<https://code-boxx.com/simple-csrf-token-php/>

Lisätään lomakkeelle CSRF-token. Tällä varmistetaan, että kyseinen henkilö on lähettänyt lomakkeen ja lomake on peräisin oikeasta paikasta.

ostossovellus-CRUD-login-CSRF esimerkissä lomakkeille CSRF-token, kuten alla.

//CSRF-suojaustokeni: https://code-boxx.com/simple-csrf-token-php/

// varmista, että session\_start(); on ajettu ennen tätä tiedostoa.

if (!isset($\_SESSION['token'])) {

    $\_SESSION['token'] = bin2hex(random\_bytes(32));

}

|  |
| --- |
| <form action="<?php echo htmlspecialchars($\_SERVER["PHP\_SELF"]); ?>" method="post">      <!-- Alla on piilotetussa input kentässä csrf-token. Liitetty valueen shorthand echolla      eli voisi myös olla myös ihan normaalit php-tagit ja echo $\_SESSION['token']; -->     <input type="hidden" name="token" id="csrf\_token" value="<?=$\_SESSION['token']?>">     <div class="form-group <?php echo (!empty($username\_err)) ? 'has-error' : ''; ?>">       <label>Käyttäjänimi</label>       <input type="text" name="username" class="form-control" value="<?php echo htmlspecialchars($username); ?>">       <span class="help-block"><?php echo $username\_err; ?></span>     </div>     <div class="form-group <?php echo (!empty($password\_err)) ? 'has-error' : ''; ?>">       <label>Salasana</label>       <input type="password" name="password" class="form-control">       <span class="help-block"><?php echo $password\_err; ?></span>     </div>     <div class="form-group">       <button type="submit" class="btn btn-primary"><i class="fas fa-sign-in-alt"></i> Kirjaudu sisään</button>     </div>     <p>Jos sinulla ei ole vielä käyttäjätiliä. <a href="register.php">Rekisteröidy täällä</a>.</p>     <p><a class="btn btn-danger" href="index.php">Takaisin</a></p>  </form> |

Lomakkeen käsittelyyn on lisätty tarkistus siitä onko CSRF-token asetettu ja onhan se sama kuin SESSION-muuttujassa.

if (!isset($\_SESSION['token']) || !isset($\_POST["token"])) {

    exit("Missing token");

}

if (hash\_equals($\_SESSION['token'], $\_POST['token'])) {

    exit("Token did not match. Please reload form.");

}

**Mikä on CSRF?**

* [**Cross-Site Request Forgery (CSRF)**](https://owasp.org/www-community/attacks/csrf)
  + [**https://resources.infosecinstitute.com/topic/fixing-csrf-vulnerability-in-php-application/**](https://resources.infosecinstitute.com/topic/fixing-csrf-vulnerability-in-php-application/)
  + [**https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site\_Request\_Forgery\_Prevention\_Cheat\_Sheet.html#synchronizer-token-pattern**](https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html#synchronizer-token-pattern)
  + [**https://github.com/mebjas/CSRF-Protector-PHP**](https://github.com/mebjas/CSRF-Protector-PHP)