

Описание уязвимости

На сайте http://192.168.56.103/dvwa/vulnerabilities/xss_d/ отсутствует фильтрация вводимых пользователем данных. Это позволяет удалённо выполнять JS код на странице и инжектировать HTML-сущности.

Где найдена уязвимость

Уязвимость расположена по адресу http://192.168.56.103/dvwa/vulnerabilities/xss_d/.
Наименование продукта: DVWA.

Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить, если выбрать любой из предоставленных в списке языков, нажать кнопку «Select». После этого в адресной строке появится переменная «default» со значением того языка, который был выбран.
Теперь в значение этой переменной можно написать любой HTML-тег, и нажать Enter.

192.168.56.103/dvwa/vulnerabilities/xss_d/?default=<script>alert('DOM-based XSS')</script>

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection


CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection



Vulnerability: DOM Based Cross Site Scripting (XSS)

Please choose a language:

Select

More Information

- [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](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.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001))
- <https://www.acunetix.com/blog/articles/dom-xss-explained/>

Elements

Console

Sources

Network

Performance

Memory

Application

Security

▼<select name="default">

▶<script>...</script>

▼<option value="%3Cscript%3Ealert(%27DOM-based%20XSS%27)%3C/script%3E">

<script>alert('DOM-based XSS')</script> == \$0

</option>

<option value disabled="disabled">----</option>

<option value="English">English</option>

<option value="French">French</option>

<option value="Spanish">Spanish</option>

<option value="German">German</option>

</select>

Выводы и рекомендации по устранению

Выводы:

Тип уязвимости: DOM-based XSS.

Контекст уязвимости: HTML.

Уязвимость позволяет получить доступ к конфиденциальной информации. Не требует дополнительных уязвимостей для эксплуатации.

Рекомендации по устранению:

- Сделать фильтрацию вводимых пользователем данных на уровне разработки.

Используемое программное обеспечение

- Google Chrome