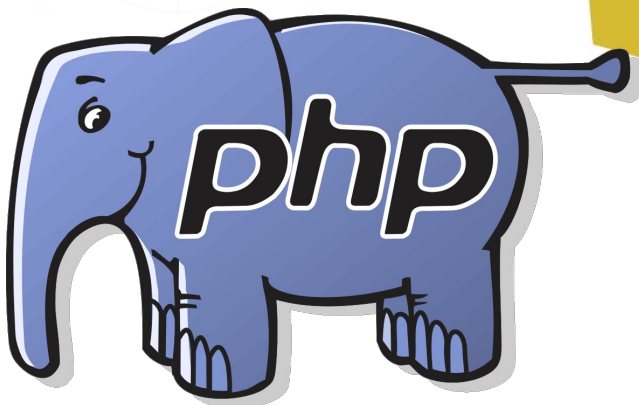




WEB



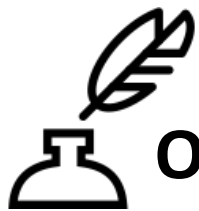
CSS



729G28

Webbprogrammering och databaser

Webbprogrammering(2)
Sahand Sadjadee
Linköping University, IDA



Outline

1. VSCode
2. PHP
3. Validering
4. Säkerhet
5. Autentisering

VSCode

- VSCode är en avancerad editor som kan användas för att skriva HTML/CSS/Javascript/PHP kod.
- Kan laddas ner från <https://code.visualstudio.com/download> kostandsfritt.

Några andra alternativ

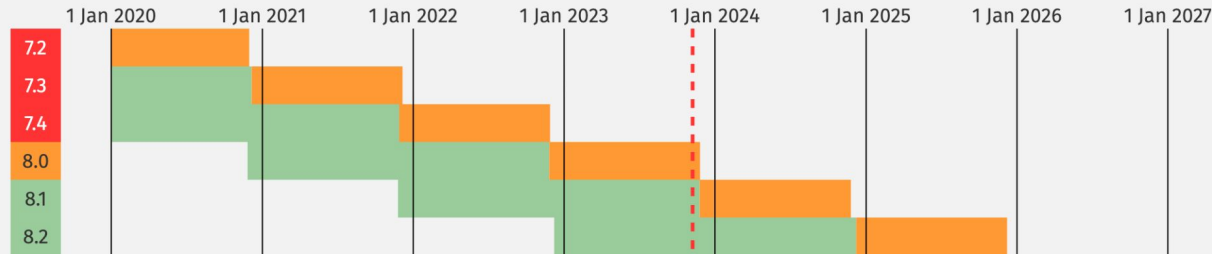
- Atom
- Brackets
- Notepad++
- Sublime
- Vim

PHP(Personal Home Page)/Versioner

Currently Supported Versions

Branch	Initial Release		Active Support Until		Security Support Until	
8.0	26 Nov 2020	<i>2 years, 11 months ago</i>	26 Nov 2022	<i>11 months ago</i>	26 Nov 2023	<i>in 17 days</i>
8.1	25 Nov 2021	<i>1 year, 11 months ago</i>	25 Nov 2023	<i>in 16 days</i>	25 Nov 2024	<i>in 1 year</i>
8.2	8 Dec 2022	<i>11 months ago</i>	8 Dec 2024	<i>in 1 year</i>	8 Dec 2025	<i>in 2 years</i>

Or, visualised as a calendar:



<http://php.net/supported-versions.php>

PHP/Nyckelord

```
$keywords = array('__halt_compiler', 'abstract', 'and', 'array', 'as', 'break', 'callable', 'case', 'catch', 'class', 'clone', 'const', 'continue', 'declare', 'default', 'die', 'do', 'echo', 'else', 'elseif', 'empty', 'enddeclare', 'endfor', 'endforeach', 'endif', 'endswitch', 'endwhile', 'eval', 'exit', 'extends', 'final', 'for', 'foreach', 'function', 'global', 'goto', 'if', 'implements', 'include', 'include_once', 'instanceof', 'insteadof', 'interface', 'isset', 'list', 'namespace', 'new', 'or', 'print', 'private', 'protected', 'public', 'require', 'require_once', 'return', 'static', 'switch', 'throw', 'trait', 'try', 'unset', 'use', 'var', 'while', 'xor');
```

```
$predefined_constants = array('__CLASS__', '__DIR__', '__FILE__', '__FUNCTION__', '__LINE__', '__METHOD__', '__NAMESPACE__', '__TRAIT__');
```

<http://php.net/manual/en/reserved.keywords.php>

PHP/Datatyper

- String
- Integer
- Float (floating point numbers - also called double)
- Boolean
- Array
- Object
- NULL
- Resource

https://www.w3schools.com/Php/php_datatypes.asp

PHP/Operatorer

Operatorer används för att utföra operationer på variabler och literaler, värden som vi skriver direkt i koden. PHP delar upp operatorerna i följande grupper:

- Arithmetic operators
- Assignment operators
- Comparison operators
- Increment/Decrement operators
- Logical operators
- String operators
- Array operators

https://www.w3schools.com/php/php_operators.asp

PHP/Funktioner

Användardefinierade funktioner startar med nyckelordet “funktion”.

Syntax

```
function functionName() {  
    code to be executed;  
}
```

https://www.w3schools.com/php/php_functions.asp

PHP/Arrays

```
<?php
$cars = array("Volvo", "BMW", "Toyota"); // Att skapa en array(Indexed array)
echo "I like " . $cars[0] . ", " . $cars[1] . " and " . $cars[2] . ".";

$age = array("Peter"=>"35", "Ben"=>"37", "Joe"=>"43"); // Att skapa en array(Associative array)
foreach($age as $x => $x_value) {
    echo "Key=" . $x . ", Value=" . $x_value;
    echo "<br>";
}

$cars = array // Att skapa en array(Multidimensional array)
(
    array("Volvo",22,18),
    array("BMW",15,13),
    array("Saab",5,2),
    array("Land Rover",17,15)
);
echo $cars[0][0].": In stock: " . $cars[0][1].", sold: " . $cars[0][2]."<br>";
echo $cars[1][0].": In stock: " . $cars[1][1].", sold: " . $cars[1][2]."<br>";
echo $cars[2][0].": In stock: " . $cars[2][1].", sold: " . $cars[2][2]."<br>";
echo $cars[3][0].": In stock: " . $cars[3][1].", sold: " . $cars[3][2]."<br>";
?>
```

https://www.w3schools.com/php/php_arrays.asp

https://www.w3schools.com/php/php_arrays_multi.asp

PHP/Kontrollstrukturer/if

```
<?php
$x=1;

if ($x == 1) print '$x is equal to 1';
?>
```

```
<?php
$x=1;

if ($x == 1) {
    print '$x is equal to 1';
    $x++;
    print 'now $x is equal to 2';
}
?>
```

```
<?php
if ($x == 1) print '$x is equal to 1';
?>
```

```
<?php
if ($x == 1) {
    print '$x is equal to 1';
}
?>
```

```
<?php
if ($x == 1 OR $x == 2) print '$x is
equal to 1 (or maybe 2)';

if ($x == 1 AND $x != 2) print '$x is
equal to 1';

$x=1;

if ($x == 2) {
    print '$x is equal to 2';
} else {
    print '$x is not equal to 2';
}
?>
```

https://www.w3schools.com/php/php_functions.asp

PHP/Kontrollstrukturer/loops

```
<?php
$x=1;

while ($x <=10) {
    print "$x<br>";
    $x++;
}

$x=11;

do {
print "$x<br>";
$x++;
} while ($x <=10);
?>
```

```
<?php
for($x=1; $x<=10; $x++) {
print "$x<br>";
}
?>
```

<http://www.developer.com/lang/php/article.php/947911/PHP-Control-Structures.htm>
<http://php.net/manual/en/language.control-structures.php>

HTTP(Hypertext Transfer Protocol)

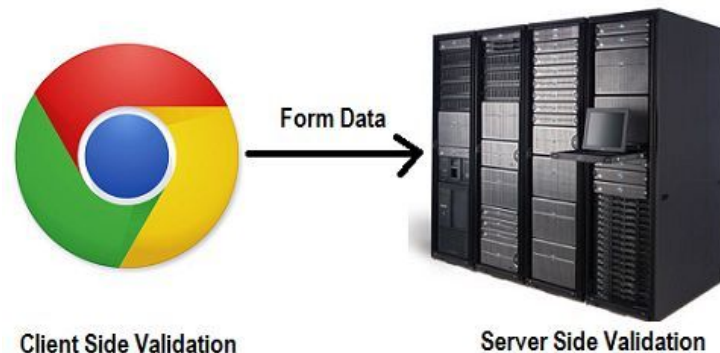
Hypertext Transfer Protocol (HTTP) är ett kommunikationsprotokoll som används för att överföra webbsidor från servrar till klienter.

- **GET** – Ber servern att skicka den utpekade filen (eller resultatet av en programkörning, databasförfrågan eller motsvarande) till klienten. Detta är i särklass det mest använda HTTP-kommandot.
- **POST** – Sänder någon form av information till servern, utöver själva förfrågan, vanligen motsvarande en webblankett. Detta används dels då förfrågan ändrar information på servern, såsom då man gör en bokning, dels då innehållet väntas vara större än vad som är lämpligt att hantera som en webbadress (eller annars olämpligt, såsom lösenord).
- **DELETE** – Raderar den utpekade filen. Detta kommando används sällan och många webbservrar har inget stöd för det.

https://sv.wikipedia.org/wiki/Hypertext_Transfer_Protocol

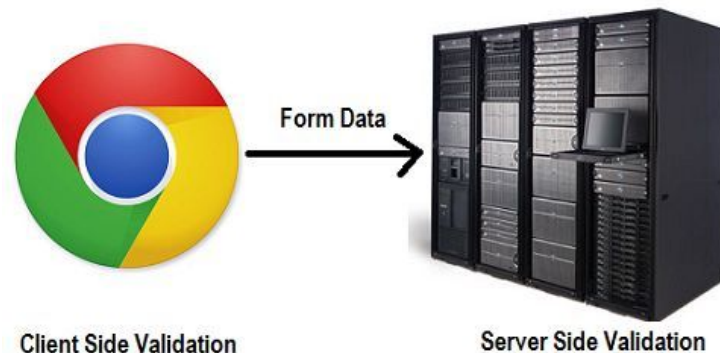
Datavalidering på serversidan(Säkerhet)

- Användaren kan skicka fel data (ibland med avsikt)
- Vad ska valideras?
 - Datan som man inte kan lita på att den är korrekt.
 - Datan som kan ställa till problem om den inte är korrekt.
 - Nästan all data.
- Det är också jätte viktigt att validera data på klient-sidan.

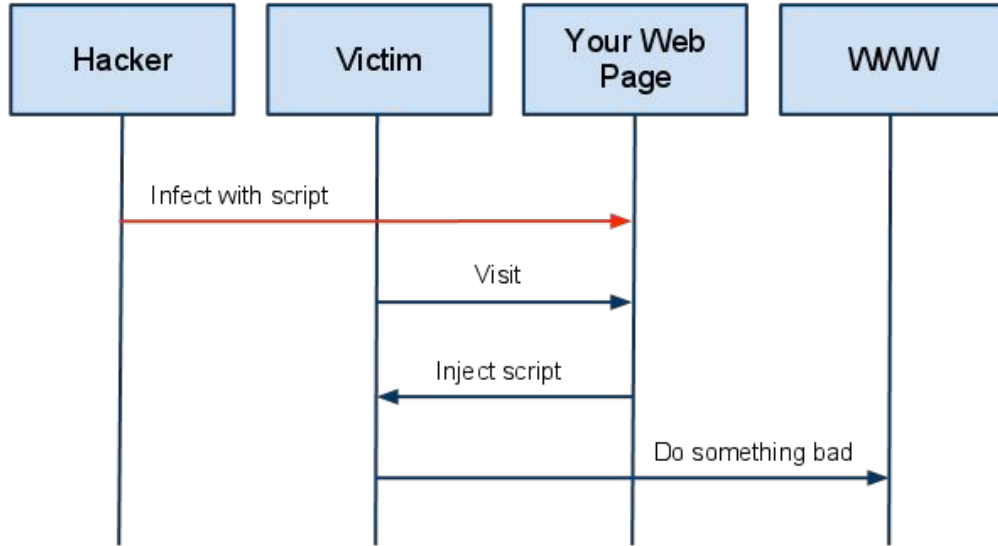


Datavalidering på klientsidan(utförande)

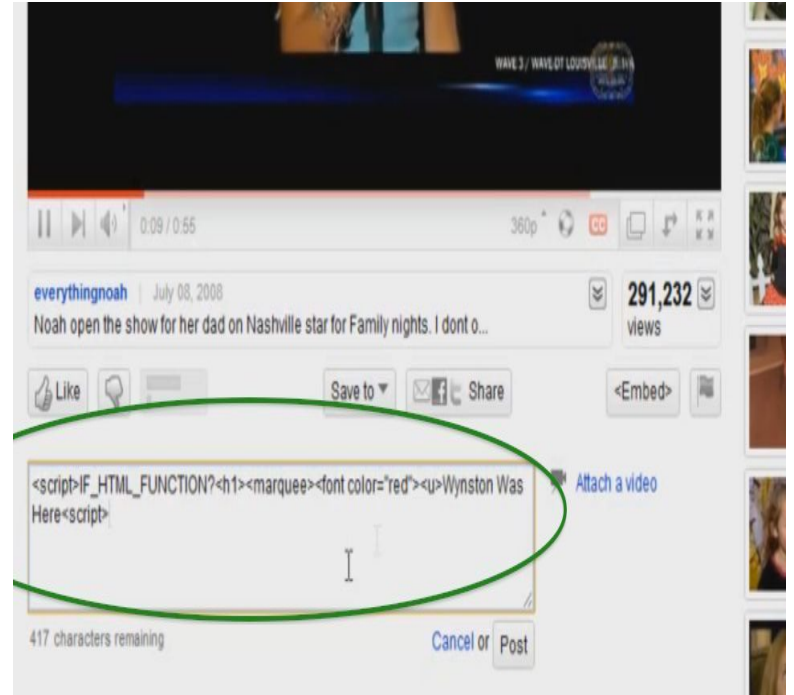
- Man kan validera data inför den skickas till servern via formulär.
 - Validering på klient-sidan kan göras genom att använda Javascript och/eller HTML.
 - Tredjepart bibliotek kan också användas. E.g. JQuery validator.
 - HTML5 hjälper mycket för att förenkla valideringen.



Säkerhet/Cross-site Scripting (XSS)



A High Level View of a typical XSS Attack



SQL Injection

```
String SQLQuery ="SELECT Username, Password  
FROM users WHERE Username='" + Username +  
"' AND Password='" + Password +"'";
```

```
Statement stmt = connection.oreateStaement();  
ResultSet rs = stmt.executeQuery(SQLQuery);  
while (rs.next()) { ... }
```

SQL Injection.

User-Id:

Password:

`select * from Users where user_id= 'srinivas'
and password = 'mypassword'`

User-Id:

Password:

`select * from Users where user_id= `` OR 1 = 1; /*'
and password = '*/--'`

9lessons.blogspot.com

Funktioner

- `is_int(n)` - är `n` ett heltal
- `is_float(n)`, `is_bool(n)`
- `intval(s)` - returnerar heltalsvärdet av `s`
- `floatval`, `doubleval`
- `ctype_alnum(text)` - kollar om alla tecken i `text` är bokstäver eller siffror
- Finns även: `ctype_alpha`, `ctype_digit`, `ctype_lower`, med flera



Funktioner

- `strlen(s)` - kollar längden på `s`
- `trim(s)` - tar bort mellanslag i början och slutet av `s`
- `strpos(s)` - letar reda på vilken position ett tecken, eller flera, har i `s`
- `addslashes(s)` - lägger till backslashes på kritiska tecken - `\`
`'`
- `htmlspecialchars(s)` - gör om `s` till html-specialtecken, t ex `<` blir `<`
- `is_email(s)`
- Skriv egna funktioner



Koden som ni inte skrivit själva

- Man får inte använda om samma kod från nätet fast det är OK att använda kod som ligger på nätet som inspirationskälla och för inlärnings syfte.

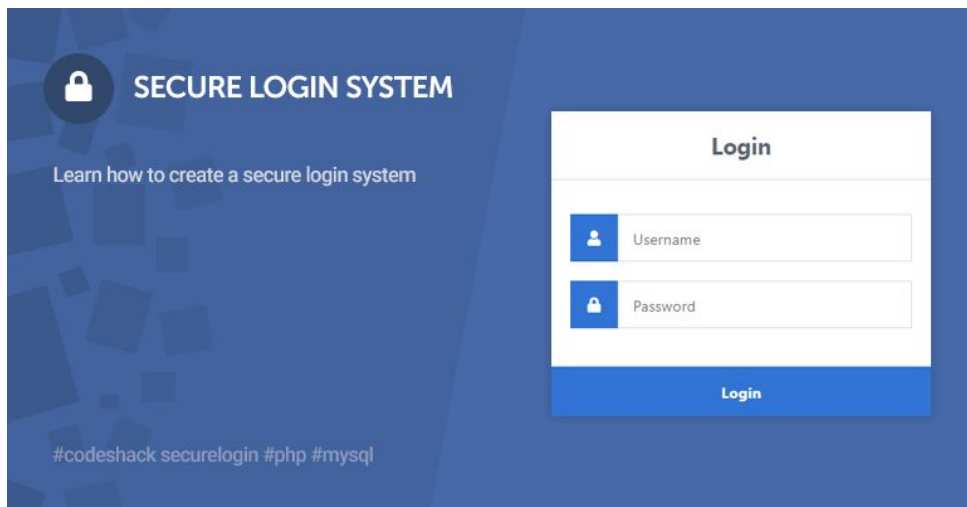


Exempel

<http://www.ida.liu.se/~sahsa74/729G28/examples/php/>

Autentisering

- Användare får identifiera sig en gång och sedan kommunicera med servern utan att behöva identifiera sig igen.
- Vanligtvis får användaren först skapa ett konto och bestämma ett användarnamn och lösenord.
- Sedan ska användaren använda samma användarnamn och lösenord för att identifiera sig.
- Så fort användaren är identifierad vet hemsidan vem det är som kommunicerar med servern.



Autentisering

facebook

Facebook hjälper dig att hålla kontakten med vänner och familj.

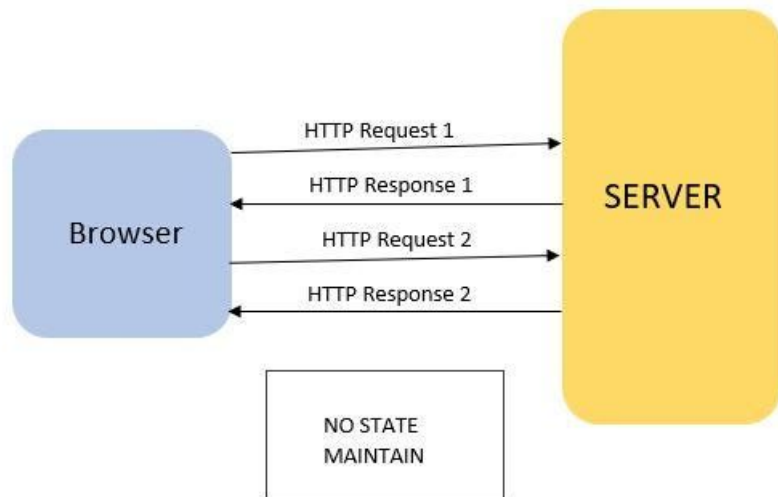
[Logga in](#)
[Har du glömt lösenordet?](#)

[Skapa nytt konto](#)

Skapa en sida för en kändis, ett varumärke eller ett företag.

HTTP är stateless

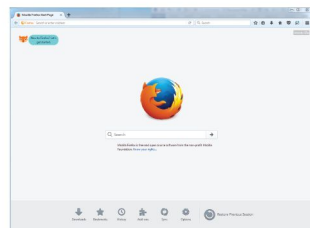
Severn vet inte om användaren/webbläsaren gjort andra tidigare anrop eller inte.



<https://medium.com/@jaimietn/http-and-statelessness-5e290fec80c0>

Cookies

Cookie är data som automatiskt skapas av webbservern och skickas till klienten. Klienten skickar cookies tillbaka till servern tillsammans med nästa anrop.



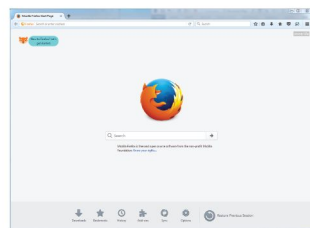
1) Browser sends request

GET /list.html HTTP/1.1



2) Server sets a cookie

Set-Cookie: language=english
Set-Cookie: PHPID:4AE5RE2234



3) Browser sends cookie back in subsequent requests

GET /login.cgi?user=john
Cookie: language=english
PHPID: 4AE5RE2234



Cookies

DevTools - www.google.com/


Elements Console Sources Network Performance Memory Application >>

Storage

- Local Storage
- Session Storage
- IndexedDB
- Web SQL
- Cookies
 - https://www.google.com**
 - Trust Tokens
 - Interest Groups
 - Shared Storage
 - Cache Storage

Background Services

- Back/forward cache

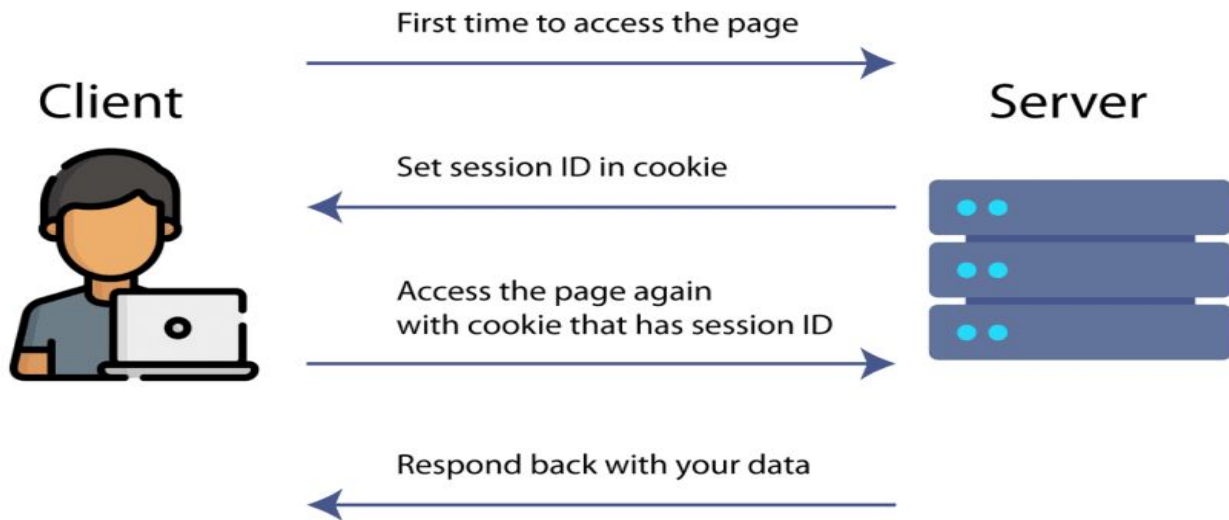
Filter  Only show cookies with an issue

Name	Value	Do...	P..	Expires...	Size	H.	S...	Sa...	P...	Priority
DEVTOOLS!	value	ww...	/	Session	14	✓	✓	Lax		Medium
CONSENT	PENDING+095	.go...	/	2024-0...	18		✓			Medium
SOCS	CAISHAgBE...	.go...	/	2024-0...	58		✓	Lax		Medium
NID	511=Tsugv0...	.go...	/	2023-0...	178	✓	✓	No...		Medium
AEC	ARSKqsJsU...	.go...	/	2023-0...	61	✓	✓	Lax		Medium
S	sso=sA0bSc...	.go...	/	Session	37	✓	✓			Low

Select a cookie to preview its value

PHP Sessions

- All data och aktioner relaterade till samma klient kallas för en session.
- Sessioner i Php skapas med hjälp av Cookies.
- Autentisering i php implementeras med hjälp av sessioner.



Ett simpelt exempel

https://www.tutorialspoint.com/php/php_login_example.htm



Tack och lycka till!