作者是 Administrator
週一, 13 十月 2014 15:10 - 最近更新 週一, 13 十月 2014 15:28

1. Cookie set without HttpOnly flag

原因:意思是:httponly設置為true則只能通過http操縱cookie,這樣防止了javascript等腳本語言對cookie做修改,幫助我們有效的防止XSS攻擊
.

解決方法:

PHP中的設置

PHP5.2以上版本已支持HttpOnly參數的設置，同樣也支持全局的HttpOnly的設置，在php.ini中

---------------- - - - - - - - - - ---------------- - - - - - - - - - - - -

session.cookie_httponly =

---------------- - - - - - - - - - ---------------- - - - - - - - - - - - -

設置其值為1或者TRUE，來開啟全局的Cookie的HttpOnly屬性，當然也支持在代碼中來開啟：

---------------- - - - - - - - - - ---------------- - - - - - - - - - - - -

<?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');