Erhvervsakademi
MidtVest

Systemsikkerhed

Xbi aug. 2020

Mål

- **Systemsikkerhed** undgå XSS dos attack
- Database undgå SQL injection
- Data sikkerhed, hash funktion

SQL injection

- SQL-injektion er en kodeinjektionsteknik, der kan ødelægge din database.
- SQL-injektion er en af de mest almindelige webhacketeknikker.
- SQL-injektion er placeringen af ondsindet kode i SQL-sætninger via input fra websiden.

https://www.esecurityplanet.com/threats/how-to-prevent-sql-injection-attacks.html

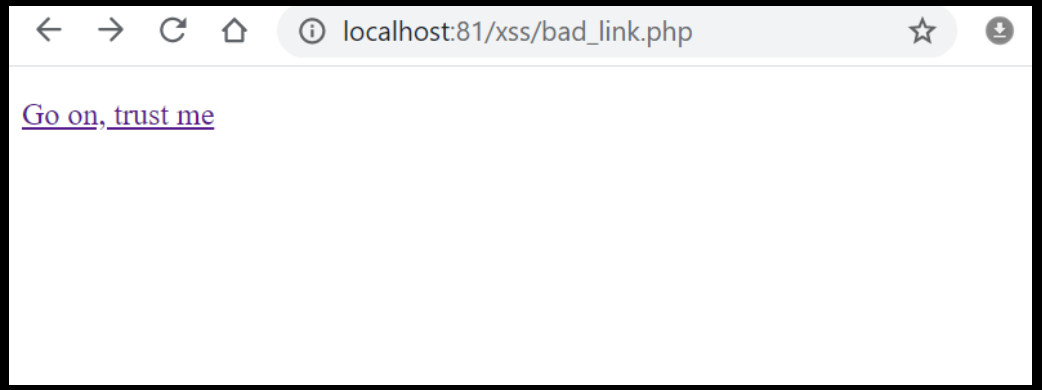
How to prevent SQL injection?

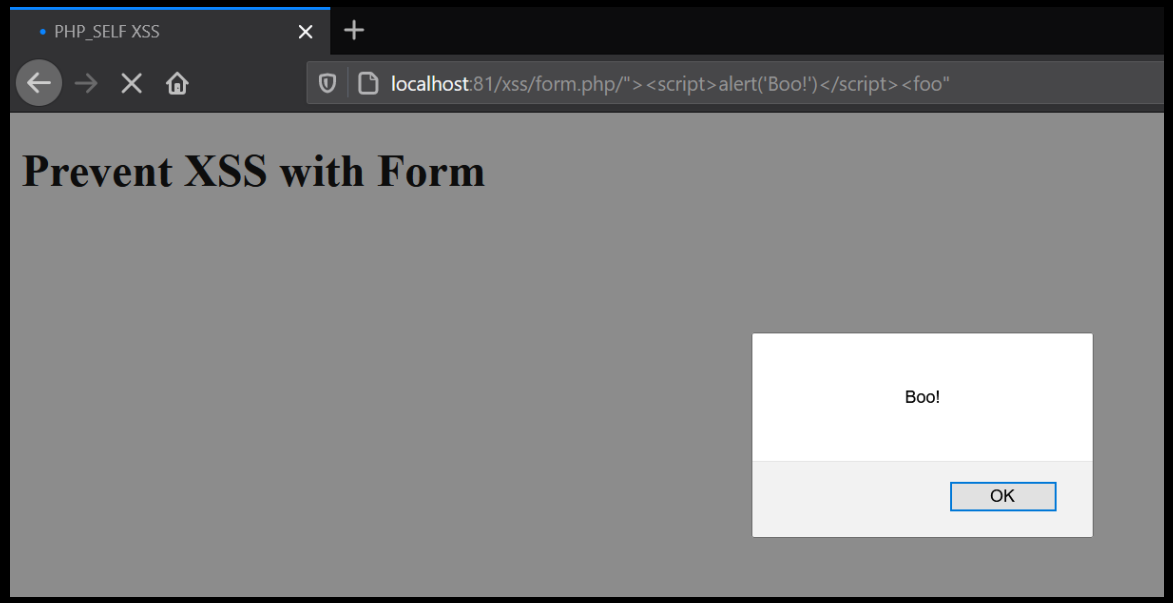
XSS

cross-site scripting (XSS)

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

demo





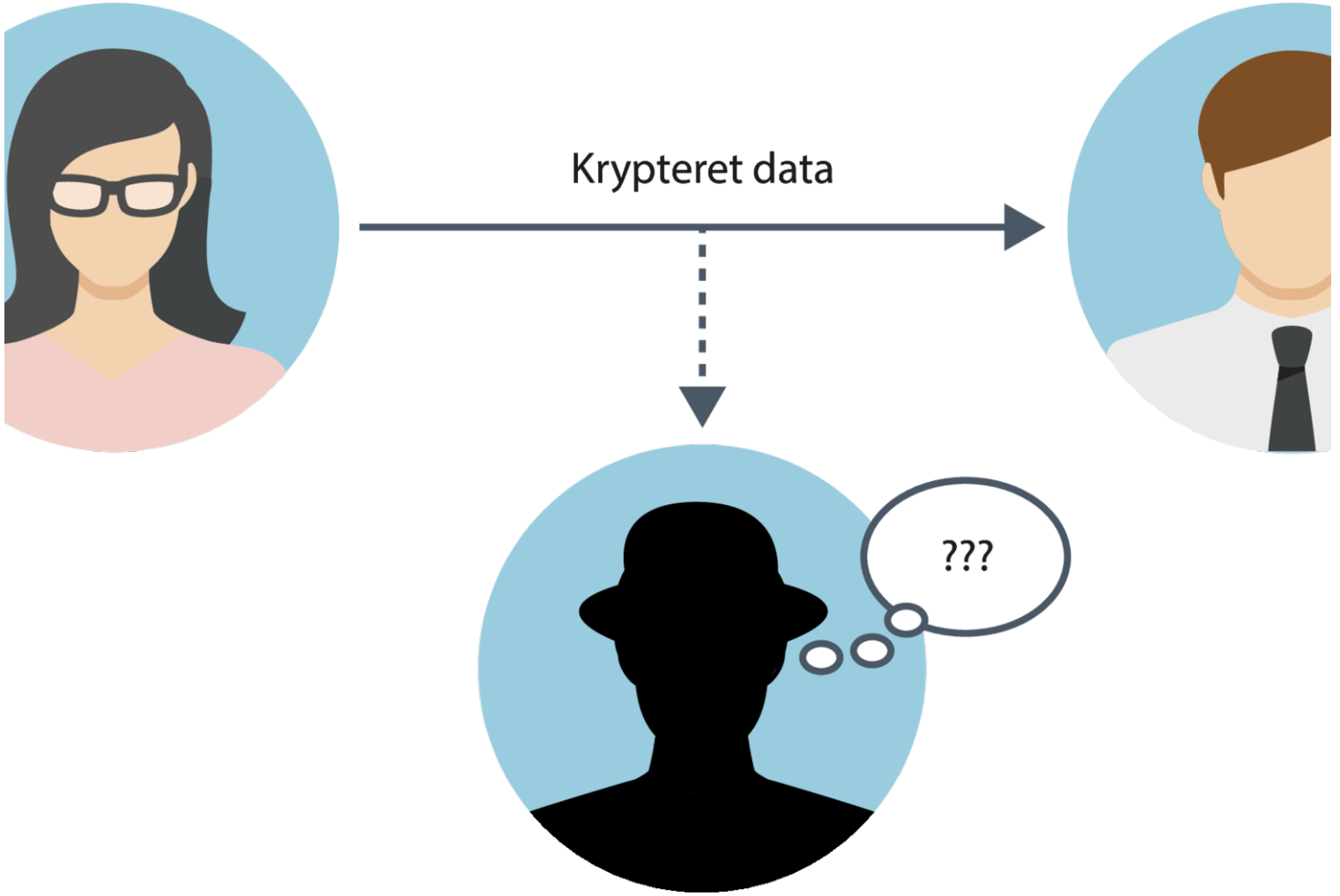
bad_link.php C:\...\xss | bad_link.php C:\...\ch06

C: > MAMP > htdocs > xss > bad_link.php

```
1   <!doctype html>
2   <html>
3   <head>
4   <meta charset="utf-8">
5   <title>XSS Link</title>
6   </head>
7
8   <body>
9       <p><a href="form.php/%22%3E%3Cscript%3Ealert('Boo!')%3C/script%3E%3Cfoo%22">Go on, trust me</a><
10  </body>
11  </html>
```

How to FIX XSS?

- A simple, but effective, way to neutralize this type of XSS attack is to pass
- $_SERVER['PHP_SELF'] to the htmlentities() function like this:
- <form method="post" action="<?= htmlentities($_SERVER['PHP_SELF']) ?>">



Kryptografi

Krypteringstyper

Kryptering af symmetrisk nøgle

Asymmetrisk nøglekryptering

Hash-kryptering

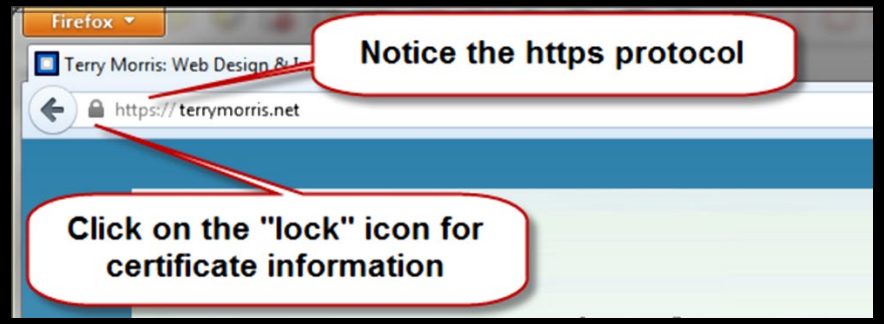
S S L (Secure Sockets Layer)

Udnytter disse krypteringsteknologier

Giver mulighed for sikker transmission of data

Secure Sockets Layer (SSL) (1 of 2)

- En protokol, der gør det muligt at udveksle data privat over offentlige netværk
- Udviklet af Netscape
- Krypterer data, der sendes mellem en klient (normalt en webbrowser) og en webserver.
- Bruger både symmetriske og asymmetriske metode

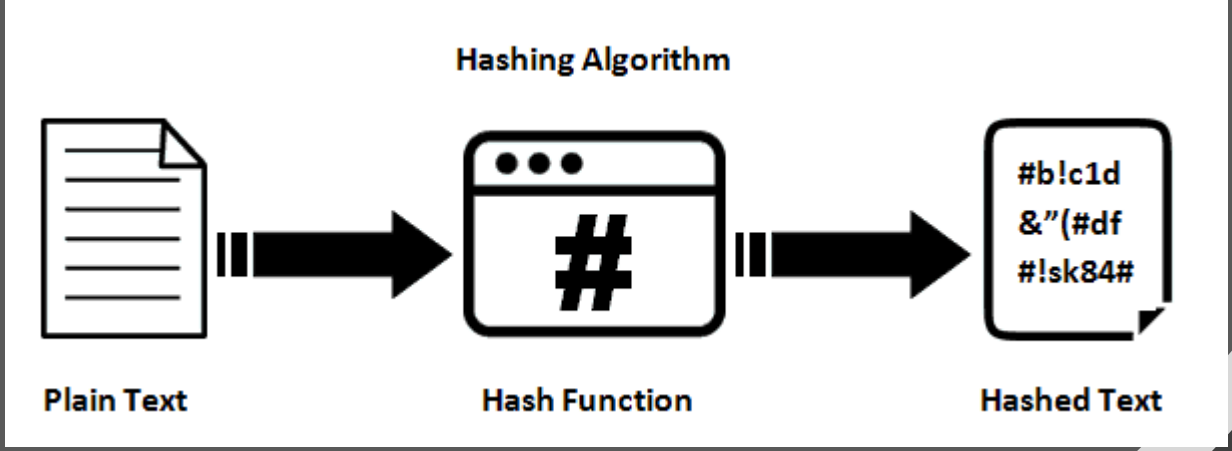


Video forklaring

https://www.e-c-s.dk/blog/hvad-er-et-ssl-certifikat-ssl-forbindelse/

HASH-FUNKTION

Til hashing bruges en *hash-funktion*. Hash-funktionen er en algoritme, der tager en besked (kort eller lang) som input og leverer en hash-værdi af en bestemt størrelse som output. En hash-funktion beregner altid samme output-hash-værdi for den samme input-besked. En hash-funktion er *en-vejs*: Ud fra en hash-værdi kan den oprindelige besked ikke genskabes.



video

Øvelse

- Hvad er password_hash funktion i PHP
- Forklar MD5 og Hash funktion

```
password_hash ( string $password , mixed $algo [, array $options ] ) : string
```

password_hash() creates a new password hash using a strong one-way hashing algorithm. **password_hash()** is compatible with crypt(). Therefore, password hashes created by crypt() can be used with **password_hash()**.

Aflevering

Opgave : Sikkerhed

- Betragt en mindre virksomhed som brug PHP til CMS system.
- Hvilke handlinger skal virksomheden foretage med hensyn til sikkerhed ? (max 10 slide)