Список тестируемых сайтов

Название сайта	ФИО студента	Адрес	Разработан
1. ScienceRise: Medical Science	Дідковський Д.Є.	http://med.sr.org.ua/	CMS «JOOMLA 3.9.3»
2. Scientific Route	Загребельний В.В.	http://journal.eu-jr.eu/	CMS «OJS 3»
3. ScienceRise: Pedagogical Education	Козюберда Д.О.	http://edu.sr.org.ua/	CMS «JOOMLA 3.9.3»
4. Technology audit and production reserves	Кононенченко А.В.	http://www.tarp.net.ua/	CMS «JOOMLA 3.9.3»
5. Eastern-European Journal of Enterprise Technologies	Кравченко Є.М.	http://jet.com.ua/	CMS «JOOMLA 3.9.3»
6. Scientific Route	Малишев С.В.	https://www.route.ee/	CMS «JOOMLA 3.9.8»
7. ScienceRise: Pharmaceutical Science	Пономаренко В.В.	http://pharm.sr.org.ua/	CMS «JOOMLA 3.9.3»
8. ScienceRise: Biological Science	Попенко В.О.	http://bio.sr.org.ua/	CMS «JOOMLA 3.9.3»
9. Technology Center	Поповська Є.О.	http://monograph.com.ua/	CMS «OMP 3»
10. ScienceRise: Juridical Science	Суслик М.І.	http://law.sr.org.ua/	CMS «JOOMLA 3.9.3»

Для прохождения практики необходимо использовать дистрибутив **Kali Linux**

Полезные источники:

- Восстановление сайта Joomla (инструкция):

https://tryhimself.ru/joomla/vosstanavlivaem-sajt-na-dzhumla-kopiej-iz-akeeba-backup

- Скачать дистрибутив Kali Linux:

https://www.kali.org/downloads/

- Инструменты Kali Linux для взлома

https://www.fossmint.com/kali-linux-hacking-and-penetration-tools/

https://itsfoss.com/best-kali-linux-tools/

- Официальный сайт ПО PKP (CMS “OJS”, “OMP”)

https://pkp.sfu.ca/

Пример оформления результатов проверки:

⚠ Раскрытие исходного кода

Опасность	Высокая

Описание

Получение исходного кода скрипта.

Возможные последствия

Злоумышленник может получить важную информацию, для использования в дальнейшей атаке.

Рекомендации

Проанализируйте свой исходный код и устраните проблему.

Уязвимость

Уязвимый скрипт: /showimage.php

Уязвимый параметр: file

Детали

GET запросом параметр file был установлен в showimage.php
Был получен исходный код:

```
<?php
// header("Content-Length: 1" /*. filesize($name)*/);
if( isset($_GET["file"]) && !isset($_GET["size"]) ){
        // open the file in a binary mode
        header("Content-Type: image/jpeg");
        $name = $_GET["file"];
        $fp = fopen($name, 'rb');

        // send the right headers
        header("Content-Type: image/jpeg");

        // dump the picture and stop the script
        fpassthru($fp);
        exit;
}
elseif (isset($_GET["file"]) && isset($_GET["size"])){
        header("Content-Type: image/jpeg");
        $name = $_GET["file"];
        $fp = fopen($name.'.tn', 'rb');

        // send the right headers
        header("Content-Type: image/jpeg");

        // dump the picture and stop the script
        fpassthru($fp);
        exit;
}
?>
```

Заголовки запросов HTTP

```
GET /showimage.php?file=showimage.php HTTP/1.1
Cookie: mycookie=3
Host: site.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
```