Лабораторная работа 7

Предотвращение атак, связанных с инъекциями команд

Индивидуальность отчетов:

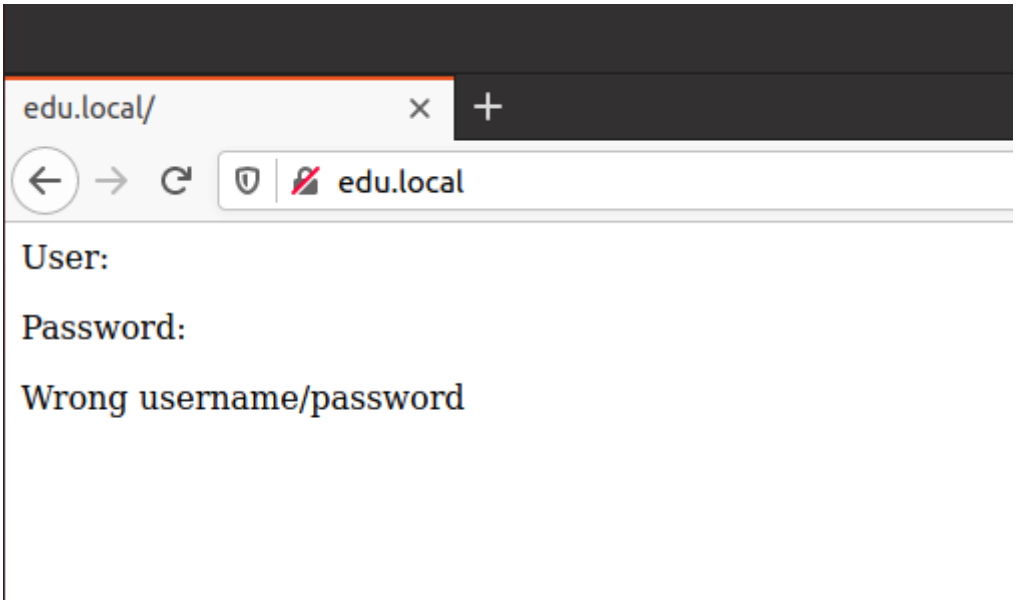
Как минимум, в имени пользователя ОС

Обязательно скриншотить каждый этап и пояснять

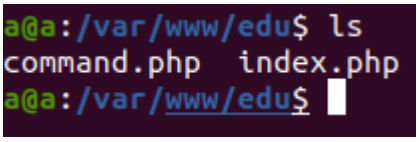
Обязательно выводы должны быть

1. Откроем ранее созданную виртуальную машину Ubuntu

2. Убедимся, что веб-сервер работает

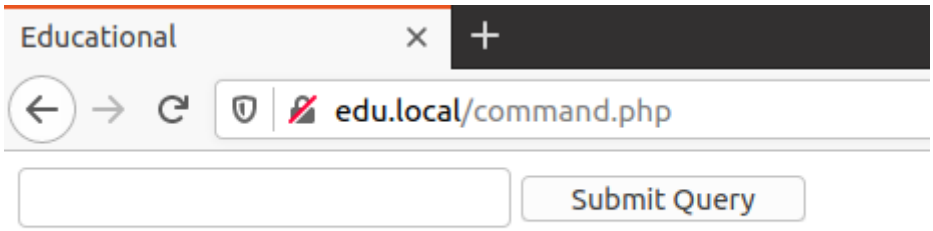


3. Создадим файл command.php в /var/www/edu и убедимся в этом



4. Создадим форму на нашей странице

```
<html>
  <head>
    <title>Educational</title>
  </head>
  <body>
    <form action="" method="POST">
      <input name="destination" type="text">
      <input type="submit">
    </form>
   </body>
</html>
```

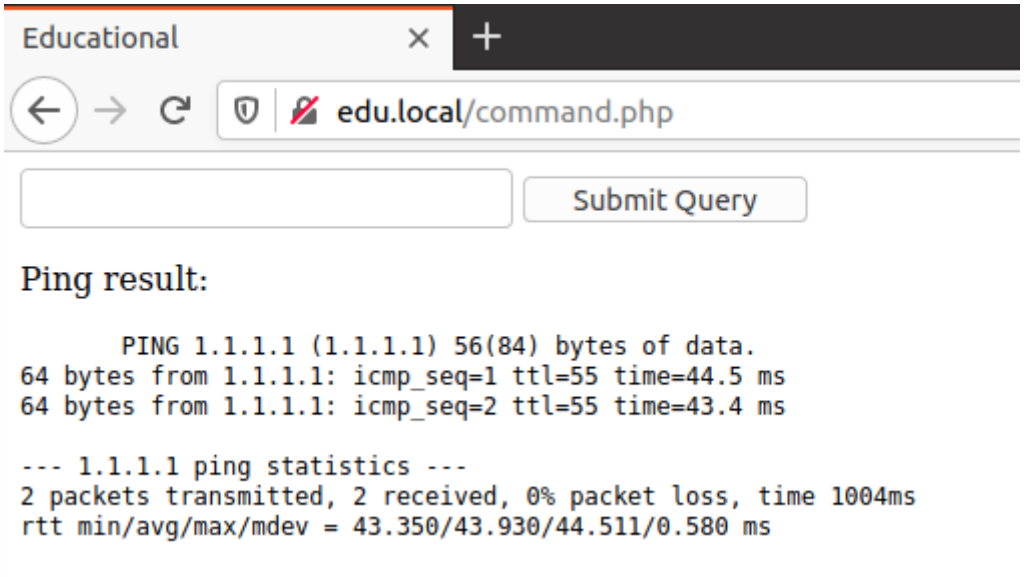


5. Добавим возможность проверки ping до вводимого пользователем адреса

В отчете указать метод отправки данных

```
<html>
  <head>
    <title>Educational</title>
  </head>
  <body>
    <form action="" method="POST">
      <input name="destination" type="text">
      <input type="submit">
    </form>
    <div>
     <p>Ping result:</p>
     <pre>
       <?php
         if(isset($_POST["destination"])){
           $command = "ping -c 2 " . $_POST["destination"];
           passthru($command);
         }
       ?>
     </pre>
    </div>
   </body>
</html>
```

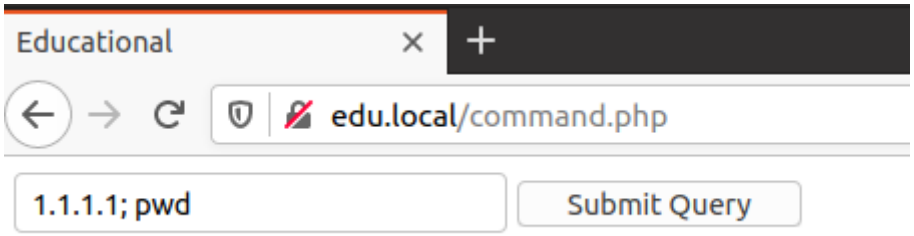
6. Убедимся в работоспособности

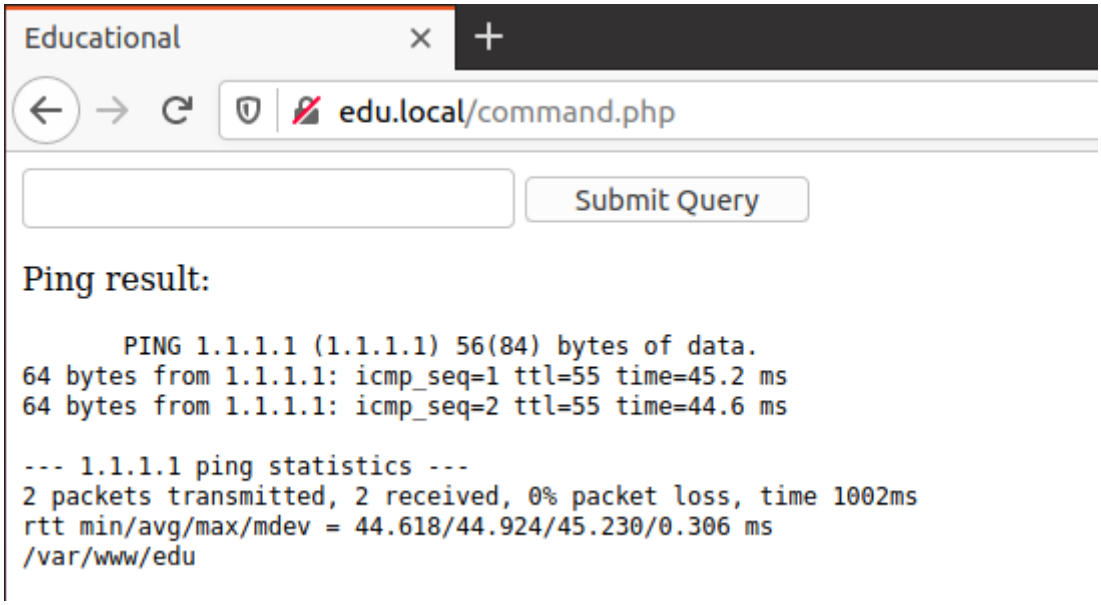


7. Убедимся в работе через curl

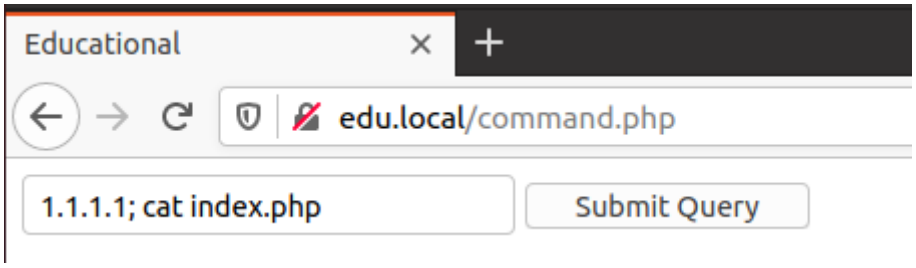
```
a@a:/var/www/edu$ curl -s http://edu.local/command.php -d "destination=1.1.1.1"
<html>
  <head>
    <title>Educational</title>
  </head>
  <body>
    <form action="" method="POST">
      <input name="destination" type="text">
      <input type="submit">
    </form>
    <div>
     <p>Ping result:</p>
     <pre>
       PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=55 time=45.7 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=55 time=44.6 ms

--- 1.1.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 44.555/45.124/45.693/0.569 ms
     </pre>
    </div>
   </body>
</html>
a@a:/var/www/edu$
```

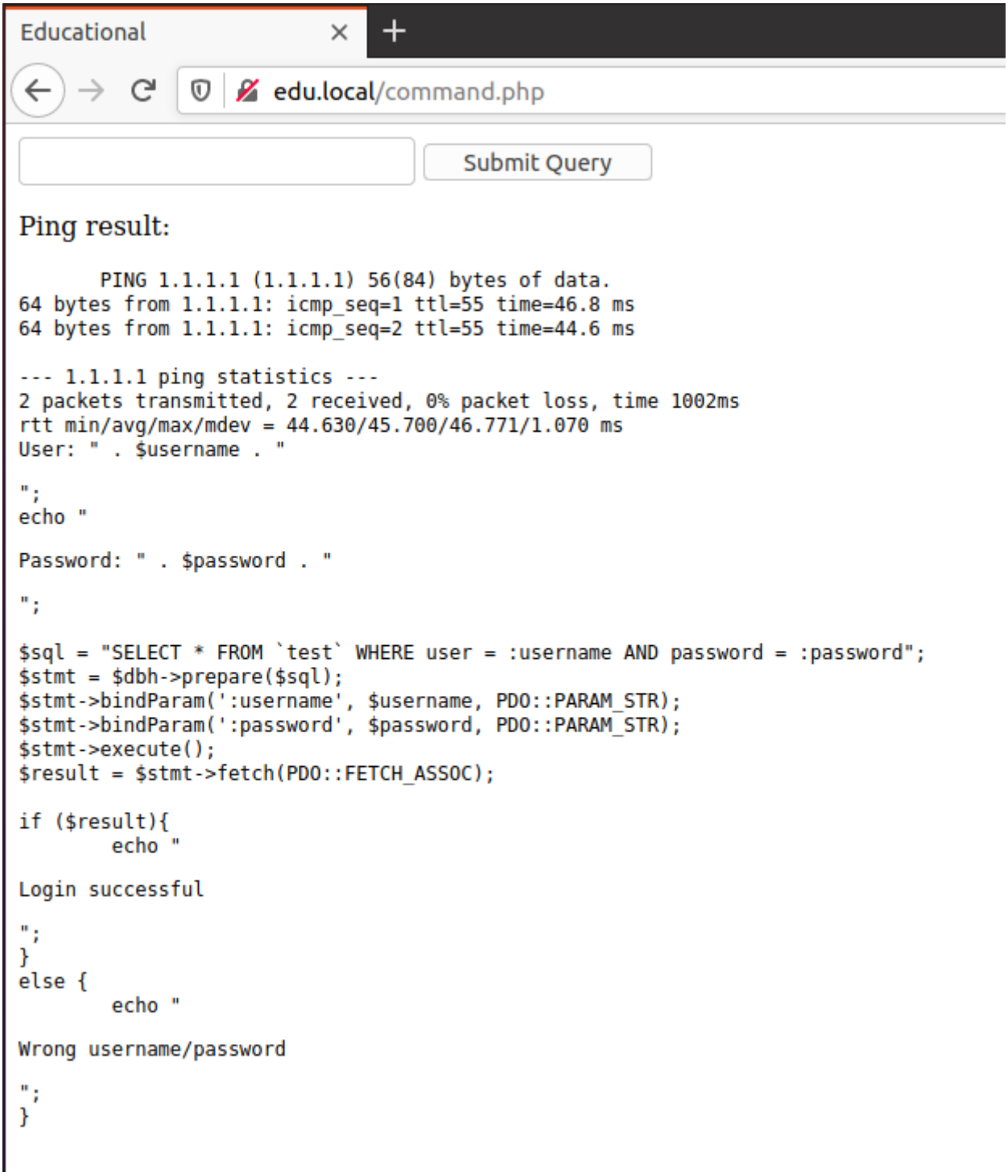
8. Ввести в поле ввода адреса проверки строку “1.1.1.1; pwd”





9. Ввести в поле ввода адреса проверки строку “1.1.1.1; cat index.php”





10. Нажать ctrl + u, чтобы посмотреть исходный код

Educational | http://edu.local/command.p

view-source:http://edu.local/command.php

```
1  <html>
2    <head>
3      <title>Educational</title>
4    </head>
5    <body>
6      <form action="" method="POST">
7        <input name="destination" type="text">
8        <input type="submit">
9      </form>
10     <div>
11      <p>Ping result:</p>
12      <pre>
13        PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
14 64 bytes from 1.1.1.1: icmp_seq=1 ttl=55 time=44.7 ms
15 64 bytes from 1.1.1.1: icmp_seq=2 ttl=55 time=44.5 ms
16
17 --- 1.1.1.1 ping statistics ---
18 2 packets transmitted, 2 received, 0% packet loss, time 1001ms
19 rtt min/avg/max/mdev = 44.522/44.620/44.718/0.098 ms
20 <?php
21 $dbh = new PDO('mysql:host=localhost;dbname=edu', 'newuser', '123');
22
23 $username = $_GET["user"];
24 $password = $_GET["pass"];
25
26 echo "<p>User: " . $username . "</p>";
27 echo "<p>Password: " . $password . "</p>";
28
29 $sql = "SELECT * FROM `test` WHERE user = :username AND password = :password";
30 $stmt = $dbh->prepare($sql);
31 $stmt->bindParam(':username', $username, PDO::PARAM_STR);
32 $stmt->bindParam(':password', $password, PDO::PARAM_STR);
33 $stmt->execute();
34 $result = $stmt->fetch(PDO::FETCH_ASSOC);
35
36 if ($result){
37     echo "<p>Login successful</p>";
38 }
39 else {
40     echo "<p>Wrong username/password</p>";
41 }
42
43
44      </pre>
45     </div>
46    </body>
47 </html>
48
```

11. Обнаружить адрес, а также логин и пароль для подключения к базе данных из прошлой лабораторной работы

12. Повторить тоже самое с помощью curl

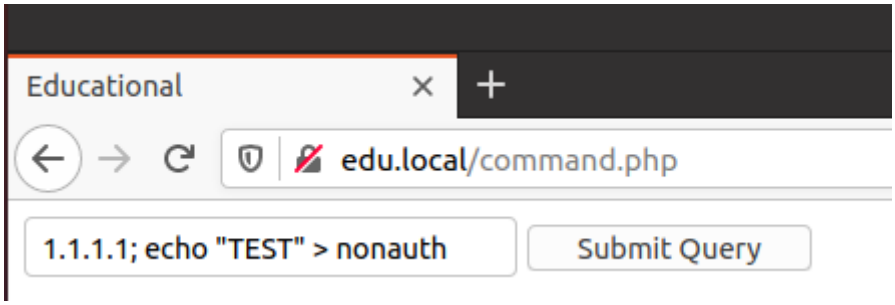
```
a@a: /var/www/edu
a@a:/var/www/edu$ curl -s http://edu.local/command.php -d "destination=1.1.1.1; pwd"
<html>
  <head>
    <title>Educational</title>
  </head>
  <body>
    <form action="" method="POST">
      <input name="destination" type="text">
      <input type="submit">
    </form>
    <div>
     <p>Ping result:</p>
     <pre>
       PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=55 time=45.2 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=55 time=44.9 ms

--- 1.1.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 44.910/45.058/45.206/0.148 ms
/var/www/edu
     </pre>
    </div>
   </body>
</html>
a@a:/var/www/edu$
```

```
a@a: /var/www/edu
a@a:/var/www/edu$ curl -s http://edu.local/command.php -d "destination=1.1.1.1; cat index.php"
<html>
  <head>
    <title>Educational</title>
  </head>
  <body>
    <form action="" method="POST">
      <input name="destination" type="text">
      <input type="submit">
    </form>
    <div>
     <p>Ping result:</p>
     <pre>
       PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=55 time=44.9 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=55 time=42.5 ms

--- 1.1.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 42.548/43.747/44.946/1.199 ms
<?php
$dbh = new PDO('mysql:host=localhost;dbname=edu', 'newuser', '123');

$username = $_GET["user"];
$password = $_GET["pass"];

echo "<p>User: " . $username . "</p>";
echo "<p>Password: " . $password . "</p>";

$sql = "SELECT * FROM `test` WHERE user = :username AND password = :password";
$stmt = $dbh->prepare($sql);
$stmt->bindParam(':username', $username, PDO::PARAM_STR);
$stmt->bindParam(':password', $password, PDO::PARAM_STR);
$stmt->execute();
$result = $stmt->fetch(PDO::FETCH_ASSOC);

if ($result){
        echo "<p>Login successful</p>";
}
else {
        echo "<p>Wrong username/password</p>";
}


     </pre>
    </div>
   </body>
</html>
a@a:/var/www/edu$
```

13. Убедимся ещё раз, что правильно настроены владелец и права файлов /var/www/edu

```
a@a:/var/www/edu$ sudo chown www-data:www-data ./ -R
a@a:/var/www/edu$ sudo chmod 755 ./ -R
a@a:/var/www/edu$
```

14. Создадим файл на веб-сервере с нужным нам содержимым




```
a@a:/var/www/edu$ cat nonauth
TEST
a@a:/var/www/edu$
```

15. Сделаем тоже самое с помощью curl

```
a@a:/var/www/edu$ curl -s http://edu.local/command.php -d "destination=1.1.1.1; echo 'TEST2' > nonauth2"
<html>
  <head>
    <title>Educational</title>
  </head>
  <body>
    <form action="" method="POST">
      <input name="destination" type="text">
      <input type="submit">
    </form>
    <div>
     <p>Ping result:</p>
     <pre>
       PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=55 time=45.6 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=55 time=44.3 ms

--- 1.1.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 44.292/44.963/45.635/0.671 ms
     </pre>
    </div>
   </body>
</html>
a@a:/var/www/edu$ cat nonauth2
TEST2
a@a:/var/www/edu$
```

16. Заэкранируем данные от пользователя

```
<html>
  <head>
    <title>Educational</title>
  </head>
  <body>
    <form action="" method="POST">
      <input name="destination" type="text">
      <input type="submit">
    </form>
    <div>
     <p>Ping result:</p>
     <pre>
       <?php
         $destination = $_POST["destination"];
         $destination = escapeshellcmd($destination);
         $destination = escapeshellarg($destination);

         if(isset($destination)){
           $command = "ping -c 2 " . $destination;
           passthru($command);
         }
       ?>
     </pre>
    </div>
   </body>
</html>
```

17. Повторим пункты 8 – 15 и убедимся, что уязвимость более недоступна

```
a@a:/var/www/edu$ curl -s http://edu.local/command.php -d "destination=1.1.1.1; pwd"
<html>
  <head>
    <title>Educational</title>
  </head>
  <body>
    <form action="" method="POST">
      <input name="destination" type="text">
      <input type="submit">
    </form>
    <div>
     <p>Ping result:</p>
     <pre>
            </pre>
    </div>
   </body>
</html>
a@a:/var/www/edu$ curl -s http://edu.local/command.php -d "destination=1.1.1.1; cat index.php"
<html>
  <head>
    <title>Educational</title>
  </head>
  <body>
    <form action="" method="POST">
      <input name="destination" type="text">
      <input type="submit">
    </form>
    <div>
     <p>Ping result:</p>
     <pre>
            </pre>
    </div>
   </body>
</html>
```

```
a@a: /var/www/edu
a@a:/var/www/edu$ sudo rm nonauth2
a@a:/var/www/edu$ curl -s http://edu.local/command.php -d "destination=1.1.1.1; echo 'TEST2' > nonauth2"
<html>
  <head>
    <title>Educational</title>
  </head>
  <body>
    <form action="" method="POST">
      <input name="destination" type="text">
      <input type="submit">
    </form>
    <div>
     <p>Ping result:</p>
     <pre>
            </pre>
    </div>
   </body>
</html>
a@a:/var/www/edu$ cat nonauth2
cat: nonauth2: No such file or directory
```

```
a@a:/var/www/edu$ curl -s http://edu.local/command.php -d "destination=1.1.1.1"
<html>
  <head>
    <title>Educational</title>
  </head>
  <body>
    <form action="" method="POST">
      <input name="destination" type="text">
      <input type="submit">
    </form>
    <div>
     <p>Ping result:</p>
     <pre>
       PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=55 time=44.0 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=55 time=45.3 ms

--- 1.1.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 43.950/44.640/45.331/0.690 ms
     </pre>
    </div>
   </body>
</html>
a@a:/var/www/edu$
```