Buzzle Online Site Review

Including Security Report

v1.3, 2/2/2001 - Review by & © Leefe Hicks, wyvern@nectar.com.au

Table Of Contents

1. Introduction

> "Buzzle understand that security is a vital consideration of all our clients in shopping over the Internet. We have invested a significant amount of time and money to ensure that your details are kept confidential and secure.", Buzzle Online

This document is a review of the Buzzle Online store, including a security review of the online store.

The document details the process of ordering *free* products from Buzzle Online, security problems with customer transactions and a collection of other problems found with the site. And there is a list of recommendation for fixing the problems.

2. Order_free_G4s_from_Buzzle-HOWTO

i. Go to http://www.buzzle.com.au/.

ii. Click the **Register** link.
[If you click **Submit** now you will get a JavaScript error stating your first name needs to be entered. You will get errors for other fields left blank if your enter just a first name.]

iii. Turn off JavaScript in your browser. [1]

iv. Click **Submit**.
You will not see the *'Welcome to the Buzzle Members Area'* page.
(You can now turn JavaScript back on.)

v. Click on the **Store** link.

vi. Click on the **G4** link (other products will produce the same result).
All the G4s are listed for '$0.00'.

vii. Click **Buy me**.
You will now be presented with a page to select how many $0 G4s you want.

viii. Click **check out**.
You will not see an invoice for your G4.

ix. Fill out the address you want to have your free G4 delivered to. [2]

x. Click **Submit**.

xi. You will now see the **Final Invoice**.
Your G4 will now be displayed for $0, with a small delivery charge (approx $30). The delivery address will be displayed, but no billing address (only the variable names). [see Screen Shot A]

Footnotes

[1] If you don't know how to turn off JavaScript in your browser read the help section for your browser.

[2] Make sure you don't use your real name or address.

3. Other Faults of the Site

i. Invalid security certificate

The first time I used the secure part of the site I was presented with an error message saying the security certificate was not registered for this site did I want to still except it. The message also stated that the security certificate was using 40 bit encryption. [see Screen Shot B]

ii. Encryption 40 bit or 128 bit, that is the question

On the page:
http://www.buzzle.com.au/webcatalog/cca1site/store/shopterm/credsec.tpl

It states: '*Your credit card details are protected by the latest DES 128 bit encryption techniques*.' But the security certificate received was only 40 bit.

I wonder which is correct. Is Buzzle using 40 bit encryption with the customer and 128 bit encryption withe the bank? Why are they not using 128 bit encryption for transactions with the customer?

iii. Keeping credit card details

On the page:
http://www.buzzle.com.au/webcatalog/cca1site/store/shopterm/credsec.tpl

The question '*Does Choice Connections store my credit card details ?*' is asked. And answered '*No. Your credit card details are not retained or stored by Buzzle at any time*.'.

Does this mean the Choice Connections does store the credit card details, but Buzzle does not? The question being asked is not answered.

iv. Hijack other orders

Because the 'cart' id is displayed as part of the URL it is possible to hijack another cart by changing the card id number in the URL.

A similar problem was present in the ATO website used to register an ABN.

v. Order nothing

It is possible to order nothing. And that only costs you $8 delivery.

vi. Crash server

When testing the 'free G4' process I believe the server crashed as the Buzzle web site was reported unavailable for a time afterwards. Making an educated guess this is probably due to zero divide errors.

vii. Suggestions & Requests

The '*Suggestions & Requests'* link at the bottom of the '*Final Invoice*' links to:

file:///Macintosh HD/Desktop Folder/store/shopterm/suggest.tpl?cart=

Giving some indication of where the site is stored, or was developed.

viii. Remaining HTTPS

After entering the secure part of the site the site remains secure (uses https) for any link you click on. This includes all of the site that is normally accessed via http.

This may not seem like a big problem but it will slow the server down. Encrypting each web page, and all the graphics, places a much bigger load on the server.

ix. Incorrect grammar & spelling/typos

The site needs to have someone check the grammar and spelling. I saw at least 1 '*ew*' & a few grammatical mistakes.

x. Incorrect characters

There are lots of 'O's with accents on them from using 'smart' quotes on the site and not converting them to special characters.

xi. Wrong mouseover

The top menu has mouse overs to change the images when you put your mouse over them. But the mouseover on the *'education'* logo changes the *ecommerce'* logo.

4. Final Notes

i. There is no server side checking of data submitted

Don't explicitly trust data sent to the server by a client machine.
It may be possible to save the source of page and insert a price that looks reasonable and submit that. This has not been tested but it looks possible.

ii. Zero prices

The end price is most likely calculated by multiplying the price by a discount for registered customers. And if a customer goes to the registered customers section but has no customer ID, using the free G4s method, the value of the discount is also zero. So multiplying the price by zero gives a price of zero.

5. Recommendations

i. As a default customers should be required to pay full price and the discount variable should be set accordingly.

ii. Perform server side checking of the data that comes back from the each client's browser. (4i)

iii. Use cookies to store the cart id and track customers, rather then putting the cart id in the URL. To be more secure you could cross reference the cookie with the client computers IP address. (3iv)

iv. Get a 128 bit security certificate that is valid for the buzzle.com.au domain name. (3i, ii)

v. Update the privacy page so that the answers answer the questions. (3iii)

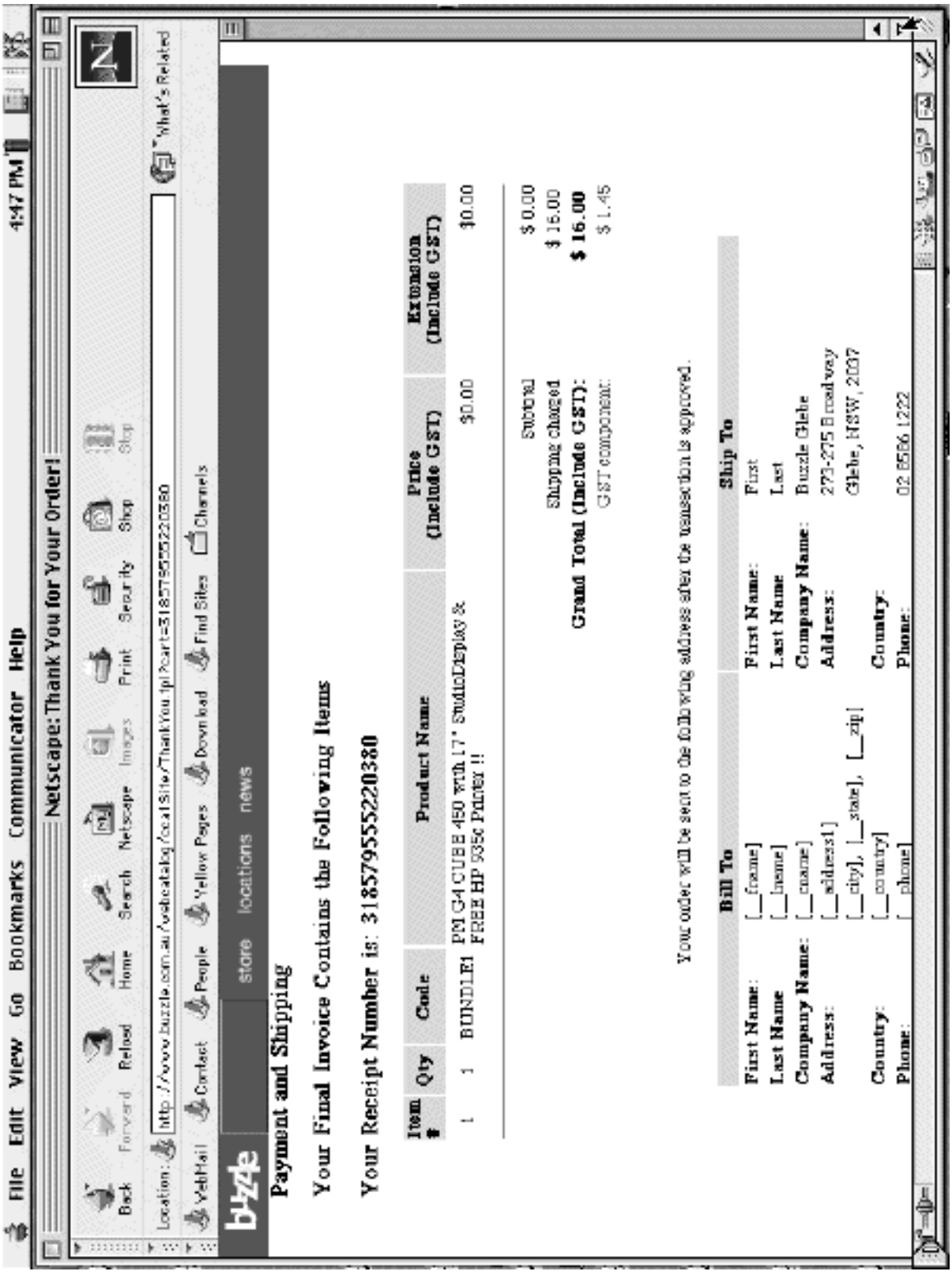
vi. Have links take you back to HTTP, rather than continuing with HTTPS, after the client has finished the invoice section. (3viii)

vii. Have someone check the site for typos, grammatical errors, dead links & bad characters. (3vii, ix, x)

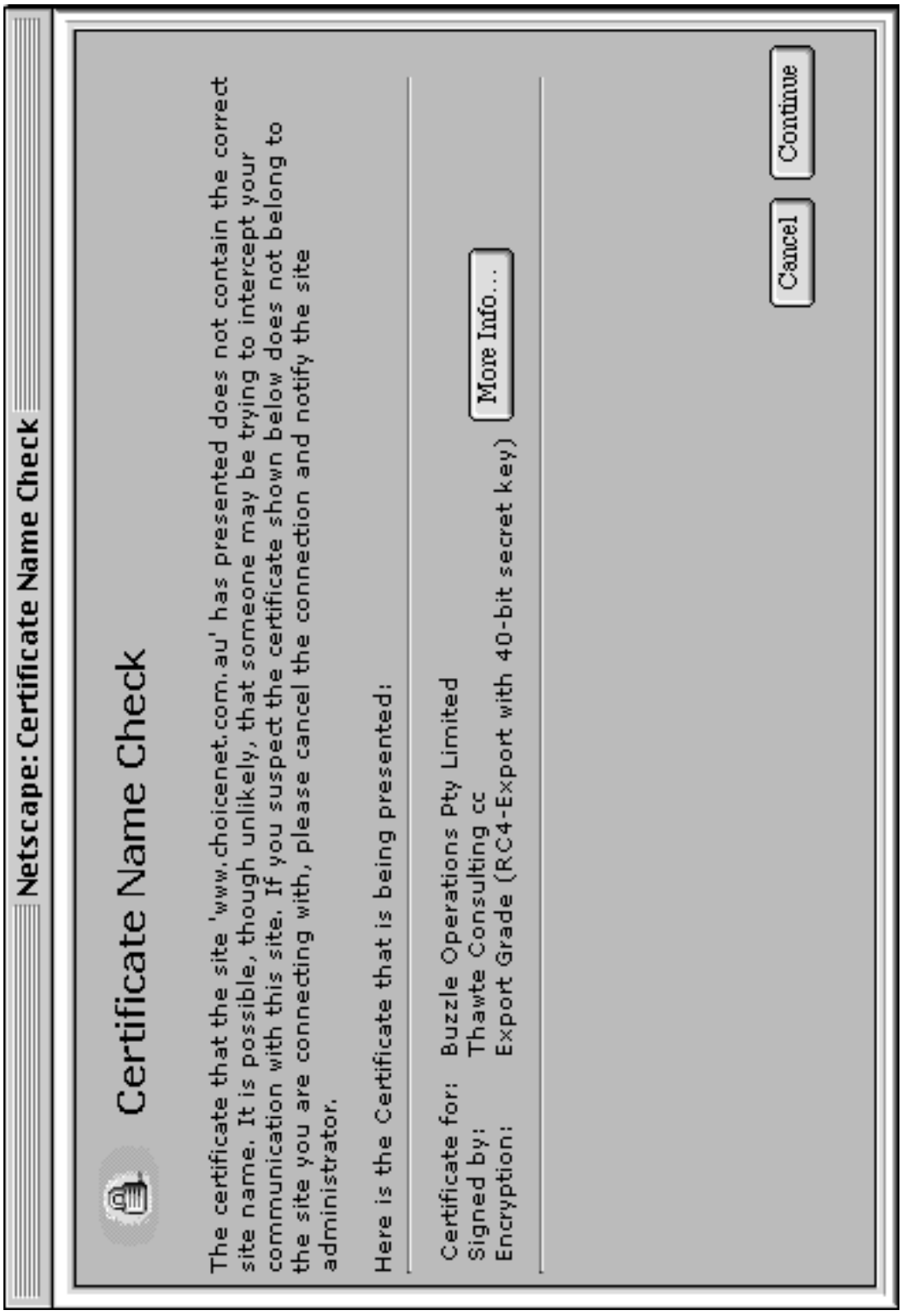
viii A quick fix for the problem would be to make the submit button only submit via JavaScript. Remove *TYPE="submit"* from the BUTTON tag and have the JavaScript do the submit. This will stop people submitting that form with JavaScript turned off but there are still other problems that need to be addressed. (2iv)

6. Screen Shots

A.



B.


Netscape: Certificate Name Check
Certificate Name Check
The certificate that the site 'www.choicenet.com.au' has presented does not contain the correct site name. It is possible, though unlikely, that someone may be trying to intercept your communication with this site. If you suspect the certificate shown below does not belong to the site you are connecting with, please cancel the connection and notify the site administrator.
Here is the Certificate that is being presented:
Certificate for: Buzzle Operations Pty Limited
Signed by: Thawte Consulting cc
Encryption: Export Grade (RC4-Export with 40-bit secret key)
More Info...
Cancel
Continue