

[NEWS] C2IT.com Security Holes

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0029.html>

From: support@securiteam.com

Date: 01/08/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 8 Jan 2002 23:37:48 +0100 (CET)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

C2IT.com Security Holes

SUMMARY

CitiBank's online cash site, C2IT.com, has several Cross Site Scripting vulnerabilities. The site is similar to PayPal in that it lets users attach Bank and Credit Card account to this online system. Users can then "send" cash to any user via their email address. The site leaves nearly every form field unfiltered, and also displays credit card numbers, bank account numbers, security codes, and other data with no obfuscation. This info is therefore available to JavaScript through cross-site scripting. Citibank was notified 4 months ago about problems with their sites and many times since, however, no noticeable actions have been taken yet.

This alert documents two sample attacks:

- Gaining access to user's credit card and bank account numbers
- Scripting cash transfers out of users accounts

DETAILS

Background:

CERT alerted to Cross Site Scripting over a year ago and gave many specific recommendations on how to prevent such attacks.

<<http://www.securiteam.com/exploits/5IP000KOLI.html>>

<http://www.securiteam.com/exploits/5IP000KOLI.html>

Securiteam: [NEWS] C2IT.com Security Holes

Citibank seems to think their site is secure

<<https://www.c2it.com/C2IT/privacypromise.jsp#security>>
<https://www.c2it.com/C2IT/privacypromise.jsp#security>

Alert User's Account Numbers (Credit Card / Bank account)

Bank and Credit Card account numbers that are attached to the users C2IT account are hidden in the SendCash form. They are accessible by JavaScript and by Cross Site Scripting. This code can be passed to the ACCOUNT input variable and escaped by "> .. The script sets a time out so that the full form can load. It then accesses the SRC_ACCOUNT form field that has an array of bank/credit card numbers in it.

Page Location: <https://www.c2it.com/C2IT/SendCash>

Vulnerable Variable: AMOUNT

Pre-Requisite: User must be logged in and have attached account.

Sample Script:

```
<script>
  setTimeout("alert(document.forms[0].SRC_ACCOUNT.options[1].value)",
400);
</script>
```

Additional info: The whole list of account numbers could be sent to another site using document.location. The credit card expiration date and 3-digit security code are on the edit account nickname page.

Automatically Transfer Cash out of Account.

Forms and actions on the site can be scripted through the Cross Site Scripting hole. One thing to script is the Send Cash function that lets attackers send money to any email address. This script populates the send cash form with email address and amount to send (source account could also be selected, by default it comes out of C2IT account). The script then confirms the action.

Page Location: <https://www.c2it.com/C2IT/SendCash>

Vulnerable Variable: AMOUNT

Pre-Requisite: User must be logged in and have cash or credit card attached.

Sample Script:

```
<script>
  w=window.open("SendCash", "s", "");
  setTimeout("f=w.document.forms[0];f.DEST_EMAIL.value='u@you.com';
f.AMOUNT.value=10;f.submit();",15000);
  setTimeout("w.document.forms[0].submit();", 15000);
</script>
```

Securiteam: [NEWS] C2IT.com Security Holes

Additional info: This could also be called from a dozen other pages / variables on the site.

Covering your tracks

A full attack may include ways to mask actions that have occurred. C2IT's transaction history page can also be corrupted with non-escaped HTML characters. In the above transfer, simply adding some HTML to the NOTE_TO_SELF field would show up on the user's transaction history log in an "A HREF"! A simple ">" escape that, and html could be used to obscure other info on the page. HTML code is left to your imagination.

Conclusions:

The good news is that simple updates to C2IT.com can completely fix their site. They should also be able to track any accesses to their system. The bad news is that this attack is very simple and anyone with JavaScript knowledge could create devious code. In addition, many other sites online still have not fixed their Cross Site Scripting problems and could be vulnerable to similar attacks.

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@devitry.com> dave .

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[NEWS] AIM Filter Contains Spyware and Backdoors"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)