We are given a website a live website as well as the source code for the site.

When visiting the website we can see that clicking on "what's the date?" sends a get request with a format variable.

If we open up the source code that ends up handling this format request it looks like this.

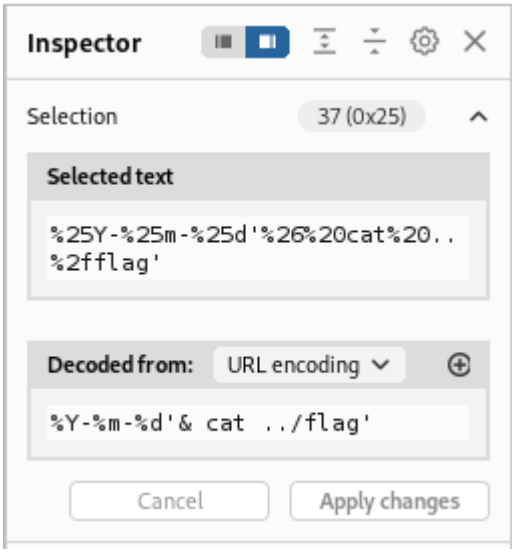
```php
<?php
class TimeModel
{
    public function __construct($format)
    {
        $this->command = "date '+" . $format . "' 2>&1";
    }

    public function getTime()
    {
        $time = exec($this->command);
        $res  = isset($time) ? $time : '?';
        return $res;
    }
}
```

Since there is no sanitization done on the input and seeing that we are returning command output my first assumption was that the site is vulnerable to command injection.

I opened up burpsuite and started attacking the format variable based on the built string in the source code.

I sent the get request to the burpsuite repeater and was able to get the flag with this payload



Solved.