Calculat3 M3 CTF Writeup

This document is a walkthrough on one way to solve the **Calculat3 M3 CTF** on **CTFLearn**. The objective is to explain how I was able to solve this CTF to my future self.

General Information

- *Difficulty:* Easy
- *Category:* Web
- *Link:* Calculat3 M3 - CTFLearn

Solution

Calculat3 M3 **80** points Hard

Here! http://web.ctflearn.com/web7/ I forget how we were doing those calculations, but something tells me it was pretty insecure.

We're given a website, with just a calculator which can do basic operations.

Now, looking at the javascript and HTML source code, we can guess how it works:

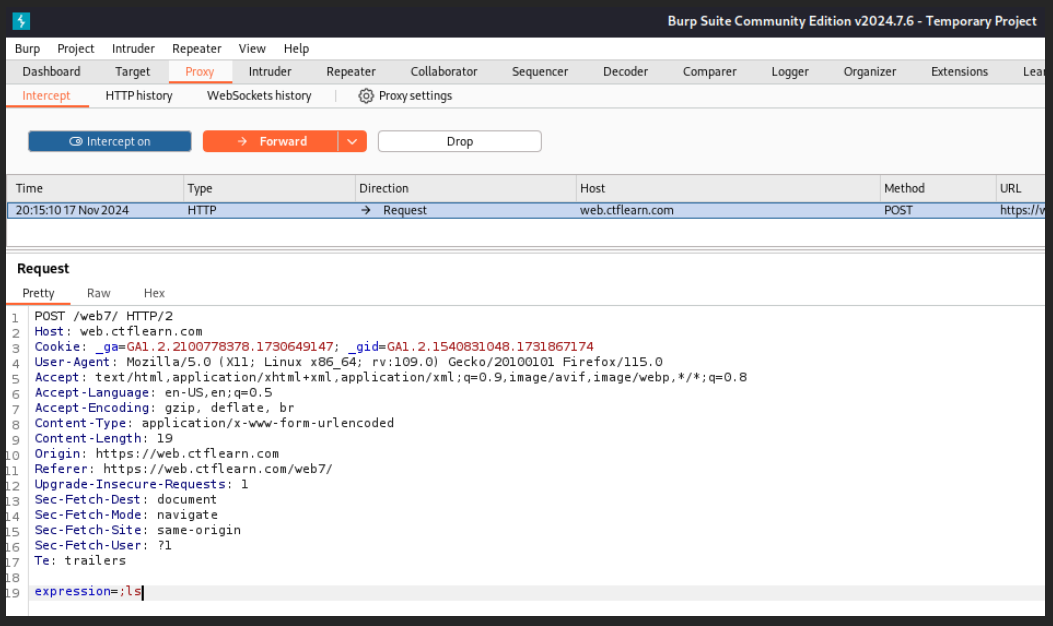
```
<html>
<head>
  <link rel="stylesheet" href="main.css">
    <script type="text/javascript" src="calc.js"></script>

    </head>
    </body>
<div class="box">
<div class="display">
    <form action='.' method="post">
    <input type="text" name="expression" readonly size="18" id="d"></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>
```

```
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')
}
}
```

– The calculator takes input from the user, appends it to a variable called **“expression”**
– Upon submit, it sends the **“expression”** variable to the server, which executes the e() function, which will evaluate the **expression,** using the eval function. For example, expression = “3 + 3”.

But what if were able to modify the value of expression, and **injected some code** into it, since it’s sent to the server via **POST** method, so the client has full control over it.

Using Burp Suite, we’ve intercepted the POST request, and modified the expression value to **“;ls”**. Now, the eval function which interprets the string as code, and executes it. In this case the “ls” command lists all directories in a UNIX-like system, and javascript can execute it here.



And there we have it, it seems like one of the directories’ name is literally the flag

```
calc.js ctf{watch_0ut_f0r_th3_m0ng00s3} index.php main.css main.css
```

ctf{watch_0ut_f0r_th3_m0ng00s3}