# Web application security

**Task 0:**

Watch the demo on how to use Burp Proxy debugger and how to use level1 of the game. Demo recording can be found on the following link (It shows the usage of older version of Burp Proxy debugger. This should be enough to understand how to use the tool no matter which version.

[https://1drv.ms/f/s!Ajm-3AdyO3sSh4tnyIfmztQ6Nes10Q?e=WUy83J](https://1drv.ms/f/s%21Ajm-3AdyO3sSh4tnyIfmztQ6Nes10Q?e=WUy83J)

**Task 1:**

On Windows 10 VM download Burp Proxy from the Internet and install Java if needed (or use Burp Proxy on Kali Linux VM!).

RECOMMENDATION is to use Kali Linux VM!

**Task 2:**

Start Internet browser and Burp Proxy debugger. Setup Internet browser to use localhost:8080 as the proxy server (If you don’t know how, watch the DEMO in Task 0.

A better option is to use the Internet browser (Chrome) directly from Burp Proxy debugger. The Chrome browser will be automatically configured to use Burp Proxy as proxy server.

If turned on, turn off the option to automatically intercept the Internet traffic in Burp Proxy debugger.

Visit [**http://play.h4ck3r.one:9020/packman/level1/**](http://play.h4ck3r.one:9020/packman/level1/)

This link hosts the Packman game. Play the game!

After you lose all available lives in the game, press refresh to restart the game!

If refresh doesn’t restart the game, click on the link in the browser and press ENTER.

Play the game ONLY ONCE and then continue with the exercise!!!

**Task 3**

Start the game and then configure Burp Proxy to intercept the browser traffic (if you don’t know how, watch the demo!). When you do – all the traffic sent by the configured Internet browser will be intercepted by the Burp Proxy, and it will wait for you to forward it to the server.

Play the game, and when done, check the packet sent by the game in the Burp Proxy debugger. If you didn’t enable the packet interception, this should be the last packet in the packet list.

**NOTE**: When the traffic interception is enabled, surfing will be impacted because Burp Proxy will intercept each packet sent by the browser waiting for your action (forward or drop). If you choose to use Internet explorer or Chrome on windows OS, changes made to proxy settings will be system wide, meaning that all the Web traffic your computer sends to the Internet will be proxied through Burp proxy. Because of that it is recommended to use Firefox as the Internet browser, because Firefox will change the proxy settings only for the browser, not system wide. Hence the recommendation to run the exercise on Kali Linux VM. On the other hand, if you choose to start the browser from Burp Proxy, it will use preconfigured Chrome, and this is the recommended option today.

**Identify the Header values (if applicable):**

GET:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

HOST:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

User-Agent

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This application doesn't use session cookie. Is this good or bad? Why?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Are there any parameters in the GET request? If so, what is the value?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Answer the question based on the collected information: Is it possible top change the score? If so, how?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Task 4:**

Change the x parameter to change the score. Were you successful? If not, ask for help.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Task 5:**

Start the game on [**http://play.h4ck3r.one:9020/packman/level2/**](http://play.h4ck3r.one:9020/packman/level2/)

**Repeat the Task 3!**

Which parameters is the game using now? Write down the parameter names:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Can you change the score now? If the answer is yes, how?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If not, why?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Task 6:**

If unable to change the score in Task 5, try to answer the following questions:

Name some of the encoding algorithms:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Look at the x parameter value. Which encoding was used to create the parameter value? Can you change the score now?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Taks 7:**

Start the game on [**http://play.h4ck3r.one:9020/packman/level3/**](http://play.h4ck3r.one:9020/packman/level3/)

**Repeat the task 3!**

Which parameters is the game using now? Write down the parameter names: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Can you change the score now? If the answer is yes, how?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If not, why?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Task 8:**

If unable to change the score in Task 7, try to answer the following questions:

What is parameter y?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If you don’t know the answer, try to google the parameter y value. What is it?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If you don’t know the answer, ask the professor.

Try to change the score based on collected information. Can you?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What must be changed to change the score in level 3?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**For advanced students (if time permits):**

**Bonus task 1:**

The game is written in HTML5 in Java language.

Instead of changing the score as explained in the previous steps, try to create a cheat by changing the ghosts speed, or by removing ghosts, change the number of points assigned for each dot or try to flip the dots (change the ones that allow you to eat the ghosts with normal and vice versa), etc.

**If you want to learn more (homework – recommended for developers!)**

There are other games on this server in folders mc and nivo1/nivo2.

Identify programming languages and frameworks used and try to decompile the source code. When decompiled, try to understand the code.

Hint:Dnspy/ilspy or JDGui