7.

Håndtering af tekststrenge i software

Sikker software, hvorfor?

- Usikker software
- GDPR
  - Etik
  - Ansvarlighed
- ‘Prevention is cheaper than the cure’
- NotPetya omkostninger på $1.2B

Phase	Relative cost to correct
Definition	$1
High-level Design	$2
Low-level Design	$5
Code	$10
Unit test	$15
Integration test	$22
System test	$50
Post-delivery	$100

Hvordan bliver software usikkert?

- Design fejl
  - Privelegier
  - Insecure defaults
  - Defence in depth
- Implementations fejl
  - Input validering
  - Fejlhåndtering
- Maintainence
  - Patching
  - Udfasning
- Højkvalitetssoftware = Bedre sikkerhed

Strings

- Hvad er en string?
- Forskellige sprog håndterer strings forskelligt
  - C strings
  - Python strings

Metacharacters

- ` # $ & ; %
- Interpreters findes alle steder
- Loginformularer, søgefelter…

Mutation Based-XSS

```
<noscript><p title="</noscript><img src=x onerror=alert(1)>">
```

```
<noscript><p title="</noscript>
<img src="x" onerror="alert(1)">
"">
"
```