Input Validation

Christian Wenz

@chwenz

Demo

Introducing our online shop

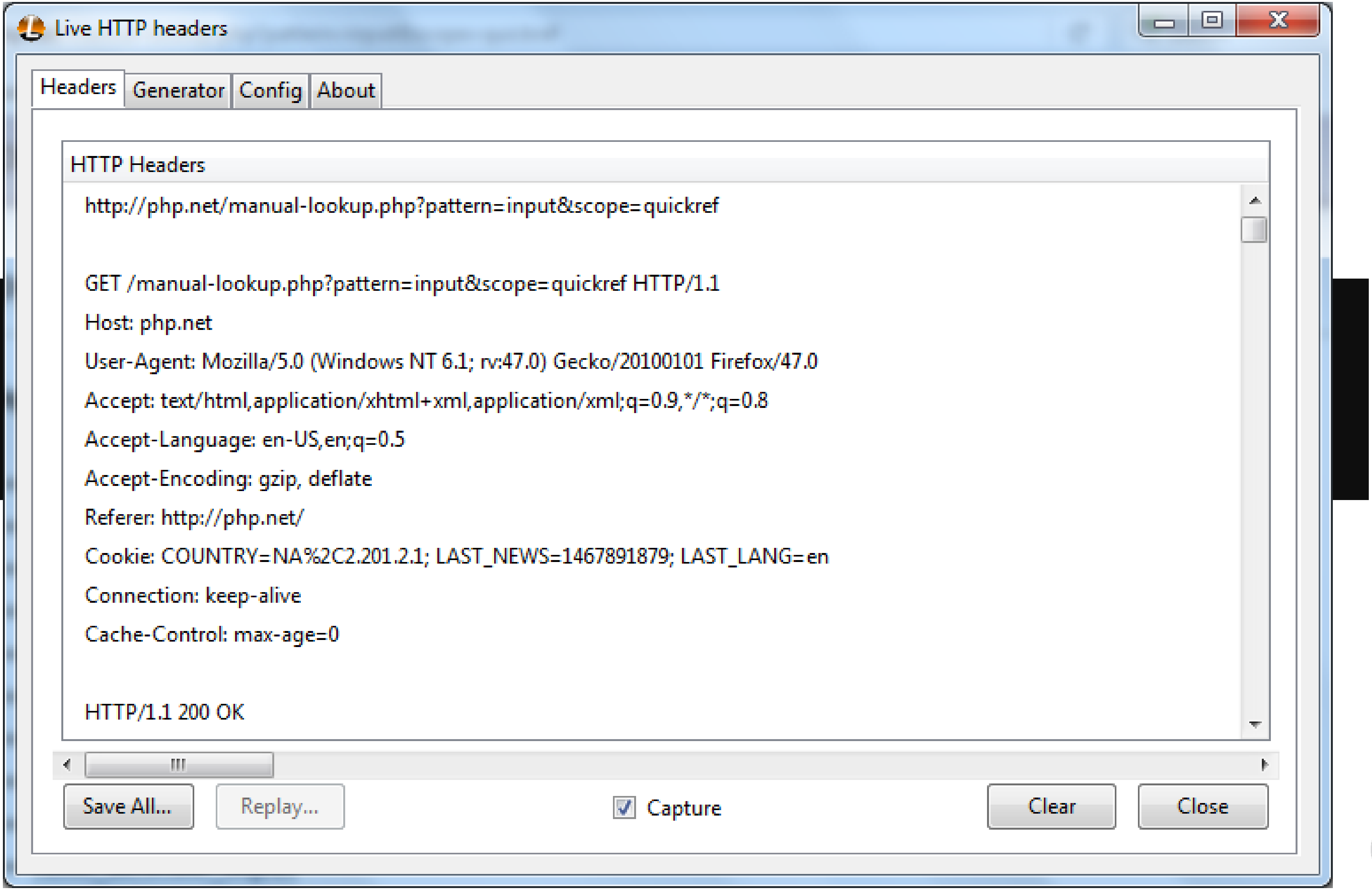
Registration

Logging in

Putting items up for sale

Searching for items

Buying items



```
http://php.net/manual-lookup.php?pattern=input&scope=quickref


GET /manual-lookup.php?pattern=input&scope=quickref HTTP/1.1
Host: php.net
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://php.net/
Cookie: COUNTRY=NA%2C2.201.2.1; LAST_NEWS=1467891879; LAST_LANG=en
Connection: keep-alive
Cache-Control: max-age=0


HTTP/1.1 200 OK
```

Further Input Sources

$_REQUEST

$_ENV

$HTTP_*_VARS

$_SESSION

Demo

Hacking our shop

Sending spam

Getting a deep discount

Validating Input

Is there any data?

isset()

?? operator

is_*()

Searching strings

strpos()

stripos()

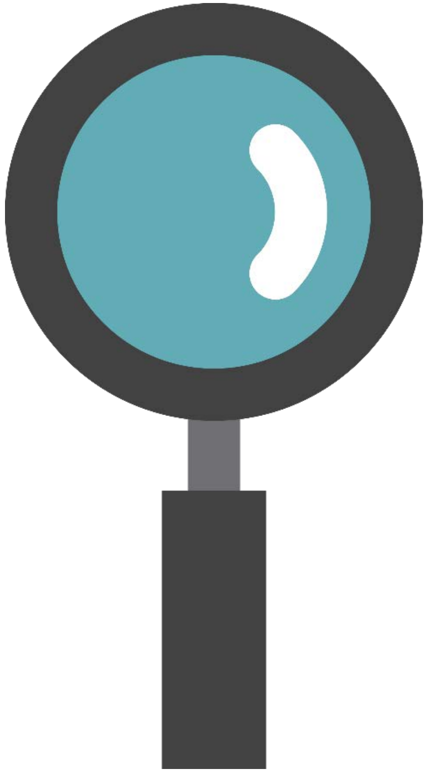
strrpos()

strripos()

Searching patterns

Regular expressions

ctype Extension



ctype_alnum

ctype_alpha

ctype_cntrl

ctype_digit

ctype_graph

ctype_lower

ctype_print

ctype_punct

ctype_space

ctype_upper

ctype_xdigit

is_numeric

```
filter_var(
  ' doe€snöt@€x!st',
  FILTER_SANITIZE_EMAIL)
```

- Validate or sanitize a variable

```
filter_var(
  'X-123.456E789Y',
  FILTER_SANITIZE_NUMBER_FLOAT,
  FILTER_FLAG_ALLOW_SCIENTIFIC
    |
  FILTER_FLAG_ALLOW_FRACTION)
```

- Validate or sanitize a variable, using options

```
filter_has_var(
  INPUT_GET, 'id')
```

- Check whether an input variable has been set

```
filter_input(
  INPUT_GET,
  'id',
  FILTER_VALIDATE_INT);
```

- Validate or sanitize an input variable

PHP 7+ Type Declarations

```php
<?php
declare(strict_types=1);

function add(int $a, int $b): int {
    return $a + $b;
}

$three = add('1', 2);
```

Summary

Validate input

Everything in the HTTP request can be manipulated

Use PHP's ctype and filter extensions