Урок 7. Content-Security-Policy

<u>Задание 3:</u>

Составить план защиты сервиса Mutillidae, в рамках которого можно внедрить CSP, не нарушив при этом работу сервиса. Указать, какие дополнительные средства можно внедрить для защиты от XSS.

Ответ:

План составлял с помощью расширения "CSP Tester" в браузере google chrome.

CSP получилось таким:



Задание 4*:

Реализовать защиту сервиса Mutillidae согласно разработанному выше плану.

Ответ:

Для начала я решил найти все вхождения **<script** в файлах mutillidae и заменить их на **<script nonce="123456789"**.

Сделал я это так:

Сначала я нашёл все вхождения **<script** в файлах mutillidae и записал пути к ним в **script.txt**.

grep -r -l "<script" /var/www/html/mutillidae/ | cat > /home/student/scripts.txt

После этого я прошёлся циклом по путям в файле script.txt и при помощи утилиты sed заменил найденные вхождения.

for i in \$(cat /home/student/scripts.txt); do sed -i 's/<script/<script nonce="123456789"/g' \$i;done

Следующим шагом я добавил политику CSP на сервер

<Directory "/mutilidae/">
Header set Content-Security-Policy "default-src 'self'; script-src 'strict-dynamic' 'nonce-123456789'; style-src 'self' 'unsafe-inline'; img-src https://www.paypalobjects.com 'self'
Girectory>

Перезапустил apache и политика CSP внедрена.