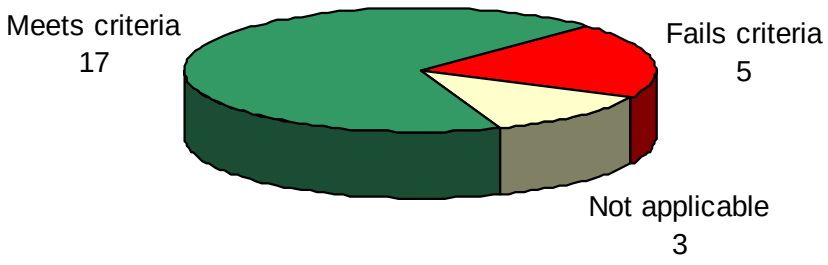
Name	Shah Nawaz
Email address	shah.nawaz@plynt.com

Client contact

Name	Demo Bank
Email address	contact@demobank.com

Certification Status

The Demo Bank Application was tested against the Plynt certification standard and the graph below shows the overall status of the application against the certification criteria.



The application fails on 5 of the certification criteria and thus does not qualify for Plynt certification as of now, however the application can be certified against the Plynt criteria after appropriate mitigation has been carried out on the failed criteria.

NO	CRITERIA LABEL	STATUS	MITIGATION DETAILS
	Section 1: Security Protection Criteria		
1.	Safe against popular attacks	**Fails criteria**	on page 8 on page 19
2.	Defend against Threat Profile	**Fails criteria**	on page 8 on page 11 on page 19 on page 16
3.	Sensitive data protected in transmission	**Meets criteria**	
4.	Safeguard passwords	**Fails criteria**	on page 19
5.	Protect against automated password guessing	**Meets criteria**	
6.	Protect against manual password guessing	**Meets criteria**	

NO	CRITERIA LABEL		STATUS	MITIGATION DETAILS
7.	Secret questions safe against guessing		**Not Applicable**	
8.	Protect configuration files and directory lists		**Meets criteria**	
	Section 2: Security Requirements Criteria			
9.	Sensitive data not stored on client		**Meets criteria**	
10.	Sensitive data not hidden in pages		**Meets criteria**	
11.	No sensitive data in error messages		**Meets criteria**	
12.	Known, strong cryptographic algorithms		**Fails criteria**	on page 19
13.	Code obfuscation for secrets		**Meets criteria**	
14.	Session timed out after period of inactivity		**Meets criteria**	
15.	Re-authentication required after log out		**Fails criteria**	on page 19
16.	Warning required for “Remember Me”		**Not Applicable**	
17.	Password not stored in plain text for “Remember Me”		**Not Applicable**	
18.	Old password required before changing password		**Meets criteria**	
19.	Random session token		**Meets criteria**	
20.	New authentication token on log in		**Meets criteria**	
21.	No sensitive data in requests to external sites		**Meets criteria**	
22.	Services patched		**Meets criteria**	

NO	CRITERIA LABEL		STATUS	MITIGATION DETAILS
23.	Access to server filtered		**Meets criteria**	
24.	No sample or test applications		**Meets criteria**	
25.	No sensitive data in source code		**Meets criteria**	

Threat profile

A Threat profile was developed by the Plynt team to list down all possible threats specific to Demo Bank Application, and tests were conducted against the identified threats.

THREAT CODE	OBSERVED THREAT		STATUS	MITIGATION DETAILS
T1	A malicious user can by pass authentication to access the application		Unsafe	on page 8
T2	A malicious user can perform unauthorized fund transfers		Unsafe	on page 11
T3	A malicious user views financial statements of other users		Unsafe	on page 16
T4	A malicious user gains authentication credentials of other users		Unsafe	on page 19
T5	A malicious user defaces the online banking site		Safe	

Findings and Action Items Summary

The Demo Banks Vulnerable Application was found to have 3 high risk and 1 medium risk security weaknesses. They are as summarized below.

SI NO.	FINDINGS	RISK RATING	ACTION ITEM	MITIGATION DETAILS
1.	An attacker can gain unauthorised access to any account.	HIGH	Proper Input validation should be implemented to escape special characters in the input.	on page 8
2.	A malicious user can siphon off funds from any account to his account.	HIGH	Check account numbers in the request to ensure they belong to the logged in users.	on page 11
3.	A malicious user can view account summary of other users.	HIGH	The PDF documents should be generated dynamically and streamed to the browser.	on page 19
4.	An attacker can steal user credentials through browser refresh even after the user has logged out but not closed the browser window.	MEDIUM	An intermediate redirection page should be introduced immediately after successful authentication before displayed.	on page 16

Findings

1. An attacker can gain unauthorised access to any account

It is possible to log into the application by giving special inputs in place of valid credentials (SQL injection) and gain access to any account.

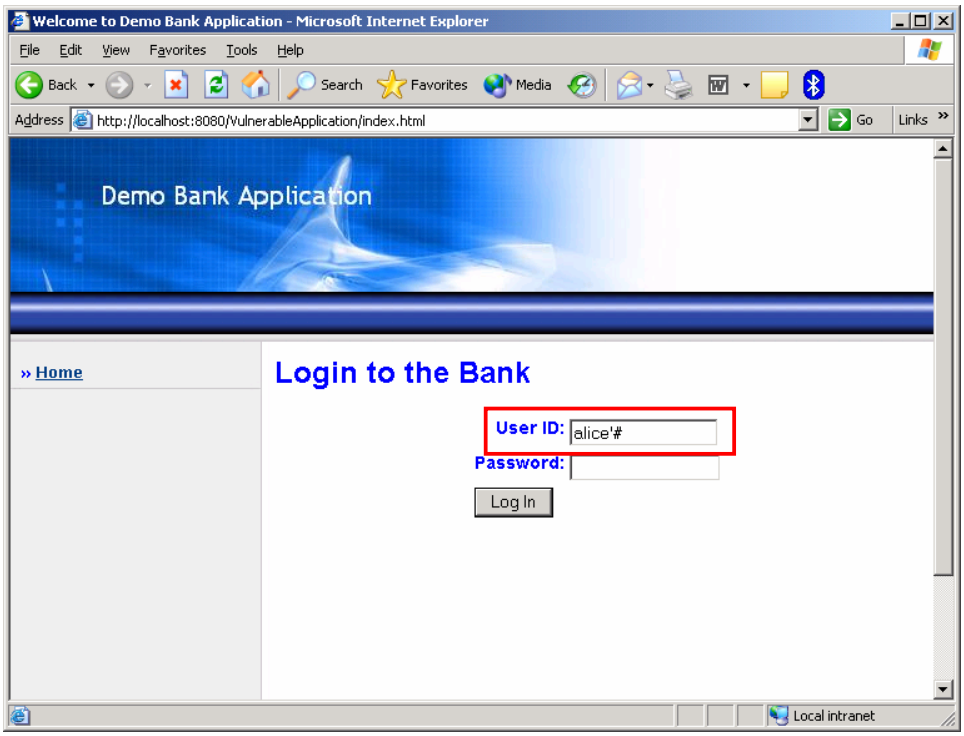
RISK LEVEL

HIGH

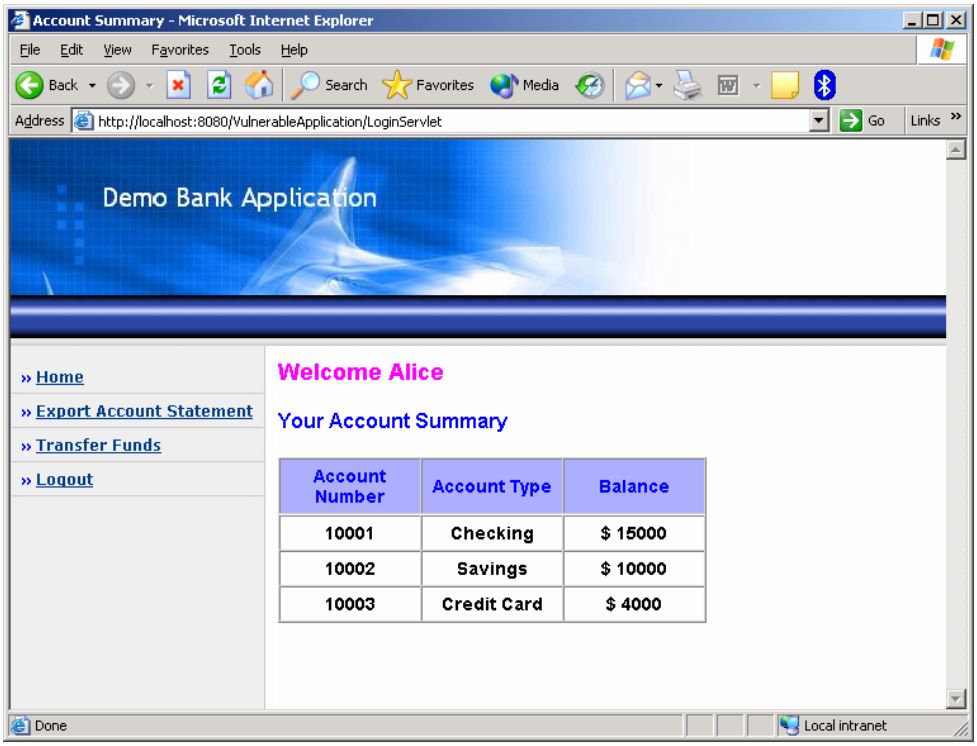
Relevant certification criteria	• Safe against popular attacks • Defend against Threat Profile
Relevant threats in Threat profile	A malicious user can by pass authentication to access the application
Impact	The impact is high as this flaw allows an attacker to gain complete access of the target account
Ease of exploitation	This attack is easy to exploit as it does not require any special tools.

Exploit

Step1: On the login screen of the application, enter user id as alice'# (assuming the attacker knows the user id) as shown below and click on login button.



The following screenshot shows a successful login with user id alice but no password.



View animation titled Finding1of the exploit

Solution

User input should be validated for all special characters like single quotes, double quotes etc. These special characters should be escaped wherever appropriate.

Go to			
Certification Status	Findings and Action Items Summary	Threat Profile	Mitigation Tracker

2. A malicious user can siphon off funds from any account to his account.

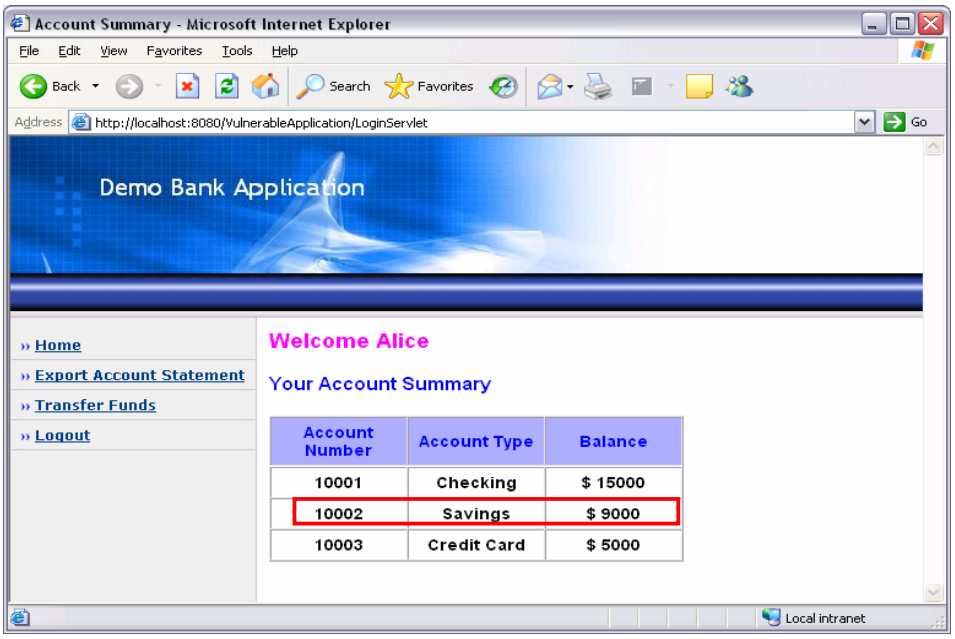
RISK LEVEL
HIGH

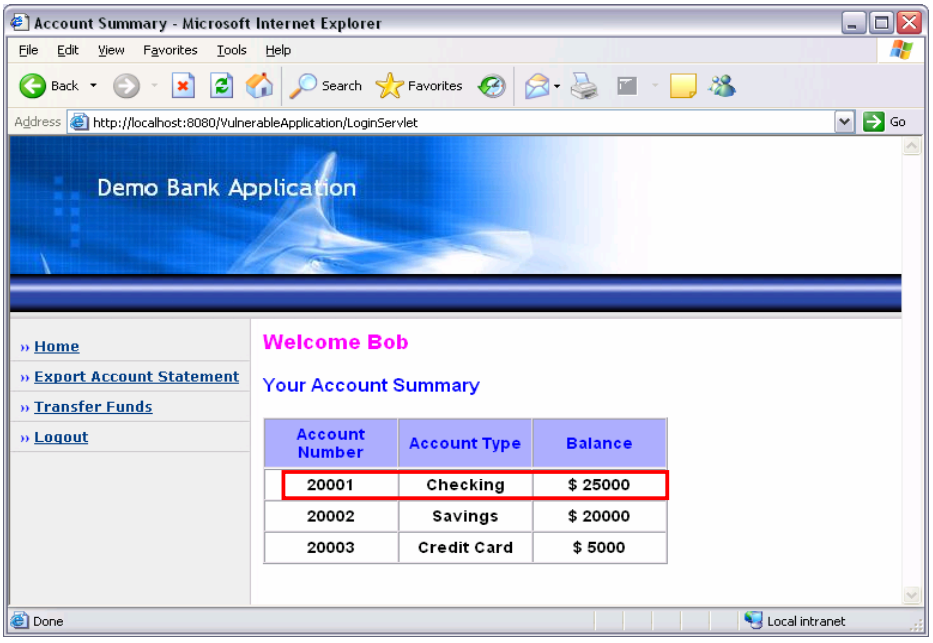
A malicious user can siphon off funds from any account to his account. This attack is possible because the application is not checking the source account number in the request to ensure it belongs to the logged in user.

Relevant to which all certification criteria	Defend against Threat Profile
Relevant to which all threats in the Threat profile	A malicious user can perform unauthorized fund transfers
Impact	The impact is high because a malicious user can siphon off funds from any user's account.
Ease of exploitation	This attack is easy to exploit as the malicious user only needs to know the target account number and knowledge of web proxy editor tools.

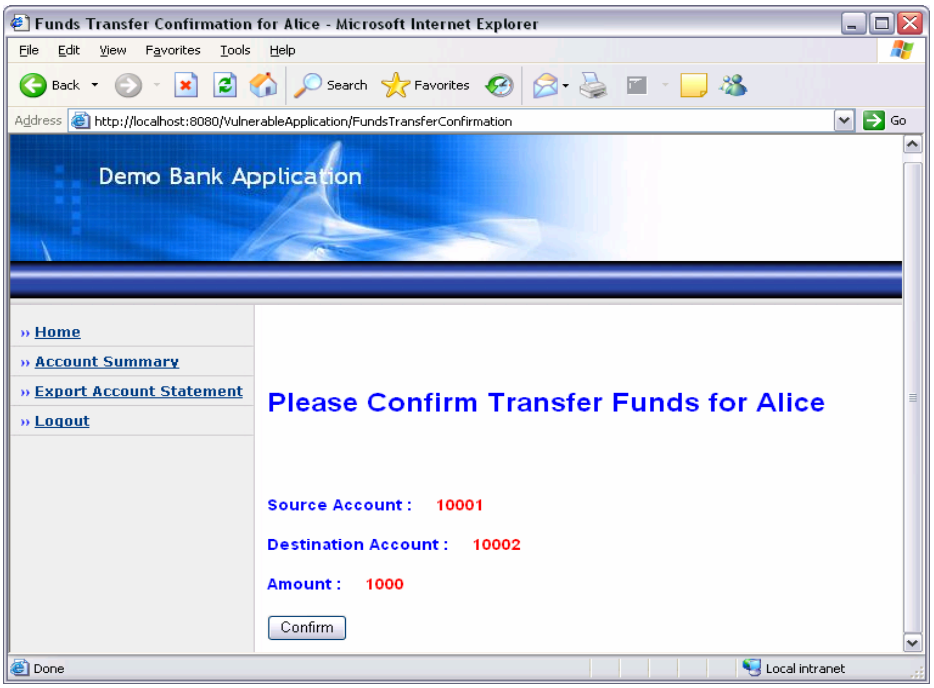
Exploit

We shall use two accounts of Alice and Bob to demonstrate this exploit. To begin with, the current account summary of both the users is noted. They are as shown below.

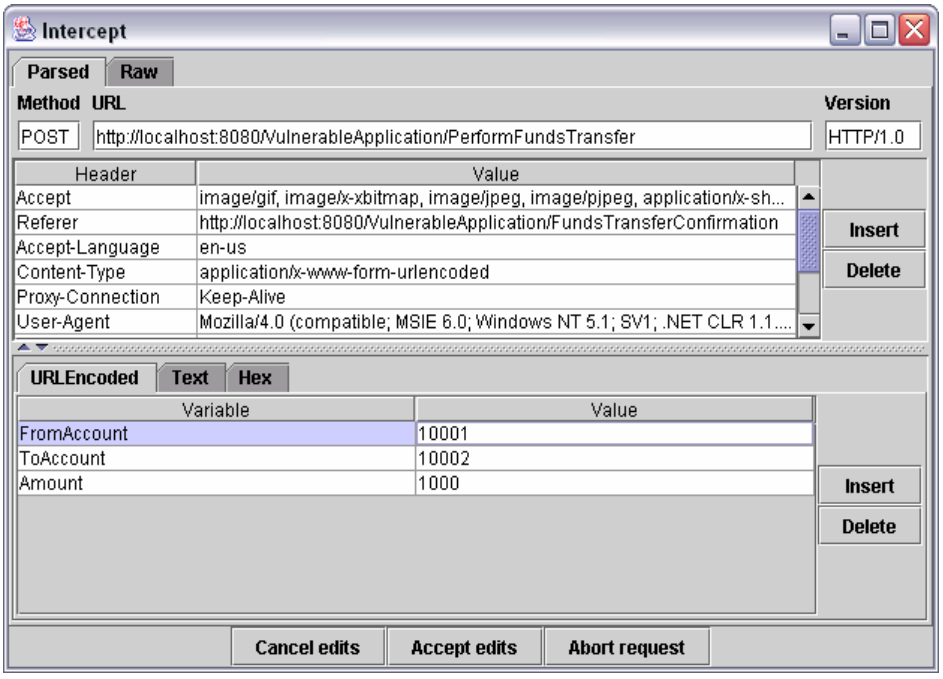




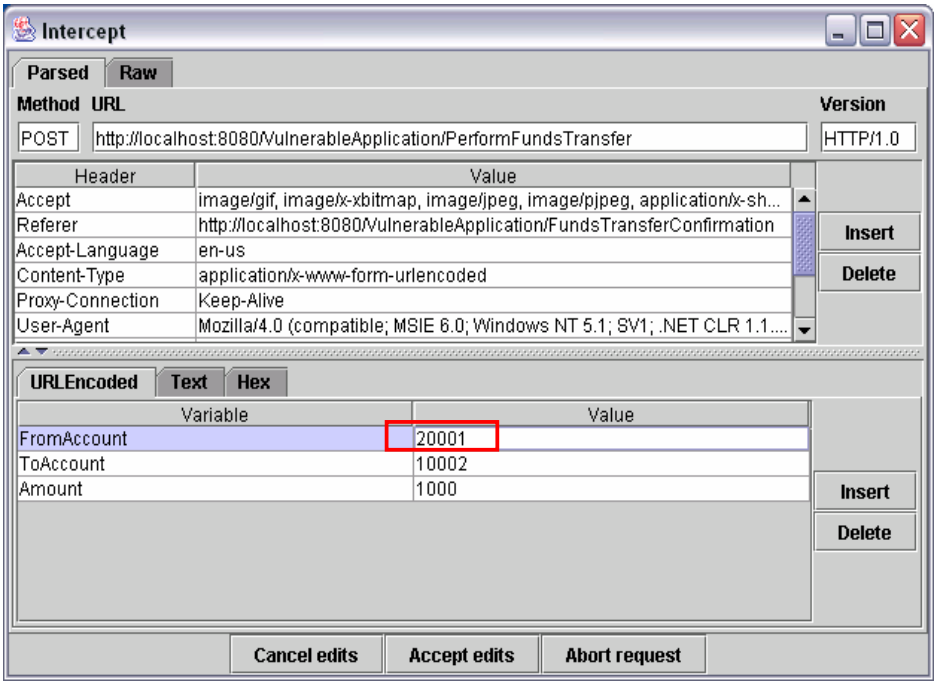
Step1: Login to the application as a valid user, say Alice and go to "transfer funds" page to initiate a fund transfer. Select the source and destination account numbers, enter the amount and click on transfer. A page to confirm the details submitted earlier will be shown.



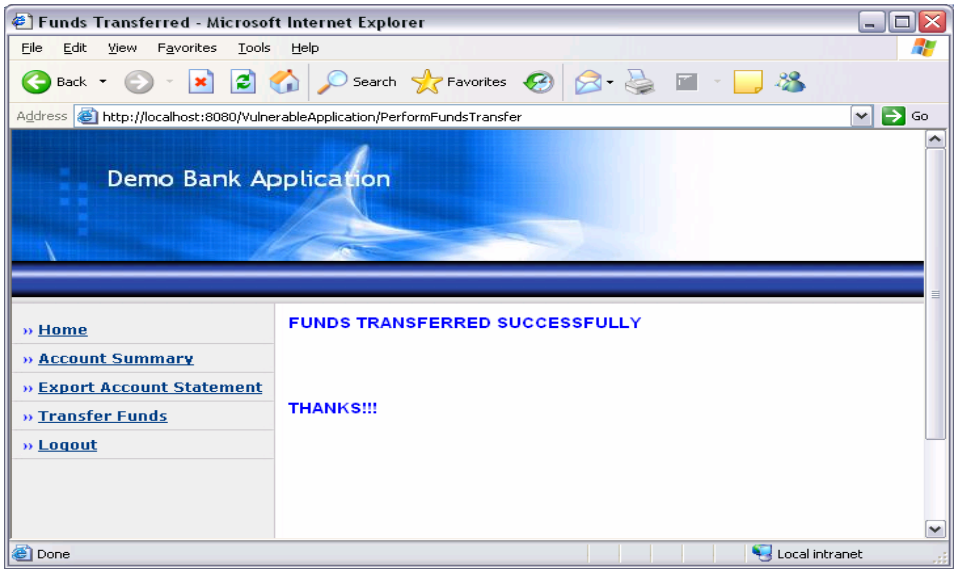
Step 3: Click on "Confirm" and intercept this request using a web proxy editor. The following screenshot shows the original request being sent to the application.

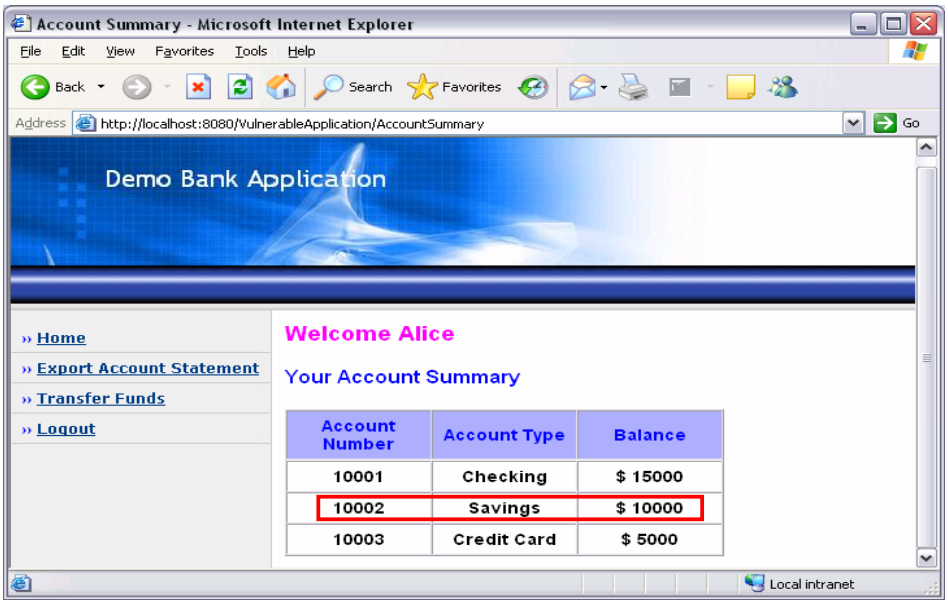


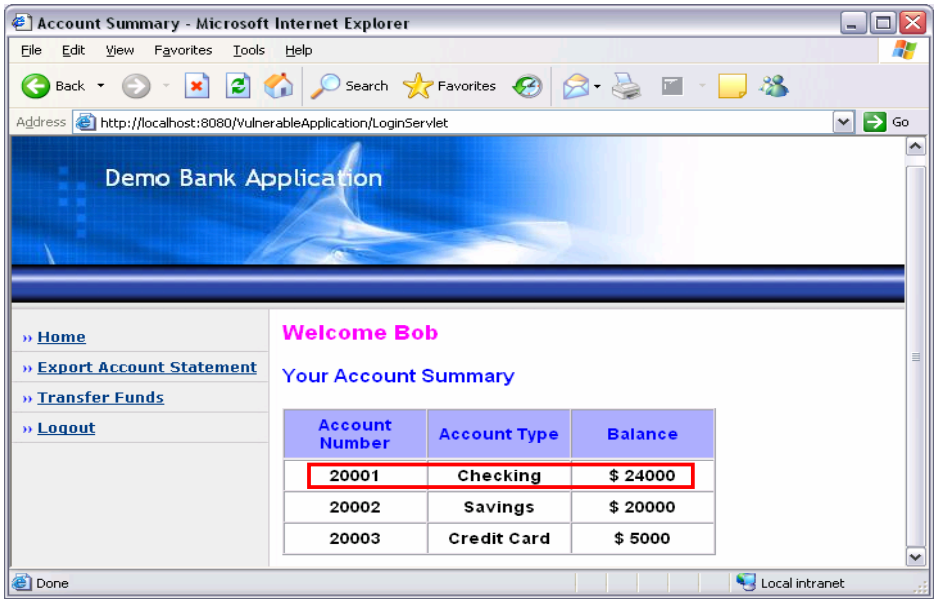
Step 4: Modify the intercepted request such that the From Account is now Bob's account no. i.e. 20001.



The application performs the transfer. It can be verified by checking the account summary of both the users.







View animation titled Finding2 of the exploit

Solution

The application should:

a. Link the valid account numbers of a user to the session ID issued at the time of login.

b. Before committing such critical transactions, check that the account number in the request is of one of the accounts belonging to the logged in user.

As a best practice, such attempts for cross account access should be logged and reviewed.

Go to			
Certification Status	Findings and Action Items Summary	Threat Profile	Mitigation Tracker

3. A malicious user can view account summary of other users.

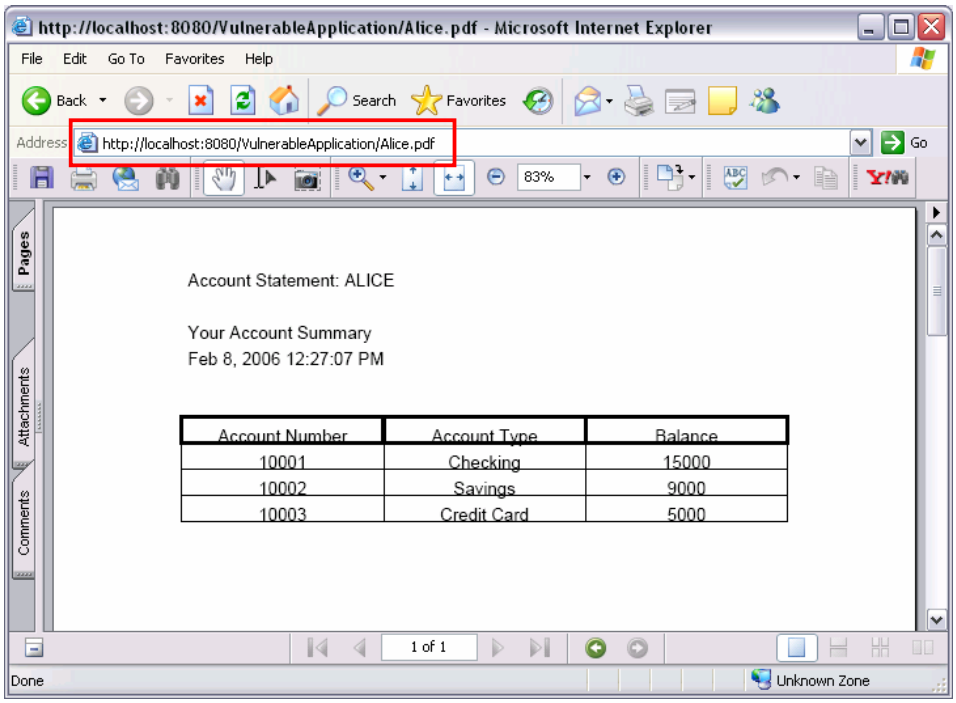
The application provides a feature of viewing the account summary of a user in PDF document format through the "Export Account Summary" link. The application stores the PDF documents on the server and users directly access them. Thus a malicious user can directly access this stored file by specifying the URL to this file directly.

RISK LEVEL
HIGH

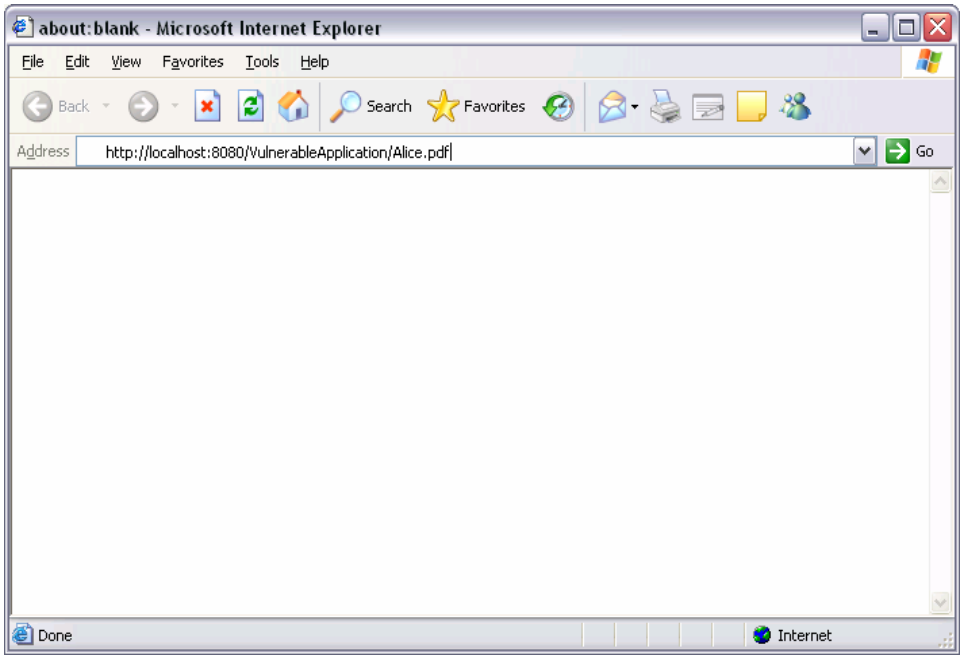
Relevant to which all certification criteria	Defend against Threat Profile
Relevant to which all threats in the Threat profile	A malicious user views financial statements of other users
Impact	The impact is high as sensitive information of users can be seen.
Ease of exploitation	This attack is easy to exploit as the malicious user only needs the user id to construct the link for retrieving the document.

Exploit

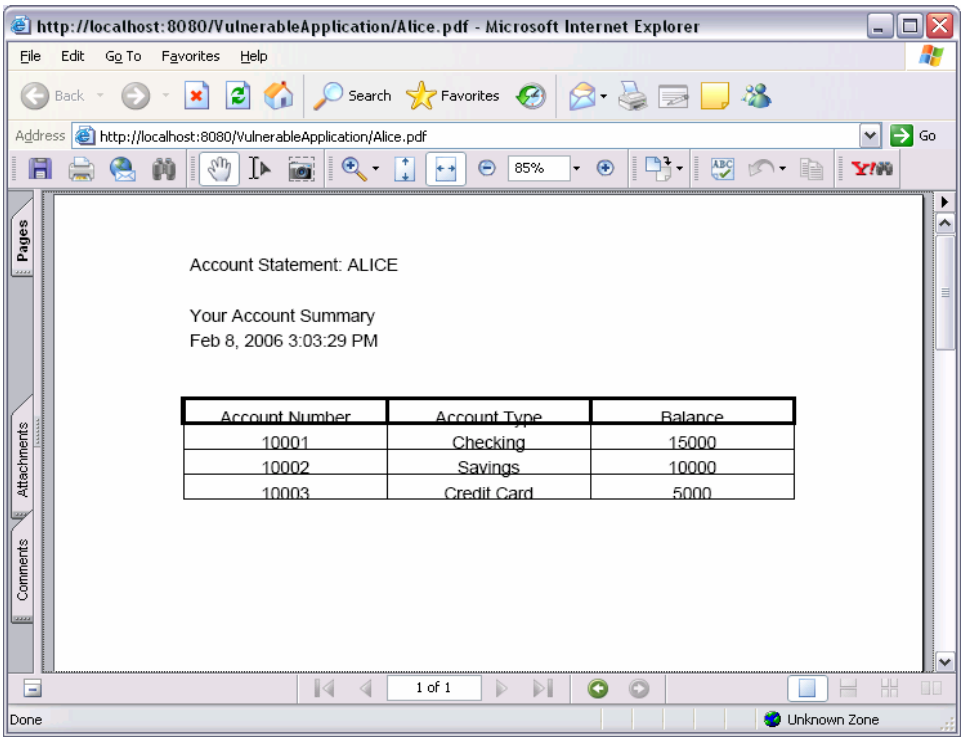
Step 1: Login as a valid user and click on "Export Account Summary" link. A new page showing the account summary in PDF format is displayed.



Step2: Copy the URL of this page, log off from the application and paste the URL in a fresh browser window.



The document is displayed in the browser.



View animation titled Finding3 of the exploit

Solution

The PDF documents should be generated dynamically and streamed to the browser. The content type tag in the response should be set to the correct document format.

Go to			
Certification Status	Findings and Action Items Summary	Threat Profile	Mitigation Tracker

4. An attacker can steal user credentials through browser refresh even after the user has logged out but not closed the browser.

RISK LEVEL

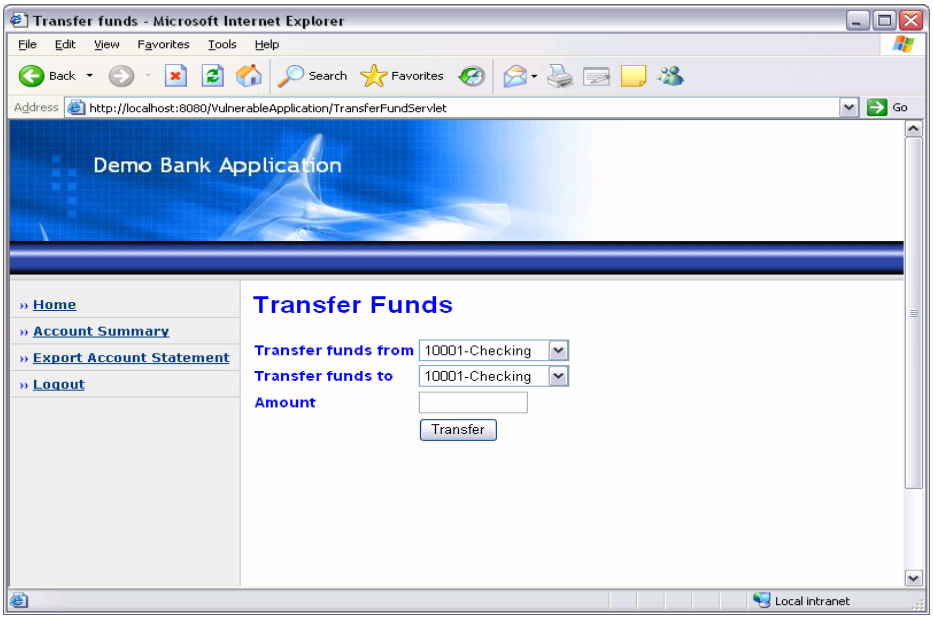
MEDIUM

After browsing the application, suppose a legitimate user logs out but leaves the browser window open. An attacker can navigate back to the page obtained immediately after login using the back button of the browser and refresh the page. This will result in the previous POST request being resubmitted. The attacker can intercept this request with a web proxy editor tool and obtain the plaintext password being sent.

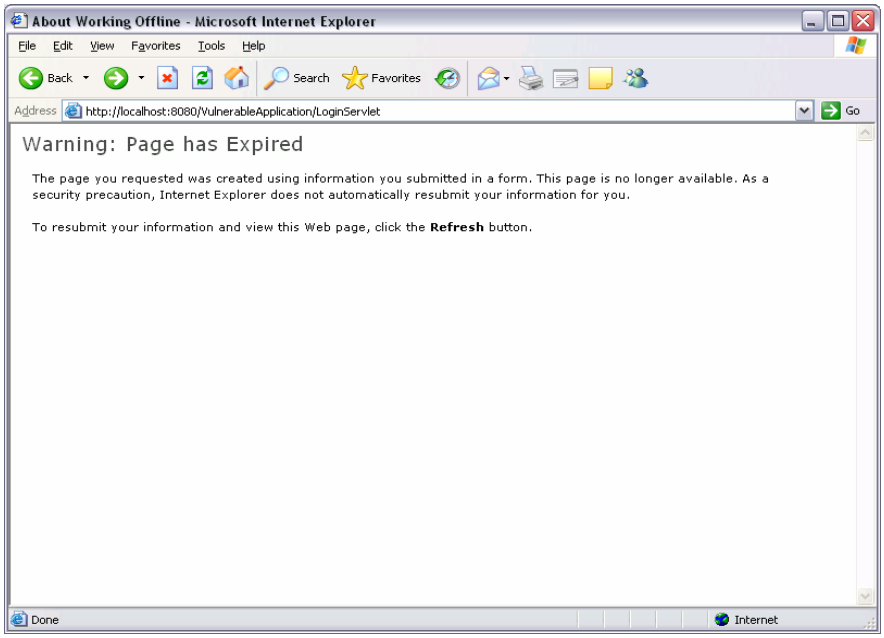
Relevant to which all certification criteria	• Safe against popular attacks • Defend against Threat Profile • Safeguard passwords • Re-authentication required after log out
Relevant to which all threats in the Threat profile	A malicious user gains authentication credentials of other users
Impact	The impact is high as this flaw allows an attacker to gain the user credentials which leads to complete control of the target account
Ease of exploitation	This attack is difficult to exploit as the attacker needs to have physical access to the target machine. Knowledge of web proxy editor tools is required. The attack will only work if the user has left the browser open after logging out.

Exploit

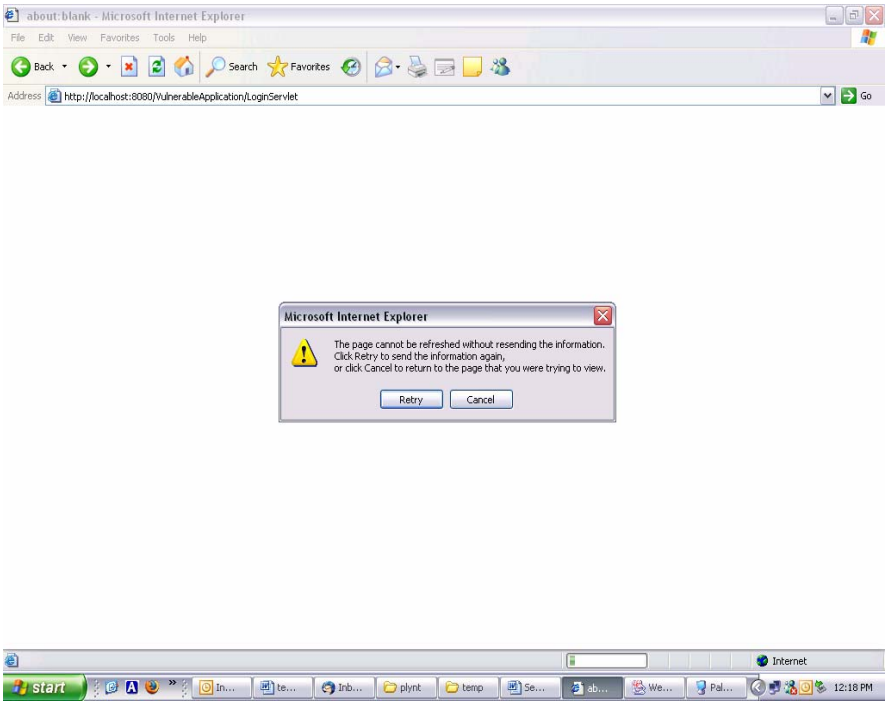
Step1 : Log in to the application as a valid user and click on transfer funds.



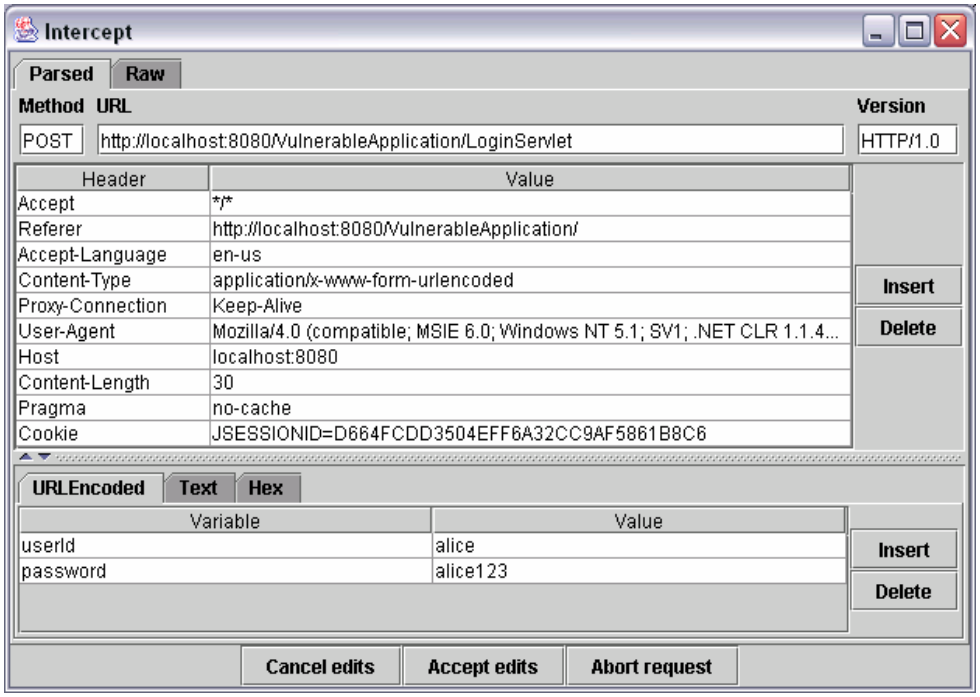
Step 2: Click on back button of the browser.



Step 3: Click on refresh and then the retry button.



Step 4: Capture the request through a web proxy editor to view the credentials being sent.



View animation titled Finding4 of the exploit

Solution

Introduce an intermediate page after the user is successfully authenticated before redirecting to the next page.

Go to			
Certification Status	Findings and Action Items Summary	Threat Profile	Mitigation Tracker

Mitigation Tracker

ACTION ITEM NO.	NAME/LABEL	RISK RATING	REQUIRED FOR CERTIFICATION	PERSON RESPONSIBLE FOR FIXING	DEADLINE FOR FIXING	INTERNAL PERSON FOR VERIFYING THE FIX	DEADLINE FOR VERIFYING INTERNALLY	CURRENT STATUS
1.	Implement proper input validation to escape special characters in the input. (on page 8)	HIGH	YES					
2.	Check the account numbers in the request to ensure they belong to the logged in user. (on page 11)	HIGH	YES					
3.	An intermediate redirection page should be introduced immediately after successful authentication before displaying the next page. (on page 19)	HIGH	YES					
4.	The account statement documents generated should be streamed on the fly and not stored localy. (on page 16)	MEDIUM	YES					

Website: http://plynt.com/

PLYNT, INC.

12801 Worldgate Dr., Ste 500

Herndon, VA 20170, USA

Phone: 1(866)759-6824 or 1(866)PLYNT24

Fax: 1-703-871-3936

Email: plynt@plynt.com