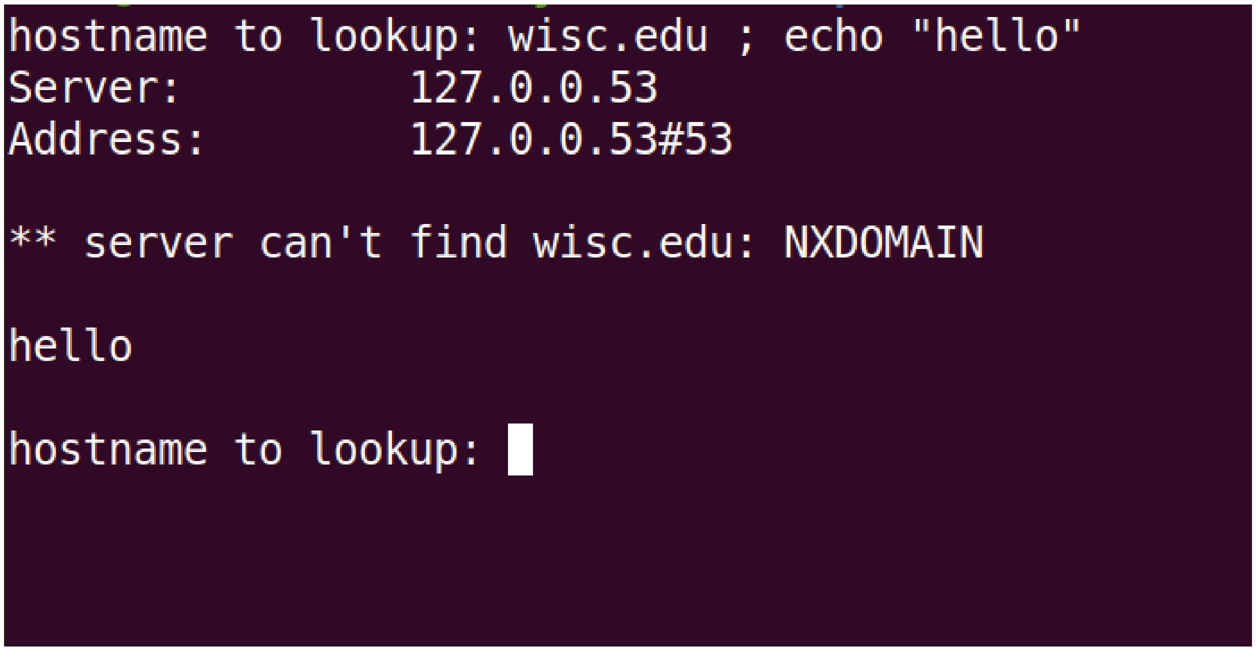
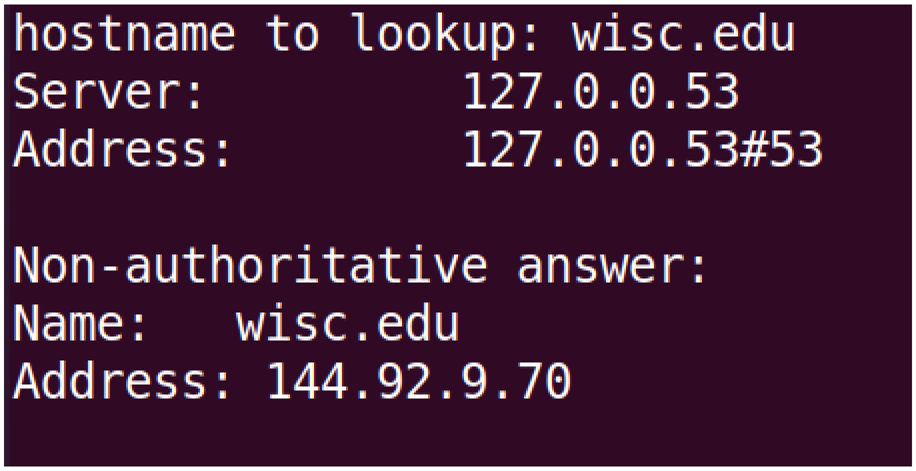


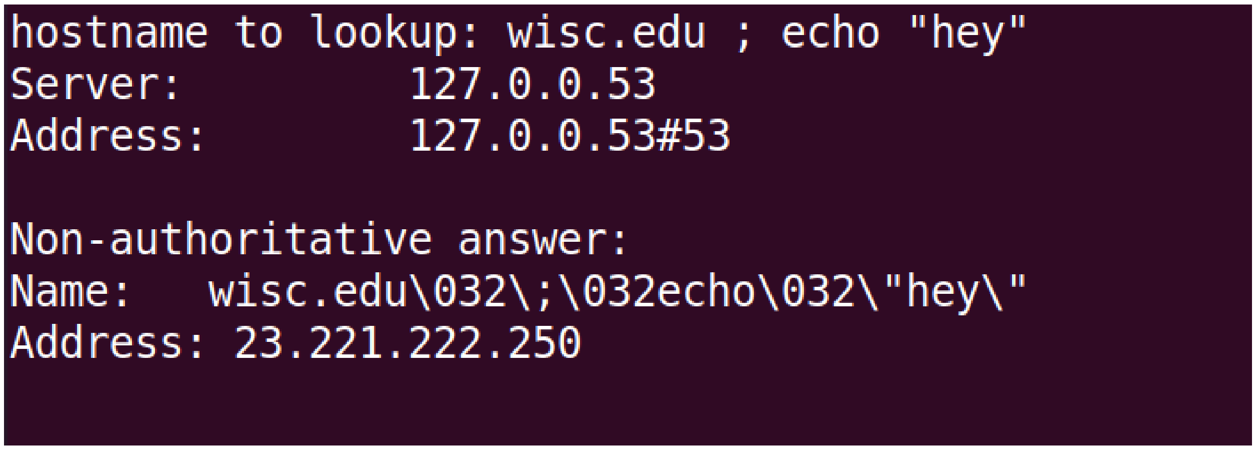
```
hostname to lookup: wisc.edu ; echo "hello"
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find wisc.edu: NXDOMAIN

hello

hostname to lookup: 
```

```
import java.io.BufferedReader;
import java.io.Console;
import java.io.IOException;
import java.io.InputStreamReader;
import java.net.InetAddress;

/**
 * Main execution class for cmd_injection exercise. Prompts user for input to
 * the nslookup command and prints the output.
 *
 * @author Joseph Eichenhofer
 *
 */
public class Main {

	/**
	 * Prompts user for hostname to lookup. Performs DNS resolution and prints
	 * address/info for the given hostname.
	 *
	 * @param args
	 *            n/a
	 */
	public static void main(String[] args) {
		Console terminal = System.console();

		if (terminal == null) {
```

```
                System.out.println("Error fetching console. Are you running from an IDE?");
        private static String rDomainName2(String hostname) throws IOException {
            InetAddress IP = null;
            try {
                IP = java.net.InetAddress.getByName(hostname);
            } catch (Exception e) {
                System.out.println(e);
            }
            String name = IP.getHostName();
            String address = IP.getHostAddress();
            return ("name: " + name + "\n" +  "address: " + address);
        }
    }


                System.exit(-1);
            }

            while (true) {
                String hostname = terminal.readLine("hostname to lookup: ");

                if (hostname.toLowerCase().equals("exit"))
                    break;

                try {
                    System.out.println(rDomainName2(hostname));
                } catch (IOException e) {
                    System.out.println("error executing nslookup");
                }
            }
        }

        /**
         * Lookup given hostname using nslookup command. Return the output/error of the
         * nslookup command as string.
         *
         * @param hostname
         *          hostname/domain to lookup
         * @return string output of nslookup command
         * @throws IOException
         *          if unable to execute the command or read its output
         */
        private static String rDomainName(String hostname) throws IOException {
            // execute the nslookup command
            Process proc2 = Runtime.getRuntime().exec(new String[]{"nslookup", hostname});
            // capture output from command
            BufferedReader stdOut = new BufferedReader(new
InputStreamReader(proc2.getInputStream()));
            BufferedReader stdErr = new BufferedReader(new
InputStreamReader(proc2.getErrorStream()));

            StringBuilder output = new StringBuilder();
            String currLine = null;
            while ((currLine = stdOut.readLine()) != null) {
                  output.append(currLine + "\n");
            }
            while ((currLine = stdErr.readLine()) != null) {
                  output.append(currLine + "\n");
            }

            // return the result
            return output.toString();
      }


      private static String rDomainName2(String hostname) throws IOException {
            InetAddress IP = null;
            String name = null;
            String address = null;
            try {
                  IP = java.net.InetAddress.getByName(hostname);
                  name = IP.getHostName();
                  address = IP.getHostAddress();


            try {
                  IP = java.net.InetAddress.getByName(hostname);
            } catch (Exception e) {
                  System.out.println(e);
            }
            String name = IP.getHostName();
            String address = IP.getHostAddress();
            return ("name: " + name + "\n" +  "address: " + address);
      }
}
```

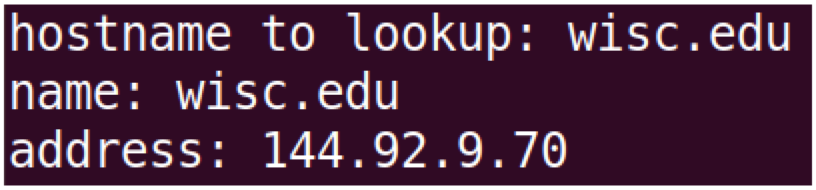


```
hostname to lookup: wisc.edu
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   wisc.edu
Address: 144.92.9.70
```

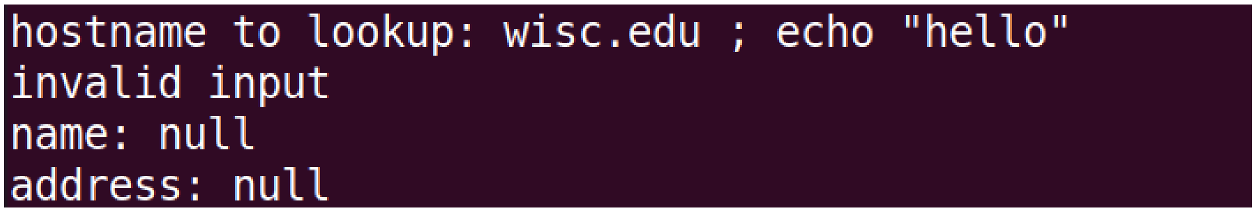


```
hostname to lookup: wisc.edu ; echo "hey"
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   wisc.edu\032\;\032echo\032\"hey\"
Address: 23.221.222.250
```

Result of first mitigation: forcing nslookup to be its own command rather than a shell command



```
hostname to lookup: wisc.edu
name: wisc.edu
address: 144.92.9.70
```



```
hostname to lookup: wisc.edu ; echo "hello"
invalid input
name: null
address: null
```

Result of second mitigation: not using a runtime.exec() command at all, rather used java.net.InetAddress commands

The first mitigation refuses to allow command injection by not reading the user input as a shell command but rather it executes it as its own program. This disallows more than one command to be executed at once

The second mitigation removes the runtime.exec() function in the first place by using an Internal API service, which takes only real domain hostnames as a parameter and thus doesn’t have a place for command injections to be functional