Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

Задание 1: Шйdχdнх VQQ ʒй ʜнлйʒdъх VQQ&Qrmpcb' Ллʒхdнй BTU ? ʒй Лл ʒʜнʒъ &Jmu' Gлʒʓʒх ʜъʒxʒʒʜнd d ʒЛлхχхъdнх хх нdЛ, Ьʒʜнйʓqнх ʒнЄхн ʒ ʒйdχхʒʒʒdʒ G d ʓdъʒʜнd, H ʒнЄхнх Gdйxdнх* ʓ dйdʒъ dʒʒнхdʜнх ЛлdʜGнʜнʓGхн VQQ,

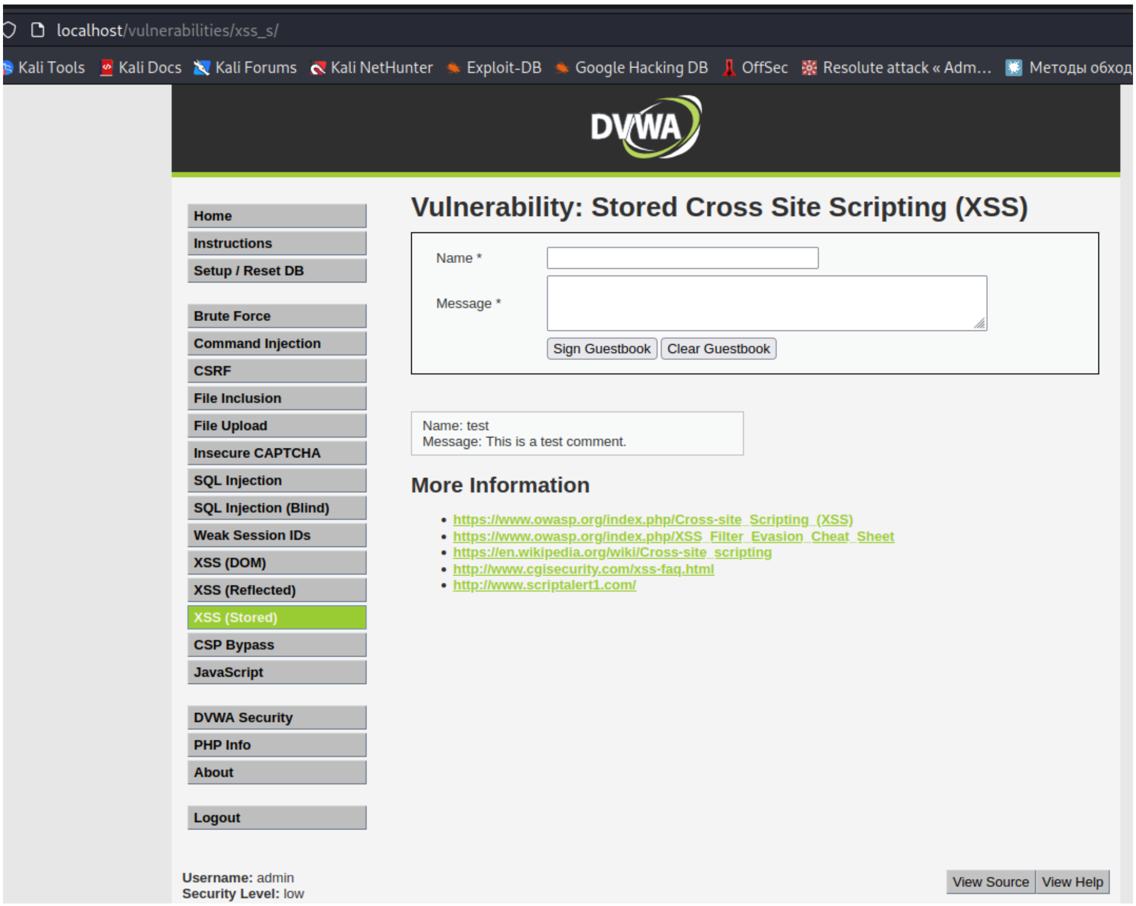
Oχх ʒйdχхʒй G dʓdъʒʜнq
Э dʓdъʒʜнq ʒйdχхʒй Лʒ йχлхʜG
frrnq8--localhost/vulnerabilities/xss_s/

Наименование продукта: DVWA

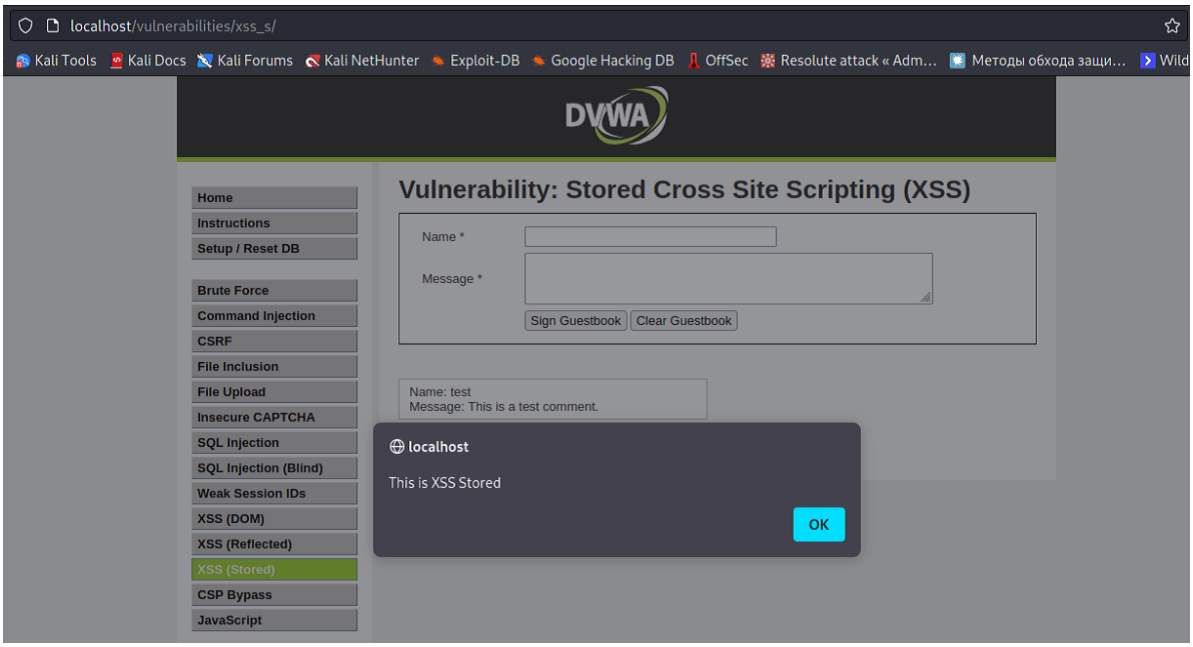
ЭхЂʒdЄхʜdх χхнйъd ʒʓʒйлGxхʒd dʓʒʜЛлʒddʓхχхʒd :
Э dʓdъʒʜнq ʓQъй ʒʓʒйлGxхʒй ʓ Ђʒχх "исследования представленного сайта" на котором представлена форма вида "форум" с возможностью оставлять сообщения на сайте. Форма ввода "Сообщение" уязвима для атаки XSS-Stored. Данная уязвимость присутствует в контексте JavaScript.

Выводы и рекомендации по устранению:
Необходима настройка валидации входных данных. Экранирование вывода. Настройка CSP.

Используемое ПО:
MлйGdхл Dgpcdmv `pmuqcp /.0,6,.cqp &42+`gr'



```php
<?php

if( isset( $_POST[ 'btnSign' ] ) ) {
    // Get input
    $message = trim( $_POST[ 'mtxMessage' ] );
    $name    = trim( $_POST[ 'txtName' ] );

    // Sanitize message input
    $message = stripslashes( $message );
    $message = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $message ) : ((trigger_error("
[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Sanitize name input
    $name = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_escape_string($GLOBALS["___mysqli_ston"],  $name ) : ((trigger_error("
[MySQLConverterToo] Fix the mysql_escape_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));

    // Update database
    $query  = "INSERT INTO guestbook ( comment, name ) VALUES ( '$message', '$name' );";
    $result = mysqli_query($GLOBALS["___mysqli_ston"],  $query ) or die( '<pre>' . ((is_object($GLOBALS["___mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_c

    //mysql_close();
}

?>
```



Задание 2: Найдите XSS на странице XSS(Reflected) проекта DVWA на простом (Low) уровне сложности и определите ее тип. Составьте отчет о найденной уязвимости. В отчете укажите, в каком контексте присутствует XSS.

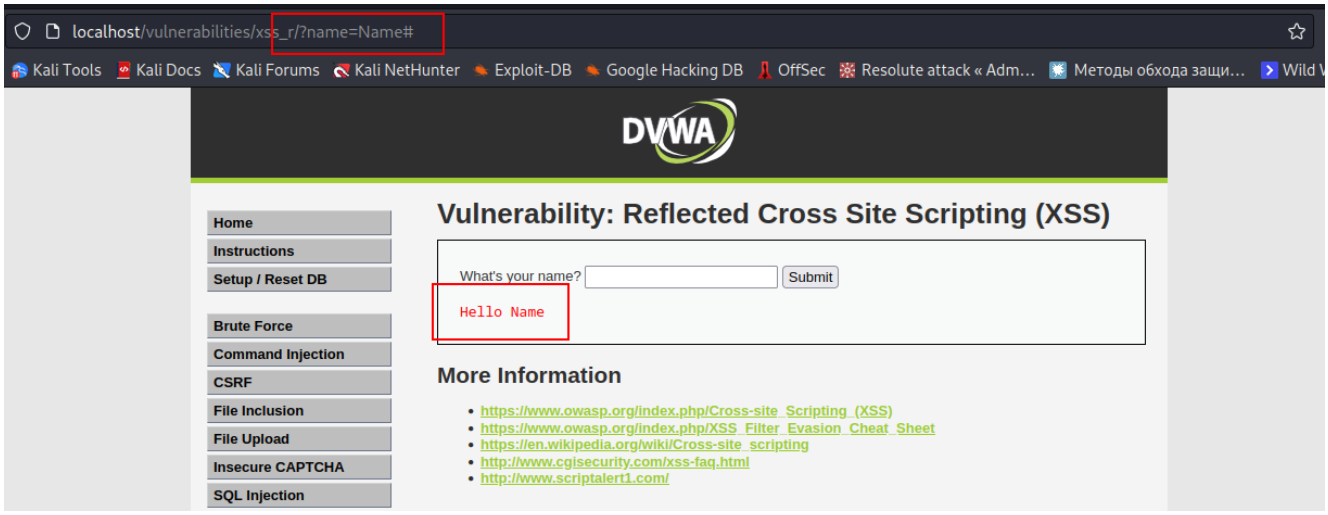
Где найдена уязвимость
Уязвимость найдена по адресу
https://localhost/vulnerabilities/xss_r/

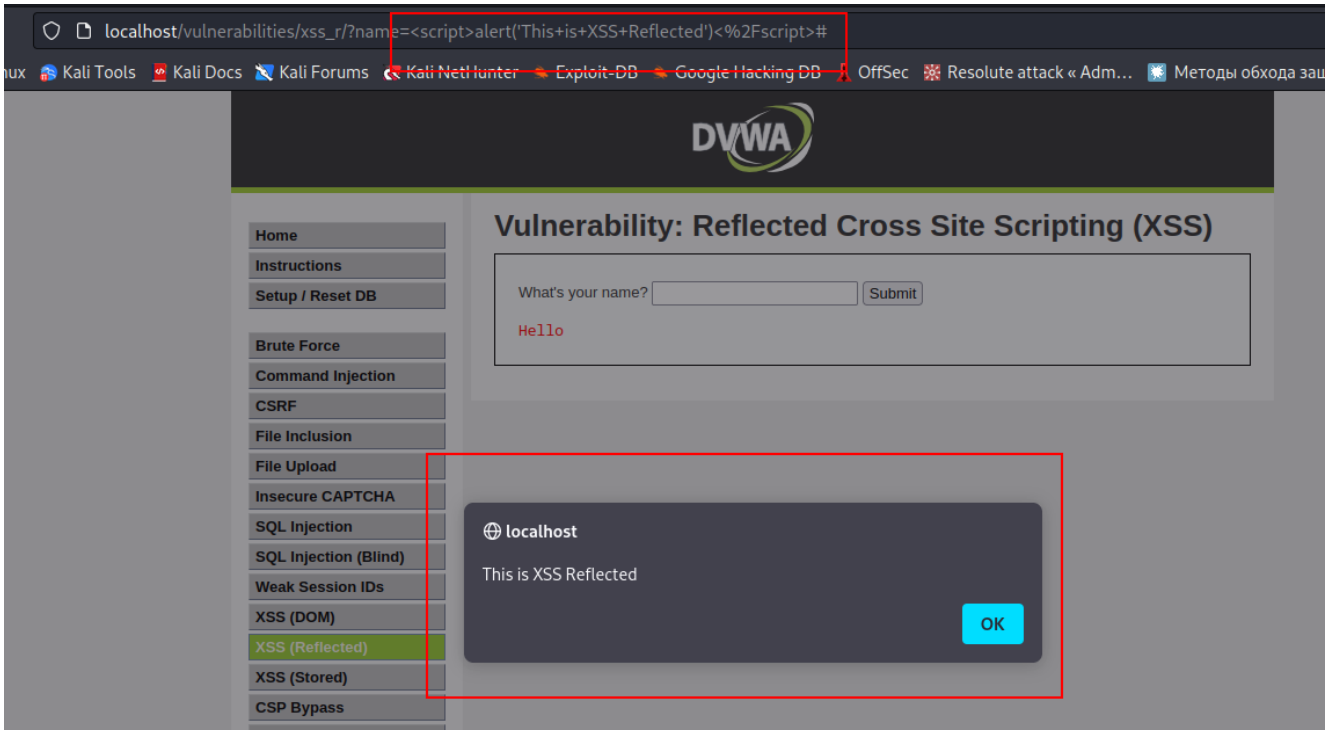
Наименование продукта: DVWA

Технические детали обнаружения и воспроизведения:
Уязвимость была обнаружена в ходе "исследования представленного сайта" на котором представлена форма вида "форум" с возможностью оставлять сообщения на сайте. Форма ввода "Сообщение" уязвима для атаки XSS-Reflected. Данная уязвимость присутствует в контексте JavaScript.

Выводы и рекомендации по устранению:
Необходима настройка валидации входных данных. Экранирование вывода. Настройка CSP.

Используемое ПО:
Браузер Firefox browser 102.8.0esr (64-bit)





Задание 3: Найдите XSS на странице XSS(DOM) проекта DVWA на простом (Low) уровне сложности и определите ее тип. Составьте отчет о найденной уязвимости. В отчете укажите, в каком контексте присутствует XSS.

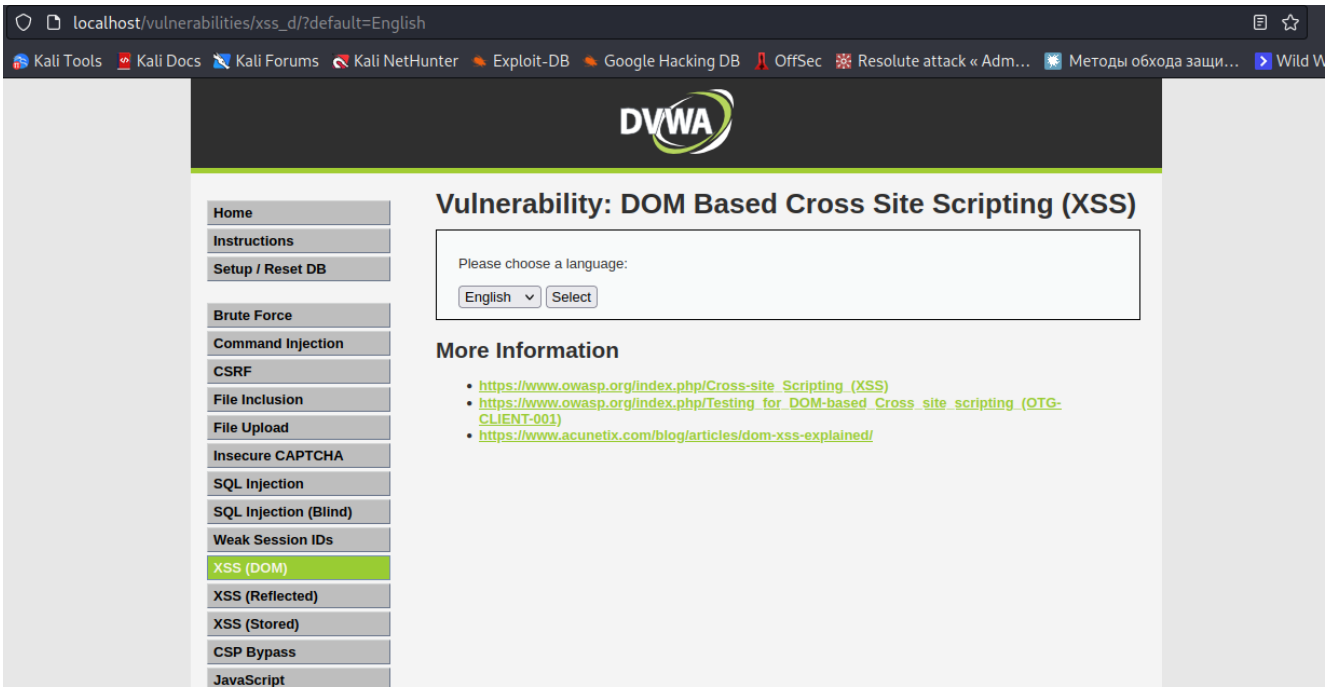
Где найдена уязвимость
Уязвимость найдена по адресу
https://localhost/vulnerabilities/xss_d/

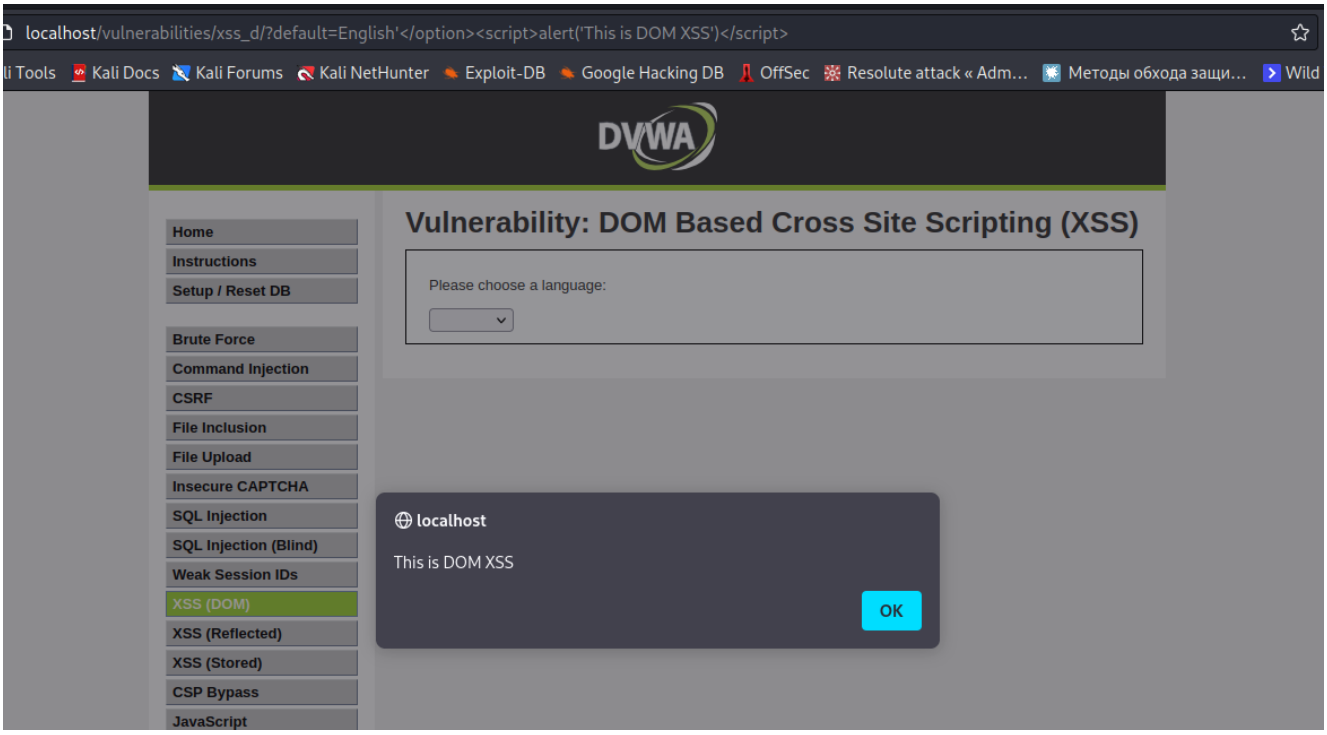
Наименование продукта: DVWA

Технические детали обнаружения и воспроизведения:
Уязвимость была обнаружена в ходе "исследования представленного сайта" на котором представлена форма выбора из выпадающего списка. Уязвимость обнаружена и проэкслплуатирована строке браузера - XSS-DOM. Данная уязвимость присутствует в контексте document.write.

Выводы и рекомендации по устранению:
Необходима настройка валидации входных данных. Экранирование вывода. Настройка CSP.

Используемое ПО:
Браузер Firefox browser 102.8.0esr (64-bit)


localhost/vulnerabilities/xss_d/?default=English
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Resolute attack « Adm...
Методы обхода защи...
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: DOM Based Cross Site Scripting (XSS)
Please choose a language:
English
Select
More Information
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)
https://www.acunetix.com/blog/articles/dom-xss-explained/


localhost/vulnerabilities/xss_d/?default=English'</option><script>alert('This is DOM XSS')</script>
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Resolute attack « Adm...
Методы обхода защи...
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Vulnerability: DOM Based Cross Site Scripting (XSS)
Please choose a language:
localhost
This is DOM XSS
OK