Aplikacje webowe

Bezpieczeństwo systemów komputerowych
semestr zimowy, 2020/21

Omówienie zadania na XXE

Atakowanie klienta

Atakowanie klienta - podatność XSS

http://bsk2020.kazet.cc:8012/

Pomocne: https://requestbin.com/

Atakowanie klienta - podatność XSS

http://bsk2020.kazet.cc:8024/

Pomocne do modyfikacji żądań: Burp albo “copy as cURL…” w przeglądarce

Atakowanie klienta - podatność XSS - filtry

http://bsk2020.kazet.cc:8013/

Zbanowałem słowo script (we wszystkich wariantach duże-małe litery)

Omijanie filtrów po stronie serwera

https://portswigger.net/web-security/cross-site-scripting/cheat-sheet

Mniej i bardziej odjechane sposoby omijania filtrów.

Atakowanie klienta - co robić?

Kod

- HTML templates
- Uważać z kodem HTML od użytkownika (edytory WYSIWYG)
- JSON zamiast umieszczania danych surowo w skryptach Javascript

Upload

- Uważać na pliki .html w tej samej domenie (i .svg, i .swf, i co jeszcze czyjej przeglądarce przyjdzie do głowy - Google ma np. upload w innej domenie)
- whitelist typów MIME serwowanych jako nagłówek HTTP plus X-Content-Type: nosniff

Content Security Policy

- co to jest?
- default-src
- connect-src, font-src, frame-src, img-src, manifest-src, media-src, object-src, prefetch-src, script-src, script-src-elem, script-src-attr, style-src, style-src-elem, style-src-attr, worker-src
- nonce

Filtry XSS w przeglądarkach

- co to jest?
- czemu nie warto

Cross-Site Request Forgery

Wyślij w imieniu administratora formularz.

http://bsk2020.kazet.cc:8015/

Cross-Site Request Forgery

A jak się przed tym zabezpieczyć?

Cross-Site Request Forgery

Tutaj też trzeba wysłać w imieniu administratora formularz. Formularz jest zabezpieczony tokenem.

Tokeny CSRF (które trzeba znać, aby wysłany formularz został przyjęty) są standardowym sposobem uniemożliwiania ataków typu CSRF (por. https://sekurak.pl/czym-jest-podatnosc-csrf-cross-site-request-forgery/). Czasem można je obejść, np. tu - jak?

http://bsk2020.kazet.cc:8016/

Zadania nie było na zajęciach - w razie czego, proszę pisać z pytaniami na krzysztof.zajac2@gmail.com.

(bonus) Atakowanie klienta - podatność XSS - CSP

http://bsk2020.kazet.cc:8023/

Zadania nie było na zajęciach - w razie czego, proszę pisać z pytaniami na krzysztof.zajac2@gmail.com.