Calculat3 M3

Calculat3 M3

Here!
http://web.ctflearn.com/web7/

I forget how we were doing those calculations, but something tells me it was pretty insecure.

Flag: CTFlearn{watch_0ut_f0r_th3_m0ng00s3}

Writeup:

captured request with Burp, and found 3 functions, with 1 passing values to the vulnerable eval function.
using 'HTTP Request Maker' toolbar I added the expression function and gave it a value 0f 1=1 (encoded as 1%2B1) and server replied with '2'

using same tool I gave the expression function a value of ;ls, and was given flag as returned data:
calc.jsctf{watch_0ut_f0r_th3_m0ng00s3}index.phpmain.cssmain.css

calc.js

```
function c(val)
{
document.getElementById("d").value=val;
}
function v(val)
{
document.getElementById("d").value+=val;
}
function e()
{
try
{
  c(eval(document.getElementById("d").value))
}
catch(e)
{
 c('Error')
}
}
```

web7.html

```
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=windows-1252">
  <link rel="stylesheet" href="web7_files/main.css">
    <script type="text/javascript" src="web7_files/calc.js">
    </script>
    </head>
    <body>
<div class="box">
<div class="display">
    <form action="." method="post">
    <input type="text" name="expression" readonly="readonly" size="18" id="d">
    </form>
    </div>
<div class="keys">
    <p>
    <input type="button" class="button gray" value="mrc" onclick='c("Created....................")'>

    <input type="button" class="button gray" value="m-" onclick='c("...............by............")'>

    <input type="button" class="button gray" value="m+" onclick='c(".....................Anoop")'>

    <input type="button" class="button pink" value="/ " onclick='v("/ ")'>
    </p>
    <p>
    <input type="button" class="button black" value="7 " onclick='v("7 ")'>
    <input type="button" class="button black" value="8" onclick='v("8 ")'>

    <input type="button" class="button black" value="9 " onclick='v("9 ")'>
    <input type="button" class="button pink" value="* " onclick='v("* ")'>
    </p>
    <p>
    <input type="button" class="button black" value="4" onclick='v("4 ")'>
    <input type="button" class="button black" value="5 " onclick='v("5 ")'>

    <input type="button" class="button black" value="6 " onclick='v("6 ")'>
    <input type="button" class="button pink" value="- " onclick='v("- ")'>
    </p>
    <p>
    <input type="button" class="button black" value="1 " onclick='v("1 ")'>
    <input type="button" class="button black" value=" 2" onclick='v("2 ")'>

    <input type="button" class="button black" value=" 3" onclick='v("3 ")'>
    <input type="button" class="button pink" value=" +" onclick='v("+ ")'>
    </p>
    <p>
    <input type="button" class="button black" value=" 0" onclick='v("0 ")'>
    <input type="button" class="button black" value="." onclick='v(".")'>

    <input type="button" class="button black" value="C" onclick='c("")'>
    <input type="submit" class="button orange" value="=">
    </p>
</div>
</div>




</body>
</html>
```