BADSTORE™

SEE HOW THE HACKERS THINK

Badstore.net User Manual

Version 1.2

1 February 2005

Updates and Enhancement Requests to BadStore.net

BadStore.net will be periodically updated to introduce new functionality and to introduce more bugs. Information on the most current version of BadStore.net can be found at www.badstore.net.

BadStore.net has been developed by and is maintained by:

Kurt R. Roemer, CISSP
Chief Security Officer
NetContinuum, Inc.
847-548-5390 Office
kroemer@netcontinuum.com
kurt_roemer@yahoo.com

To submit an enhancement request to BadStore.net, send an email to kroemer@netcontinuum.com with the subject "BadStore.net Enhancement Request" and an explanation of what you'd like to see and why you feel it would be particularly useful. Enhancement Requests for technical aspects of the system, usability, and documentation are welcome.

Credits and Thanks

Thanks to NetContinuum, Inc. for sponsoring the development of and for hosting the download site for BadStore.net. Thanks also to Matthew Franz for continuing to maintain Trinux.

Table of Contents

1 Welcome to BadStore.net!

1.1 What is BadStore.net

BadStore.net is an insecure application used for demonstration, security training, and testing purposes. BadStore.net has been developed to illustrate the common vulnerabilities present in many applications exposed to intranets, extranets, and the Internet. *Many people tasked with designing operating, and securing Web Applications have never seen the variety of attacks available to compromise these applications – or what they can do to protect these applications.*

BadStore.net exists as a bootable CD running the Trinux operating system. It includes the Apache web server, a CGI (Common Gateway Interface) application, and a full MySQL implementation with multiple database tables. This is a full-featured application that uses standard coding methods – BadStore.net is not a simulation.

To run the BadStore.net application, boot the BadStore.net CD in your host machine (see the sections on Installation and System Requirements). BadStore.net launches as a network server that can be accessed with a Web browser. Optionally, BadStore.net can be used under a virtual environment, such as VMWare. When you reboot, default settings are automatically reset. There's no need to rebuild after successful "hacks".

BadStore.net is currently available in English and Japanese language versions and is released under the terms of the GNU General Public License.

1.2 Where to obtain BadStore.net

The current version of BadStore.net can be downloaded from the appropriate links for your platform at www.badstore.net.

BadStore.net exists as an ISO image that can be downloaded and burned to CD.

1.3 Purpose of BadStore.net

Many information security professionals and business associates who are responsible for application security have never "seen" the business impact of vulnerabilities. By illustrating these vulnerabilities, attacks and their business impact can be clearly shown. In this way, BadStore.net assists with security awareness, vulnerability discovery, security training, security testing, and determining remediation options.

1.4 Vulnerabilities Presented in BadStore.net

BadStore.net application platform contains dangerous vulnerabilities that expose the application and environment to attack. BadStore.net should only be used in a lab or test environment, and must never be installed on a production system. BadStore.net contains the following security vulnerabilities:

Cross Site Scripting (XSS)
SQL Injection
Command Injection
Cookie/Session Poisoning
Parameter/Form Tampering
Buffer Overflow
Directory Traversal/Forceful Browsing
Cookie Snooping
Log Tampering
Error Message Interception
Denial of Service
… and more!

These vulnerabilities can give hackers the total ability to *own* your application, Web server, SQL databases, application logic, operating system, and sensitive data.

Please refer to www.netcontinuum.com/welcome/threats for more information on the 21 Classes of Application Threats.

2 Installation

2.1 Installation of BadStore.net

BadStore.net application platform contains dangerous vulnerabilities that expose the application and environment to attack. BadStore.net should only be used in a lab or test environment, and must never be installed on a production system.

BadStore.net boots from CD-ROM and runs as a Trinux/Apache server. There is no installation necessary, and nothing is copied to the hard drive of your PC. Please note, however, that vulnerabilities in BadStore.net would allow an attacker to access the hard drive on the host PC. It is highly recommended that BadStore.net only be used in non-production environments (see the Disclaimer for more information).

BadStore.net also runs well under VMWare.

Once the BadStore.net application server has booted, go to the following site:
http://*serveripaddress*/cgi-bin/badstore.cgi

If JavaScript support is unavailable:
http://*serveripaddress*/cgi-bin/badstore.cgi

Alternatively, you may add an entry to the local 'hosts' file on the client, and then access the server by name.

2.2 System Requirements for BadStore.net

BadStore.net runs as a client/server system. The BadStore.net CD boots in the designated server system, and a client system with a Web browser accesses the BadStore.net application over a network.

The following are system requirements:

- Host PC with a Pentium 200MMX w/ 64MB RAM (or more)
- CD-ROM (PC must be able to boot from CD)
- Active network adapter on the BadStore.net host
- A network that connects the BadStore.net server to the client (or an Ethernet crossover cable)
- Client system, also with active network adapter and Web browser
- Cookies enabled in the client browser
- JavaScript support enabled in the client browser

2.3 Network Configuration

To securely contain BadStore.net within your test environment, you may wish to use a crossover Ethernet cable between the client and the BadStore.net host. BadStore.net should only be used in a lab or test environment, and must never be installed on a production system.

On boot-up, the BadStore.net server attempts to assign an IP address via DHCP to the host's network adapter. If a DHCP server is unavailable, BadStore.net will boot without an IP address assignment. Use `ifconfig` to assign an address, as follows:

Example: *To assign an address of `10.10.100.52` on a Class-C (/24) subnet (enter on one line):*

```
 ifconfig eth0 up 10.10.100.52 netmask 255.255.255.0 broadcast
 10.10.100.255
```

For a list of supported Ethernet adapters, see the Trinux documentation at http://trinux.sourceforge.net/network.html.

2.4 Further Information: Links to Application Security Information and Tools

Class	Name	Description	Link
Security Tools	ActiveState PERL	PERL Programming / Runtime environment for Windows	http://www.activestate.com
	Ethereal	Network Protocol Analyzer	http://www.ethereal.com
	HTTrack	Website Copier	http://www.httrack.com
	John the Ripper	Password Assessment	http://www.openwall.com/john/

	Kiwi	Syslog daemon for Windows	http://www.kiwisyslog.com
	Knoppix	Bootable Graphical Linux Distro w/ Security Tools	http://www.knopper.net/knoppix/index-en.html
	Nessus	Security Scanner	http://www.nessus.org
	Netcat	TCP/IP Connection Tool	http://netcat.sourceforge.net
	Nikto	Web Application Security Scanner	http://www.cirt.net
	NMAP	Network Mapper and Auditing Tool	http://www.insecure.org
	Paros	Web Proxy / Assessment	http://www.parosproxy.org
	Putty	Telnet/SSH Client for Windows	http://www.chiark.greenend.org.uk/~sgtatham/putty/
	SSLDump	SSLv3/TLS Network Protocol Analyzer	http://www.rtfm.com/ssldump/
	Trinux	Bootable Linux Distro w/ Security Tools	http://www.trinux.org
Security Organizations	AVDL	Application Vulnerability Description Language	http://www.avdl.org
Recommended Vendors	NetContinuum	Application Security	http://www.netcontinuum.com

3 Important Disclaimer

This section explains important considerations for the use of BadStore.net.

No Lifeguard on Duty – Use at Your Own Risk!

BadStore.net has been developed to illustrate the common vulnerabilities present in many applications exposed to intranets, extranets, and the Internet. As such, the BadStore.net application platform contains dangerous vulnerabilities that expose the application and environment to attack.

BadStore.net should only be used in a lab or test environment, and must never be installed on a production system. You have been warned! This site has been developed using common HTML, CGI (PERL), and JavaScript coding techniques. Any similarity to an existing free or commercial application is purely coincidental. All images used are believed to be in the public domain - please notify Kurt R. Roemer, Chief Security Officer, NetContinuum, Inc. (kroemer@netcontinuum.com) if there's a problem.

There is no implied warranty for any use of this application.

4 Cheat Sheet

This section presents a sample of the vulnerabilities present in the BadStore.net application.

If you really want to know where the vulnerabilities exist in BadStore.net, read on:

- Robots.txt directory disclosure (*http://www.badstore.net/robots.txt*).
- Apache platform attacks (run Nessus and Nikto.)
- SQL Injection in Search and Login functions – including DROP and UNION (try logging in as a normal user with *joe' OR 1=1 OR 'mary* as a simple example.)
- Blind SQL Injection in Supplier Login (try single quote ('), *OR 1=1*, *OR 1=1--*, and other SQL commands and watch them fail, until you hit the "magic" combination.
- Cross-Site Scripting (XSS) in Guestbook, URL's, Search (try *alert('This is an XSS attack!!!')</script>*).
- Credential Disclosure via proxy, XSS, and Brute Force (use proxy to decode the Base-64 encoded SSOID cookie, try *<script>alert(document.cookie)</script>*, and run Brutus to force a login.)
- Command Injection via Parameter Tampering.
- Privilege Escalation via Cookie and Hidden Field Tampering (what's that Role parameter?)
- Ability to decode cookies and view sensitive information (use the proxy.)
- "Secret" Admin access via URL parameter (try *?action=admin* in the URL.)
- Access to Supplier Portal through referer header manipulation, cookie, SQL Injection (use proxy to manipulate referer header and cookie, try logging in to the form using SQL Injection techniques.)
- Denial of Service (DoS) to application and platform.
- Ability to obtain free or discounted merchandise (use the proxy to manipulate the CartID cookie.)
- Site Defacement (you can upload files from the Supplier Portal – can you also traverse directories?)
- MD5-hashed passwords, many of which are easily crackable (try John the Ripper.)
- Personally Identifiable Information disclosure, including Credit Cards (in Previous Orders and Secret Admin Portal.)
- Ability to login without a known password (try SQL Injection and Brute Force.)
- Ability to view other's orders and information (use proxy to manipulate cookie.)

Known account: big@spender.com
Password: money

5 License

5.1 GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

5.1.1 Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.
The precise terms and conditions for copying, distribution and modification follow.

5.1.2 TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> **a)** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
> **b)** You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
> **c)** If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)
> These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.
> Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.
> In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)
The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.
If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.
It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to

distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

6 BadStore.net Change Log

v1.0 – Original version for 2004 RSA Show

v1.1 – Added:

- More supported NICs.
- Referrer checking for Supplier Upload.
- badstore.old in /cgi-bin/
- Select icons added to the /icons/ directory.

v1.2 – Version presented at CSI 2004

Added:

- Full implementation of MySQL.
- JavaScript Redirect in index.html.
- JavaScript validation of a couple key fields.
- My Account services, password reset and recovery.
- Numerous cosmetic updates.
- ‘Scanbot Killer” directory structure to detect scanners.
- favicon.ico.
- Reset files and databases to original state without reboot.
- Dynamic dates and times in databases.
- Additional attack possibilities.