

Все скрины предоставлены для уровня LOW

## XSS\_Stored

Нормальное состояние -

**Vulnerability: Stored Cross Site Scripting (XSS)**

Name \*

Message \*

Name: test  
Message: This is a test comment.

**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/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Уязвимость со вставкой frame- прописывает скрипт

**Vulnerability: Stored Cross Site Scripting (XSS)**

Name \*

Message \*

Name: test  
Message: This is a test comment.

**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/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

На выходе получаем

Name \*

Message \*

Sign Guestbook Clear Guestbook

Name: test  
Message: This is a test comment.

Name: Test  
Message:

WIKIPEDIA  
The Free Encyclopedia

Main page  
Contents  
Featured content

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/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)

т.е. отображается страничка

Уязвимость с выводом через alert

Вводим скрипт

**Vulnerability: Stored Cross Site Scripting (XSS)**

Name \* Test

Message \* `<script>alert('xss_test!')</script>`

Sign Guestbook Clear Guestbook

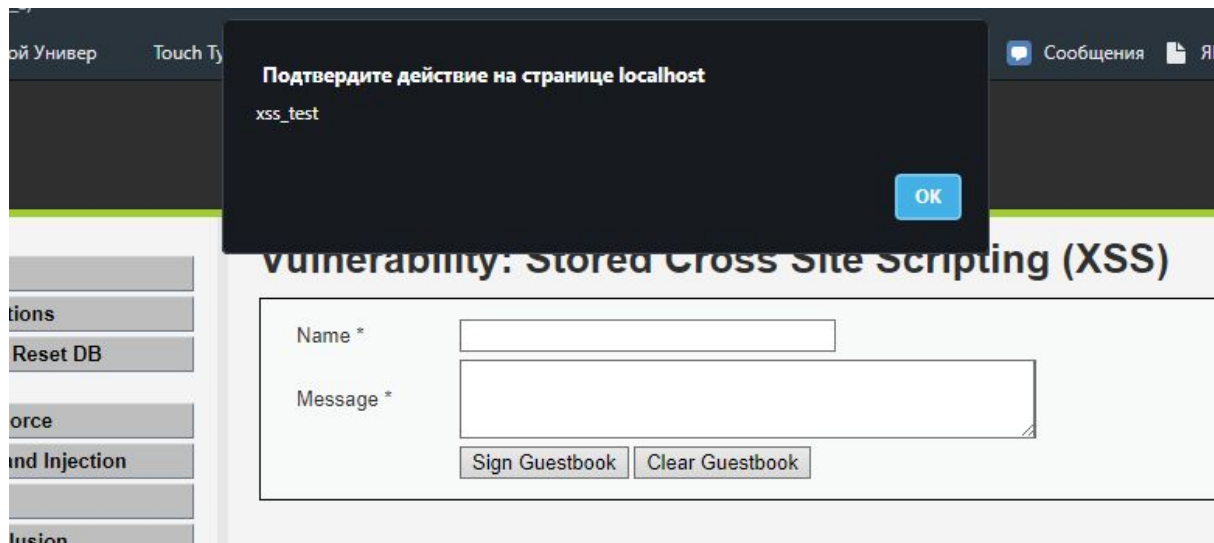
Name: test  
Message: This is a test comment.

Name: Test  
Message:

Name: Test  
Message:

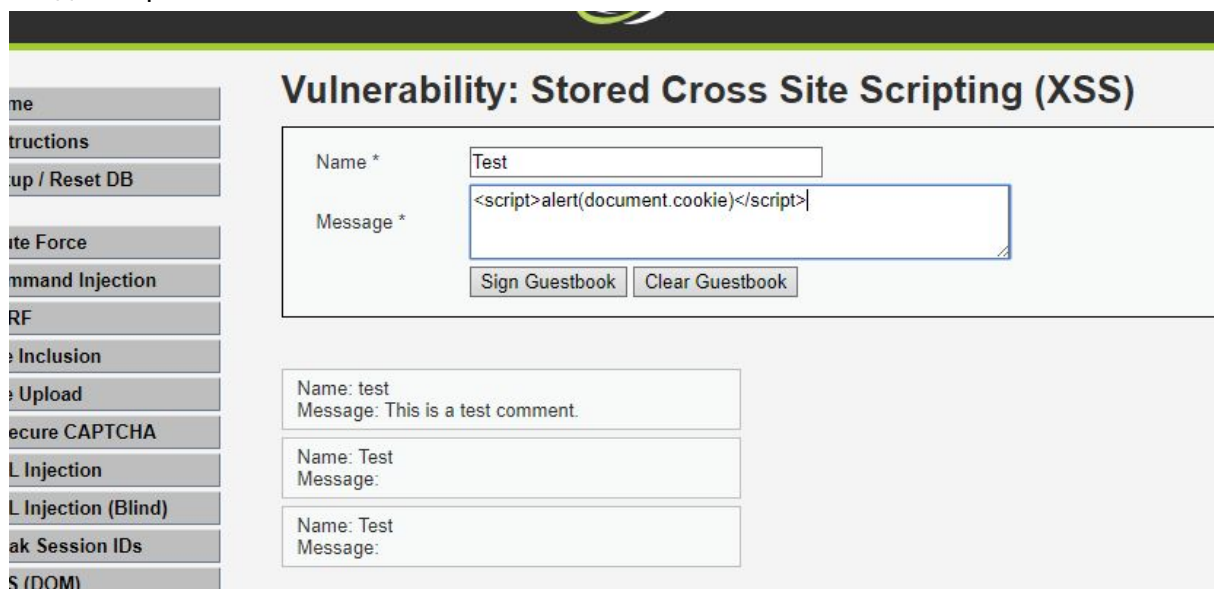
Name: Test  
Message:

Получаем

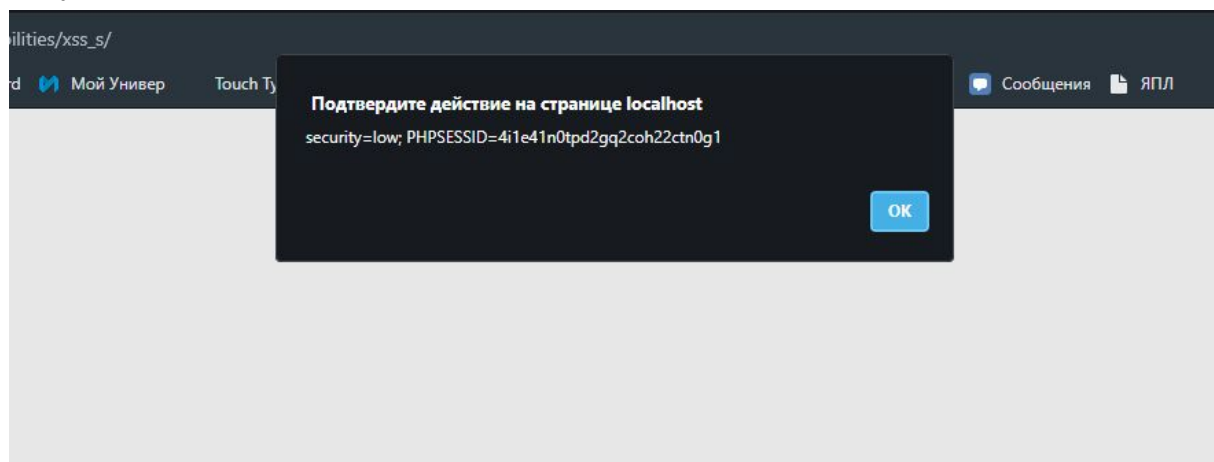


Уязвимость с получением cookie

Вводим скрипт



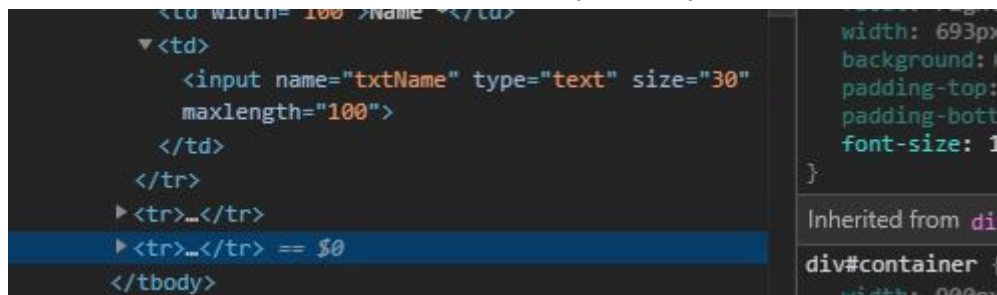
Получаем



Также данные скрипты возможно ввести в поле Name, но там стоит ограничение длины сообщения



чтобы это исправить меняем максимальную длину сообщения



И вводим нужный нам скрипт



Разница различных уровней защиты:

LOW - нет проверки на спецсимволы

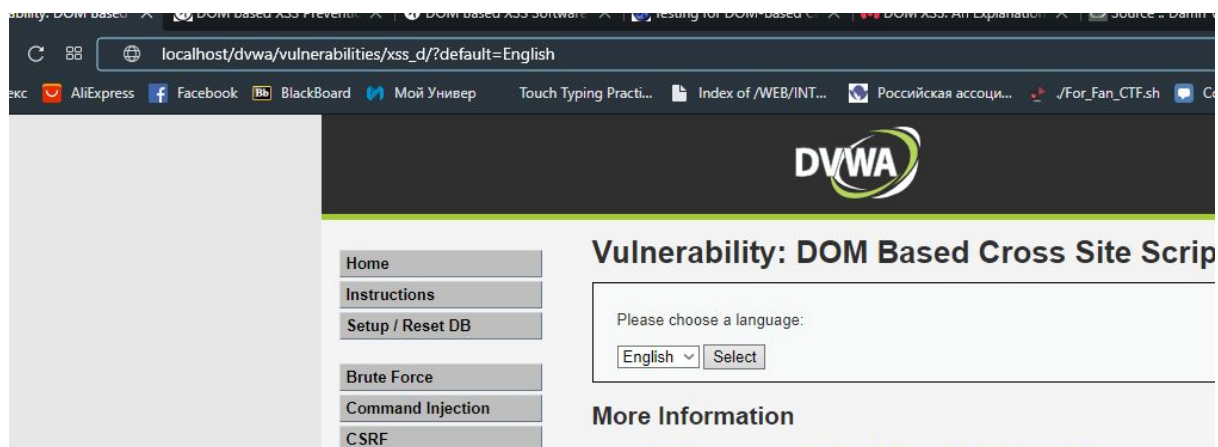
MEDIUM - проверка на спецсимволы для сообщений, для name ограничение на `<script>`

HIGH - проверка на спецсимволы для сообщений, для name ограничение на `<script>` через регулярки

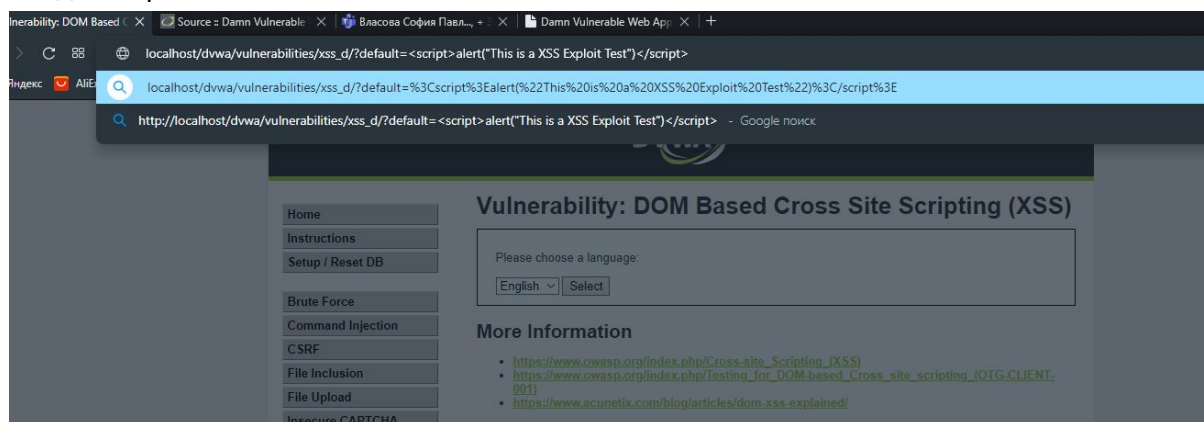
IMPOSSIBLE - проверка на спецсимволы для имени и сообщений

## XSS\_Dom

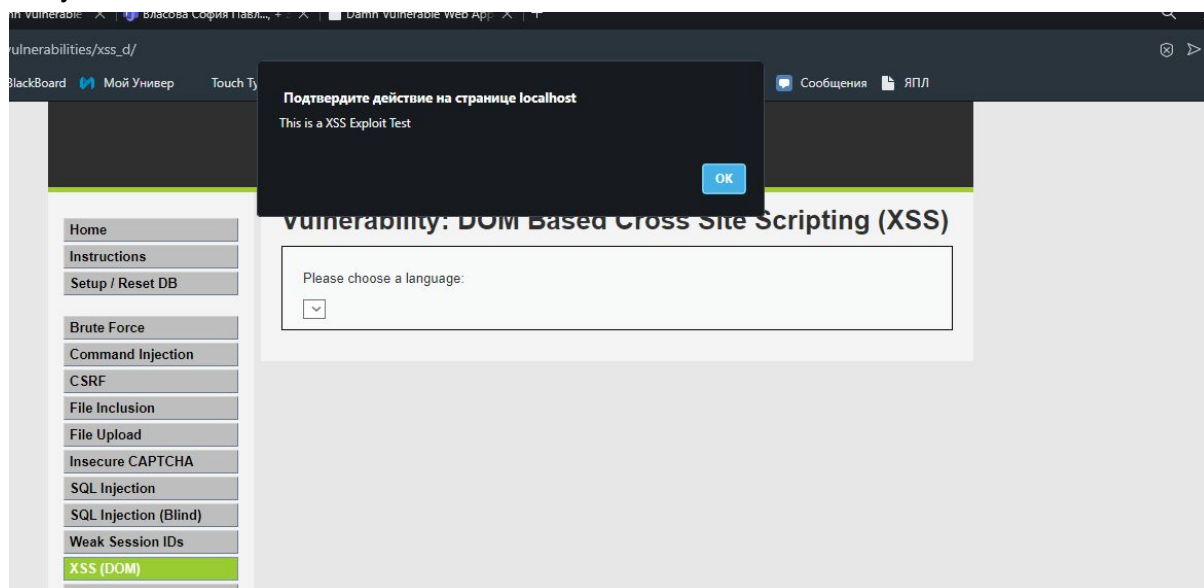
Нормальное состояние



Уязвимость через alert  
Вводим скрипт после `*?default=`

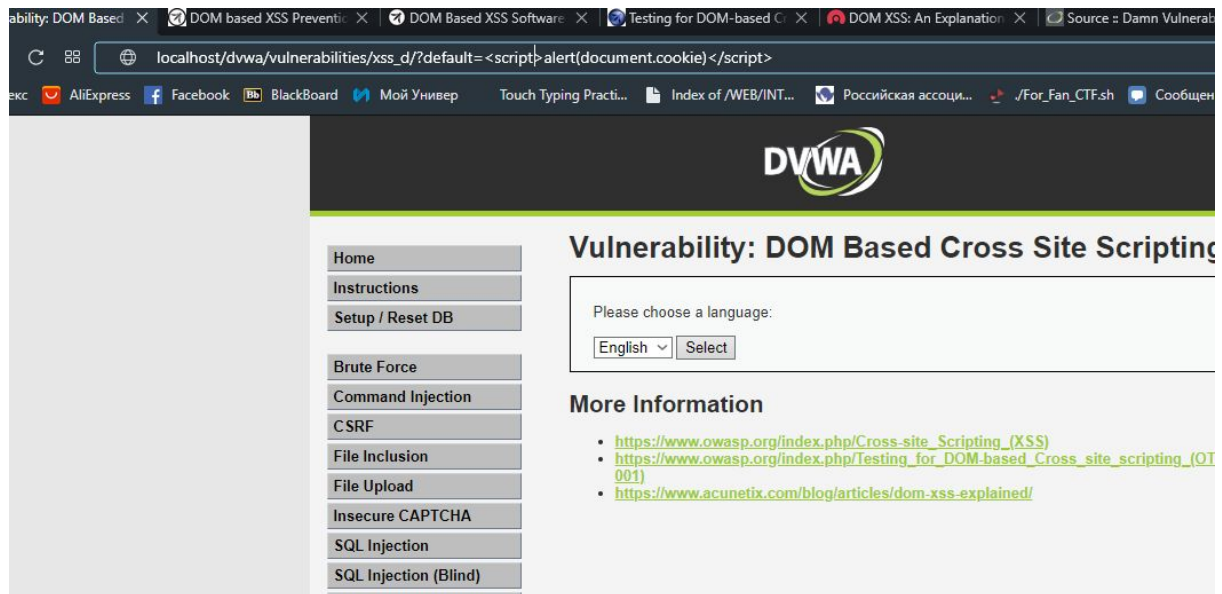


Получаем

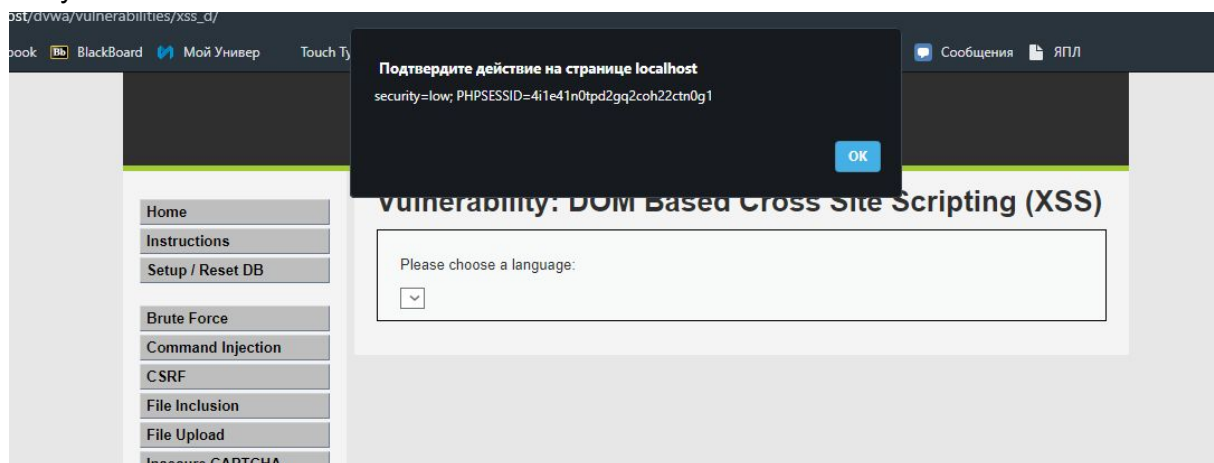


Уязвимость с cookie  
Вводим скрипт





Получаем



Различия уровней защиты:

LOW - нет защиты

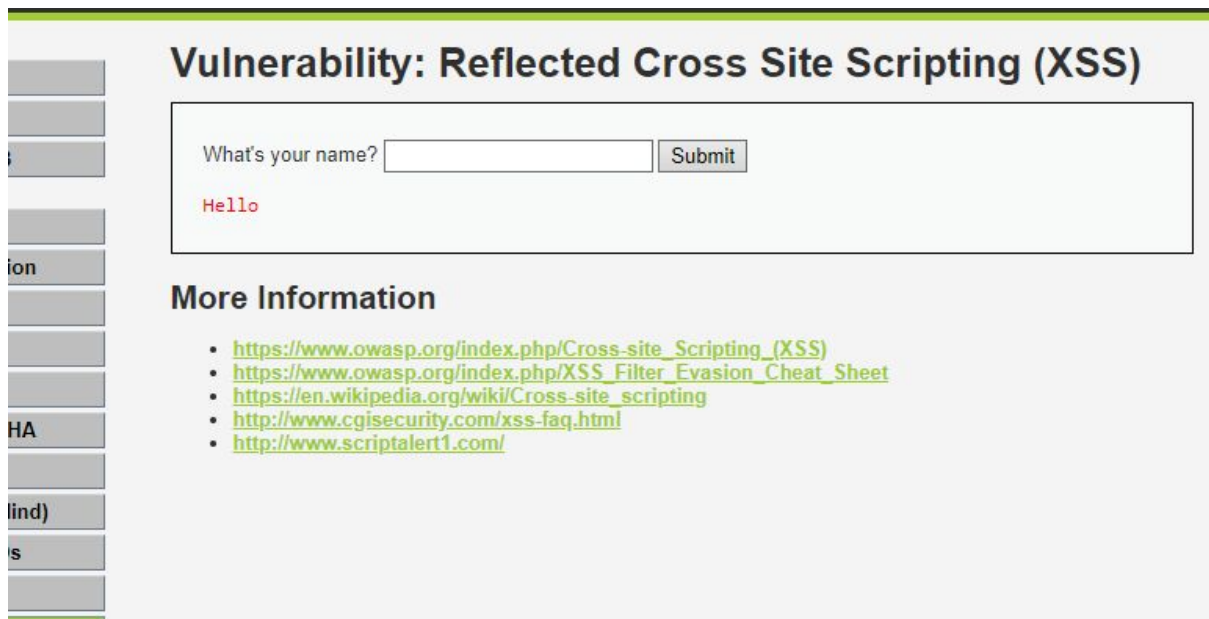
MEDIUM - проверка на <script, поэтому необходимы другие способы, например onload=alert("XSS")

HIGH - возможны только predefined значения, поэтому нужно запустить скрипт не заходя на сервер, тут помогает #, т.е. пишем, после \*default=English#скрипт

IMPOSSIBLE - описания нет, но судя по всему ничего не сделать

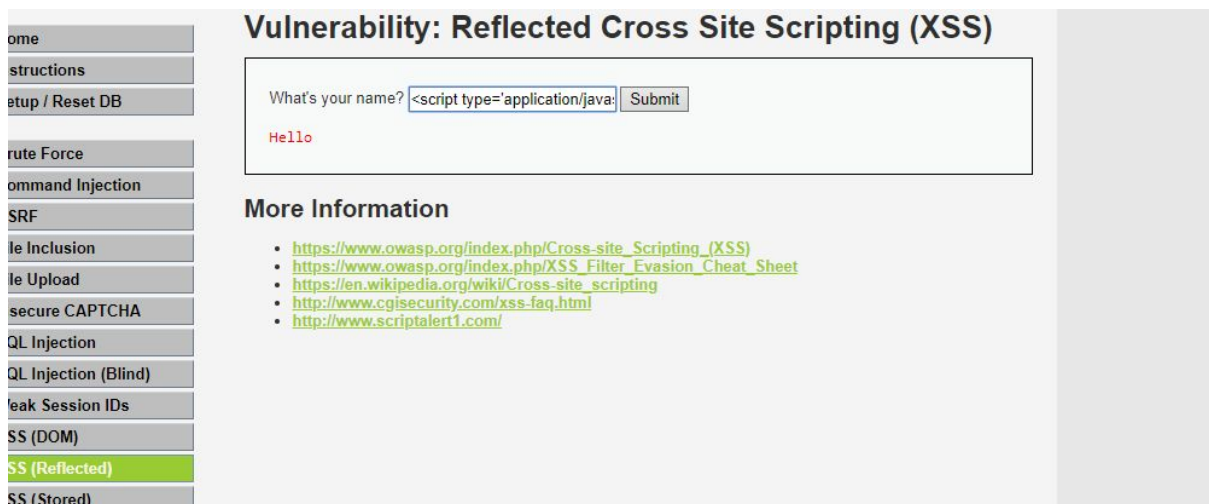
**XSS\_Reflected**

*Нормальное состояние*

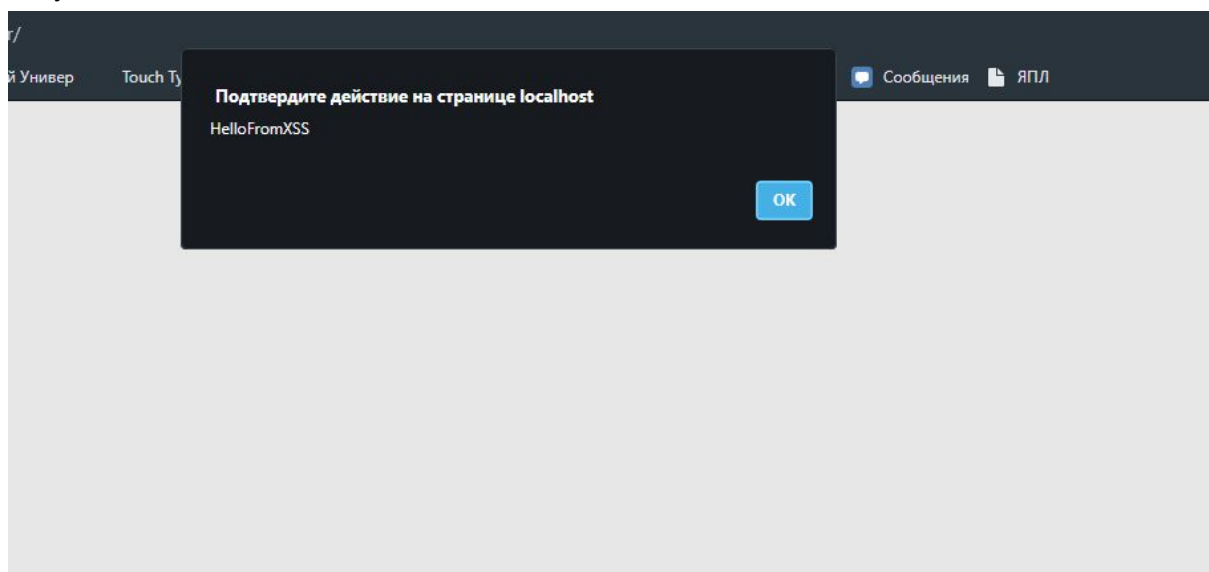


Уязвимость через alert

Вводим скрипт



Результат



Уязвимость с cookie

Вводим скрипт

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)**

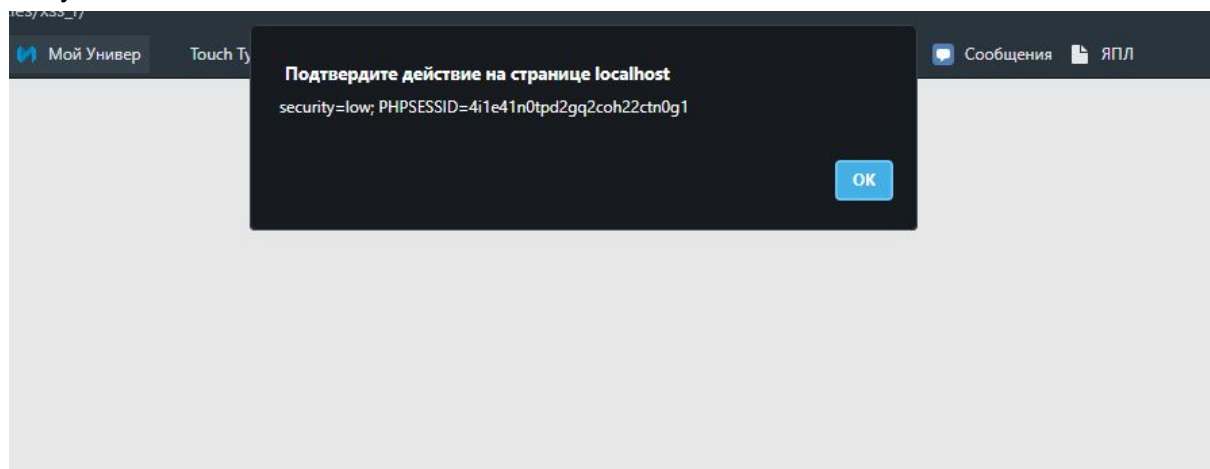
## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

### 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/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Получаем



Уязвимость с frame

Вводим скрипт

DB

ection

TCHA

(Blind)

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello

### 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/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Получаем



DB
  
ction
  
CHA
  
Blind)
  
IDs

What's your name?



Not logged in  
[Talk](#) [Contributions](#)  
[Create account](#)  
[Log in](#)

More  Search

Hello **WIKIPEDIA**

### 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/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)

Уязвимость с ссылкой на другой сайт(href)

Вводим скрипт

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)**

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

### 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/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Получаем

Home
  
Instructions
  
Setup / Reset DB
  
Brute Force
  
Command Injection
  
CSRF
  
File Inclusion
  
File Upload
  
Insecure CAPTCHA
  
SQL Injection
  
SQL Injection (Blind)

## Vulnerability: Reflected Cross Site Scripting (XSS)

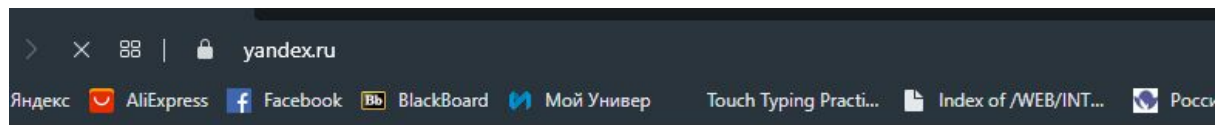
What's your name?

Hello [Click here](#)

### 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/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Кликаем по ссылке, нас перекидывает на другой сайт



Владивосток Конфиденциальность

Сейчас в СМИ во Владивостоке Коронавирус 5.05, 17 33

В России запретили работу «наливаек» в жилых домах

Пилот сгоревшего в Шереметьево Superjet впервые дал интервью

Инициатор демонтажа памятника Коневу в Праге пожаловался на Россию

Уровни безопасности:

LOW - нет защиты

MEDIUM - проверка на <script

HIGH - проверка на <script через регулярки

IMPOSSIBLE - проверка на спецсимволы