Hoe werkt het hacken van websites?

We proberen het uit op http://puchack.cs.ru.nl

Waarschuwing

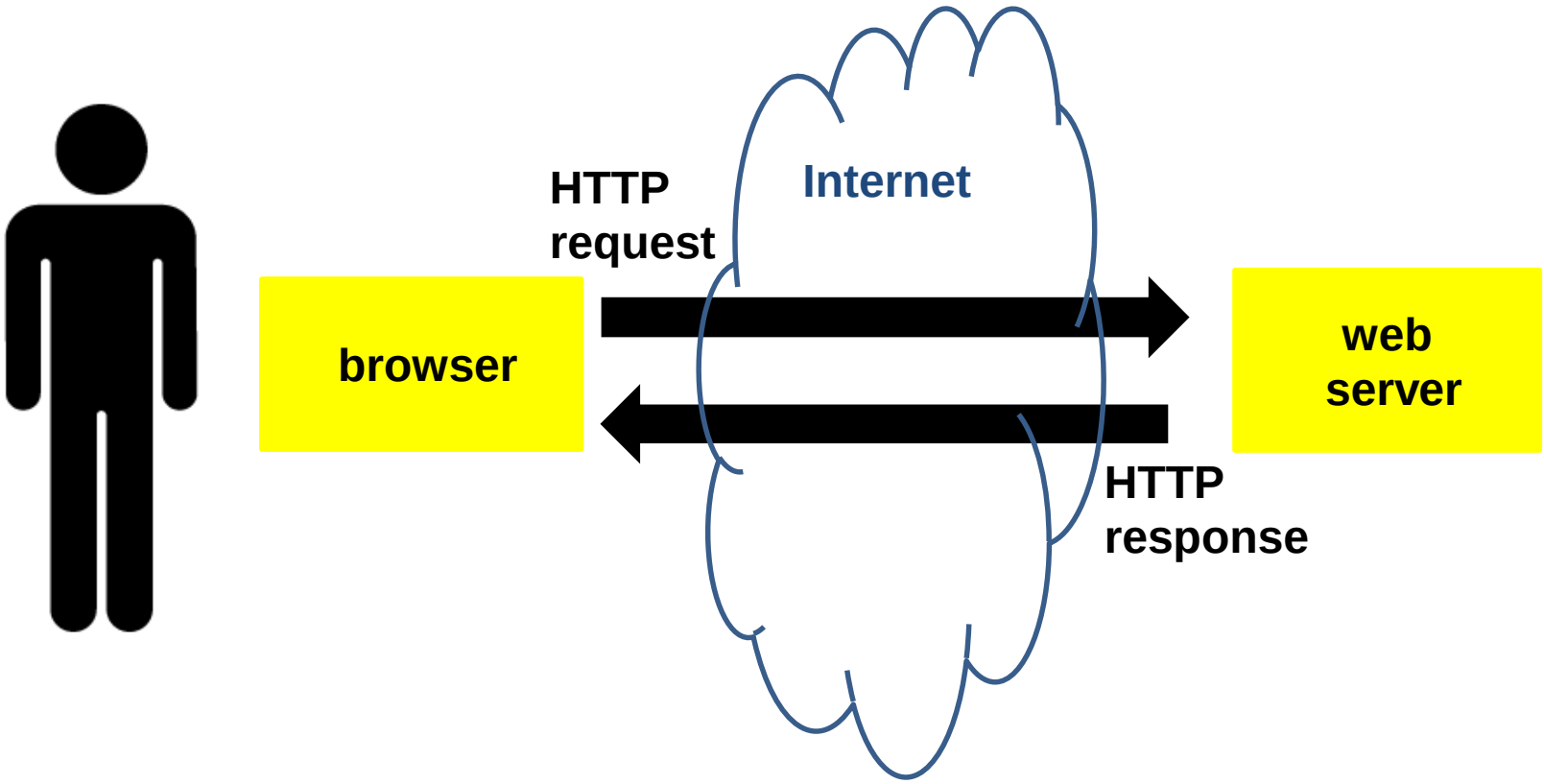
Ongevraagd websites hacken is een vorm van computercriminaliteit en strafbaar.

Ga dus verantwoord om met je skills!

Gebruik responsible disclosure:

- Als je een gat in de beveiliging van een website merkt, rapporteer het aan de eigenaar van deze site en ga niet verder wroeten!

Surfen op het web



Talen & protocollen: HTML & HTTP

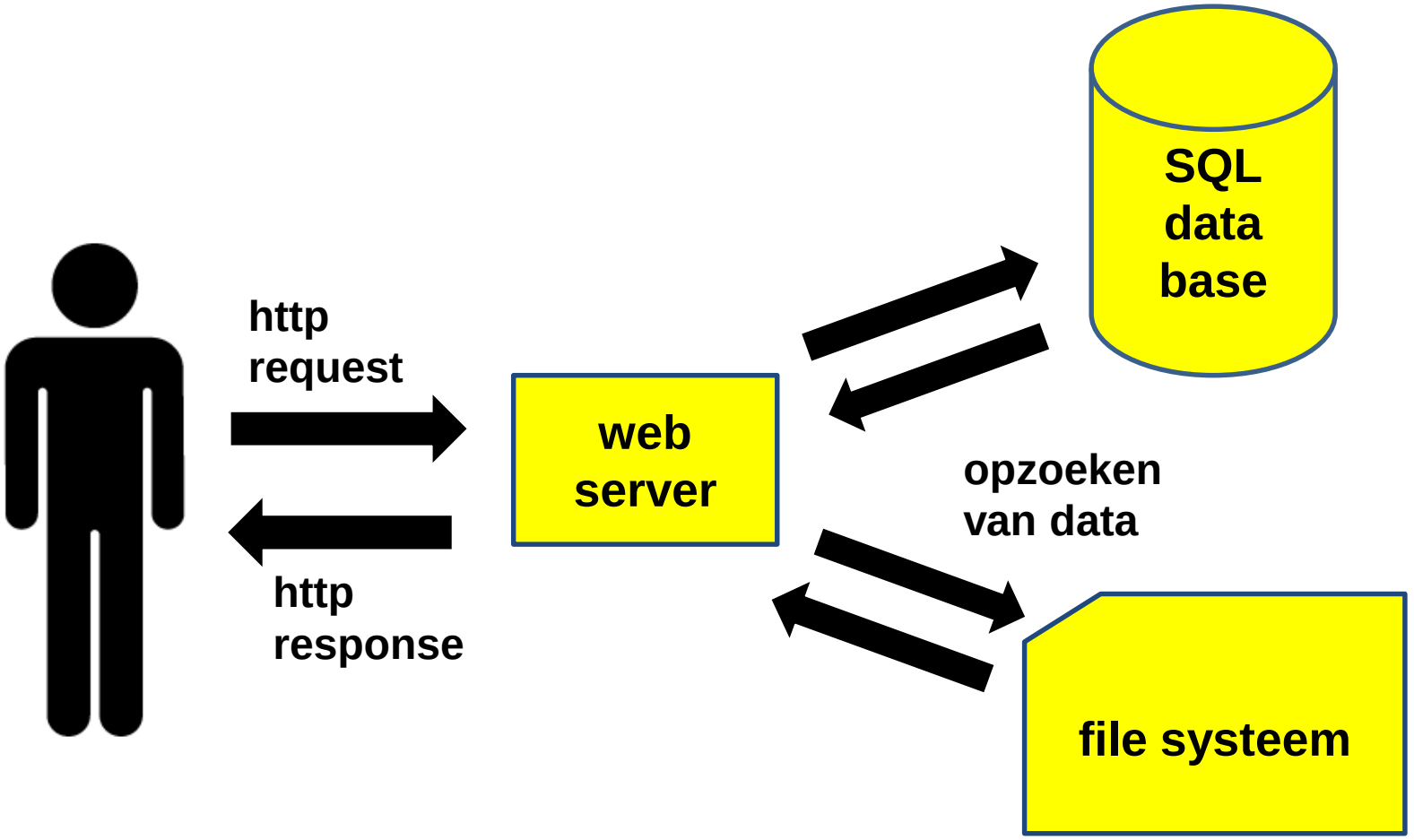
Webpagina's geschreven in **HTML**

De rauwe HTML kun je in Firefox zien met
`rechtermuis & Paginabron bekijken`

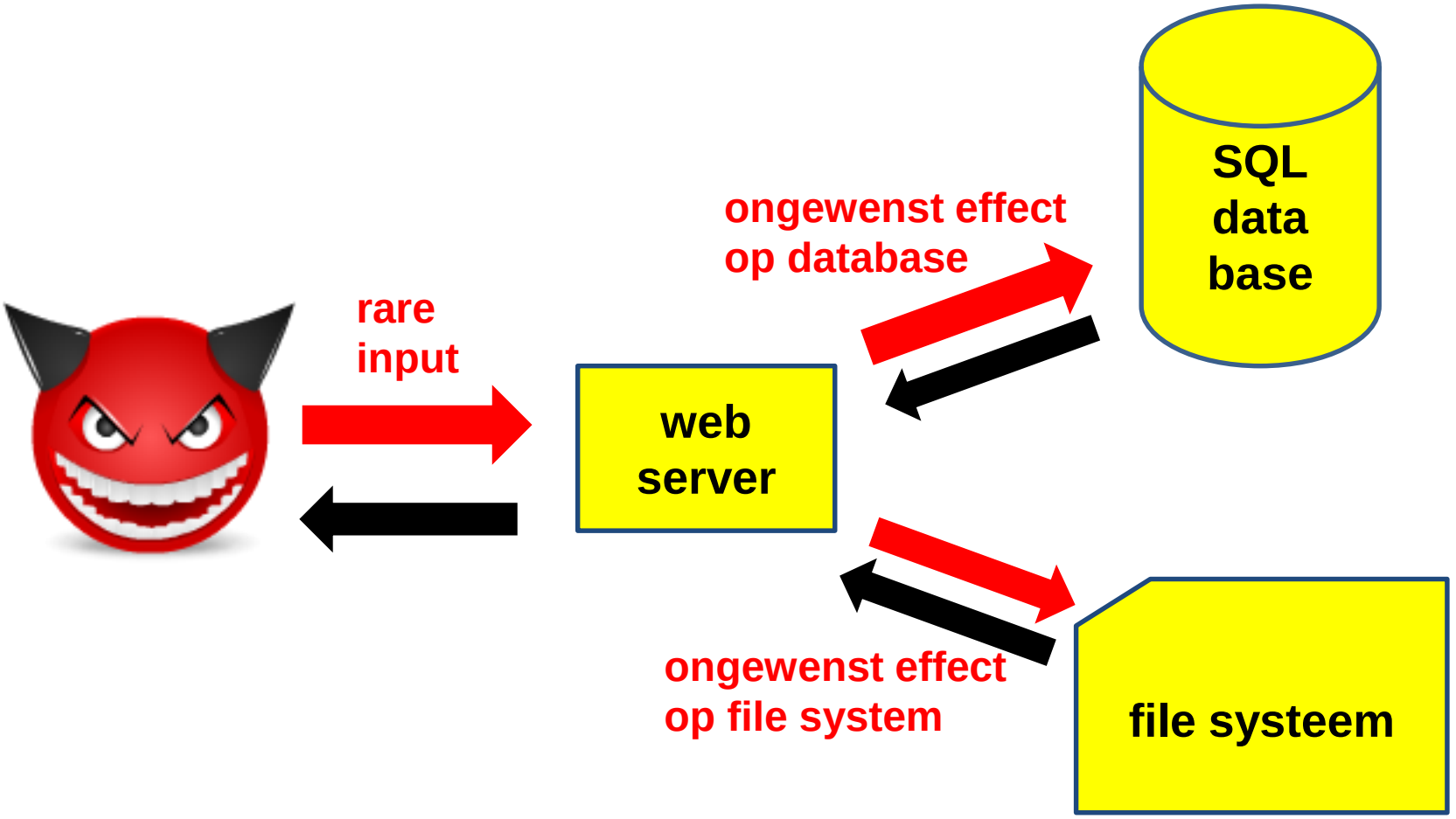
Webpagina's opgevraagd van website met op **HTTP**

De HTTP request & response kun je in Firefox zien met
`CTRL SHIFT I` in de kolom **`Netwerk`**

Moderne websites



Het hacken van websites



Nog meer talen: SQL

SQL is taal om data uit database op te vragen
Je selecteert data uit tabellen op basis van bepaalde kenmerken

```
SELECT * FROM FacebookPosts
        WHERE  user = 'Lars'
            AND date = '31032015'  # alles van Lars van vandaag
```

```
SELECT contents,date FROM Tweets WHERE user = 'Willem'
  UNION
SELECT contents,date FROM Tweets WHERE user = 'Lars'
```

De kenmerken kun je combineren met oa. AND, OR, =, UNION, en literals tussen quotes '…'

Commentaar kun je toevoegen achter # of --

Meer websites hacken?

- hackthissite.org
- Meer voorbeelden en uitleg: OWASP Webgoat

Nog meer talen: paden

Een pad bepaalt een file of het file system, bijv.

```
/home/website/level3/password_file.xls
```

Soms kun je bij een website per ongeluk ook rechtstreeks op het filesysteem

```
http://lekke_site.nl/public/../private/customerdata.xls
```

Hier hebben sommige symbolen een special betekenis. Bijvoorbeeld, met `..` ga je een map omhoog op het file-system. Dit is iets wat een aanvaller kan misbruiken.

Het gebruik van een null character, geschreven als `\0` , kan rare effecten hebben in een pad- of file-naam, aangezien het vaak als eindsymbool wordt gezien en wat er na de `\0` komt dan niet gelezen wordt.