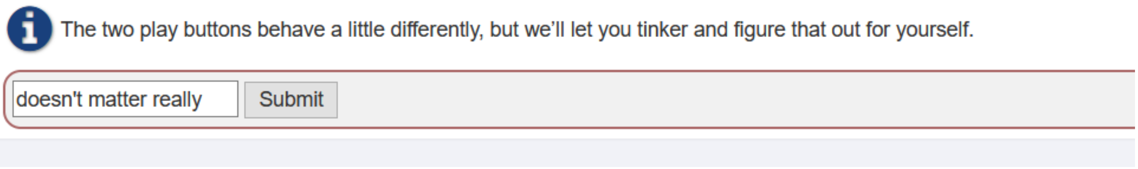
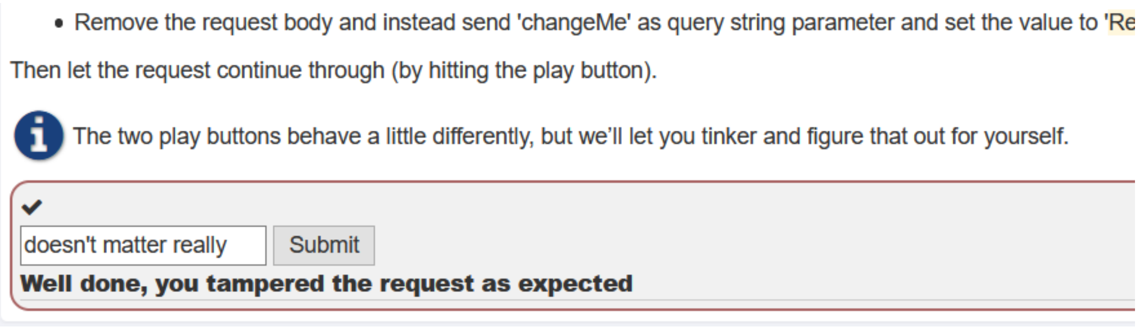
Tarea WebGoat

Ejercicio 2: HTTP Proxies.6



The two play buttons behave a little differently, but we'll let you tinker and figure out that out for yourself.

doesn't matter really



- Remove the request body and instead send 'changeMe' as query string parameter and set the value to 'Re

Then let the request continue through (by hitting the play button).

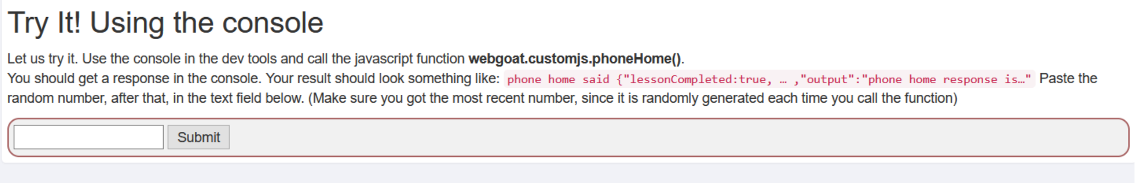
The two play buttons behave a little differently, but we'll let you tinker and figure out that out for yourself.

✓

doesn't matter really

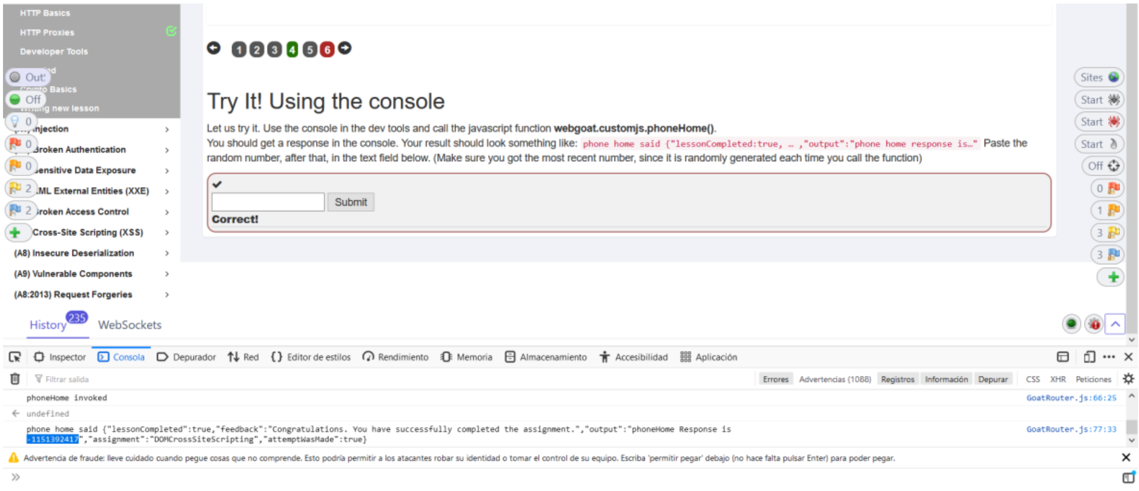
Well done, you tampered the request as expected

Ejercicio 3: Developer Tools.4



Try It! Using the console

Let us try it. Use the console in the dev tools and call the javascript function **webgoat.customjs.phoneHome()**.
You should get a response in the console. Your result should look something like: `phone home said {"lessonCompleted:true, … ,"output":"phone home response is…"` Paste the random number, after that, in the text field below. (Make sure you got the most recent number, since it is randomly generated each time you call the function)



Try It! Using the console

Let us try it. Use the console in the dev tools and call the javascript function **webgoat.customjs.phoneHome()**.
You should get a response in the console. Your result should look something like: `phone home said {"lessonCompleted:true, … ,"output":"phone home response is…"` Paste the random number, after that, in the text field below. (Make sure you got the most recent number, since it is randomly generated each time you call the function)

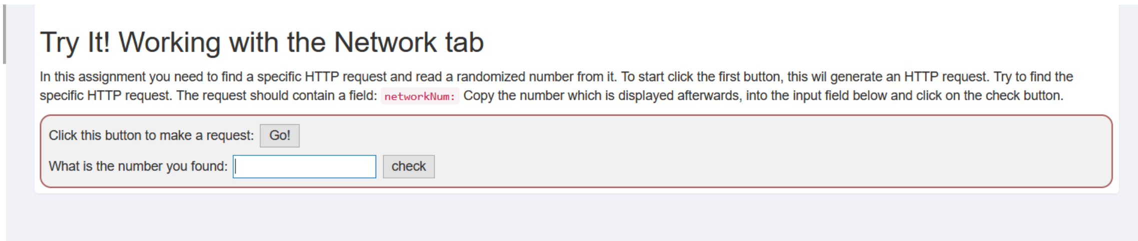
✓

Correct!

```
phoneHome invoked                                                                     GoatRouter.js:66:25
← undefined
phone home said {"lessonCompleted":true,"feedback":"Congratulations. You have successfully completed the assignment.","output":"phoneHome Response is
-1151392417","assignment":"DOMCrossSiteScripting","attemptWasMade":true}              GoatRouter.js:77:33
```

⚠ Advertencia de fraude: lleve cuidado cuando pegue cosas que no comprende. Esto podría permitir a los atacantes robar su identidad o tomar el control de su equipo. Escriba 'permitir pegar' debajo (no hace falta pulsar Enter) para poder pegar.

Ejercicio 3: Developer Tools.6

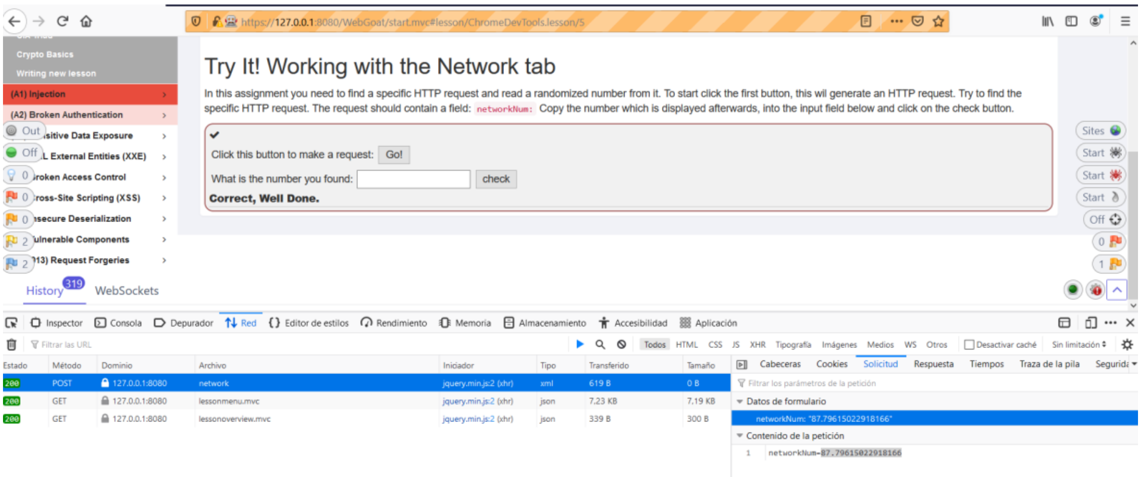


Try It! Working with the Network tab

In this assignment you need to find a specific HTTP request and read a randomized number from it. To start click the first button, this wil generate an HTTP request. Try to find the specific HTTP request. The request should contain a field: `networkNum:` Copy the number which is displayed afterwards, into the input field below and click on the check button.

Click this button to make a request: Go!

What is the number you found: check



https://127.0.0.1:8080/WebGoat/start.mvc#lesson/ChromeDevTools.lesson/5

Try It! Working with the Network tab

In this assignment you need to find a specific HTTP request and read a randomized number from it. To start click the first button, this wil generate an HTTP request. Try to find the specific HTTP request. The request should contain a field: `networkNum:` Copy the number which is displayed afterwards, into the input field below and click on the check button.

✓

Click this button to make a request: Go!

What is the number you found: check

Correct, Well Done.

Estado	Método	Dominio	Archivo	Iniciador	Tipo	Transferido	Tamaño
200	POST	127.0.0.1:8080	network	jquery.min.js:2 (xhr)	xml	619 B	0 B
200	GET	127.0.0.1:8080	lessonmenu.mvc	jquery.min.js:2 (xhr)	json	7.23 KB	7.19 KB
200	GET	127.0.0.1:8080	lessonoverview.mvc	jquery.min.js:2 (xhr)	json	339 B	300 B

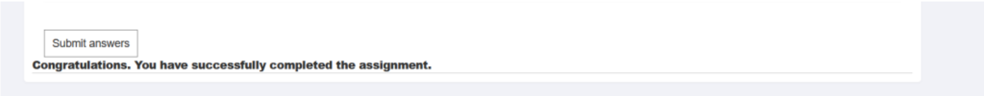
Datos de formulario

networkNum: "87.79615022918166"

Contenido de la petición

```
networkNum=87.79615022918166
```

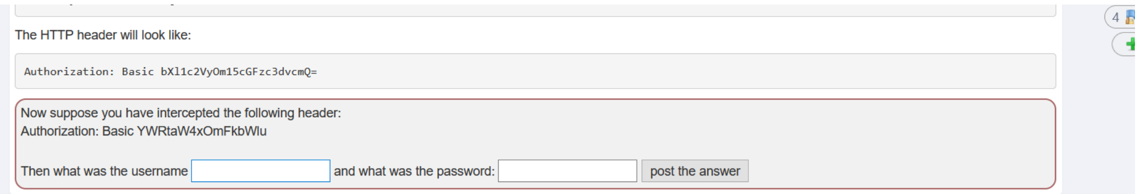
Ejercicio 4: CIA.5



Submit answers

Congratulations. You have successfully completed the assignment.

Ejercicio 5: Cripto Basics.2

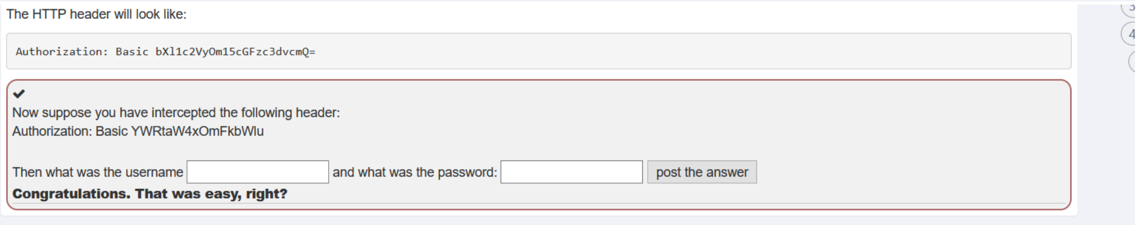


The HTTP header will look like:

```
Authorization: Basic bXl1c2VyOm15cGFzc3dvcmQ=
```

Now suppose you have intercepted the following header:
Authorization: Basic YWRtaW4xOmFkbWlu

Then what was the username and what was the password: post the answer



The HTTP header will look like:

```
Authorization: Basic bXl1c2VyOm15cGFzc3dvcmQ=
```

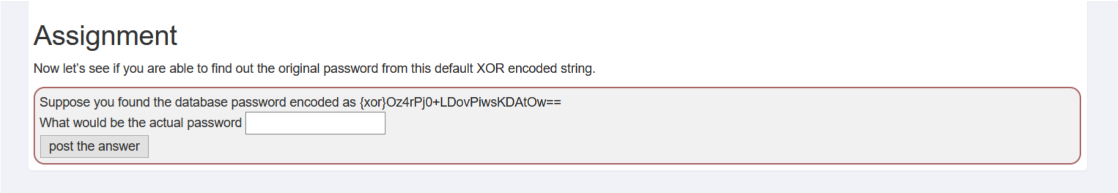
✓

Now suppose you have intercepted the following header:
Authorization: Basic YWRtaW4xOmFkbWlu

Then what was the username and what was the password: post the answer

Congratulations. That was easy, right?

Ejercicio 5: Cripto Basics.3



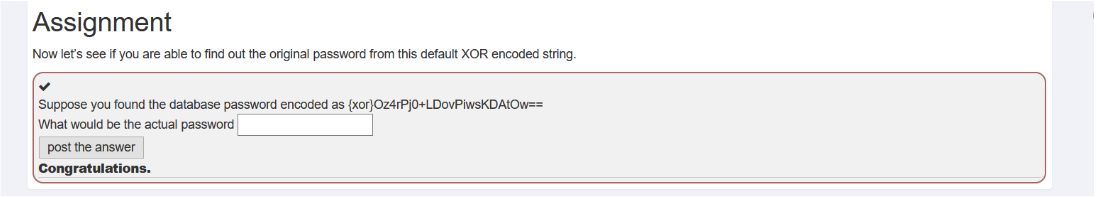
Assignment

Now let's see if you are able to find out the original password from this default XOR encoded string.

Suppose you found the database password encoded as {xor}Oz4rPj0+LDovPiwsKDAtOw==

What would be the actual password

post the answer



Now let's see if you are able to find out the original password from this default XOR encoded string.

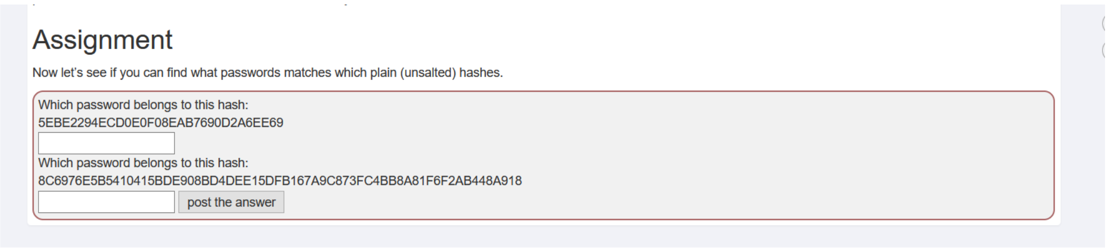
✓

Suppose you found the database password encoded as {xor}Oz4rPj0+LDovPiwsKDAtOw==

What would be the actual password

Congratulations.

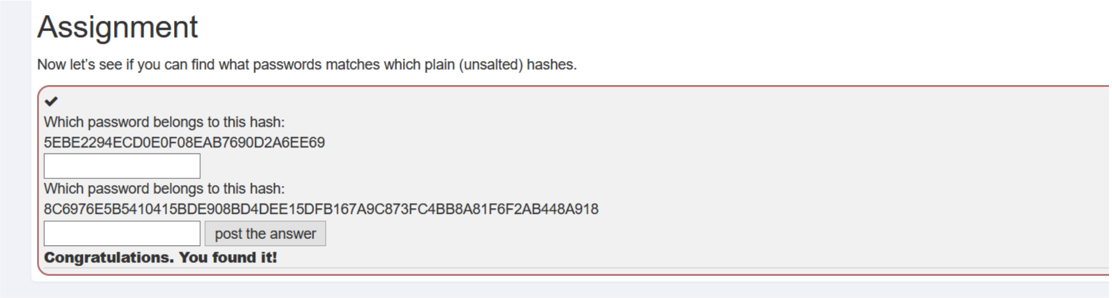
Ejercicio 5: Cripto Basics.4



Now let's see if you can find what passwords matches which plain (unsalted) hashes.

Which password belongs to this hash:
5EBE2294ECD0E0F08EAB7690D2A6EE69

Which password belongs to this hash:
8C6976E5B5410415BDE908BD4DEE15DFB167A9C873FC4BB8A81F6F2AB448A918



Now let's see if you can find what passwords matches which plain (unsalted) hashes.

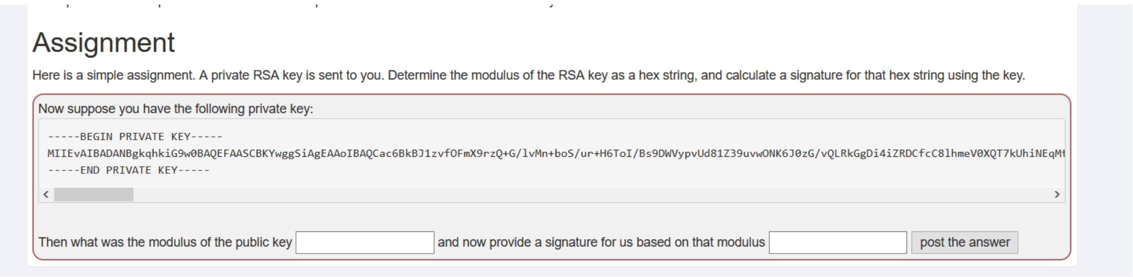
✓

Which password belongs to this hash:
5EBE2294ECD0E0F08EAB7690D2A6EE69

Which password belongs to this hash:
8C6976E5B5410415BDE908BD4DEE15DFB167A9C873FC4BB8A81F6F2AB448A918

Congratulations. You found it!

Ejercicio 5: Cripto Basics.6

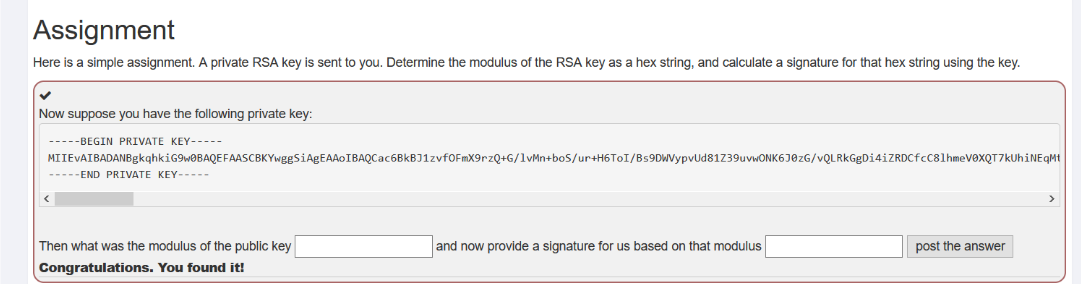


Here is a simple assignment. A private RSA key is sent to you. Determine the modulus of the RSA key as a hex string, and calculate a signature for that hex string using the key.

Now suppose you have the following private key:

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCac6BkBJ1zvfOFmX9rzQ+G/lvMn+boS/ur+H6ToI/Bs9DWVypvUd81Z39uvwONK6J0zG/vQLRkGgDi4iZRDCfcC8lhmeV0XQT7kUhiNEqMt
-----END PRIVATE KEY-----
```

Then what was the modulus of the public key and now provide a signature for us based on that modulus



Here is a simple assignment. A private RSA key is sent to you. Determine the modulus of the RSA key as a hex string, and calculate a signature for that hex string using the key.

✓

Now suppose you have the following private key:

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCac6BkBJ1zvfOFmX9rzQ+G/lvMn+boS/ur+H6ToI/Bs9DWVypvUd81Z39uvwONK6J0zG/vQLRkGgDi4iZRDCfcC8lhmeV0XQT7kUhiNEqMt
-----END PRIVATE KEY-----
```

Then what was the modulus of the public key and now provide a signature for us based on that modulus

Congratulations. You found it!