Deliverable 5

Tao Li (TAL88)

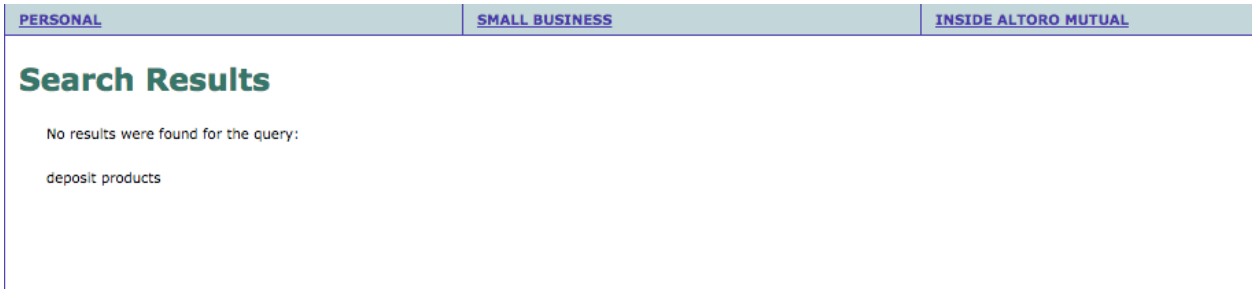
Zhaoxuan Ren (ZHR5)

Vulnerability 1: Cross-site Scripting

URL: http://demo.testfire.net/

Step taken to exploit the vulnerability: When trying to use search function, input keywords in, and after click "search" button, there shows "no results were found for the query" no matter how to change the search keywords.

Screenshot:



Search Results

No results were found for the query:

deposit products

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

Integrity. The output should show some useful information which user required, but for the result, it shows nothing so we know that it changed the data. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser.

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

Modification: The data is changed that the web can not show the search result.

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

Active. Because the data is changed.

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

Data loss. The users can not get the search result due to changing data.

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

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

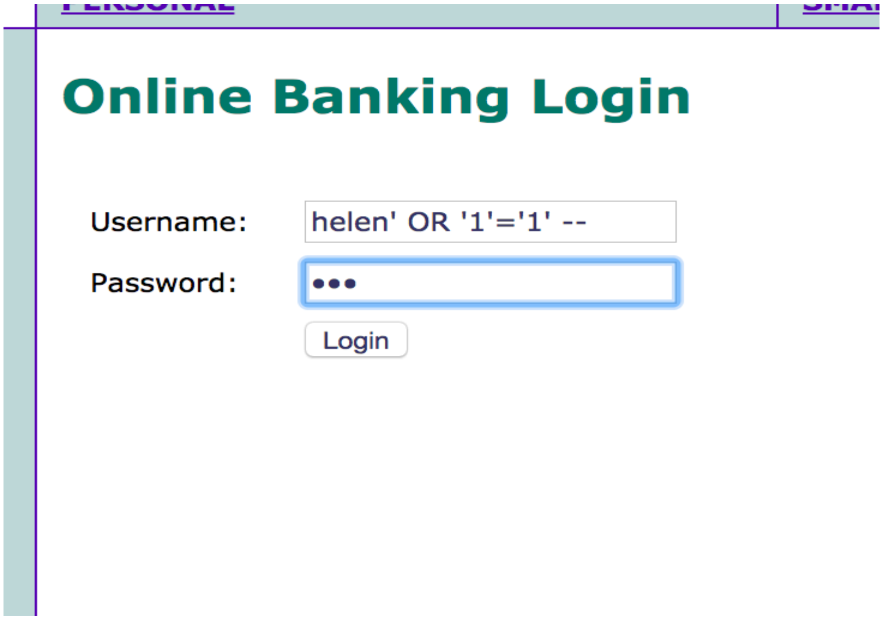
Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

Vulnerability 2: SQL Injection

URL: http://demo.testfire.net/bank/login.aspx

Step taken to exploit the vulnerability: Opening the login page, enter " helen' OR '1'='1' --" as Username and enter '123' as password. Then, click "Login" and we can login the website.

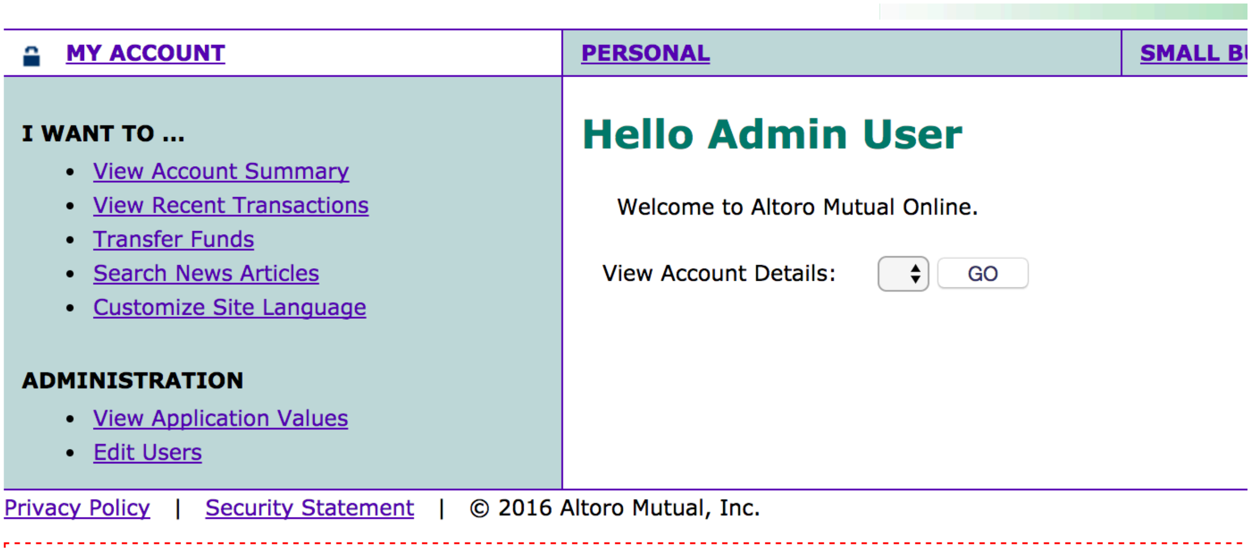
Screenshot:



Online Banking Login

Username: helen' OR '1'='1' --

Password: •••



Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

© 2016 Altoro Mutual, Inc.

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

It is confidentiality for this part because the unauthorized user can login the system and get some sensitive information.

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

It is interception because attackers can get into the system and read data

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

Passive. Because it does not change the system.

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

This vulnerability will cause unauthorized access. Attackers can get the users' information without using correct username and password.

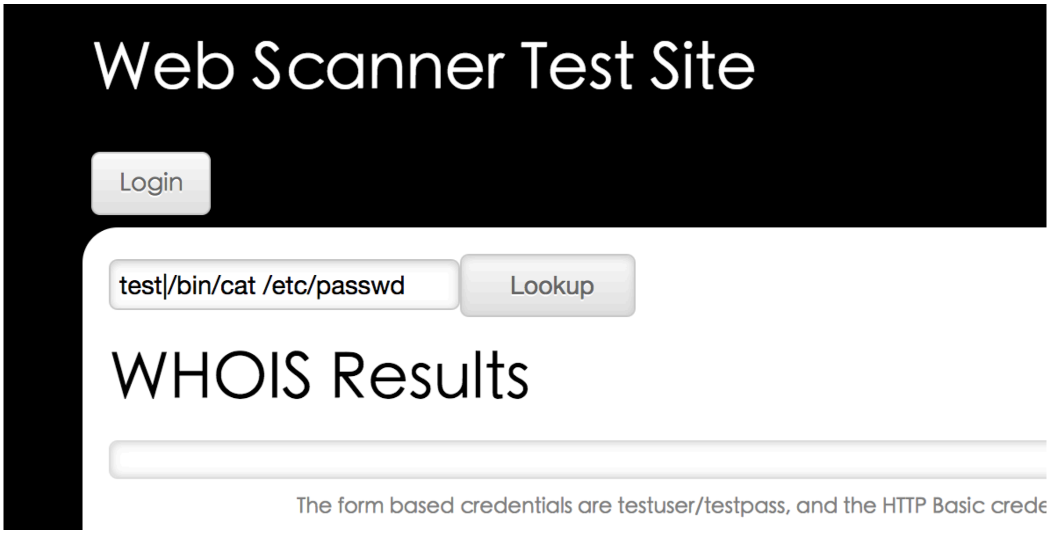
5.What steps should the development team take to fix this vulnerability?

Script should filter characters from user input

Vulnerability 3 Command Injection

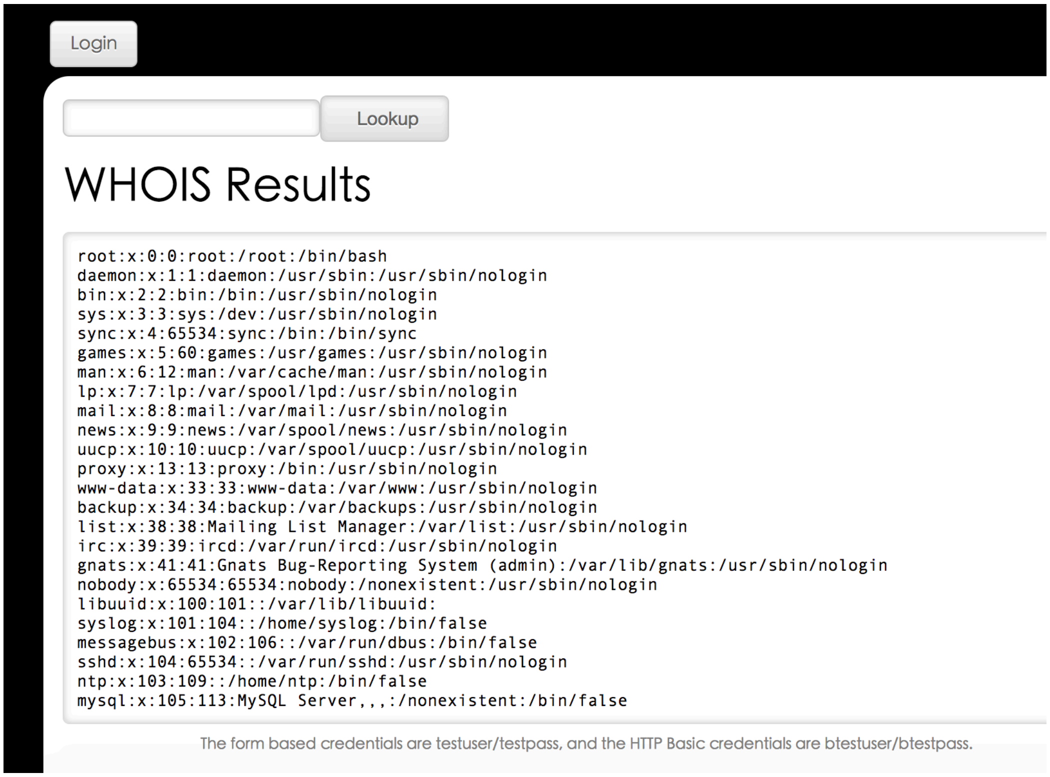
URL: http://webscantest.com/osrun/whois.php

Step taken to exploit the vulnerability: Opening the web page and input " test|/bin/cat /etc/passwd" and then we can see many useful information
Screenshot:



test|/bin/cat /etc/passwd

The form based credentials are testuser/testpass, and the HTTP Basic crede



```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
ntp:x:103:109::/home/ntp:/bin/false
mysql:x:105:113:MySQL Server,,,:/nonexistent:/bin/false
```

The form based credentials are testuser/testpass, and the HTTP Basic credentials are btestuser/btestpass.

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

Confidentiality, Unauthorized users can read the system data.

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

Interception. Hackers can get system information by changing commend.

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

Passive. Because it does not change the system.

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

Unauthorized access. Hackers can get the sensitive information.

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

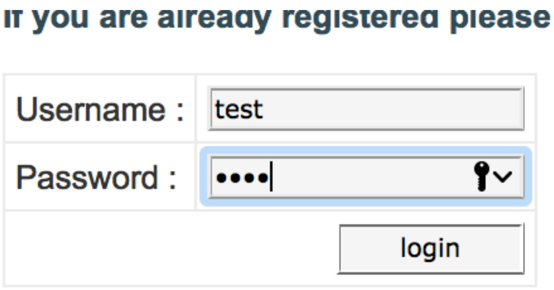
Use library calls rather than external processes to recreate the desired functionality
Filter user input

Vulnerability 4 Weak Password

URL: http://testphp.vulnweb.com/userinfo.php

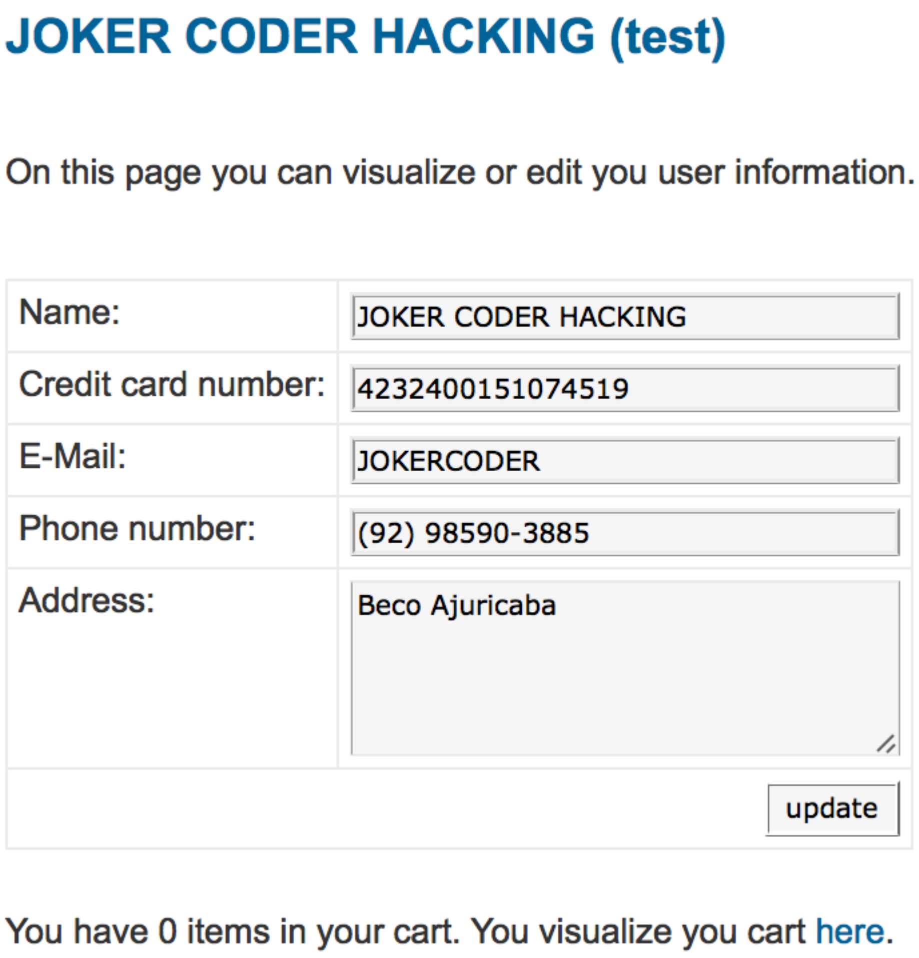
Step taken to exploit the vulnerability: Opening the signup page, input 'test' as username and 'test' as password. Click 'Login' and the page shows user information.

Screenshot:



If you are already registered please enter your login information below:

Username :	test
Password :	••••



JOKER CODER HACKING (test)

On this page you can visualize or edit you user information.

Name:	JOKER CODER HACKING
Credit card number:	4232400151074519
E-Mail:	JOKERCODER
Phone number:	(92) 98590-3885
Address:	Beco Ajuricaba

You have 0 items in your cart. You visualize you cart here.

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

Confidentiality. The password is to short and weak that hackers can easily get it and login the system.

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

Interception. Unauthorized user can get the sensitive information.

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

Passive. Because it does not change the system.

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

Unauthorized access.

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

Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.