# Objective 4 Slot Machine Investigation

Now that we’ve opened the doors to Frost Tower, we can go inside and play the slot machines. Since this is a hacking challenge, our job is to hack the slot machines to make them give away money instead of taking it. But before starting the objective head to the far-left side of the North Pole, at the left side of the entrance to Santa’s castle, to help Noel Boetie with his terminal.

A screenshot of a computer

Description automatically generated with medium confidence A picture containing text

Description automatically generated

## Terminal: Logic Munchers

You need to play Noel Boetie’s Logic Muncher game to gain hints to use to break the slot machine.

|  |  |
| --- | --- |
| Graphical user interface  Description automatically generated | Graphical user interface, text  Description automatically generated  A green screen with white text  Description automatically generated with medium confidence |
| Text  Description automatically generated with medium confidence  Boolean link: <http://notes.imt-decal.org/sets/cheat-sheet.html>  AND, OR, NOT, XOR link: <http://www.natna.info/English/Teaching/CSI30-materials/Chapter1-cheat-sheet.pdf> |

### Assignment

This terminal is a basic test of your knowledge of binary AND, OR, XOR, and other computations. You will probably learn the most if you actually play the game. You need to win a stage starting at Stage 3 in Potpourri mode to get credit for the achievement and get the hints.

I was able to do much of the binary math in my head but had to use a calculator set to programmer mode when it started giving hex problems. If you want to hack a little, look carefully at what shows up in the console tab of the webdev of your browser. It will be a great help. If you use either a calculator or the console of your browser, it may be easier to do this with two people at the higher levels.

### Step 1 question

Play the game and win stage 3 or above in potpourri mode.

### Step 1 answer

There’s not an easy way to tell you how to play the game, but this may be helpful if you want to give yourself extra help by hacking.

Graphical user interface

Description automatically generated

## Hints from the Logic Muncher Terminal

Noel give us two good hints.

|  |  |
| --- | --- |
| A green screen with white text  Description automatically generated with medium confidence | A picture containing text  Description automatically generated |
| <https://owasp.org/www-community/attacks/Web_Parameter_Tampering> | <https://portswigger.net/burp/communitydownload>  <https://itectec.com/superuser/how-to-edit-parameters-sent-through-a-form-on-the-firebug-console/> |

## Objective 4 Slot Machine Investigation

As Noel says, this site is susceptible to parameter tampering. In this case, when the slot machine app tells the server how much you bet and what size coin you used, you can change what it sends to whatever you want. If you can input the correct weird value, maybe you can make the machine do weird things. In the early days of the web, the sites foolishly made price a parameter that the browser sent back to the server. Imagine tampering with the price and buying a computer for $1.00!

## Assignment

In this objective you will learn about the Network tab in the Firefox webdev tools and use the Edit/Resend feature to tamper with the parameters your browser sends to the server.

Read Noel’s link on parameter tampering. Then read his link about Edit and Resend with Firefox. Burp Suite is a fancier way to tamper with parameters, but the Edit and Resend feature of Firefox is much easier and works well for this challenge.

### Step 1 question: Where is the Network tab?

Open Kringlecon.com in Firefox. Enter the Lobby of Frost Tower and click on one of the slot machines and click Play Game in the frame that opens. Then open the webdev tools and click spin on the slot machine gui. Can you find network traffic in the tool that is caused by your clicking?

### Step 1 answer

Whenever you click spin in the gui, the application reports that to the server. You should be able to see it here.

Graphical user interface, text, application, email

Description automatically generated

If you click on the POST message, you see the contents. The headers and cookies are interesting, but we are interested in something else. You found the networking data though—good job!  
Graphical user interface, text, application, email

Description automatically generated

### Step 2 question: Where is the data?

Dig into the data in the POST request and see if you can find the three values that were sent to the server. Also look for the data the server back after the POST request.

### Step 2 answer

The data we send to the server is in the request tab, and the response from the server is in the response tab.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

### Step 3 question: I want to win!

Now comes the hard part, and the hacking. You need to find a value for one of the three parameters, betamount, numline, and cpl, that the browser sends to the server so that you can get your credit over 1000. You need to make it so that your credit goes up instead of down when you lose.

The Edit/Resend selection is available when the Headers tab is selected. Important note: when you use the Resend feature you are bypassing the code that drives the GUI, and it will not show the results of your spin. Instead, look at the Response tab.Graphical user interface, text, application, email

Description automatically generated

If you receive error codes (400 or 500) ignore them and move on to another parameter or direction. In other investigations a 500 server error indicates you’ve done something worth pursuing. In this challenge, a successful change will not generate an error.

There should be some interesting messages at the bottom of the Response tab if you cheat successfully. The message you get when your credit goes above 1000 is the one you need to enter into the objective on your badge.

### Step 3 answer

The only parameter that gives a desirable result is the cpl parameter when you change it to a negative number. I believe cpl is the size of coin you are using in the slot machine. The developer did not do proper range checking on the parameter value, so you can sneak in a negative number. This causes the server to give you credit instead of taking it away when you lose.

Graphical user interface, text, application, email

Description automatically generated

Change cpl to a negative number and send the packet.

Graphical user interface, text, application, email

Description automatically generated

Check the response. Your credit has gone up.

Graphical user interface, text, application, email

Description automatically generated

Keep sending until your credit is over 1000 and your answer is at the bottom of the Response tab.

Graphical user interface, application

Description automatically generated  
<snip>  
Graphical user interface, text, application

Description automatically generated