



Национална програма
"Обучение за ИТ умения и кариера"
<https://it-kariera.mon.bg/e-learning/>

Министерството на
образованието и науката
<https://www.mon.bg>

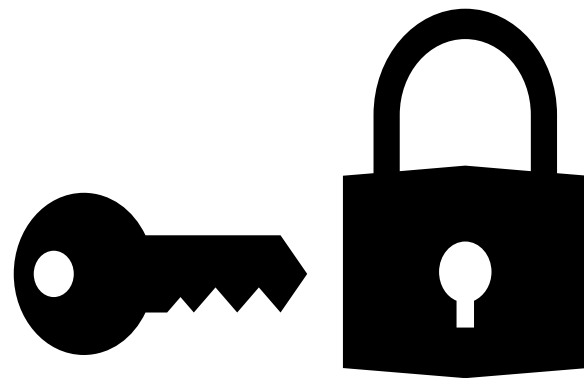


Сигурност на уеб приложенията

Security

Съдържание

- Основи на сигурността
- Най-често срещаните атаки:
 1. SQL Injection
 2. XSS
 3. CSRF
 4. Parameter Tampering



ОСНОВИ НА СИГУРНОСТТА

Концепциите за уеб сигурност

Основи на сигурността [1/4]

- Уеб сигурността включва мерки за подобряване на сигурността на приложението
 - Често се прави чрез поправяне и предотвратяване на уязвимости в сигурността
- Уязвимостите се развиват непрекъснато

"Едно нещо се счита за сигурно, когато разходите за пробив струват повече от стойността, получена по този начин"

Основи на сигурността [2/4]

- Нарушенията на сигурността често се случват спонтанно
 - Уязвимостта може да бъде напълно непреднамерена
- Нарушенията на сигурността са резултат от злонамерени атаки
 - Тези атаки може да имат много мотиви, които ги подкрепят
 - Предизвикателство, любопитство, вандализиране, кражба
- Нарушенията на сигурността могат да бъдат напълно дискретни
 - Силно опитни нападатели няма да оставят следа
 - Най-вероятно ще разберете, че сте били нападнати доста по-късно

Основи на сигурността [3/4]

Съществува широк спектър от известни видове заплахи и атаки.

Категория	Атаки
Валидиране на входа	Преливане на буфер, скриптове, SQL инжекция, канонизация
Подправяне на параметри	Манипулиране на низове за заявки, манипулация на полето на формуляра, манипулиране на бисквитки, манипулация на HTTP хедъри
Управление на сесии	Открадване на сесия, session replay, man-in-the-middle
Криптография	Лошо генериране на ключове или управление на ключове, слабо или персонализирано криптиране
Чувствителна информация	Достъп до чувствителен код или данни в хранилището, подслушване на мрежата, подправяне на код / данни, администраторска парола
Управление на изключенията	Разкриване на информация, отказ на услугата

Основи на сигурността [4/4]

- Някои от най-добрите действия, които един програмист може да предприеме, за подsigуряване на приложението:
 - Максимална простота
 - Подsigуряване на най-слабата връзка
 - Ограничаване на публично достъпните ресурси
 - Неправилно, докато не се докаже правилно
 - Принципът "Weakest Privilege"
 - Сигурност при грешки
 - Осигуряване на постоянна защита



SQL Injection

SQL Injection [1/2]

- Следните SQL команди се изпълняват:
 - Обичайно търсене(без SQL инжектиране):

```
SELECT * FROM Messages WHERE MessageText LIKE '%Nikolay.IT%'
```

- Търсене с SQL инжектиране(съвпада с всички записи):

```
SELECT * FROM Messages WHERE MessageText LIKE '%%%'
```

- Команда за вмъкване със SQL инжектиране:

```
SELECT * FROM Messages WHERE MessageText LIKE '%' or 1=1 --%'
```

```
SELECT * FROM Messages WHERE MessageText  
LIKE '%'; INSERT INTO Messages(MessageText, MessageDate) VALUES  
( 'Hacked!!!', '1.1.1980' ) --%'
```

SQL Injection [2/2]

- Оригинална SQL заявка:

```
string sqlQuery = "SELECT * FROM user WHERE name = ' " +  
username + "' AND pass=' " + password + "'";
```

- Задаване на потребителско име на John & парола на ' OR '1'='1

```
string sqlQuery = "SELECT * FROM user WHERE name = 'Admin' AND  
pass=' ' OR '1'='1'";
```

- Резултатът:
 - Потребителят с потребителско име – "Admin" ще влезе БЕЗ парола
 - Заявката за преминаване ще се превърне в bool израз, който винаги е верен

XSS

Cross Site Scripting

XSS [1/2]

- Cross-site scripting (XSS) е често срещана уязвимост в уеб приложенията
- Уеб приложенията показват JavaScript код
 - Изпълнява се в браузъра на клиента
 - Хакерите могат да поемат контрол над сесиите, бисквитките, паролите и т.н.
- Как да се предпазим от XSS?
 - Проверете потребителския вход (вградено в ASP.NET Core)
 - Изпълнявайте HTML escaping при показване на текстови данни

XSS [2/2]

- Cross-site scripting атака:
 - Кражба на бисквитки
 - Кражба на акаунт
 - Промяна на съдържанието
 - Променете потребителските настройки
 - Изтеглете зловреден софтуер
 - Изпращане на CRSF атаки
 - Подказване на парола



Изпълнение на скрипта



Изпраща скрипт в
неподсигурена форма

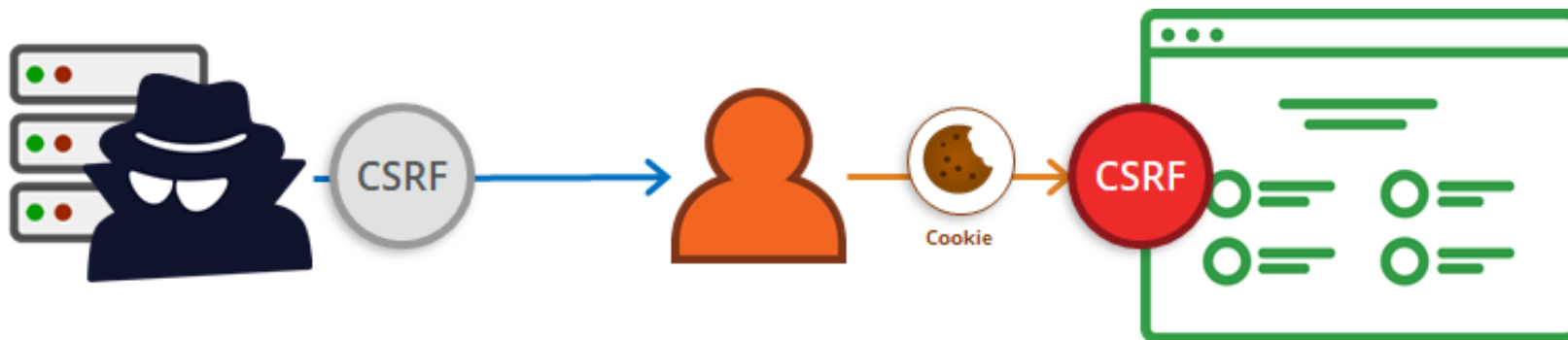


CSRF

Cross-Site Request
Forgery

Cross-Site Request Forgery [1/4]

- Това е атака на уеб сигурност над HTTP протокола
 - Позволява изпълнението на неоторизирани команди от името на някой потребител
 - Потребителят има валидни разрешения за изпълнение на заявената команда
 - Нападателят използва тези разрешения злонамерено, без знанието на потребителя



Cross-Site Request Forgery [2/4]

- Процесът не е толкова сложен за разбиране:
 - Потребителят има валидна бисквитка за автентикация до victim.org
 - Съхранява се в браузъра
 - Нападателят моли потребителя да посети <http://evilsite.com>
 - Нападателят взема съхранената бисквитка
 - Злият сайт изпраща HTTP Заявка до victim.org чрез бисквитката
 - victim.org извършва действия от името на потребителя
 - Действията се извършват с данните на потребителя

Cross-Site Request Forgery [3/2]


- Как изглежда най-често:

CONGRATULATIONS
YOU ARE OUR 42069 WINNER

A1IN A12947198247109247881029398135812
CHANGE!!>!?!?!1/11//

**DONT MISS YOUR
CHANCE**

[CLICK HERE TO COLLECT YOUR
XXX-SUPER-DUPER-MEGA-ULTRA-TURBO-DIEZEL-4X4-XXX-PRIZE](#)

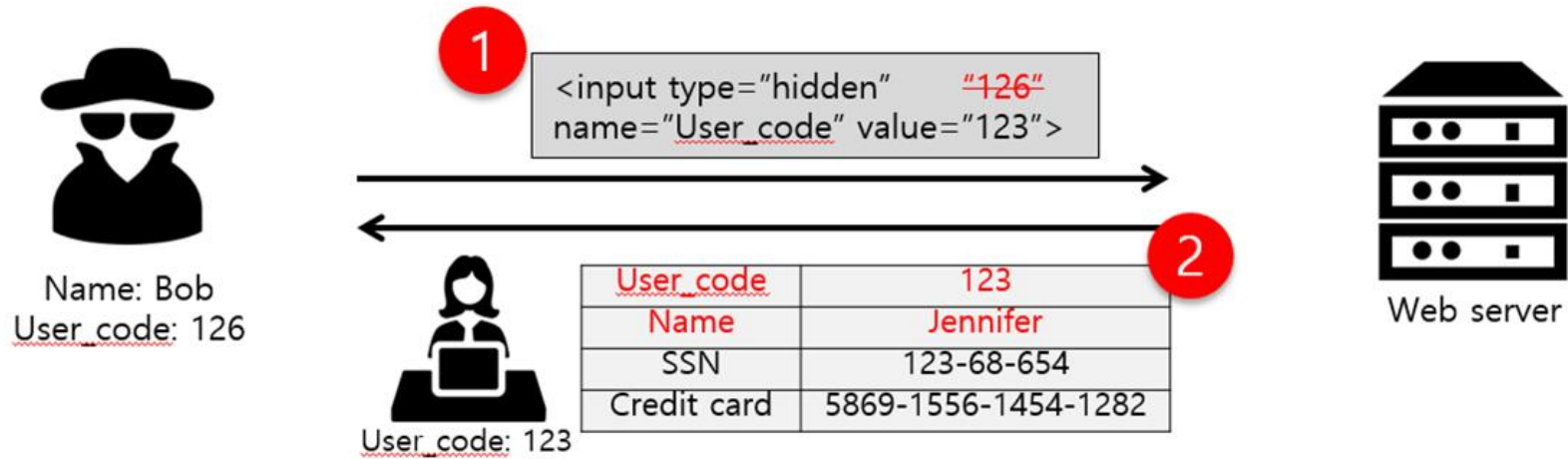
A photograph of professional wrestler John Cena, shirtless, wearing orange wristbands and an orange armband with the word "CENATION" on it. He is making a hand gesture with his right hand.

Cross-Site Request Forgery [4/4]

- Какво е всъщност Cross-Site Request Forgery:

```
<!-- SOME MULTI-COLOR USELESS CLICKBAIT CONTENT -->
<form action="http://good-banking-site.com/api/account" method="post">
  <input type="hidden" name="Transaction" value="withdraw">
  <input type="hidden" name="Amount" value="1000000">
  <input type="submit" value="Click to collect your prize!">
</form>
```

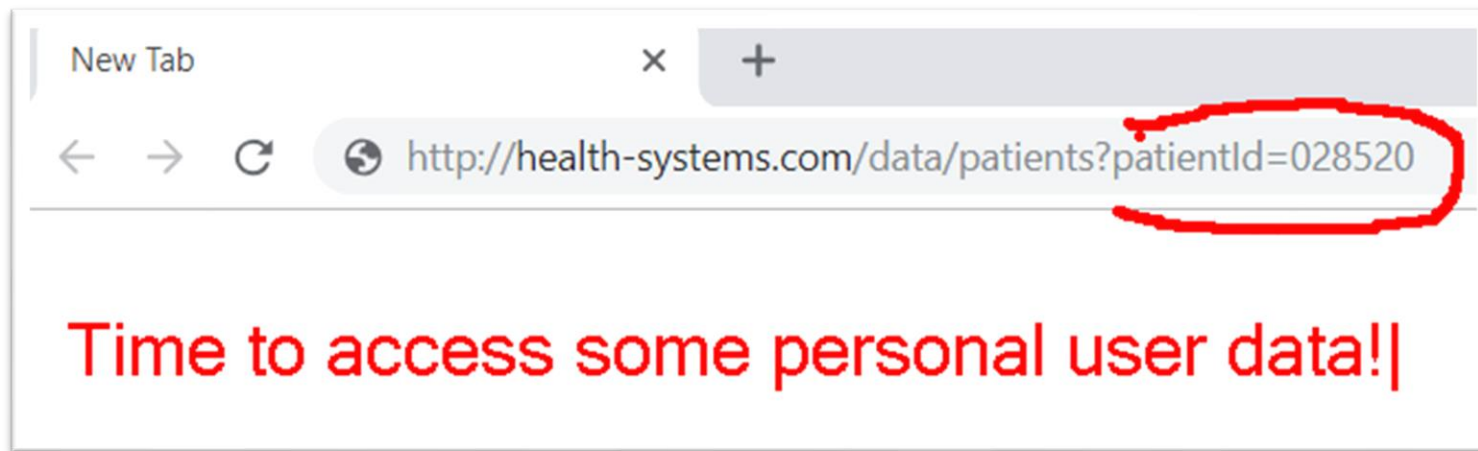
- Потребителят дори може грешно да кликне бутона
 - Това ще активира атаката
 - Сигурността срещу подобни атаки е необходима
 - Защитава както вашето приложение, така и вашите клиенти



Parameter Tampering

Parameter Tampering

- Parameter Tampering е манипулиране на параметри, обменяни между клиент и сървър
 - Променени низове за запитвания, тяло на заявка, бисквитки
 - Пропуснати валидации на данните, инжектирани допълнителни параметри

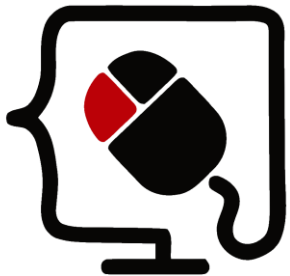


Други заплахи за сигурността

- Семантични URL/HTTP атаки (URL/HTTP манипулация)
 - Винаги проверявайте данните от страна на сървъра
- Man in the Middle (винаги ползвайте SSL)
- Недостатъчен контрол на достъпа
- Други видове инжектиране на данни (винаги санирайте данните)
- DoS и DDoS и Brute Force attacks (CAPTCHA и Firewall)
- Phishing и Social Engineering (образовайте потребителите си)
- Пропуски в сигурността на други софтуери (използвайте последните версии)

Обобщение

- Основи на сигурността
- Най-често срещаните атаки:
 1. SQL Injection
 2. XSS
 3. CSRF
 4. Parameter Tampering



Национална програма
"Обучение за ИТ умения и кариера"
<https://it-kariera.mon.bg>

Министерството на
образованието и науката
<https://www.mon.bg>



Документът е разработен за нуждите на Национална програма "Обучение за ИТ умения и кариера" на Министерството на образованието и науката (МОН) и се разпространява под свободен лиценз CC-BY-NC-SA (Creative Commons Attribution-Non-Commercial-Share-Alike 4.0 International).