

Forum:[Hack Forums](#)

Thread: [Bruteforce Onion Address](#)

CodeZero - May 20, 2023, 2:06 pm

Hi together,

Is there currently a way to launch a bruteforce attack for a web login on an Onion address?

I tried Burpsuite and Tor, which works at first. However, I keep getting the message that the name resolution does not work.

I have tried a few things in the host file, but the message does not go away. So I'm not sure whether the attack actually works.

To get the login and password, the computer has to run for some time. I don't want to leave the computer running for days if in the end there is no attack.

Bastille - May 20, 2023, 4:38 pm

Don't know how to make it work through Burp but you could try guessTor

If someone have a tips for Burp I would be glade

CodeZero - May 21, 2023, 2:28 am

Are you sure that the tool still works? The tool is now 8 years old.

CodeZero - June 8, 2023, 1:23 pm

So I have now managed to check onion websites for security vulnerabilities using Burp Suite and Firefox.

Just download the addon FoxyProxy and set it up with 127.0.0.1 and port 9150.

Use the same data in Burp Suite in the network connections under Socks proxy.

This way I can now scan all onion websites completely.

Pallett - June 8, 2023, 1:42 pm

I've been following your thread for a few days now. Why don't you use a remote server with the correct axis?

CodeZero - June 8, 2023, 3:47 pm

How is that different from Burp Suite?

It was important to me that I could first uncover all the security vulnerabilities and then plan an attack.

I was able to do that with Burp and Firefox for the time being.

What are the advantages of the remote server with Axis?

Dread.Reaper - June 9, 2023, 5:43 am

(Jun 8, 2023 03:47 PM)CodeZer0 Wrote: [\[CITE\]](#) How is that different from Burp Suite?

It was important to me that I could first uncover all the security vulnerabilities and then plan an attack.

I was able to do that with Burp and Firefox for the time being.

What are the advantages of the remote server with Axis?

Nothing...

Try slowing your attempt down.. Takes a hell of a lot longer, but to me its sounding like a timed lockout of some sort. How often are you changing nodes?

CodeZer0 - June 9, 2023, 9:54 am

(Jun 9, 2023 05:43 AM)Dread.Reaper Wrote: [\[CITE\]](#) Nothing...

Try slowing your attempt down.. Takes a hell of a lot longer, but to me its sounding like a timed lockout of some sort. How often are you changing nodes?

Don't understand the question now. Everything works as it should for me.

A complete deep scan with Burp Suite takes about 4 hours. But then you really have all the information you need.

It's just not quite clear to me how I can apply the payloads.

Dread.Reaper - June 9, 2023, 9:57 am

(Jun 9, 2023 09:54 AM)CodeZer0 Wrote: [\[CITE\]](#) Don't understand the question now. Everything works as it should for me.

A complete deep scan with Burp Suite takes about 4 hours. But then you really have all the information you need.

It's just not quite clear to me how I can apply the payloads.

So, are you trying to brute force the login or apply an exploit???

CodeZer0 - June 9, 2023, 10:05 am

Burp Suite gave me the following vulnerabilities:

1. SQL injection

[fullname parameter]

[street parameter]

2. Cross-site scripting (stored)

3. Cross-site scripting (reflected)

3.1. [info parameter]

3.2. [info parameter]

3.3. [info parameter]

4. Cookie without HttpOnly flag set

5. Unencrypted communications

6. Path-relative style sheet import

7. Cross-site request forgery

8. External service interaction (DNS)

8.1. [fullname parameter]

9. External service interaction (SMTP)

10. Spoofable client IP address

11. Input returned in response (reflected)

11.1. [city parameter]

11.2. [country parameter]

11.3. [email parameter]

11.4. [fullname parameter]

11.5. [info parameter]

11.6. [notes%5B%5D parameter]

11.7. [shipping parameter]

11.8. [state parameter]

11.9. [street parameter]

11.10. [zip parameter]

11.11. [city parameter]

11.12. [country parameter]

11.13. [email parameter]

11.14. [fullname parameter]

11.15. [info parameter]

11.16. [notes%5B%5D parameter]

11.17. [shipping parameter]

11.18. [state parameter]

11.19. [street parameter]

11.20. [zip parameter]

11.21. [city parameter]

11.22. [country parameter]

11.23. [email parameter]

11.24. [fullname parameter]

11.25. [info parameter]

11.26. [notes%5B%5D parameter]

11.27. [shipping parameter]

11.28. [state parameter]

11.29. [street parameter]

11.30. [zip parameter]

11.31. [city parameter]

11.32. [country parameter]

11.33. [email parameter]

11.34. [fullname parameter]

11.35. [info parameter]

11.36. [notes%5B%5D parameter]

11.37. [shipping parameter]

11.38. [state parameter]

11.39. [street parameter]

11.40. [zip parameter]

12. Suspicious input transformation (reflected)

12.1. [city parameter]

12.2. [country parameter]

12.3. [email parameter]

12.4. [fullname parameter]

12.5. [info parameter]

12.6. [shipping parameter]

12.7. [state parameter]

12.8. [street parameter]

12.9. [zip parameter]

12.10. [city parameter]

12.11. [country parameter]

12.12. [email parameter]

12.13. [fullname parameter]

12.14. [info parameter]

12.15. [shipping parameter]

12.16. [state parameter]

12.17. [street parameter]

12.18. [zip parameter]

12.19. [city parameter]

12.20. [country parameter]

12.21. [email parameter]

12.22. [fullname parameter]

12.23. [info parameter]

12.24. [shipping parameter]

12.25. [state parameter]

12.26. [street parameter]

12.27. [zip parameter]

13. Cross-domain Referer leakage

- 14. Frameable response (potential Clickjacking)
- 15. Link manipulation (reflected)
 - 15.1. [language-switcher parameter]
 - 15.2. [language-switcher parameter]
 - 15.3. [name of an arbitrarily supplied URL parameter]
 - 15.4. [language-switcher parameter]
 - 15.5. [name of an arbitrarily supplied URL parameter]
 - 15.6. [language-switcher parameter]
 - 15.7. [name of an arbitrarily supplied URL parameter]
 - 15.8. [language-switcher parameter]
 - 15.9. [name of an arbitrarily supplied URL parameter]
 - 15.10. [language-switcher parameter]
 - 15.11. [name of an arbitrarily supplied URL parameter]
 - 15.12. [language-switcher parameter]
 - 15.13. [name of an arbitrarily supplied URL parameter]
 - 15.14. [language-switcher parameter]
 - 15.15. [name of an arbitrarily supplied URL parameter]
 - 15.16. [language-switcher parameter]
 - 15.17. [name of an arbitrarily supplied URL parameter]
 - 15.18. [language-switcher parameter]
 - 15.19. [name of an arbitrarily supplied URL parameter]
 - 15.20. [language-switcher parameter]
 - 15.21. [name of an arbitrarily supplied URL parameter]
 - 15.22. [language-switcher parameter]
 - 15.23. [name of an arbitrarily supplied URL parameter]
 - 15.24. [language-switcher parameter]
 - 15.25. [name of an arbitrarily supplied URL parameter]

15.26. [language-switcher parameter]

15.27. [name of an arbitrarily supplied URL parameter]

15.28. [language-switcher parameter]

15.29. [name of an arbitrarily supplied URL parameter]

15.30. [language-switcher parameter]

15.31. [name of an arbitrarily supplied URL parameter]

16. Email addresses disclosed

LeetSpeed - June 9, 2023, 10:34 am

(Jun 8, 2023 01:23 PM)CodeZer0 Wrote: [\[CITE\]](#) So I have now managed to check onion websites for security vulnerabilities using Burp Suite and Firefox.

Just download the addon FoxyProxy and set it up with 127.0.0.1 and port 9150.

Use the same data in Burp Suite in the network connections under Socks proxy.

This way I can now scan all onion websites completely.

This should work completely fine.

CodeZer0 - June 9, 2023, 1:58 pm

(Jun 9, 2023 09:57 AM)Dread.Reaper Wrote: [\[CITE\]](#) So, are you trying to brute force the login or apply an exploit???

Both. I was able to find the admin login page. I'll probably have to bruteforce it, but it's definitely not crackable, as numbers, letters, special characters, etc. of a greater length have certainly been used.

The normal websites have the vulnerabilities listed above. I think it is more realistic to access the database there.

Dread.Reaper - June 10, 2023, 4:47 am

(Jun 9, 2023 01:58 PM)CodeZer0 Wrote: [\[CITE\]](#) Both. I was able to find the admin login page. I'll probably have to bruteforce it, but it's definitely not crackable, as numbers, letters, special characters, etc. of a greater length have certainly been used.

The normal websites have the vulnerabilities listed above. I think it is more realistic to access the database there.

Yea, you will likely find better success in exploitation.

CodeZer0 - June 14, 2023, 6:59 am

Does anyone have an idea how I can exploit this SQL injection? I am somehow not getting anywhere here.

1. SQL injection

[fullname parameter]

[street parameter]

Dread.Reaper - June 15, 2023, 3:41 am

(Jun 14, 2023 06:59 AM)CodeZer0 Wrote: [\[CITE\]](#) Does anyone have an idea how I can exploit this SQL injection? I am somehow not getting anywhere here.

1. SQL injection

[fullname parameter]

[street parameter]

It does not quite work that way brother.

CodeZer0 - June 15, 2023, 3:21 pm

Then give me a little hint

Mr. Robot - June 17, 2023, 4:26 pm

If you start the tor service in your terminal then run the following - it will load in a file called directories.txt and run a directory scan against the website.

Made this for you just now.

Code sudo apt update

sudo apt install tor

Code sudo service tor start

Code import requests

```
proxies = {  
    'http': 'socks5h://localhost:9050',  
    'https': 'socks5h://localhost:9050'  
}
```

```
base_url = 'http://cashgod2w7hzaeihf2d2bwd7xwtsjtbcbzbusbsyzqoqymks2g5l46eyd.onion/'
```

```
# Read directory names from words.txt
```

```
with open('directories.txt', 'r') as file:
```

```
    directories = file.read().splitlines()
```

```
for directory in directories:
```

```
    url = base_url + directory
```

```
    try:
```

```
        response = requests.get(url, proxies=proxies)
```

```
        status_code = response.status_code
```

```
        if status_code != 404:
```

```
            print(f"Status code for {url}: {status_code}")
```

```
    except requests.RequestException as e:
```

```
        print(f"Request failed for {url}: {e}")
```

Parzival666 - June 19, 2023, 9:44 am

does anyone know a open source brute force or some kind of tool?

CodeZer0 - June 22, 2023, 9:10 am

500 Euros in Bitcoin, for whoever helps me get my money back.

meihudon - August 16, 2023, 5:41 am

hlw guyss i need to do bruteforce attack on a website but problem is website is protected by cloudflare so any body please tell how i can find the origin ip address of a domain if you intrested in this work i pay you some small amount of dollers so please contect me on telegram @siblidhop