

## Attacking Web Applications with Ffuf

### Introduction

There are many tools and methods to utilize for directory and parameter fuzzing/brute-forcing. In this module, we will mainly focus on the ffuf tool for web fuzzing, as it is one of the most common and reliable tools available for this purpose.

Tools such as ffuf provide us with a handy automated way to fuzz the web application's individual components or a web page. This means, for example, that we use a list that is used to send requests to the web server. If the page with the name from our list exists on the web server, and we get a response code 200, then we know that this page exists on the web server, and we can look at it manually.

### Basic Fuzzing

In this section, we covered the basics of using ffuf for directory and file fuzzing. We explored how to identify common directories and files within a web application by using wordlists and automated scripts. This foundational knowledge is crucial for uncovering hidden paths and resources that might otherwise go unnoticed.

### Domain Fuzzing

This part of the module focused on identifying hidden virtual hosts (vhosts) on a target server. By fuzzing subdomains and virtual hosts, we can discover additional entry points and services running on the same server, potentially leading to more vulnerabilities.

### Parameter Fuzzing

Parameter fuzzing is a technique used to identify vulnerabilities within web applications by testing various input parameters. This section covered how to use ffuf to fuzz for PHP parameters and parameter values, helping us uncover potential security flaws like SQL injection, XSS, and other input-based attacks.

## Skills Assessment

The skills assessment section provided practical exercises to test our understanding and application of the techniques learned throughout the module. These assessments reinforced our knowledge and ensured we were capable of effectively using ffuf for web application fuzzing.

## My Workstation

Throughout the module, we utilized a dedicated workstation setup specifically for security testing. This setup included all necessary tools and environments required to perform comprehensive fuzzing and vulnerability assessments using ffuf.

John\_Mbithi\_Mutave

To keep your account secure, move your 2FA to HTB Account by June 27th  
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.

Enable now

+1 🗨 In the page from the previous question, you should be able to find multiple parameters that are accepted by the page. What are they?

`user, username`

Submit

Hint

+2 🗨 Try fuzzing the parameters you identified for working values. One of them should return a flag. What is the content of the flag?

`HTB{w3b_fuzz1n6_m4573r}`

Submit

Hint

Previous

+10 Streak pts

Finish

Finance headline  
Japan's inflation...

Search

ENG UK 11:39 AM  
6/23/2024

To keep your account secure, move your 2FA to HTB Account by June 27th  
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.

Enable now

☐ Enable step-by-step solutions for all questions 🔧

Questions

Cheat Sheet

Answer the question(s) below to complete this Section and earn cubes!

Target(s): `83.136.254.189:53215` 📌  
Life Left: 65 minute(s)

+1 🗨 Try to create the 'ids.txt' wordlist, identify the accepted value with a fuzzing scan, and then use it in a 'POST' request with 'curl' to collect the flag. What is the content of the flag?

`HTB{p4r4m373r_fuzz1n6_15_k3y!}`

Submit

Hint

Previous Next

+10 Streak pts

Mark Complete & Next

Powered by HACKTHEBOX

cs-sa07-24019

John\_Mbithi\_Mutave

To keep your account secure, move your 2FA to HTB Account by June 27th  
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.

Enable now

<...SNIP...>

As we can see this time, we got a couple of hits, the same one we got when fuzzing GET and another parameter, which is id. Let's see what we get if we send a POST request with the id parameter. We can do that with curl, as follows:

Parameter Fuzzing - POST

Alb0GreeN@htb[/htb]\$ curl http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'id<br/><div class='center'><p>Invalid id!</p></div><br/><...SNIP...>

As we can see, the message now says Invalid id!.

PreviousNext

+10 Streak ptsMark Complete & Next

Powered byHACKTHEBOX

65°FPartly cloudy

Search

ENGUK11:24 AM6/23/2024

To keep your account secure, move your 2FA to HTB Account by June 27th  
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.

Enable now

Enable step-by-step solutions for all questions

Questions

Cheat Sheet

Answer the question(s) below to complete this Section and earn cubes!

Target(s): 83.136.254.189:53215 🚩

Life Left: 68 minute(s)

+0 🏆

Using what you learned in this section, run a parameter fuzzing scan on this page. What is the parameter accepted by this webpage?

user

Submit

PreviousNext

+10 Streak ptsMark Complete & Next

Powered byHACKTHEBOX

65°FPartly cloudy

Search

ENGUK11:24 AM6/23/2024

65°F Partly cloudy Search ENG UK 11:24 AM 6/23/2024

cs-sa07-24019

John\_Mbithi\_Mutave

To keep your account secure, move your 2FA to HTB Account by June 27th  
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.

Enable now

Enable step-by-step solutions for all questions

Questions

Cheat Sheet

Answer the question(s) below to complete this Section and earn cubes!

Target(s): 83.136.254.189:53215 🏆  
Life Left: 69 minute(s)

\* 0 Try running a VHost fuzzing scan on 'academy.htb', and see what other VHosts you get.  
What other VHosts did you get?

test.academy.htb

Submit Hint

Previous Next

+10 Streak pts Mark Complete & Next

Powered by HACKTHEBOX

To keep your account secure, move your 2FA to HTB Account by June 27th  
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.

Enable now

mail2 [Status: 200, Size: 900, Words: 423, Lines: 56]  
dns2 [Status: 200, Size: 900, Words: 423, Lines: 56]  
ns3 [Status: 200, Size: 900, Words: 423, Lines: 56]  
dns1 [Status: 200, Size: 900, Words: 423, Lines: 56]  
lists [Status: 200, Size: 900, Words: 423, Lines: 56]  
webmail [Status: 200, Size: 900, Words: 423, Lines: 56]  
static [Status: 200, Size: 900, Words: 423, Lines: 56]  
web [Status: 200, Size: 900, Words: 423, Lines: 56]  
www1 [Status: 200, Size: 900, Words: 423, Lines: 56]  
<...SNIP...>

We see that all words in the wordlist are returning 200 OK! This is expected, as we are simply changing the header while visiting http://academy.htb:PORT/. So, we know that we will always get 200 OK.  
However, if the VHost does exist and we send a correct one in the header, we should get a different response size, as in that case, we would be getting the page from that VHosts, which is likely to show a different page.

Previous Next

+10 Streak pts Mark Complete & Next

Powered by HACKTHEBOX

cs-sa07-24019

John\_Mbithi\_Mutave

The screenshot shows a web browser window with multiple tabs open at the top, including "CSA2", "Spotify", "ChatGPT", "TryHackMe", "HackTl", and others. The address bar displays the URL "academy.hackthebox.com/module/54/section/488". A dark blue banner at the top contains a yellow warning icon and the text: "To keep your account secure, move your 2FA to HTB Account by June 27th. The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side." An "Enable now" button is located on the right side of the banner. Below the banner, the main content area has a dark background. At the top of this area, it says "Waiting to start...". There is a toggle switch labeled "Enable step-by-step solutions for all questions" which is currently turned off. Below this is a section titled "Questions" with a "Cheat Sheet" link. The instruction reads: "Answer the question(s) below to complete this Section and earn cubes!". The first question is: "+0 Try running a sub-domain fuzzing test on 'inlanefreight.com' to find a customer sub-domain portal. What is the full domain of it?". Below the question, the text "customer.inlanefreight.com" is displayed in green. At the bottom of the question box are two buttons: "Submit" and "Hint". At the very bottom of the page, there are navigation buttons: "Previous" and "Next", along with a score indicator "+10 Streak pts" and a green button labeled "Mark Complete & Next".

cs-sa07-24019

John\_Mbithi\_Mutave

To keep your account secure, move your 2FA to HTB Account by June 27th  
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.

Success  
Enable now  
Congratulations! You earned 1 cubes!

Enable step-by-step solutions for all questions

### Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): 83.136.254.189:53215 🚩  
Life Left: 81 minute(s)

+1 🧠 Try to repeat what you learned so far to find more files/directories. One of them should give you a flag. What is the content of the flag?

HTB{fuzz1n6\_7h3\_w3bl}

SubmitHint

PreviousNext

+10 Streak ptsMark Complete & Next

Powered by HACKTHEBOX

To keep your account secure, move your 2FA to HTB Account by June 27th  
The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side.

Enable now

Enable step-by-step solutions for all questions

### Questions

Answer the question(s) below to complete this Section and earn cubes!

Target(s): 83.136.254.189:53215 🚩  
Life Left: 85 minute(s)

+1 🧠 Try to use what you learned in this section to fuzz the '/blog' directory and find all pages. One of them should contain a flag. What is the flag?

HTB{bru73\_f0r\_c0mm0n\_p455w0rd5}

SubmitHint

PreviousNext

+10 Streak ptsMark Complete & Next

Powered by HACKTHEBOX

cs-sa07-24019

John\_Mbithi\_Mutave

This screenshot displays the HackTheBox Academy interface for module 54, section 485. The page features a dark theme with a top navigation bar containing various browser tabs and a system status bar at the bottom. A prominent warning banner at the top states: "To keep your account secure, move your 2FA to HTB Account by June 27th. The 2FA of Academy, will be disabled soon, so be sure you have 2FA enabled on SSO side." Below this, a toggle switch allows users to "Enable step-by-step solutions for all questions". The main content area is titled "Questions" and includes a "Cheat Sheet" button. The current question asks: "In addition to the directory we found above, there is another directory that can be found. What is it?" with a hint input field labeled "forum". To the right, a "Weekly Goal Complete!" notification shows a streak of 30 days. At the bottom, a sidebar provides context for the current question, explaining that various types of fuzzing are used, including commonly used passwords for Password Brute Forcing. It mentions the SecLists repo and the directory-list-2.3 wordlist, which is being utilized for pages and directory fuzzing. The sidebar also includes a tip about removing copyright comments from the wordlist using the -ic flag.

64°F Partly cloudy Search ENG UK 10:55 AM 6/23/2024



cs-sa07-24019

John\_Mbithi\_Mutave

Shareable links - <https://academy.hackthebox.com/achievement/1296187/54>

## Conclusion

Completing the Attacking Web Applications with Ffuf module on Hack The Box has been an enlightening experience. The hands-on approach and in-depth coverage of fuzzing techniques have significantly enhanced my skills in web application security testing. Armed with the knowledge and tools from this module, I am now better equipped to identify and exploit vulnerabilities in web applications, making the internet a safer place.