УДК 004.415.5
М. Потикевич
(Тернопільський національний технічний університет імені Івана Пулюя)

ЗАХИСТ CMS 1С:БІТРІКС ВІД АТАК ТИПУ «МІЖСАЙТОВИЙ СКРИПТИНГ» ЗАСОБАМИ BITRIX FRAMEWORK

UDC 004.415.5
M. Potykevych
(Ternopil Ivan Puluj National Technical University, Ukraine)

PROTECTING CMS 1:C BITRIX FROM CROSS-SITE SCRIPTING ATTACKS BY BITRIX FRAMEWORK

Веб-форми – це стандартний модуль у CMS 1С:Бітрікс. Часто трапляється так, що спам боти надсилають повідомлення з Javascript-ом у тексті і при відвідуванні сторінок з цими скриптами на сторінці відбуваються якісь дії, надсилються на зовнішні ресурси інформація про сесії користувачів також можливі витоки конфіденційної інформації.

Для запобігання такии випадкам, нами було написано скрипт-фільтр, який відслідковує небезпечні комбінації символів, які потрапляють у результати веб-форм.

Даний скрипт поміщається у файл init.php, що знаходиться за адресою /bitrix/php_interface/init.php.

```
function my_onBeforeResultAdd($WEB_FORM_ID, &$arFields, &$arrVALUES){
	global $APPLICATION;
	//form_text_25 - Sм'я користовача, form_text_58 - текст повідомлення
	if ($WEB_FORM_ID == 12 && !empty($arrVALUES['form_text_25']) &&
!empty($arrVALUES['form_text_58']){
		$values_for_filter = array('<','>','script','$(',').','function','ById','$(\"','getElement','<s','/>');

		if (in_array($arrVALUES['form_text_25'],$values_for_filter)
			|| in_array($arrVALUES['form_text_58'],$values_for_filter)){
			//Віддаємо помилку
			$APPLICATION->ThrowException('Вміст текстових було визнано
небезпечними. Ваше повідомлення не буде надіслано.');
			$el = new CIBlockElement;
			$arLoadProductArray = Array(
				"IBLOCK_ID"	=> 21,	//ID інфоблоку попереджень
				"NAME"		=> "Помилка додавання результату веб-форми",
				"ACTIVE"	=> "Y",	// Активність
				"DETAIL_TEXT"	=> "Була спроба додати потенційно шкідливий
результат ")
			);
			$el->Add($arLoadProductArray)
		}
	}
}
```

Отже, в результаті розробки даного скрипа було підвищено рівень захисту CMS 1С-Бітрікс, а саме створено додатковий фільтр для веб-форм, який перевіряє вхідний текст на наявність можливих атак типу «Міжсайтовий скриптинг».