

Saugumas

Pagrindiniai principai ir dažniausiai paliekamos spragos

Marius Grigaitis | NFQ
marius.grigaitis@nfq.lt



OWASP Top 10 2013

1. Injection
2. Broken session management (auth)
3. Cross-site scripting (XSS)
4. Insecure object access
5. Misconfiguration

Injection

```
$query = "UPDATE usertable SET pwd='$pwd'  
WHERE uid='$uid';";
```

[https://github.com/search?q=\\$_GET+mysql_query](https://github.com/search?q=$_GET+mysql_query)

Injection

- ORM
- PDO
- prepared statements
- mysql_real_escape_string

```
$stmt = $dbh->prepare('SELECT * FROM users  
where username = :username'); $stmt->execute  
( array( ':username' => $_REQUEST  
[ 'username' ] ) ) ;
```

Injection

Ne tik SQL:

- preg_match /e
- shell_exec

Broken session management / auth

- Slaptažodžių saugojimas
- Sesijos ID perduodamas per parametrus
- Pamiršau slaptažodį
- Sesijos ID pergeneravimas prisijungiant
- Perteklinės informacijos išvedimas
prisijungiant (neteisingas vartotojo vardas)
- MITM

Slaptažodžių saugojimas

- Plaintext?
- CRC32?
- MD5?
- SHA1?
- SHA2?

Salt?

Slaptažodžių saugojimas

- `md5("slaptazodis") = "42a92d3b636db32fef4edb3308e0804d"`

Added:

Fri 11th Feb, 2011 09:33 am

Hash:

42a92d3b636db32fef4edb3308e0804d

Plain:

slaptazodis

Slaptažodžių saugojimas

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

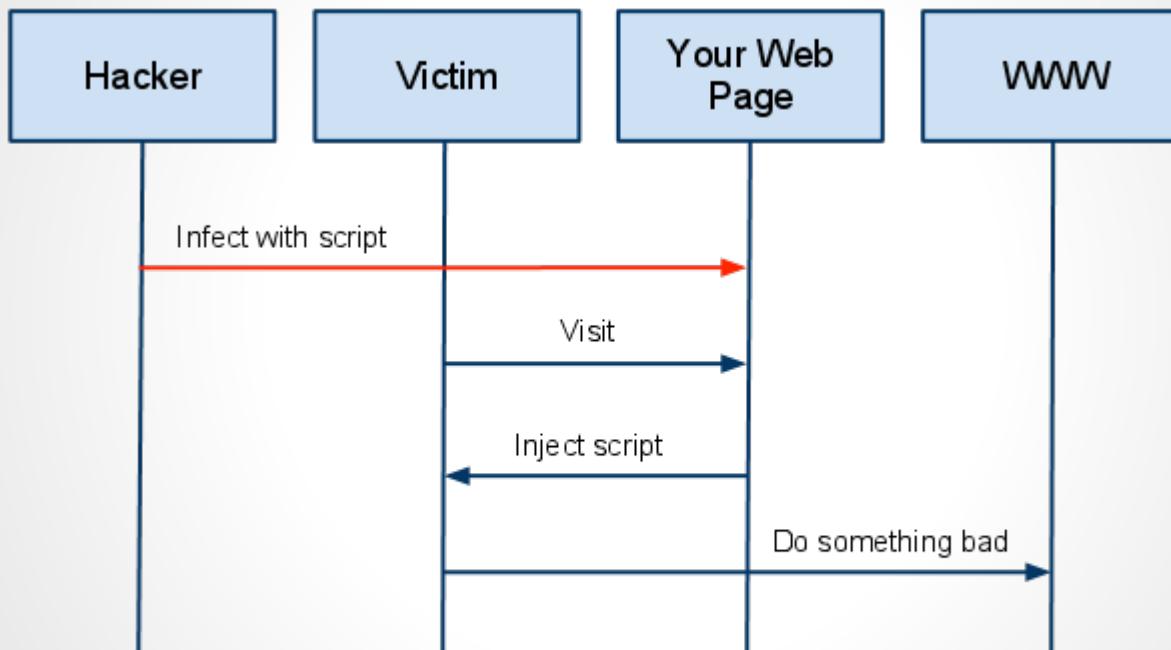
PHP >= 5.5.0

PASSWORD_DEFAULT (šiuo metu bcrypt)

Broken session management / auth

- Naudotis jau parašytomis bibliotekomis slaptažodžių saugojimui
- Pernaudoti esamas implementacijas (FOSUserBundle)
- SSL

Cross-site scripting (XSS)



A High Level View of a typical XSS Attack

Cross-site scripting (XSS)

```
index.php?name=<script>window.onload =  
function() {var link=document.  
getElementsByName ("a");link[0].href="  
http://not-real-xssattackexamples.com/";}  
</script>
```

Cross-site scripting (XSS)

Persistent? Front page redirect to disney.com ;)

Cross-site scripting (XSS)

- Nepamiršti “escapinti”
- Pasinaudoti template engine, kuris tai padaro už jus (Twig)

Insecure object access

?order_id=15 =>

?order_id=16



Misconfiguration

- Pasiekiamas app_dev.php? (Symfony)
- /phpinfo.php
- Neteisingas document_root, a.k.a.
/app/config/parameters.yml (DB
slaptažodžiai, woohoo!)

Misconfiguration

- Silpni slaptažodžiai
- Servisai, prieinama iš išorės (firewall)
- Neatnaujinamas serveris
- Neatnaujinami projekto dependencies (composer)
- Directory Index

User input



Bet vartotojas atsiunčia...



Ir gali atsiųsti daug kur

- Komentaras (DELFI)
- Headeriai (User-Agent, etc)
- Paveikslėlis
- Username

Išvada: Never Trust User Input

Secure By Default



Secure By Default

Twig: escapina automatiškai, jeigu nenorim kad escapintų - padarom “išimtį”

Firewall: draudžiam viską, leidžiam tik ten kur reikia

ORM / QueryBuilder: escapina visus parametrus, bet jeigu nenorim, kad escapintų - nurodom

Naujienu sekimas

- Galbūt išėjo heartbleed v2.0?

Klausimai?

Ačiū!