



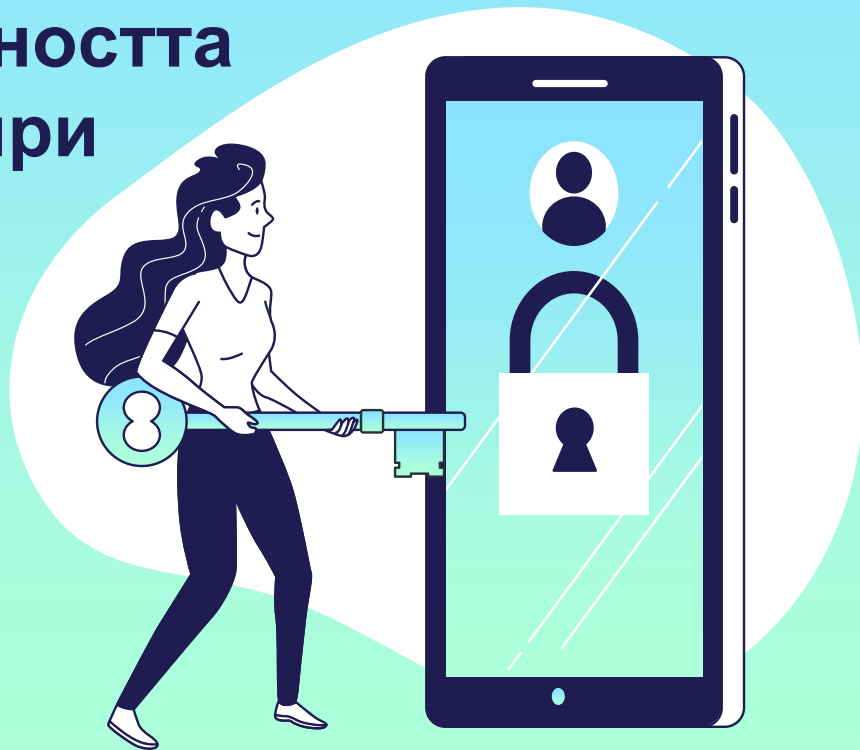
**Дупки в сигурността при
неправилно валидирани данни.
Синтактично и семантично
валидиране.
Черен или бял списък.
Криптография.**

Изготвили:

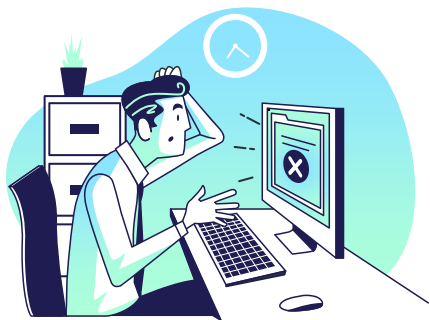
Берна Сали, Бетина Младенова,
Цветан Габровски, Калоян Шарков

Какви дупки в сигурността могат да се появят при неправилно валидиране?

Какво е валидация?



Какви са последиците от неправилно валидиране?



Потребителско изживяване

Липсата или недостатъчното валидиране на входа може да влоши потребителското изживяване на други нива.



Сигурност

Освен последиците за сигурността, валидирането на данни е също от решаващо значение за производителността, стабилността и използваемостта на софтуера

Как да осигурим правилно валидиране в уеб приложения?

```
input:invalid {  
  border: 2px dashed red;  
}  
  
input:invalid:required {  
  background-image: linear-gradient(to right, pink, lightgreen);  
}  
  
input:valid {  
  border: 2px solid black;  
}
```

Повечето езици и рамки имат вградени валидатори, които правят валидирането на формуляра много по-лесно и по-надеждно.

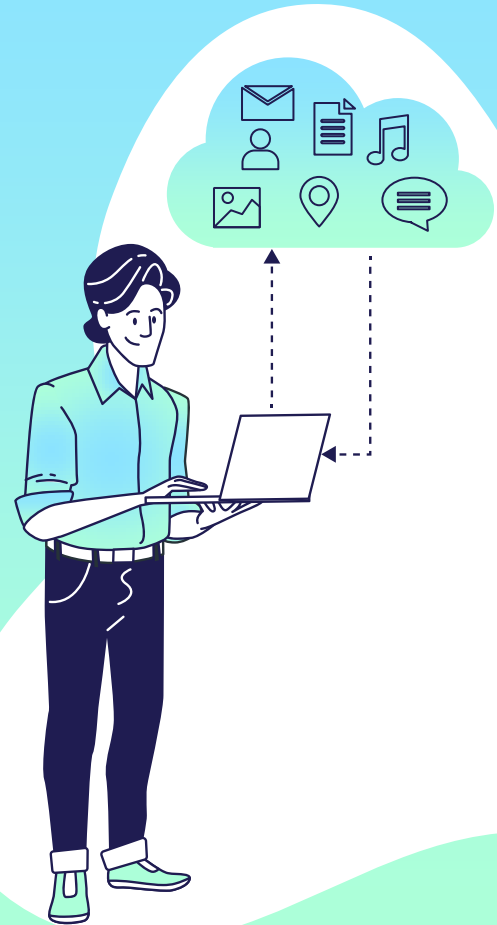
```
}  
border: 2px solid black;  
background-image:
```



```
<form>  
  <label for="choose">Would you prefer a banana or cherry? (required)</label>  
  <input id="choose" name="i_like" required>  
  <button>Submit</button>  
</form>
```

```
<input type="text">
```

Синтактично и семантично валидиране



Синтактично валидиране

Синтактичното валидиране трябва да наложи правилния синтаксис на структурираните полета (например дата, символ на валута, в емайла трябва да имеме символ @, дължината на паролата)

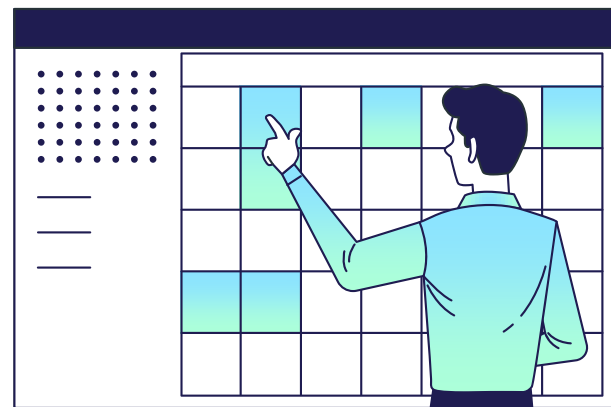


Семантично валидиране



Семантичното валидиране е по- скоро логическо валидиране и то трябва да наложи коректността на стойностите в конкретния контекст (например началната дата да е преди крайната дата, цената да е рамките на очаквания диапазон, когато избираме дата, тази дата да не е изминала)

Включване в черен или бял списък



Разлика между черен и бял списък

Whitelist

Списък от доверени приложения, уеб сайтове, които имат позволение на работят на нашата мрежа или компютър.

START



Blacklist

Списък от подозрителни или злонамерени обекти, на които се забранява изпълнението на нашата мрежа или система.

START

Кога да използваме черен списък и кога бял списък?




Whitelisting

Когато сигурността за нас е на първо място

Blacklisting

Когато не искаме да наблегнем на рестрикцията върху потребителите.

An illustration of a person with dark hair and glasses, wearing a light blue shirt and a dark tie, sitting in a dark blue office chair at a white desk. The person is looking at a large monitor. On the desk are two smaller monitors displaying code, a keyboard, and a mouse. A small potted plant is on the desk to the right. The background is a light blue gradient with a white circular glow behind the person and monitors.

Alice (Sender) Bob (Receiver)
 $C = E(m, k) \rightarrow m = D(C, k)$

Криптография и как да я правим сигурно

Принципи на криптографията

Конфиденциалност
/Confidentiality

Удостоверяване/
Authentication

Цялостост на
данните/**Data**
integrity

Признаване/**Non**
-repudiation

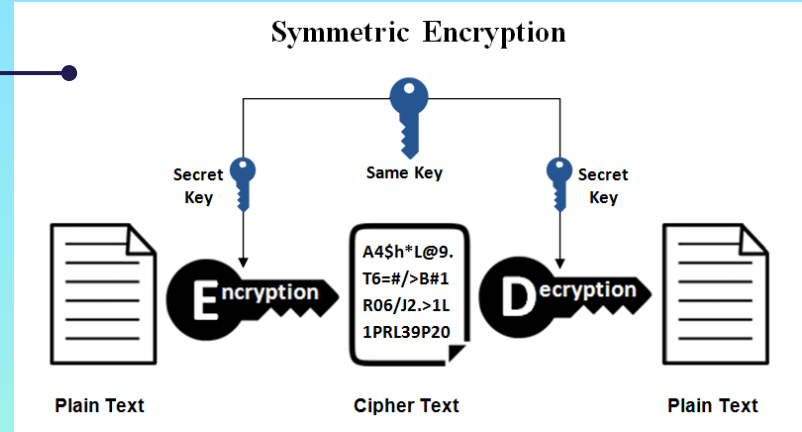


Типове криптография

Symmetric Key Cryptography

- По-бързо изпълнение, заради по-късия ключ по-прости

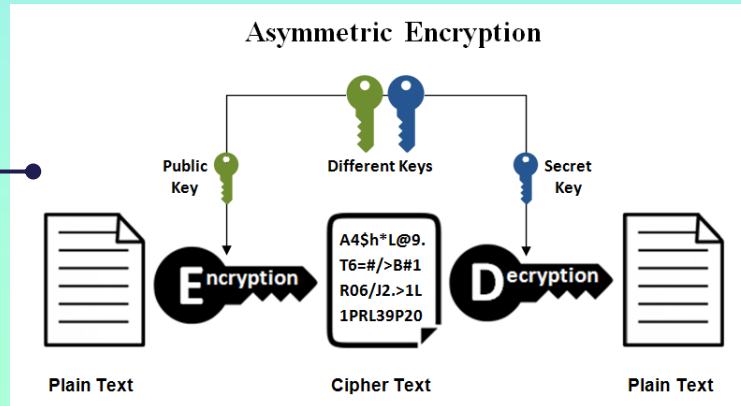
- Проблем: подателя и получателя трябва да си споделят ключа безопасно; по-малко сигурно.



Asymmetric Key Cryptography

- Без споделяне на ключа, Дигитални подписи

- Проблем: по-бавно, заради по-голямата големина на ключа



Hash Functions

- Не се използват ключове.
- Често се използва за криптиране на пароли

Не използвайте стари шифри за криптиране **01**

04 Сигурно съхранявай ключове за криптиране

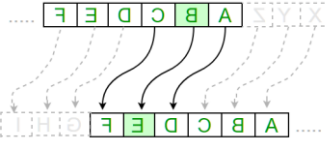
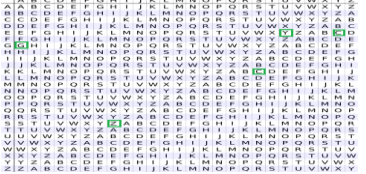
Използвай най-дългите ключове за криптиране **02**

05 Убеди се че криптирането е имплементирано правилно

Криптирай на слоеве **03**

06 Не игнорирай външните фактори

Примери

| Hill Cypher | Caesar Cypher | Keyword Cypher | Vigenère Cypher |
|---|--|--|--|
| <p>Базиран на линейната алгебра</p> | <p>Базиран на принципа на заменяне/Substitution Cipher</p> | <p>На принципа на едноазбучната субституция</p> | <p>Използва проста форма на многоазбучната субституция</p> |
| <p>Схема: $A = 0, B = 1, \dots, Z = 25$</p> | <p>Схема: $A = 0, B = 1, \dots, Z = 25$ Буква по буква</p> | <p>Plaintext: ABCDEFGHIJ KLMNOPQRSTUVWXYZ YZ Encrypted: KRYPTOSAB CDEFGHIJLMNQUV WXZ</p> | <p>$E_i = (P_i + K_i)$ Plaintext + Key</p> |
| $\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$ |  | <pre> Input : Keyword : secret Message : Zombie Here Output : Ciphertext String : ZLJEFT DTOT Take the first example, we used "secret" keyword there. Plain Text : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z When "secret" keyword is used, the new encrypting text becomes : Encrypting : S E C R T A B D F G H I J K L M N O P Q U V W X Y Z This means 'A' means 'S', 'B' means 'E' and 'C' means 'C' and so on. Lets encode the given message "Zombie Here" ZOMBIE HERE becomes ZLJEFT DTOT </pre> |  |

**Благодарим за
вниманието!**

