An Analysis of Capture the Flag Exercises for Ethical Hacking and Defense Proficiency

Donovan Roberts

St. Mary’s University of Minnesota

An Analysis of Capture the Flag Exercises for Ethical Hacking and Defense Proficiency

Abstract

To check one's proficiency in ethical hacking and defense, one should use capture the flag excersises to assess their abilities and to improve one's ethical hacking and defense skills. The methodology used in this lab to find vulnerabilities within the capture the flag excersises was a check and guess method and a combination of internet resources(articles/videos) and collaboration with peers. The check and guess method, which is the reverse of guess and check method commonly used in mathematics, is where the problem was attempted to be solved without knowing for certain that the problem was even a problem and then one guesses to see if what was discovered equates to a problem/vulnerability. The capture the flag(CTF) exercise resulted in a multitude of vulnerabilities being found and allotted an opportunity to access and improve upon one's proficiency in Ethical Hacking and Defense.

An Analysis of Capture the Flag Exercises for Ethical Hacking and Defense Proficiency

Cybersecurity is an ever-evolving industry with a multitude of threats that are evolving daily. As an aspiring cybersecurity professional, it is critical that at a minimum there is a fundamental knowledge on how vulnerabilities work, how they can be identified, and lastly how they can be defended. This lab focuses on the completion of two capture the flag (CTF's) exercises as a capstone project after taking an 8-week course, Ethical Hacking and Defense, provided in the Master of Science in Cybersecurity, to utilize skills and knowledge obtained over the course and to expand on our ever expanding knowledge base. Capture the Flag excersises can be used to access skills and increase proficiency in ethical hacking and defense. Capture the flag excersises are simulations that represent the user with environments that have vulnerabilities embedded within them that can be capitalized on. These vulnerabilities can be capitalized through utilizing ethical hacking skills and in turn can provide the user with insights on how to defend these vulnerabilities as well.

The methodology utilized for this lab was a check and guess method and a combination of internet resources such as articles and videos. The check and guess method, which is the reverse of guess and check method commonly used in mathematics, is where the problem was attempted to be solved without knowing for certain that the problem was even a problem and then one guesses to see if what was discovered equates to a problem/vulnerability. The resources that were utilized were a combination of articles and videos that focused directly on the capture the flag exercises that I was executing as well as skills that were utilized within the excersises that were needed to discover the vulnerabilities. Throughout the lab the check and guess method was used initially up until there was a series of guesses that yielded no vulnerabilities. Consequently, resources were used once the check and guess method yielded no vulnerabilities. The first resources used were pertaining to skills that could be utilized within the exercise and then secondly, resources that were directly about the capture the flag excersises were used.

The results exposed a slew of vulnerabilities that resulted in all five flags being captured between the two capture the flag excersises. Furthermore, this lab allotted an environment to practice ethical hacking skills such as XXS (Cross-site Scripting), SQL Injections, Unauthorized Access through URL manipulation, and source code exploration. This lab utilized skills learned during the course such as SQL injections that we did during our week 4 BWAAP SQL injection and expanded our knowledge base through utilizing skills such as XXS and source code exploration inadvertently providing opportunities to reflect on defensive maneuvers to those skills as well. Lastly, this lab created an environment filled with a plethora of unknowns which coincidently will be how future courses will be and ultimately how one's journey will be breaking into the cybersecurity industry upon acquiring a Master of Science in Cybersecurity. This is critical because it resulted in the fundamental building blocks to the mindset and actions one will need to have when the circumstances are unknown. This lab forced one to be patient, positive, resilient, and to lean on one's resources whether that was videos/articles or collaborating with peers which are all characteristics and actions that can fortify one's foundation as they transition from student to professional.

An Analysis of Capture the Flag Exercises for Ethical Hacking and Defense Proficiency

Literature Review

Capture the flag excersises is a great way for one to access and increase one's ethical hacking and defensive proficiency not only from the direct technical challenge of the exercise but also the methodology and mindset it takes to do them. Ethical hacking creates an environment to build on one’s skills and knowledge base but also creates and environment reminiscent to the real world of cybersecurity where one must utilize being patient, positive, resilient, and to lean on one's resources whether that be videos/articles or collaborating with peers which are all characteristics and actions that can fortify one's foundation as they transition from student to professional. In the following sections I will discuss how capture the flag excersises are a great way for one to access and increase their ethical hacking and defensive skills as well as the methodology utilized during these excersises that can prepare students for the real world of cybersecurity.

Capture the flag excersises take an alternative path to your traditional linear instruction and progression format of education by providing an "underspecified solution path and a tangible token of success." (Cole, 2022). For Capture the flag exercises, rather than give you a step-by-step direction, capture the flag excersises forces one to discover those steps to be able to find the flag. The flag itself is a very distinct thing so there is no confusion once it is found such as:

Flag0=^FLAG^3cb66b8e91f11b493d7e348399cab5b7fbf96e13abbf2b760d5b298480c9e8c4$FLAG$, which was an actual flag found in the capture the flag excersises that this lab report is about.

To further validate the use of capture the flag excersises, capture the flag excersises "have been held as online or in-person events independent of formal security education since at least 1996 [6, 34], and have grown in popularity to the point that publicly-advertised CTFs are now held at a rate of several per week"(Cole, 2022) The efficiency and validity of CTF's have been around for at least 26 years and are growing more and more into popularity into traditional educational course material. As one prepares to go from student to professional in cybersecurity CTF'S "underspecification requires players to exhibit initiative and self-direction to successfully solve them, which prepares students for real-world security scenarios involving novel and evolving threats. Pedagogically, underspecification requires independent learning by students to successfully solve challenges.”. (Cole, 2022). CTF's provide an ample number of skills and opportunities to access one's abilities through a multitude of processes such as…"

○ Cyber threat modeling

○ Threat hunting

○ Risk analysis

○ Incident response

○ Data collection

○ Detection effectiveness

○ Forensic evidence gathering

○ Critical infrastructure protection "

(Rochford, n.d.)

Capture the flag excersises can provide ample amount of opportunity for students to hone their ethical hacking and defense skills.

On the other hand, capture the flag can build students' mindset and set them up to face the challenges of the real world. The capture the flag excersises that were done during this lab forced one to be patient, positive, resilient, and to lean on one's resources whether that was videos/articles or collaborating with peers which are all things that students will need to be well equipped with going into the professional world. Some of these characteristics are connected, for instance resilience and leaning on/utilizing resources whether that's articles/videos or people in your network. Resilience can be defined as a "personal qualities that enable an individual to thrive in the face of adversity."(Windle, 2011) where adversity is simply stated as difficulties. Capture the Flag excersises are the peer essence of difficulties given they're against the grain style of educating by leaving all things underspecified creating a great environment to build's one resiliency. This also causes one to lean on their resources/networks when you force one to be in difficult situations with limited knowledge. As mentioned in "The Secret to Building Resilience" resilience "is not purely an individual characteristic but is also heavily enabled by strong relationships and networks." The beautiful thing about Capture the flag excersises is that they double dip when it comes to building resilience, not just from the challenges presented by the excersises themselves but also the environment which forces students to get out of their comfort zone and lean on resources, peers, mentors, etc. Resiliency is not something inherent to an individual but something that can be built and molded which capture the flag excersises embody.

Methodology

The methodology utilized for this lab was a check and guess method and a combination of internet resources such as articles and videos. The check and guess method, which is the reverse of guess and check method commonly used in mathematics, is where the problem was attempted to be solved without knowing for certain that the problem was even a problem and then one guesses to see if what was discovered equates to a problem/vulnerability. The resources that were utilized were a combination of articles and videos that focused directly on the capture the flag exercises as well as resources focused on the skills that were utilized within the excersises that were needed to discover the vulnerabilities. Throughout the lab the check and guess method was used initially up until there was a series of guesses that yielded no vulnerabilities. Consequently, resources were used once the check and guess method yielded no vulnerabilities where resources pertaining to skills that could be utilized within the exercise where used first and then resources that were directly about the capture the flag excersises were used last.

For the initial check and guess method used, I really relied on everything in memory from this class, my python coding course, and everything that I have dabbled in concerning cybersecurity. When I first started the Capture the Flag excersises I was shocked at how barren the webpages were that were given to us. I had created a scrapy tutorial from my python coding course that relied on getting certain tags from the source code of a website to be able to crawl the website and take inventory of certain items on the website. With that experience, one of my first things I checked was inspecting the website which coincidently enabled me to find the first flag. From inspecting the site, my next step was interacting with clickable/editable links within the website.

Once, all of the check and guessing ran its course, I started to utilize clues and resources that may have been hinted at in the clues such as markdown resources/guides for example. Once I exhausted those resources, I went to using resources directly related to Micro-CMS v1 such as articles and guided videos. It was a tricky balance when utilizing resources that related directly to Micro-CMS v1 because I didn't want to just automatically get the answers in hopes of staying in the fight but on the flip side ethical hackers in the profession stand on the shoulders of their forefathers who came before them so why limit myself in that regard.

Results

In this document are all the steps taken in two capture the flag (ctf) exercises on hackerone.com. The first exercise will be for the "Trivial" exercise which contains one flag and the second exercise will be the "Easy" exercise which contains 4 flags.

How To Play

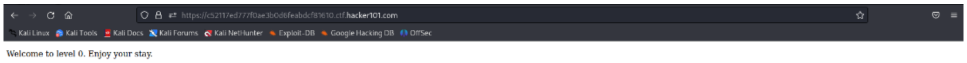
The Hacker101 CTF is split into separate levels, each of which containing some number of flags. You can play through the levels in any order you want; more than anything else, the goal is to learn and have fun doing it.

Once you enter a level, you're going to be searching for the flags, using every skill and tool in your arsenal. Flags are placed in various locations -- they might be in a file, in the database, stuck into source code, or otherwise -- and your goal is to hunt them all down. Each flag looks something like ^FLAG^37ae568362f974017fa575f08cd215044cd6bb395c3f5e5e293ee5324ba6769c$FLAG$, so you'll know the instant you see one.
Stuck?

If you get stuck, try going through a level from scratch and see if you missed something along the way. Did you inspect every page thoroughly? Press every button? Manipulate every input? Try not to overthink it too much; the flags are usually more obvious than you might think.

If you think you've looked over everything, check out the hints for the level. Click the "Hints" link next to the "Go" button that launches an instance and you'll get a helping hand.

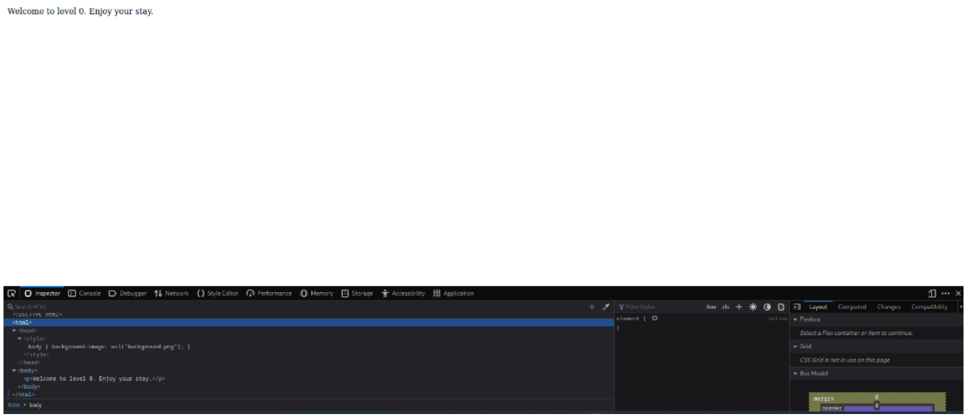
Trivial: A little something to get you started



Welcome to level 0. Enjoy your stay.

An Analysis of Capture the Flag Exercises for Ethical Hacking and Defense Proficiency

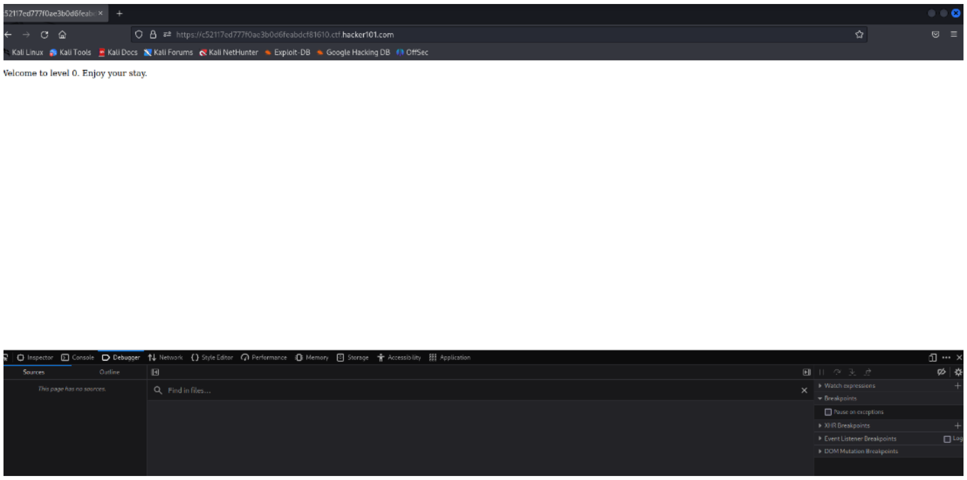
This is the opening page for Trivia CTF. I noticed that we are in a https site so I know it's secure. My first thought is to inspect the webpage by right clicking the page.



Welcome to level 0. Enjoy your stay.

```
<html>
  <head>
    <style>
      body { background-image: url("background.png"); }
    </style>
  </head>
  <body>
    <p>Welcome to level 0. Enjoy your stay.</p>
  </body>
</html>
```

After viewing the inspector, I'm not seeing much

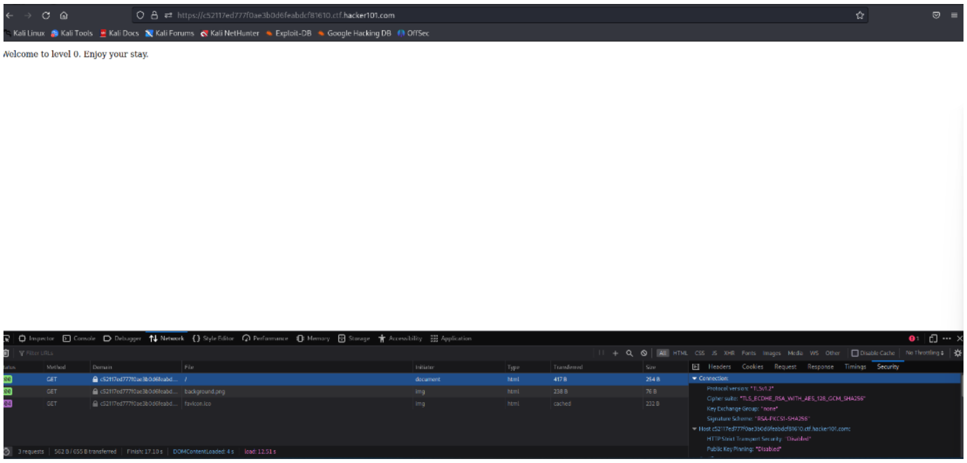


https://c52117ed777f0ae3b0d6feabdcf81610.ctf.hacker101.com

Welcome to level 0. Enjoy your stay.

This page has no sources.

I went to the debugger to see if I could I see any files and saw nothing



https://c52117ed777f0ae3b0d6feabdcf81610.ctf.hacker101.com

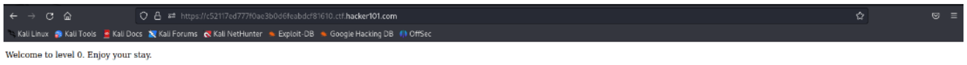
Welcome to level 0. Enjoy your stay.

atus	Method	Domain	File	Initiator	Type	Transferred	Size
00	GET	c52117ed777f0ae3b0d6feabd...	/	document	html	417 B	254 B
00	GET	c52117ed777f0ae3b0d6feabd...	background.png	img	html	238 B	76 B
04	GET	c52117ed777f0ae3b0d6feabd...	favicon.ico	img	html	cached	232 B

3 requests | 562 B / 655 B transferred | Finish: 17.10 s | DOMContentLoaded: 4 s | load: 12.51 s

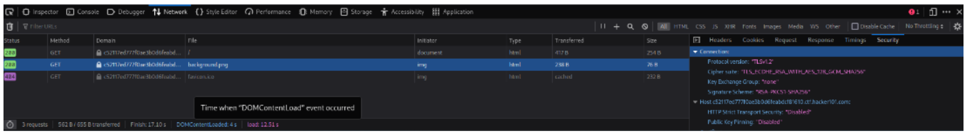
```
Connection:
  Protocol version: "TLSv1.2"
  Cipher suite: "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"
  Key Exchange Group: "none"
  Signature Scheme: "RSA-PKCS1-SHA256"
Host c52117ed777f0ae3b0d6feabdcf81610.ctf.hacker101.com:
  HTTP Strict Transport Security: "Disabled"
  Public Key Pinning: "Disabled"
```

I decided to inspect the network security of the page to see if I saw anything but nothing yet



https://c52117ed777f0ae3b0d6feabdcf81610.ctf.hacker101.com

Welcome to level 0. Enjoy your stay.



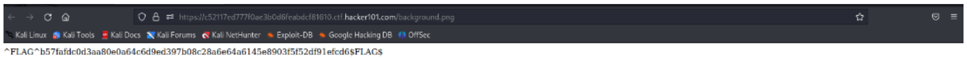
Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	c52117ed777f0ae3b0d6feabd...	/	document	html	417 B	254 B
200	GET	c52117ed777f0ae3b0d6feabd...	background.png	img	html	238 B	76 B
404	GET	c52117ed777f0ae3b0d6feabd...	favicon.ico	img	html	cached	232 B

```
Connection:
  Protocol version: "TLSv1.2"
  Cipher suite: "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"
  Key Exchange Group: "none"
  Signature Scheme: "RSA-PKCS1-SHA256"
Host c52117ed777f0ae3b0d6feabdcf81610.ctf.hacker101.com:
  HTTP Strict Transport Security: "Disabled"
  Public Key Pinning: "Disabled"
```

Time when "DOMContentLoad" event occurred

3 requests | 562 B / 655 B transferred | Finish: 17.10 s | DOMContentLoaded: 4 s | load: 12.51 s

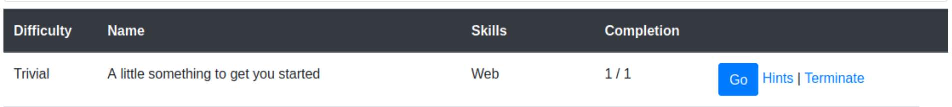
I went to explore the background.png file and bingo I found the flag!



https://c52117ed777f0ae3b0d6feabdcf81610.ctf.hacker101.com/background.png

^FLAG^b57fafdc0d3aa80e0a64c6d9ed397b08c28a6e64a6145e8903f5f52df91efcd6$FLAG$

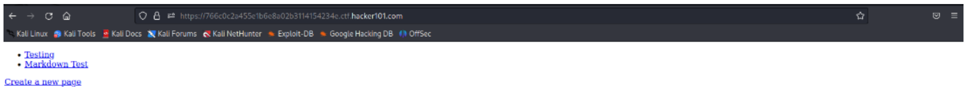
Flag noted above



Difficulty	Name	Skills	Completion	
Trivial	A little something to get you started	Web	1 / 1	Go Hints | Terminate

Evidence of Completion

Easy: Micro-CMS v1

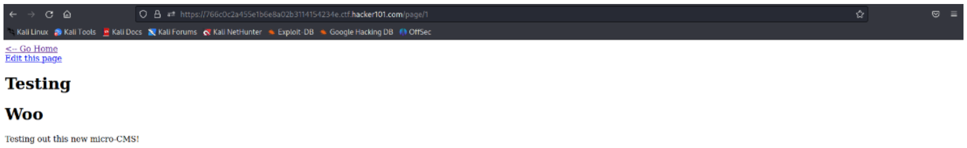


https://766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com

- Testing
- Markdown Test

Create a new page

Here is the opening page. My first thought is to explore all three links



https://766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com/page/1

<-- Go Home
Edit this page

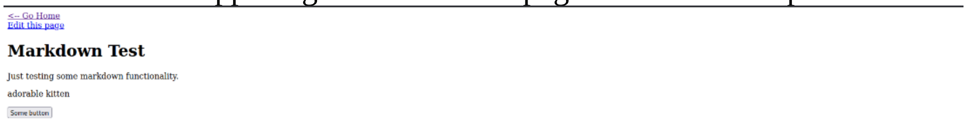
Testing

Woo

Testing out this new micro-CMS!

This is what the first link opens up to .

I went back to the home page and pressed on the Markdown Test link and it opened up to the page below and of course I pressed the "Some button" which appeared to do nothing. I'm curious to see what is happening underneath the page so I went to inspect it.



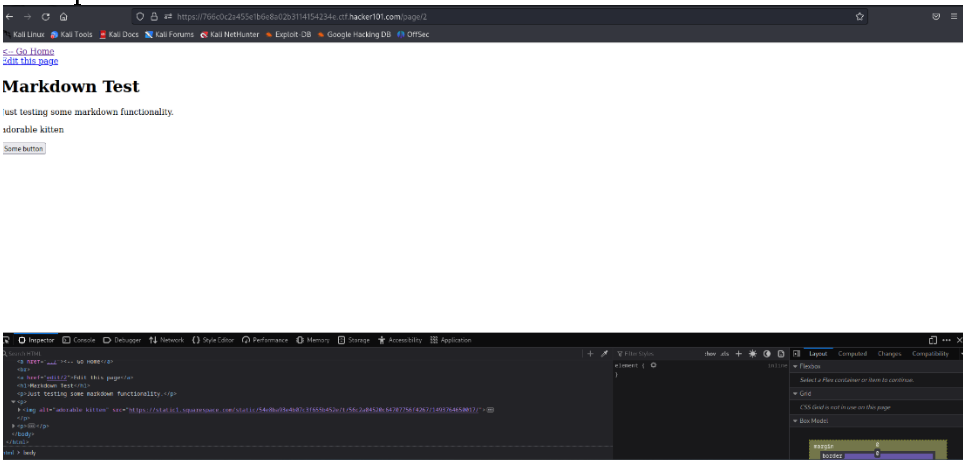
<-- Go Home
Edit this page

Markdown Test

Just testing some markdown functionality.

adorable kitten

Upon inspecting the Markdown Test Page, I noticed that "adorable kitten" has link attached to it in inspector.



https://766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com/page/2

<-- Go Home
Edit this page

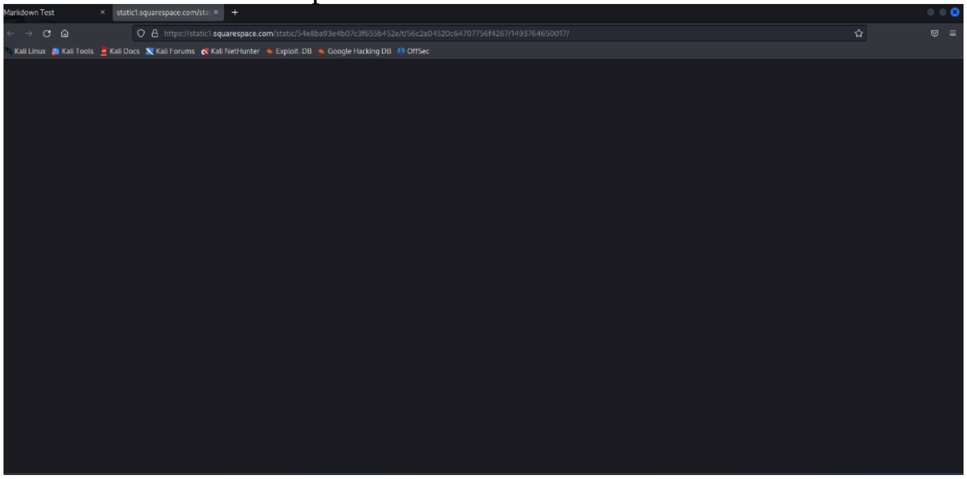
Markdown Test

Just testing some markdown functionality.

adorable kitten

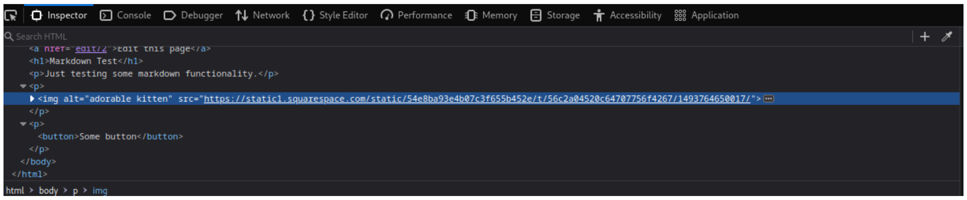
```
<a href="../"><-- Go Home</a>
<br>
<a href="edit/2">Edit this page</a>
<h1>Markdown Test</h1>
<p>Just testing some markdown functionality.</p>
<p>
  <img alt="adorable kitten" src="https://static1.squarespace.com/static/54e8ba93e4b07c3f655b452e/t/56c2a04520c64707756f4267/1493764650017/">
</p>
<p>…</p>
</body>
</html>
```

Of course I decided to open link in another tab but it lead to no results as of yet.



https://static1.squarespace.com/static/54e8ba93e4b07c3f655b452e/t/56c2a04520c64707756f4267/1493764650017/

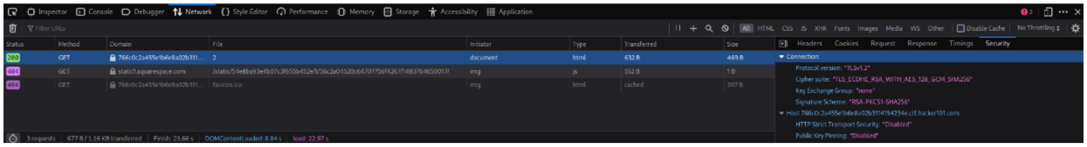
I also noted that the "Some button" indeed went to nowhere.



```
    <a href="edit/2">Edit this page</a>
    <h1>Markdown Test</h1>
    <p>Just testing some markdown functionality.</p>
  ▾ <p>
    ▸ <img alt="adorable kitten" src="https://static1.squarespace.com/static/54e8ba93e4b07c3f655b452e/t/56c2a04520c64707756f4267/1493764650017/">
    </p>
  ▾ <p>
      <button>Some button</button>
    </p>
  </body>
</html>
```

html > body > p > img

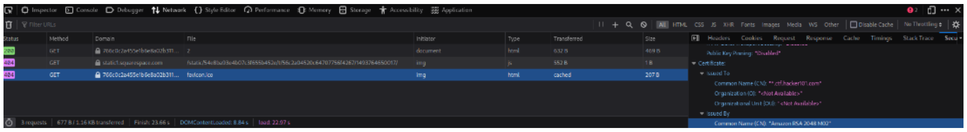
I reloaded the website with "network" opened in inspector and observed the following



```
Status  Method  Domain                           File                                                                          Initiator  Type  Transferred  Size
200     GET     766c0c2a455e1b6e8a02b311...      2                                                                             document   html  632 B        469 B
404     GET     static1.squarespace.com          /static/54e8ba93e4b07c3f655b452e/t/56c2a04520c64707756f4267/1493764650017/    img        js    552 B        1 B
404     GET     766c0c2a455e1b6e8a02b311...      favicon.ico                                                                   img        html  cached       207 B

3 requests | 677 B / 1.16 KB transferred | Finish: 23.66 s | DOMContentLoaded: 8.84 s | load: 22.97 s
```

```
▾ Connection:
    Protocol version: "TLSv1.2"
    Cipher suite: "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"
    Key Exchange Group: "none"
    Signature Scheme: "RSA-PKCS1-SHA256"
▾ Host 766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com:
    HTTP Strict Transport Security: "Disabled"
    Public Key Pinning: "Disabled"
```

I noticed that the domains are locked and I also noticed the third domain says cached..I am going to press the "Disable Cache" button and see if anything changes.

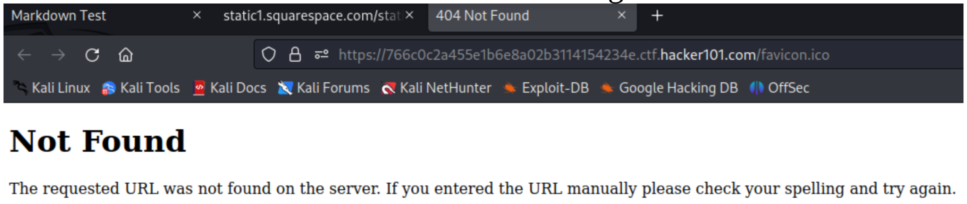


Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	766c0c2a455e1b6e8a02b311...	2	document	html	632 B	469 B
404	GET	static1.squarespace.com	/static/54e8ba03e4b07c3f655b452e/t/56c2a04520c64707756f4267/1493764650017/	img	js	552 B	1 B
404	GET	766c0c2a455e1b6e8a02b311...	favicon.ico	img	html	cached	207 B

```
Public Key Pinning: "Disabled"
▾ Certificate:
  ▾ Issued To
      Common Name (CN): "*.ctf.hacker101.com"
      Organization (O): "<Not Available>"
      Organizational Unit (OU): "<Not Available>"
  ▾ Issued By
      Common Name (CN): "Amazon RSA 2048 M02"
```

3 requests | 677 B / 1.16 KB transferred | Finish: 23.66 s | DOMContentLoaded: 8.84 s | load: 22.97 s

I double clicked on the third domain but nothing was found

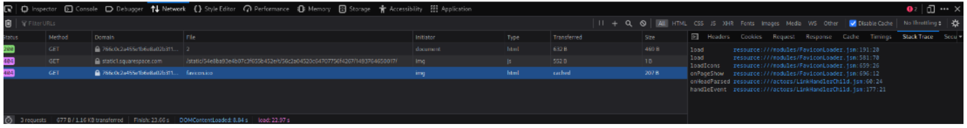


https://766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com/favicon.ico

Not Found

The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

I ended up going into "stack trace" and opening up one of the links.

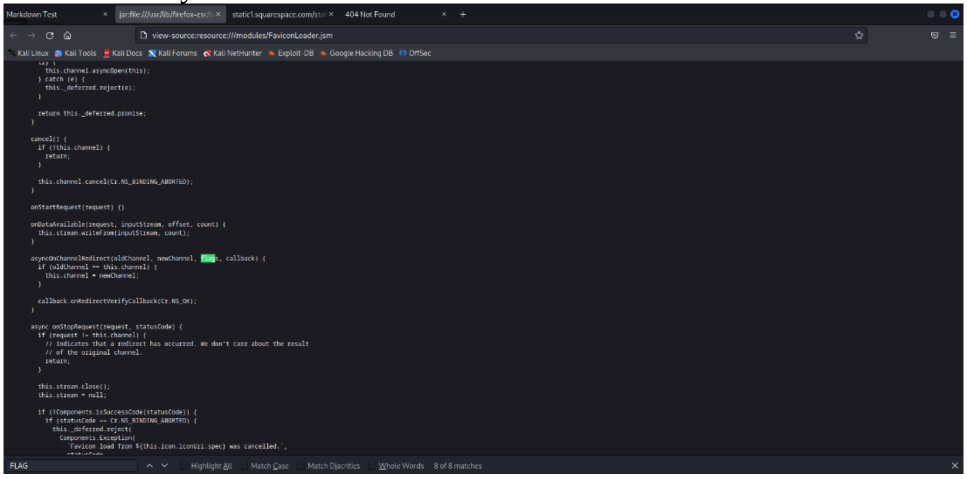


Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	766c0c2a455e1b6e8a02b311...	2	document	html	632 B	469 B
404	GET	static1.squarespace.com	/static/54e8ba03e4b07c3f655b452e/t/56c2a04520c64707756f4267/1493764650017/	img	js	552 B	1 B
404	GET	766c0c2a455e1b6e8a02b311...	favicon.ico	img	html	cached	207 B

```
load          resource:///modules/FaviconLoader.jsm:191:28
load          resource:///modules/FaviconLoader.jsm:581:78
loadIcons     resource:///modules/FaviconLoader.jsm:659:26
onPageShow    resource:///modules/FaviconLoader.jsm:696:12
onHeadParsed  resource:///actors/LinkHandlerChild.jsm:60:24
handleEvent   resource:///actors/LinkHandlerChild.jsm:177:21
```

3 requests | 677 B / 1.16 KB transferred | Finish: 23.66 s | DOMContentLoaded: 8.84 s | load: 22.97 s

From there it opened this page where I proceeded to control F and type "FLAG" and didn’t find much at least yet.

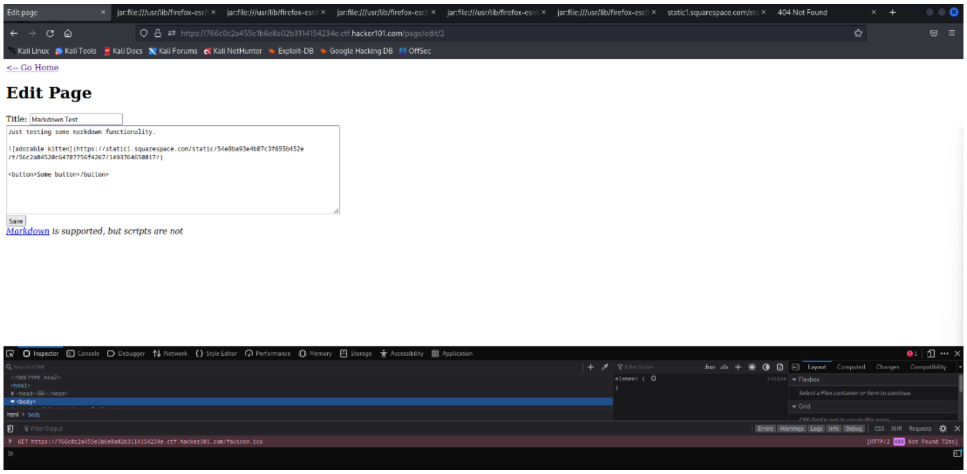


view-source:resource:///modules/FaviconLoader.jsm

```
      this.channel.asyncOpen(this);
    } catch (e) {
      this._deferred.reject(e);
    }

    return this._deferred.promise;
  }

  cancel() {
    if (!this.channel) {
      return;
    }

    this.channel.cancel(Cr.NS_BINDING_ABORTED);
  }

  onStartRequest(request) {}

  onDataAvailable(request, inputStream, offset, count) {
    this.stream.writeFrom(inputStream, count);
  }

  asyncOnChannelRedirect(oldChannel, newChannel, flags, callback) {
    if (oldChannel == this.channel) {
      this.channel = newChannel;
    }

    callback.onRedirectVerifyCallback(Cr.NS_OK);
  }

  async onStopRequest(request, statusCode) {
    if (request != this.channel) {
      // Indicates that a redirect has occurred. We don't care about the result
      // of the original channel.
      return;
    }

    this.stream.close();
    this.stream = null;

    if (!Components.isSuccessCode(statusCode)) {
      if (statusCode == Cr.NS_BINDING_ABORTED) {
        this._deferred.reject(
          Components.Exception(
            `Favicon load from ${this.icon.iconUri.spec} was cancelled.`,
```

FLAG — 8 of 8 matches

From there I messed around with more of the inspection tools and didn't find much so I decided to press the edit page button and this is what appeared.



https://766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com/page/edit/2

<-- Go Home

Edit Page

Title: Markdown Test

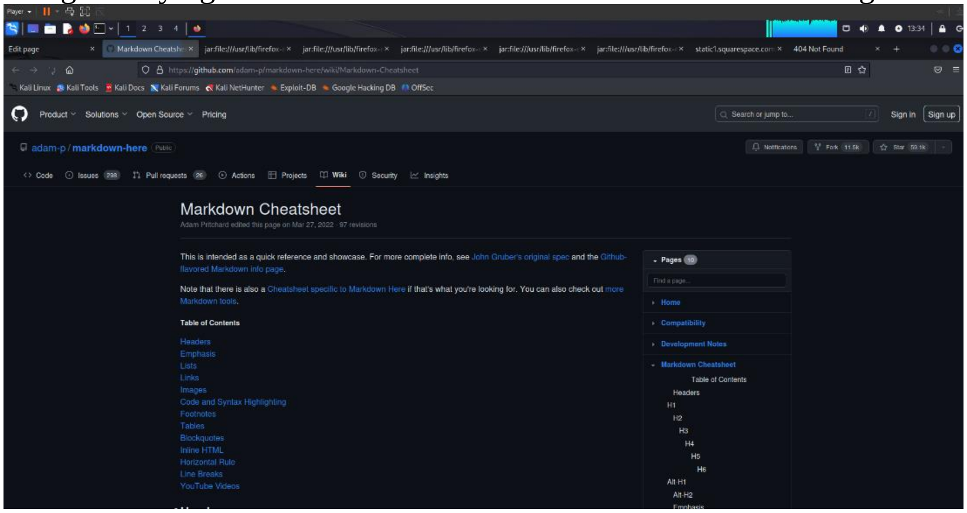
```
Just testing some markdown functionality.

![adorable kitten](https://static1.squarespace.com/static/54e8ba93e4b07c3f655b452e
/t/56c2a04520c64707756f4267/1493764650017/)

<button>Some button</button>
```

Save

Markdown is supported, but scripts are not

```
GET https://766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com/favicon.ico    [HTTP/2 404 Not Found 72ms]
```

I pressed the hyperlinked "Markdown" and it brought me to the markdown cheat sheet. My first thought is trying to reformat the website we encountered earlier to get it to hopefully work



https://github.com/adam-p/markdown-here/wiki/Markdown-Cheatsheet

adam-p / markdown-here

Markdown Cheatsheet

Adam Pritchard edited this page on Mar 27, 2022 · 97 revisions

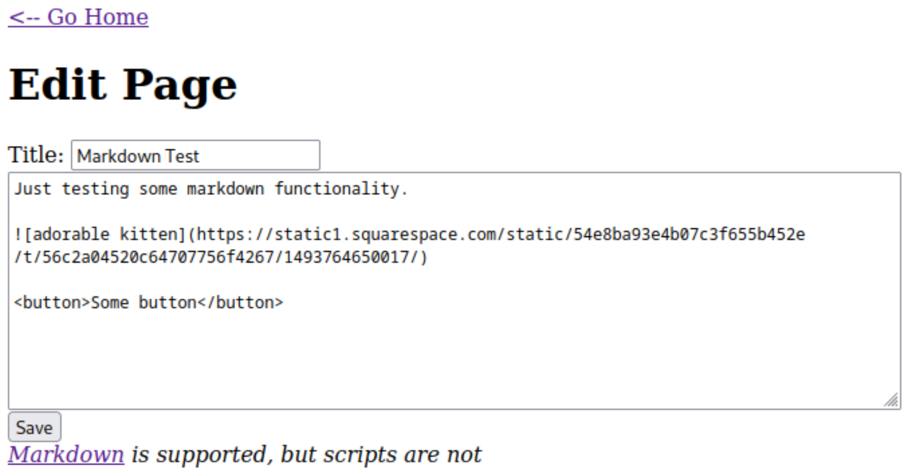
This is intended as a quick reference and showcase. For more complete info, see John Gruber's original spec and the Github-flavored Markdown info page.

Note that there is also a Cheatsheet specific to Markdown Here if that's what you're looking for. You can also check out more Markdown tools.

Table of Contents

Headers
Emphasis
Lists
Links
Images
Code and Syntax Highlighting
Footnotes
Tables
Blockquotes
Inline HTML
Horizontal Rule
Line Breaks
YouTube Videos

On the markdown cheatsheet I noticed that png links all ended in .png and I noticed that the link for what I believe is supposed to be an image doesn't have .png listed anywhere. I'll try to add it and see what happens



<-- Go Home

Edit Page

Title: Markdown Test

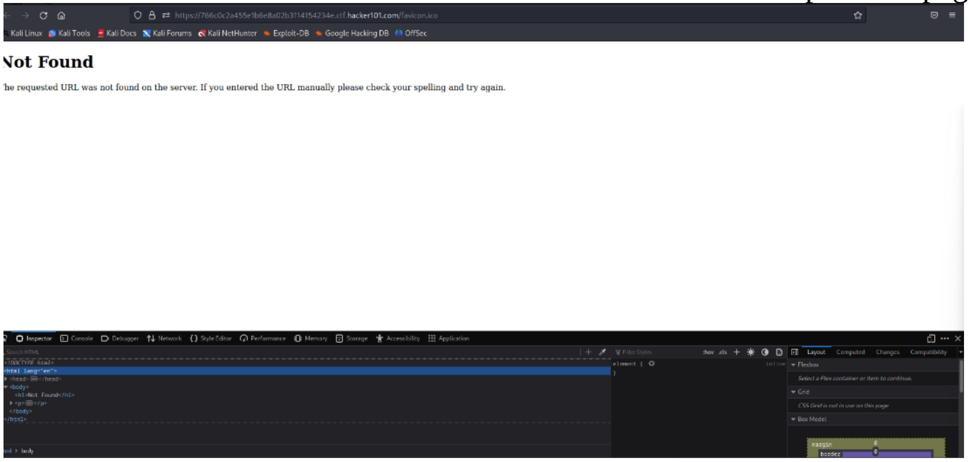
```
Just testing some markdown functionality.

![adorable kitten](https://static1.squarespace.com/static/54e8ba93e4b07c3f655b452e
/t/56c2a04520c64707756f4267/1493764650017/)

<button>Some button</button>
```

Markdown is supported, but scripts are not

I changed the link to ![adorable kitten](https://static1.squarespace.com/static/54e8ba93e4b07c3f655b452e/t/56c2a04520c64707756f4267/1493764650017/icon48.png) and saved and now we shall see what happens.

Still resulted in no result

I went back to the third domain from earlier and decided to inspect that page as well



https://766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com/favicon.ico

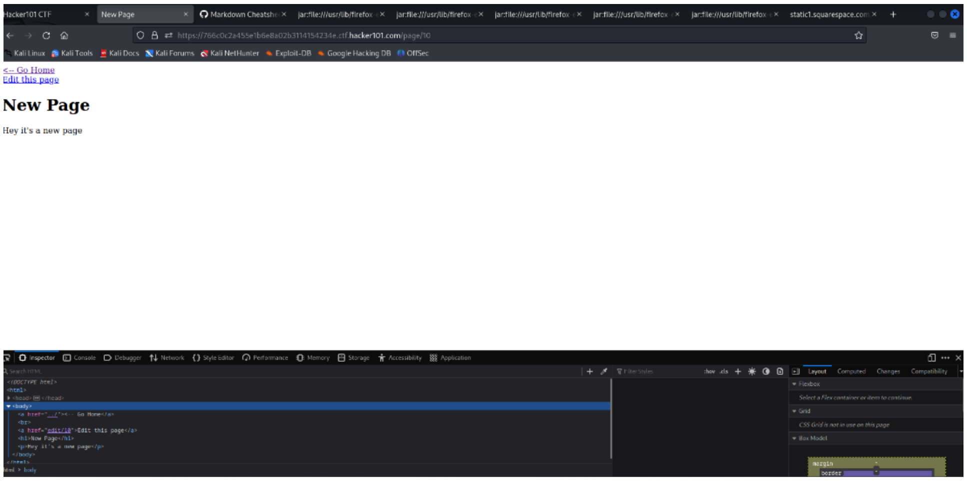
Not Found

he requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

```
<!DOCTYPE html>
<html lang="en">
 <head> ··· </head>
 <body>
   <h1>Not Found</h1>
  <p> ··· </p>
 </body>
</html>
```

```
element {
}
```

I had to get a hint so the first hint was try to create a new page
So I proceeded to do that and named it new page. Let's inspect this page now



https://766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com/page/10

<-- Go Home
Edit this page

New Page

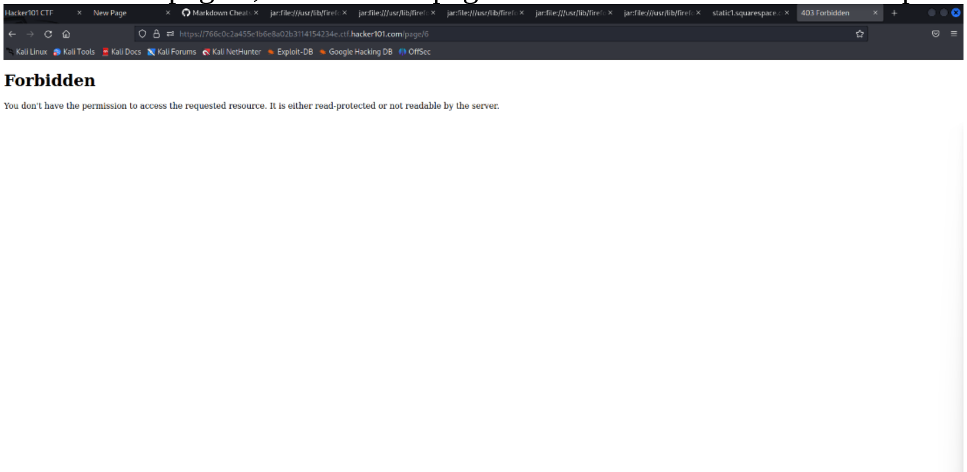
Hey it's a new page

```
<!DOCTYPE html>
<html>
<head>…</head>
<body>
  <a href="../"><-- Go Home</a>
  <br>
  <a href="edit/10">Edit this page</a>
  <h1>New Page</h1>
  <p>Hey it's a new page</p>
</body>
</html>
```

I noticed that my new page I created url was https://766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com/page/10

Which was strange because I didn't feel like the website had a total of 10 pages so I started to edit the url starting from 1 to see what pages would come up that I didn't disccover

I discovered page 6, A forbidden page I didn't have access to..let's inspect it

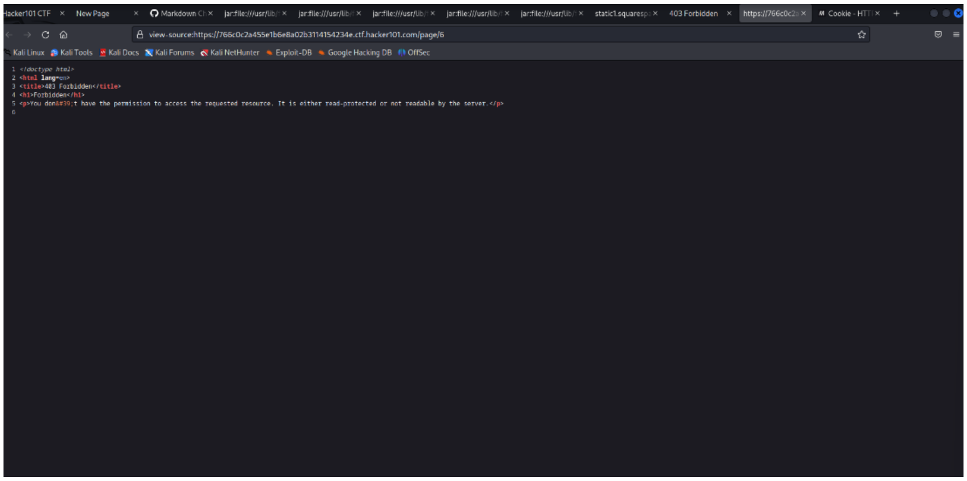


https://766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com/page/6

Forbidden

You don't have the permission to access the requested resource. It is either read-protected or not readable by the server.

After doing some inspecting I still didn't find much but I did see it's source code. I will keep look into different pages (7-9) and see if I get anywhere. (Source Code below)



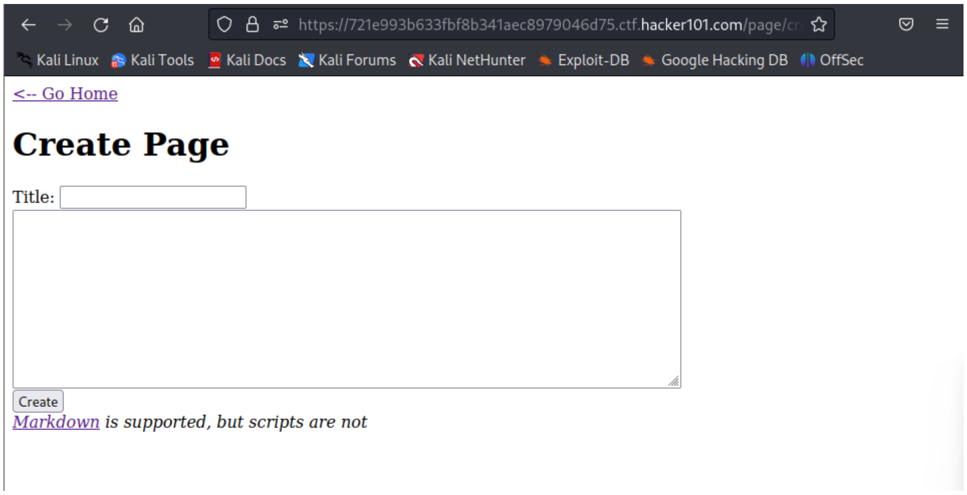
view-source:https://766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com/page/6

```
<!doctype html>
<html lang=en>
<title>403 Forbidden</title>
<h1>Forbidden</h1>
<p>You don&#39;t have the permission to access the requested resource. It is either read-protected or not readable by the server.</p>
```

I went to pages 7-9 and even 11-12 and nothing was found. So I went back to my New Page I created to analyze it's source to see if there was anything that stood out that I could edit the forbidden access page with but nothing so far.

Day 2

Unfortunately, the test didn't keep all pages open from the previous day but that's okay. I know from hint one that I need to create a page. (my "new page" that I created was deleted so I will create a new one). The only interactive aspect of creating a page is the "Markdown" page that is hyperlinked to everything Markdown via a github page. My thoughts are is that I need to exploit this website by using markdown somehow.



https://721e993b633fbf8b341aec8979046d75.ctf.hacker101.com/page/cr

<-- Go Home

Create Page

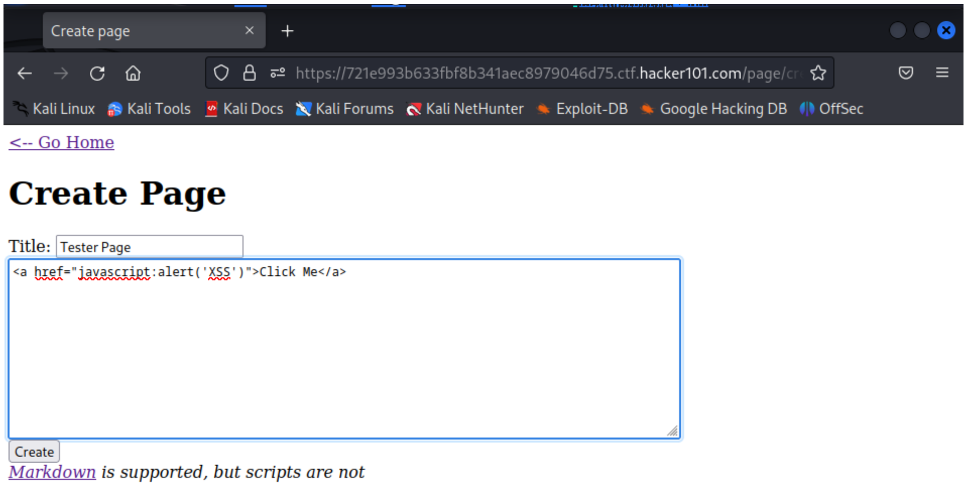
Title:

Markdown is supported, but scripts are not

Upon googling how to exploit using Markdown the first results brought me to an article refferiung to Cross Site Scripting using (XSS). Let's see what I can find from the medium article that generated during my search. https://medium.com/taptuit/exploiting-xss-via-markdown-72a61e774bf8

They dropped an exploit code in the article so I'll copy and paste it to see if anything fun happens. Here is the code:

<a href="javascript:alert('XSS')">Click Me</a>



<-- Go Home

Create Page

Title: Tester Page

```
<a href="javascript:alert('XSS')">Click Me</a>
```

Create

Markdown is supported, but scripts are not

They also mentioned this code here: [Click Me](javascript:alert('Uh oh...'))
That I pasted in but it just created clickable "click me" links that didn't go to anything

Day 3

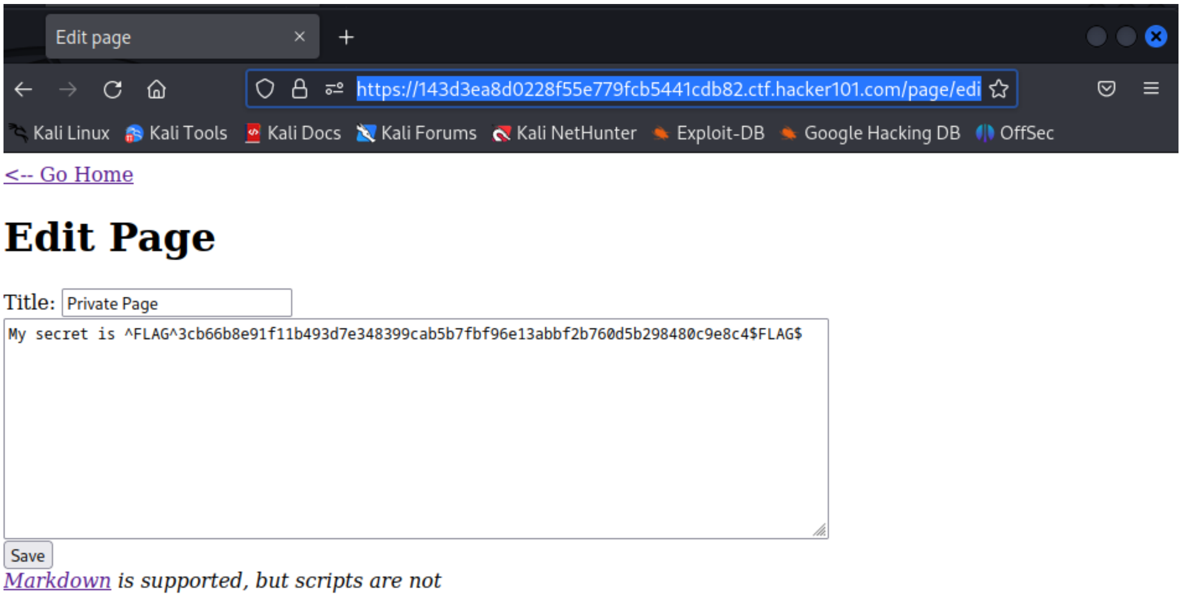
I know there is a forbidden page, page 6 so I'll attempt to access it through understanding page 10

Here is page 6
https://766c0c2a455e1b6e8a02b3114154234e.ctf.hacker101.com/page/6

Here is page 10
https://143d3ea8d0228f55e779fcb5441cdb82.ctf.hacker101.com/page/edit/10

I noticed on my created page, page 10 it has edit/10 so I will attempt to access page 6 by changing the 10 to a 6
https://143d3ea8d0228f55e779fcb5441cdb82.ctf.hacker101.com/page/edit/6

IT WORKED!



Edit Page

Title: Private Page

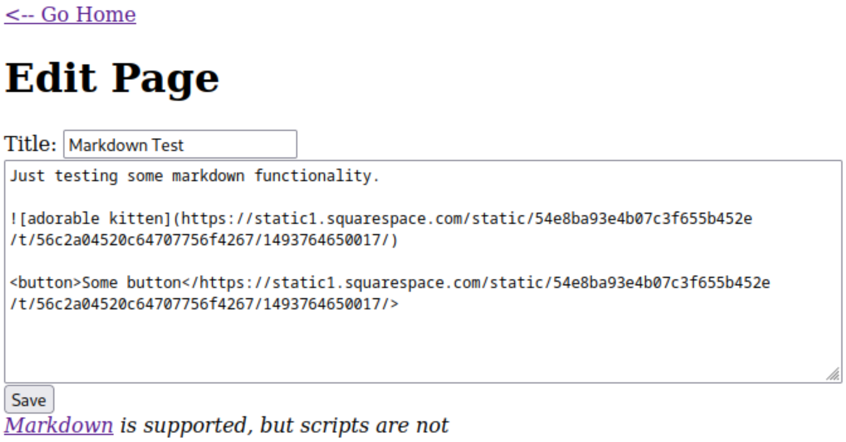
```
My secret is ^FLAG^3cb66b8e91f11b493d7e348399cab5b7fbf96e13abbf2b760d5b298480c9e8c4$FLAG$
```

Markdown is supported, but scripts are not

Flag 0=^FLAG^3cb66b8e91f11b493d7e348399cab5b7fbf96e13abbf2b760d5b298480c9e8c4$FLAG$

Now on to Flag 2. I feel like it may have to do with the adorable kitten link that is on the Markdown Test page.

After inspecting the site I didn't get anything so I attempted to attach it to the some button and still nothing came of it.



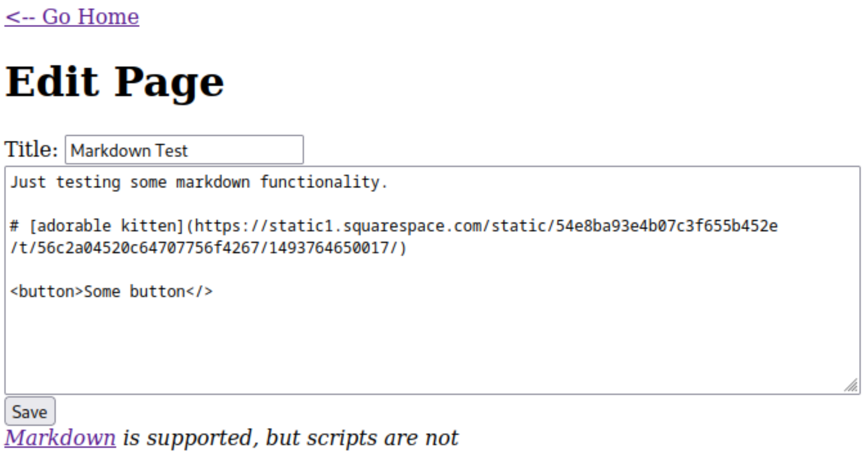
Edit Page

Title: Markdown Test

```
Just testing some markdown functionality.

![adorable kitten](https://static1.squarespace.com/static/54e8ba93e4b07c3f655b452e
/t/56c2a04520c64707756f4267/1493764650017/)

<button>Some button</https://static1.squarespace.com/static/54e8ba93e4b07c3f655b452e
/t/56c2a04520c64707756f4267/1493764650017/>
```

Markdown is supported, but scripts are not

I decided to put a # infront of the adorable kittens since I noticed a # on the other edited page and it just increased the font size



<-- Go Home

Edit Page

Title: Markdown Test

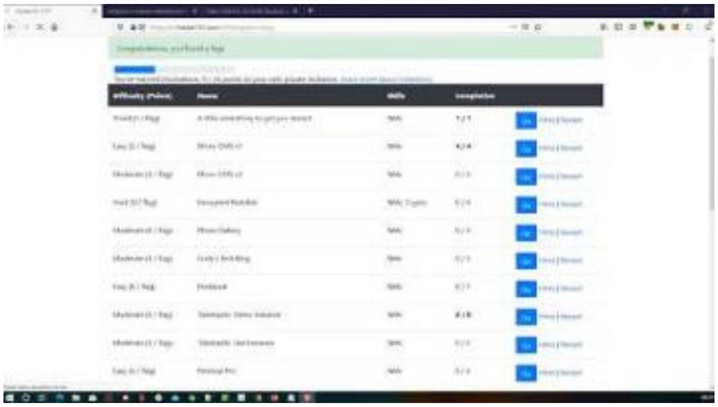
```
Just testing some markdown functionality.

# [adorable kitten](https://static1.squarespace.com/static/54e8ba93e4b07c3f655b452e
/t/56c2a04520c64707756f4267/1493764650017/)

<button>Some button</>
```

Markdown is supported, but scripts are not

Day 4

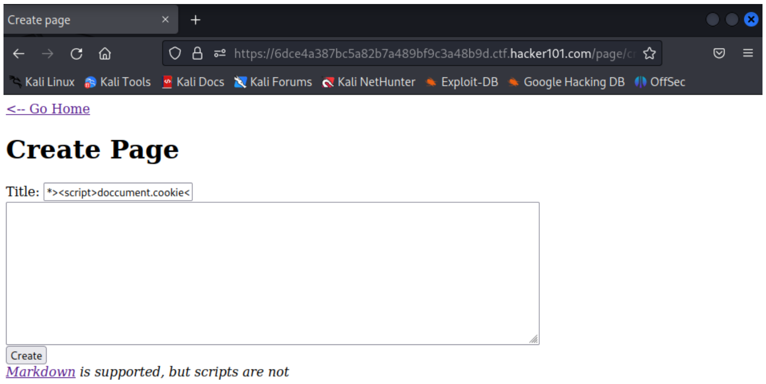
I had a peer reach out from this course, Bari, who provided this reference video for this CTF activity. I didn't have any clues for Flag 1 so I figured I would watch it and see what can happen. Here is the link:

What is CTF - Capture The Flag? Hacker101 - Trivial CTF, Micro-CMS v1 All 4/4 + 1/1 flags



I'll create a another new page based on the resource above. One of the hints for Flag 1 is "Have you tested for the usual culprits? XSS, SQL injection, and path injection. "

From the new created page I input the script *><script>doccument.cookie</script> into the title



<-- Go Home

Create Page

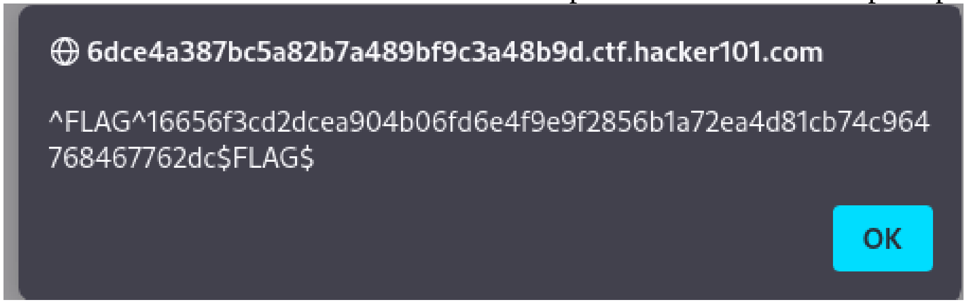
Title: *><script>doccument.cookie<

Create

Markdown is supported, but scripts are not

I also pasted that script into the contact box as well and created the page.
I realized I had a double c and also an * instead of a " so the new script for the page is
"><script>document.cookie</script>

From there I went back to home and the script was executed which prompted Flag 1 to appear

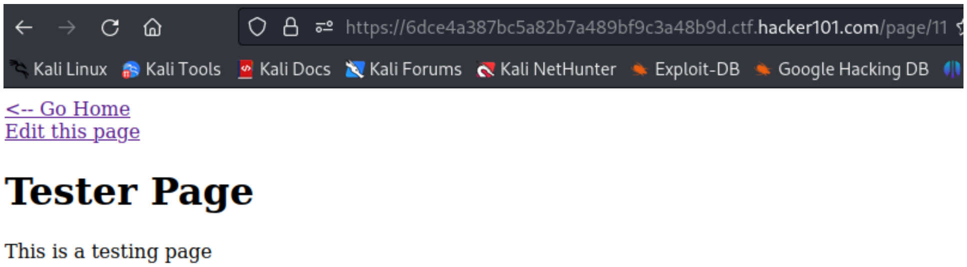


6dce4a387bc5a82b7a489bf9c3a48b9d.ctf.hacker101.com

^FLAG^16656f3cd2dcea904b06fd6e4f9e9f2856b1a72ea4d81cb74c964768467762dc$FLAG$

Now to Flag 2 the hints provided were "Sometimes a given input will affect more than one page" and "The bug you are looking for doesn't exist in the most obvious place this input is shown." I'm guess we will have to edit something in the inspection page and possible something to do with the link attached to adorable kittens but we will see.

The first attempt will be editing the url to see if we can find the flag that way. My previous pages from previous days were deleted unfortunately so I created another "Testing Page" which is now page 11 which is interesting because my old Testing page was page 10 so maybe it is being stored somewhere and I just can't see it on the home page.



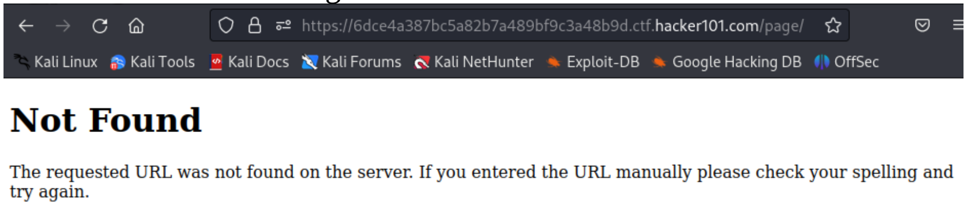
<-- Go Home
Edit this page

Tester Page

This is a testing page

Just out of curiosity, I edited the url and changed the 11 to 10 to see if my old page was stored somehow in the background. My page 10 is now the "><script>document.cookie</script> page that I created.

I'll attempt to delete all of the numbers and just have page to see if that does anything. The results are below. Nothing.



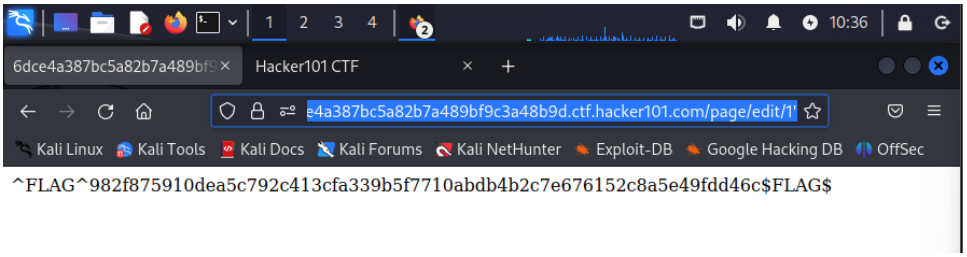
Not Found

The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.

Okay, I'll go back to my tester page and edit that and attempt to take away any numbers to see if that gets us anywhere https://6dce4a387bc5a82b7a489bf9c3a48b9d.ctf.hacker101.com/page/edit and this link resulted in "Not Found"

I went and edited pg. 1's URL like this by adding a single quote to the end https://6dce4a387bc5a82b7a489bf9c3a48b9d.ctf.hacker101.com/page/edit/1'

And the third flag was found! I did this based on this source here: https://www.bing.com/videos/search?q=cms+v1+ctf&view=detail&mid=40995FE14436986C792E40995FE14436986C792E&FORM=VIRE



^FLAG^982f875910dea5c792c413cfa339b5f7710abdb4b2c7e676152c8a5e49fdd46c$FLAG$

This makes sense since the hint noted "The bug you are looking for doesn't exist in the most obvious place this input is shown" so I figured it would have to be either in the URL or "inspection"

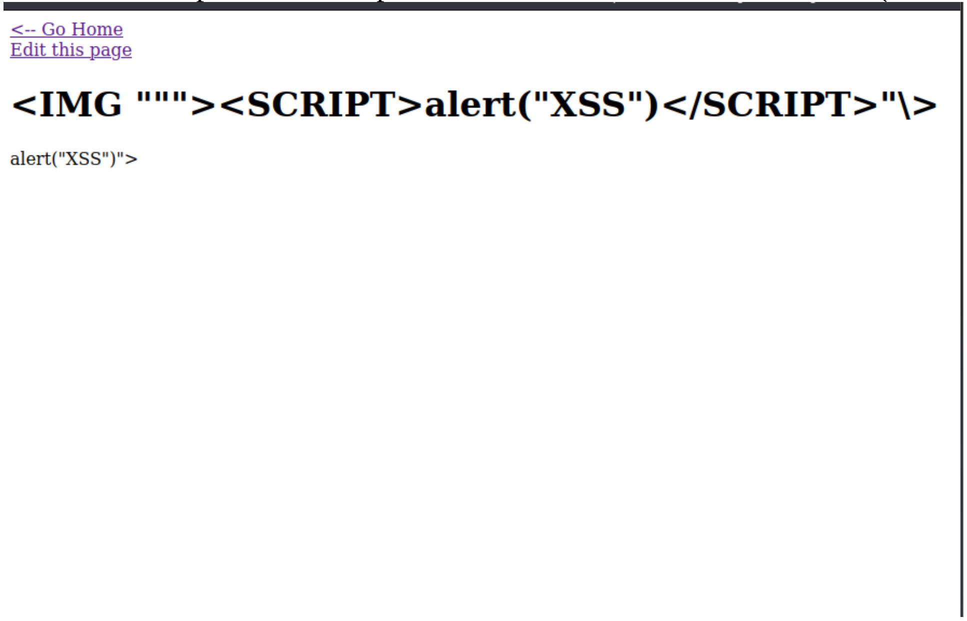
The Last flag, the last hint is "Script Tags are great, but what other options do you have?"

From the source he mentioned XSS Filter Evasion so I went to this site https://cheatsheetseries.owasp.org/cheatsheets/XSS_Filter_Evasion_Cheat_Sheet.html

I didn't know what script tagging was but from the brief google search it looked like anything with the beginnings as such <script>. Given that, I'll look for other types of code on the above mentioned link.

I still feel like the adorable cat img link has something to do with a flag so I will attempt to use a Malformed IMG Tag to see if I can access that photo link once and for all

Here is the script I will attempt to utilize <IMG """><SCRIPT>alert("XSS")</SCRIPT>"\>

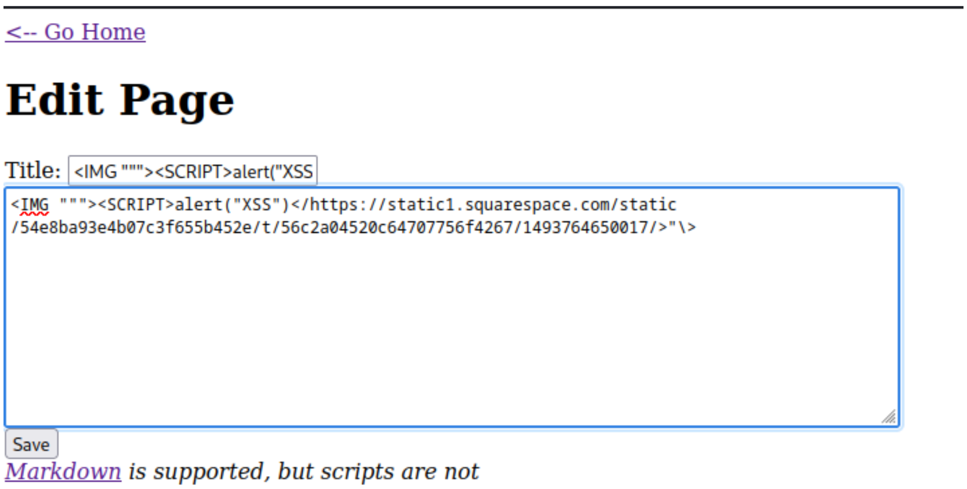


<-- Go Home
Edit this page

<IMG """><SCRIPT>alert("XSS")</SCRIPT>"\>

alert("XSS")">

From here I went to the home page and a pop up appeared, I will now attempt to put the cat image link in this script to see what happens. Here is the img link: https://static1.squarespace.com/static/54e8ba93e4b07c3f655b452e/t/56c2a04520c64707756f4267/1493764650017/



<-- Go Home

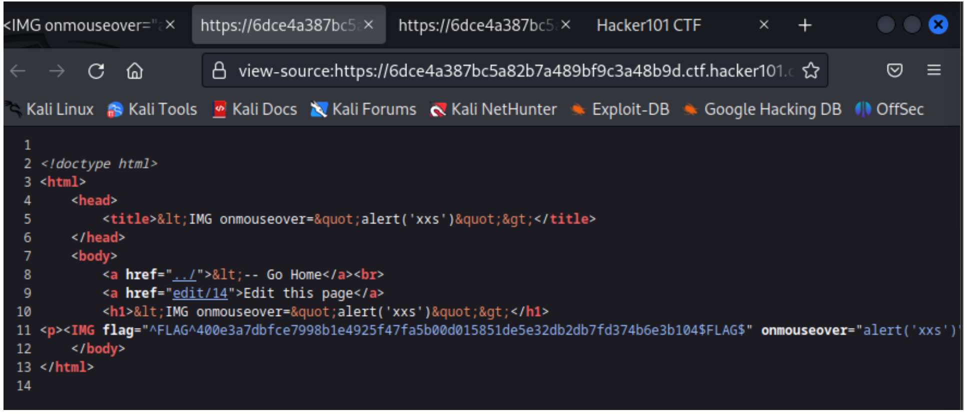
Edit Page

Title: <IMG """><SCRIPT>alert("XSS

```
<IMG """><SCRIPT>alert("XSS")</https://static1.squarespace.com/static
/54e8ba93e4b07c3f655b452e/t/56c2a04520c64707756f4267/1493764650017/>"\>
```

Markdown is supported, but scripts are not

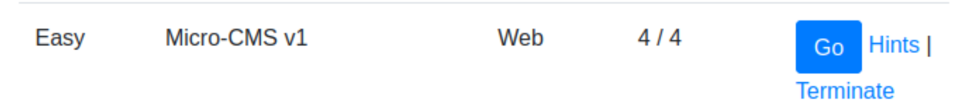
After submitting it still no access to the IMG file.
Next I'll try the Default SRC Tag to get past filters as stated in the source aforementioned.
This script here: <IMG onmouseover="alert('xxs')">
Once page was created I went to the source code as prompted by the source, https://www.bing.com/videos/search?q=cms+v1+ctf&view=detail&mid=40995FE14436986C792E40995FE14436986C792E&FORM=VIRE, and found it.



view-source:https://6dce4a387bc5a82b7a489bf9c3a48b9d.ctf.hacker101.c

```

<!doctype html>
<html>
    <head>
        <title>&lt;IMG onmouseover=&quot;alert('xxs')&quot;&gt;</title>
    </head>
    <body>
        <a href="../">&lt;-- Go Home</a><br>
        <a href="edit/14">Edit this page</a>
        <h1>&lt;IMG onmouseover=&quot;alert('xxs')&quot;&gt;</h1>
<p><IMG flag="^FLAG^400e3a7dbfce7998b1e4925f47fa5b00d015851de5e32db2db7fd374b6e3b104$FLAG$" onmouseover="alert('xxs')'
    </body>
</html>

```

I copied and pasted it and that was the final flag!



Easy	Micro-CMS v1	Web	4 / 4	Go Hints | Terminate

Discussion

Both capture the flag excersises resulted in the capture of a total of 5 flags. The first capture the flag exercise was the trivial level which contained one flag and then the easy level, Micro CSM v1, which contained 4 flags.

The first flag was found within the trivial level from doing an inspection on the website provided. From there I managed to find a flag by pressing on the security tab and exploring a domain the website connected to once I refreshed the page and analyzed it and noticed that it was a png file which I clicked to open which then exposed the flag. This expanded my knowledge base because I had never dug that deep within the inspection page of any website prior and it allowed me to familiarize myself with what it looked like and the layers it contained such as, inspector, console, debugger, network (headers, cookies, request, response, timing, security), and much more.

The second flag that was found, which was the first flag within the easy level exercise, Micro CSM v1, through URL manipulation. I was able to access a forbidden accessed page through manipulating the URL by placing the forbidden page number in the edit URL and that worked. The skills utilized in this were eerily like the ones utilized for the SQL injection that we did during our course which I'm sure assisted in my ability to see this vulnerability all the while learning a new skill in the process.

For the third through fifth flag, I relied heavily on a resources that were provided by a peer of mine from this course. Regardless of the source being directly related to Micro CSM v1, I learned a handful of skills that I didn't know previously. The third flag was located through Cross-Site Scripting (XSS) which is another type of injection, like the SQL injection that we did in our course, that injected malicious code into the website. This again, not only expanded my knowledge base on utilizing a new method to locate the vulnerability but my resilience was bolstered as I worked with a peer to remain in the fight (The lab lasted 4 days). The 4th flag was again found by URL manipulation where I added a simple " ' " to the end of a URL which exposed another vulnerability. This was specifically a query string vulnerability which is part of the URL that assigns values to specified parameters which again, was a learning opportunity for me. On the last flag it utilized XSS again, which brought things full circle because the flag was embedded in the source code which is only accessible through inspecting the page which was how the first flag was found, through inspection.

Capture the flag excersises is a great way for one to access and increase one's ethical hacking and defensive proficiency not only from the direct technical challenge of the exercise but also the methodology and mindset it takes to do them in preparation in becoming a professional in cybersecurity. This lab impacted my hard skills learned such as URL Manipulation, Query String Manipulation (form of URL Manipulation), Cross-Site Scripting (XSS), and general Inspection of websites/source code. Not only were my hard skills positively impacted, but the fundamental building blocks to the mindset and actions one will need to transition from student to professional were fortified as well. This lab forced one to be patient, positive, resilient, and to lean on one's resources whether that was videos/articles or collaborating with peers. Lastly, this lab gave one the opportunity to assess their current skill level while simultaneously improving on it. Capture the flag excersises are a phenomenal way to increase one's ethical hacking and defense proficiency.

References

Cole. (2022) Impact of Capture The Flag (CTF)-style vs. Traditional Exercises in an Introductory Computer Security Class. https://dl.acm.org/doi/pdf/10.1145/3502718.3524806

Cross, R. Dillion, K. Greenberg, D. (2021, January 29) [The Secret to Building Resilience]. Harvard Business Review.https://hbr.org/2021/01/the-secret-to-building-resilience

[Dpoint]. (2020, May 28) What is CTF- Capture the Flag? Hacker101- Trivial CTF, Micros-CMS v1 All 4/4 + 1/1 flags [Video]. Youtube.

What is CTF - Capture The Flag? Hacker101 - Trivial CTF, Micro-CMS v1 All 4/4 + 1/1 flags

[LearnCyberEH]. (2022, March 14) Hacker 101 CTF - Micro CMS v1 | All Flags Walkthrough. YouTube.

https://www.bing.com/videos/search?q=cms+v1+ctf&view=detail&mid=40995FE14436986C792E40995FE14436986C792E&FORM=VIRE

Pennington. J. (2019, February 7) [Exploiting XSS via Markdown]. Medium.

https://medium.com/taptuit/exploiting-xss-via-markdown-72a61e774bf8

Pritchard, A. (2022, March 27) [Markdown Cheatsheet]. Github.

https://github.com/adam-p/markdown-here/wiki/Markdown-Cheatsheet

Rochford, O. (n.d.) Why Capture the Flag Excersises Are Critical for Effective Cyber Security Operations, Retrieved August 18, 2023,

From https://www.securonix.com/blog/why-capture-the-flag-exercises-are-critical-for-effective-cyber-security-operations/

Wangethi, I. (2019, Novemeber 30) [Hacker101 Micro-CMS v1 CTF Walkthrough]. Medium.

https://medium.com/@isaacwangethi30/hacker101-micro-cms-v1-ctf-walkthrough-c372a9661b91

Windle, Gill. (2011). What is resilience? A review and concept analysis. Reviews in Clinical Gerontology. 21. 152 - 169. 10.1017/S0959259810000420.