

1. Cookie set without HttpOnly flag

Cookie: httponly; true; http; cookie, javascript; cookie; , XSS

:

PHP

PHP5.2 HttpOnly HttpOnly php.ini

session.cookie_httponly =

1 TRUE Cookie HttpOnly

```
<?php ini_set("session.cookie_httponly", 1);
```

```
// or session_set_cookie_params(0, NULL, NULL, NULL, TRUE);
```

```
?>
```

Cookie `setcookie` `setrawcookie` 7 `HttpOnly`

```
setcookie("abc", "test", NULL, NULL, NULL, NULL, TRUE);
```

```
setrawcookie("abc", "test", NULL, NULL, NULL, NULL, TRUE);
```

PHP5.1 PHP4 `header`

```
<?php header("Set-Cookie: hidden=value; httpOnly"); ?>
```

@=====

2.X-Frame-Option

: iframe , X-Frame-Options

```
:header('X-Frame-Options:Deny');
```

```
:header('X-Frame-Options:Deny');
```