CrossSiteRequestForgery

Bc. Josef Jebavý

www.josefjebavy.cz

7. 11. 2026

AI napověděla

Vibecoduji...

Bezpečnost CSRF

Osnova

1. AI nápověda
2. Whoami
3. CSRF
4. POST
5. Jak zapnout CSRF
6. Ukázka
7. Doporučení
8. Diskuze

whoami

Bc. Josef Jebavý
Sportovec, filozof, školitel, mentor.
Independent IT konzultant (freelancer)
Software developer, Linux admin, DevOps.
Safe backup including protection against ransomware



Zkratky

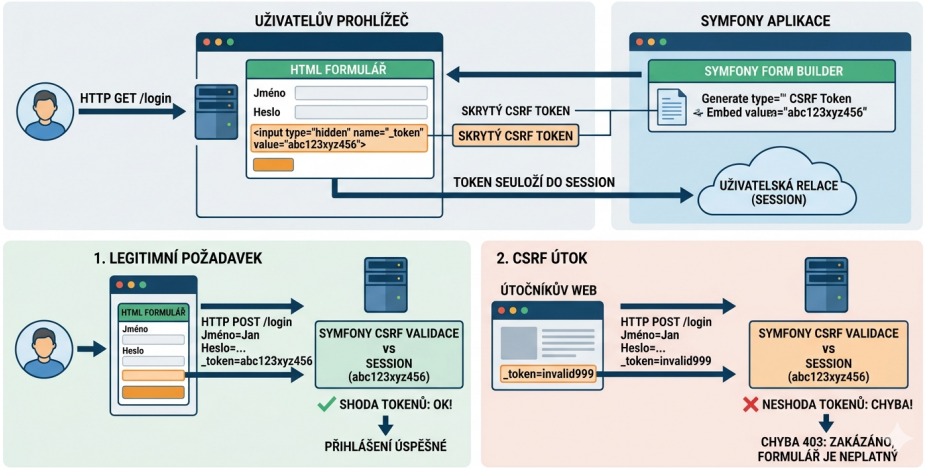
XSS
CSRF

CSRF

Cross -
Site -
Request -
Forgery -

Jak to funguje

JAK FUNGUJE CSRF OCHRANA V SYMFONY



Prohlížeč

Moderní prohlížeč: SameSite – HTML tag img

CSRF a framework

Nette
Symfony
a další

GET POST

GET $\rightarrow$ POST

Jak zapnout CSRF

- globálně ve frameworku
- v Symfony formuláři
- atributem u metody, která zpracovává routu/URL: IsCsrfTokenValid
- ručně HTML formulář + ručně ošetřit kód

ID

token + ID (entity)

Source code

Source code: https://gitlab.com/josef.jebavy/csrf-example-symfony

Živá ukázka

Symfony 8.0

- formulář
- delete GET/POST
- fake URL: img
- fake URL: link

(otevíráte e-mail přes starý webový prohlížeč,URL v diskuzi)

Používějte framework

- bezpečnost bez práce
- Upgrade – nová verze = nové zabezpečení
- Potíže s testy? Opravte prostředí
- Framework ani AI neudělá vše za vás

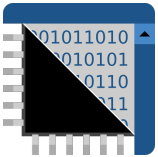
Shrnutí

Vždy hrozí bezpečnostní rizika!
Analyzujte zabezpečení ! Zvyšujte bezpečnost!

- Vývoj webu = rizika
- Nové technologie = nová rizika
- Zálohujte vždy

Diskuze

Diskuze...



Kontakt

Always open to help with your project
Bezpečné zálohování: https://www.snapbackuper.com
Web s nabídkou služeb: https://www.josefjebavy.cz

Další zdroje:
Můj YouTube kanál: https://www.youtube.com/c/josefjebavy
Blog: https://blog.josefjebavy.cz



Email: email(at)josefjebavy.cz