BadStore Project

Help

For this project, we will be using the **BadStore.net** VM, developed by Kurt Roemer and used with permission (thanks, Kurt!). It contains a vulnerable web application. Your job will be to exploit vulnerabilities we have talked about in the lectures, and answer some questions in the on-line assessment to show what you find.

You can use any web browser to interact with BadStore.net, but we recommend (and will support) using Firefox (which is freely available). The reason is that Firefox has a nice set of developer tools that allow you to inspect, and modify, the contents of web pages, which will be useful when crafting attacks. If you choose to use another browser, then you will have to figure out how/whether it will permit the same interactions.

Set up and start BadStore with Virtual Box

The first step is to set up BadStore on your machine and get it running.

BadStore is a Linux-based server application. It is distributed as a bootable ISO, which you can download from here. You may also want to download the BadStore manual, which describes the design and setup of BadStore in detail.

The BadStore ISO can be booted directly, or run using a Virtual Machine Manager, like VMWare or Virtual Box. We will explain how to set it up using Virtual Box.

The first step is to install Virtual Box; this project has been tested with the most recent version, 4.3.18. There are specific instructions for installing VirtualBox for computers running Windows, Linux, and Mac OSX.

Now we need to create and configure a Virtual Machine to run BadStore. Do this using the following steps.

1. Create a new VirtualBox VM.

Detailed instructions for doing this are here. In short: when you start Virtual Box, click the "New" icon to create a new VM. Give your VM the name BadStore; specify the operating system type as Linux; and choose 32-bit Ubuntu. You can allocate 512 MB (or more)

RAM to your VM, and specify that it should create the hard-drive now. You will be asked how the image should be stored; make it a VDI with 8 GB (the default), and *this part is important*: make sure the "Dynamically allocated" radio button is set, so that Virtual Box will not reserve the 8 GB on your hard drive, but will allocate it on the fly. In fact, we will use none of this space, so there's no sense in reserving it in advance.

2. Assign the BadStore ISO to the CD-ROM drive of the VM.

Detailed instructions are here. In short, you should select the Settings for the VM you just created, and then select the Storage tab. On the left you will see the VM's "Storage Tree" and you should see Controller: IDE as one listed. With this selected, add a new controller to this tree by clicking the little icon at the bottom with the plus on it in the lower left. It will ask you to choose whether to add CD/DVD or a Hard Disk; select CD/DVD. Then it will ask you whether to "Choose Disk" or "Leave Empty"; select "Choose Disk". A file dialog will come up and you should choose the BadStore_212.iso file that you previously downloaded. Once you do, you should see this image added below the IDE controller in the Storage Tree, and it should be the IDE Primary Master. You might also see an entry for "Empty" which was there at the start; if so, then remove it by selecting the Empty entry and clicking the icon with the minus sign on it.

3. Create a HostOnly virtual network.

You will need to configure a HostOnly networking for your VM. You need to do this in two steps. The first is to create the HostOnly network. The next step is to associate that network with your VM.

Details for creating a host-only network are in the VirtualBox manual. First, you must go to the network settings. For Linux or Windows, this will be under "File" -> "Preferences" -> "Network". For Mac OS, the settings are under "VirtualBox" -> "Preferences". Select the Network tab. You will be shown a list of possible networks, including NAT networks, and Host-only Networks. Select Host-only networks, and then click the icon on the right to add one. It will add an entry with a name like vboxnet0.

If you cannot create a host-only network, it may be because the virtualbox kernel drivers are not properly loaded; cf. this blog post. On MacOS, this problem can be fixed by doing `sudo /Library/StartupItems/VirtualBox/VirtualBox restart`.

Select the newly created network entry and edit it by clicking the appropriate icon to the right. There are two panes, one for Adapter, the other for DHCP Server. The Adapter pane will give the IP address for the network, etc. I should be something like 192.168.56.1 with a Subnet mask of 255.255.255.0. The DHCP Server pane will show the DHCP server information. If it is not enabled with the information filled in, then enable it and fill it in as follows:

```
Server Address: 192.168.56.2
Server Mask: 255.255.255.0
Lower Address Bound: 192.168.56.110
Upper Address Bound: 192.168.56.200
```

Notice that the server address is the same as the adapter address, but with 2, rather than 1. Do the same on your own machine. Likewise select the address range as 110 to 200, but using the same first three octets of the adapter address.

4. Assign the BadStore VM to the HostOnly network.

Now that you have created the HostOnly network, go back to the settings window for the BadStore VM and select the Network pane. Select "Host-only adapter" from the "Attached to" drop down. Select "vboxnet0" (or whatever it was from step 3) for Name.

5. Boot the BadStore VM.

Now you are ready to boot your VM. Start the VM by clicking the green arrow for Start on the VirtualBox console. You will see a text window show up and a bunch of text fly by, while it's booting. (Note that, during this time, VirtualBox may "capture" your mouse pointer and keyboard and you will have to press the host key to get them back.) Eventually, the messages should get to a point where you see

```
netcfg: No such file or directory
Starting syslogd
Bringing down eth0
Found configs for: eth0
Configuring eth0: using DHCP
e1000: eth0 NIC Link is Up 1000 Mbps Full Duplex
```

At this point, it will hang for a while, for some reason related to DHCP, but we aren't sure what. Within a couple of minutes (we see 2.5 minutes, consistently) the VM should finally be able to get an address. After a flurry of additional messages you should see

```
Please press enter to activate this console
```

Press enter and you'll get a prompt.

If the VM does nothing for longer than a few minutes, power off and on the VM and try again. If you still cannot get an address at all then something else has gone wrong. We have observed during testing that not removing the "Empty" CD/DVD when setting up the storage can result in this problem; see step 2, above. Another problem is not having the DHCP server enabled for the host-only network; see step 3.

6. Get the IP address for the BadStore VM.

From the command prompt in the BadStore VM, execute the command

```
ifconfig eth0
```

It will output network information. Write down the IP address following "inet addr" in the output. It will be something like 192.168.56.110, which is the lower bound configured for the DHCP server in step 3. If you get an error like

```
ifconfig: eth0: error fetching interface information: Device not found
```

Then this means that your network configuration was messed up; see troubleshooting suggestions in step 5.

7. Add the BadStore IP address to your non-virtual computer's `hosts` file.

To visit the site www.badstore.net being run by your virtual machine, you will have to edit the `hosts` file on your *host* (non-virtual, non-guest) computer so that when your host computer's web browser looks up www.badstore.net, it resolves to your virtual machine's address instead of a system on the Internet. If the IP address you wrote down in step 6 was 192.168.56.110, you should add the following on a new line in the hosts file:

```
192.168.56.110 www.badstore.net
```

Here are some instructions for finding and editing your hosts file on Windows and Mac OS. For Linux, edit `/etc/hosts` as `root` and add the above line (e.g., using the `nano` editor you could type `sudo nano -w /etc/hosts` to edit the file).

8. Point your browser at www.badstore.net.

It should show the splash page for the BadStore, which displays a black-and-white picture of an old-west-style saloon. If instead your browser hangs, or goes to a different-looking page, then the hosts file is not being accessed correctly.

Note that if you reboot the BadStore VM, its address may change, so you will have to edit the hosts file again. You should, however, be able to close the running VM, saving its state rather than powering it off. When you restart it, it should restart the network and reconnect using the same address (which you can confirm using the `ifconfig` command from step 6, above).

Tools

You will want to use various tools to interact with BadStore, to inspect and modify the contents of its pages and communications. We recommend some tools here.

Firefox developer tools

Firefox developer tools give you the ability to inspect and modify the contents of a web page and its communications (from the Developer Tools page, click the `DEBUGGING` menu item to show the tools you should be most interested in). Developer Tools come pre-installed with recent versions of Firefox; just go to the Web Developer menu to see the possible tools. We will list some useful features here, along with links to the relevant documentation.

View Source. This is a normal Firefox feature. Right-click on a page you are viewing and then select "View Source" from the menu that appears. A window pops up that gives a complete, syntax-highlighted view of the page source. This view is useful for doing quick searches. For example, use the view to search for hidden form fields (those fields with the attribute "hidden")

Page Inspector. You can use the page inspector this to examine and modify the structure of a page. Use the source inspector to find pages of interest, and then use the Page inspector to see how the different source elements map to what is displayed, and/or to modify the contents of those pages.

Developer Toolbar. The Developer Toolbar is a console prompt will allow you to inspect and/or set cookies associated with the current page, among other things.

Network traffic inspector. While viewing a page in the page inspector, you can click the *Network* tab to see the network traffic sent or received as a result of interacting with the page. Use this to see cookies sent/received, HTTP headers, request formats, etc.

Other utilities

Here are other utilities you might find useful:

- Use this on-line utility to decode or encode base64 and other formats
- Use this on-line utility to generate cryptographic hashes including MD5, SHA1, and more.

Exploit!

Perform exploits on BadStore to find answers to the following questions; once you have, complete the on-line assessment.

- One of the BadStore pages has a hidden form field that establishes a new user's privilege level. What is the name of this field?
- How many items for purchase are in BadStore's database? Use SQL injection on the quick search form field to find out.
- What operations are suppliers permitted to do once they have logged into the "suppliers only" area? Use SQL injection to bypass authentication, or find a way to create an account as a supplier.
- Log in as `joe@supplier.com` --- this is possible in a variety of ways, including SQL injection. Then look at his previous orders and answer the question: What credit card number did he use to make a purchase of $46.95? Multiple answers are possible, but we will accept all of them.
- Get administrator privileges and then use the `admin` action to look at the user database. There are two users whose emails have the form `XXX@whole.biz`; what is the `XXX` portion of either of the two users? For example, if one of the users is `jackie@whole.biz`, the right answer is `jackie`. (The answer is case-sensitive.)
- BadStore uses cookies to implement a session key, once you've authenticated, and for tracking the contents of the cart, once you've added something to it. You can figure out the cookies in use by BadStore in various ways. One way is to do an XSS attack on the guest book. Get the guest book to run the code `<script>alert(document.cookie)</script>` and it will tell you the current cookies. (Be sure you have popups enabled on your browser or this won't work.) Alternatively, you can examine the cookies directly using Firefox developer tools. Recall that cookies are pairs *key=value*. What is the key of the session cookie?
- What is the key of the cookie used for the cart?
- BadStore's session cookie format is poorly designed because it is uses a predictable structure. In particular, it is an encoded string (with a URL-encoded newline at the end) of the form XXX:YYY:ZZZ:U. What are the XXX, YYY, and ZZZ portions of this string?
- BadStore's cart cookie is also an encoded string with a predictable structure XXX:YYY:... etc., and it probably contains

information it shouldn't. Which field of the decoded string could an attacker change to give himself a discount on an item's price?

Tips and Hints

- The BadStore manual has a bunch of hints and tips about exploiting vulnerabilities.
- Recall that MySQL comments are two dashes *followed by a space* (not just two dashes alone).
- BadStore generates dynamic HTML using CGI. For example, the URL `https://www.badstore.net/cgi-bin/badstore.cgi?action=whatsnew` presents a page of "What's new" at BadStore, while the URL `https://www.badstore.net/cgi-bin/badstore.cgi?action=viewprevious` generates a page showing previous accounts. The only difference between these is what's in the `action` parameter. Try handcrafted parameters to the various CGI URLs, e.g., `?action=test` and `?action=admin`.
- Ordering from the store *should* work by just clicking on "Add to Cart" from the "What's new?" page. But this doesn't work if you reach the page via `https` rather than `http`; it seems that Firefox blocks the javascript that updates the cart. When you go to the "Supplier Login" area, it will switch you to `https` and then it will stay that way. You can flip back to `http` by just changing the URL manually.
- Some of the questions require that you get administrator privileges. You can get admin privileges in several ways, including SQL injection (if you can guess the administrator's user ID), spoofing the cookie (per the structure that you glean), or creating a user with administrative rights (using the page with the hidden form field). While normal users have role `U` administrators have role `A`.
- Visit `http://www.badstore.net/cgi-bin/initdbs.cgi` to reset the directories and databases. This is easier than rebooting BadStore, if you want a fresh start. It does not reset your cookies, though.

Created Tue 21 Oct 2014 4:58 PM PDT

Last Modified Mon 3 Nov 2014 1:22 PM PST