**Otázka 21: Skriptování pro WWW (skriptovací jazyky server/prohlížeč, php a práce s databází, formuláře - metody POST/GET, validace dat, webové útoky a ochrana, bezstavový protokol, práce s heslem, frameworky, architektura MVC, JavaScript, AJAX, objektový model dokumentu) (Kl)**

*Nerozebírá php a práci s databází protože idk jak to do toho pasuje*

**Skriptovací jazyky**

Pro přidání dynamických funkcí pro WWW stránky vytvořené s HTML nebo XML se využívají scripty. Toto umožňuje například přidání informací do stránky v průběhu čtení, vyplnění formuláře, získání dat z API, atd.

Skriptovací jazyk je ten, který je interpretovaný při spuštění programu a není potřeba pro kompilaci programu, pro web například PHP, WebAssembly nebo JavaScript.

WebAssembly:

umožňuje způsob spouštění kódu v mnoha jazycích ve

JavaScript:

Jedním ze tří základních prvků webu (s html a css)

Primárně client-side, spouští webový prohlížeč oproti serveru.

**Formuláře**

Způsob jak prohlížeč požádá server o data pomocí HTTP Protokolu (klient/server architektura)

**Metody**

Web:

GET:

Metoda “prosil bych data”  
 Pouze možnost vyžádat data, bez upravování  
 Limity v délce žádosti  
 Žádosti se mohou cachovat

POST:

Nikdy cachovaný  
 Nezůstávají v historii prohlížeče  
 Žádné omezení délky  
 Bezpečnější

HTML (všechny HTML metody jsou postavený na GET/POST metodách, jen mají jiné funkce):

PUT: Přidání/úprava lokální položky  
 PATCH: Úprava položky na serveru  
 DELETE: Mazání  
 atd.

**Validace dat**

Validování dat vložené do formuláře na odeslání, zprávy typu “Vyplňte pole”. Zabezpečuje od uložení dat v nesprávném formátu. (minlength/maxlength, min/max, required, etc.)  
Regex je užitečný nástroj pro validaci podle vzoru

**Sanitizace**

Proces úravy dat proti možným útokům na aplikaci:

SQL Injection: Data strukturovaná jako SQL dotaz pro manipulaci dat se škodlivým záměrem

XSS útok: Podstrčení škodlivého kódu do dynamické stránky. Zábrana převedením speciálních znaků.

**Komunikace**

**Bezstavový protokol**

Typ protokolu, kdy klient posílá žádost serveru a server odpoví podle aktuálního stavu, neukládá si informace o sessionu nebo status komunikace.

**Session a token**

Session

Klient dává serveru informace o svém sessionu (ID, čas přihlášení, vypršení, ...), aby server mohl ukládat stav komunikace.

Klient udělá login request -> server autentizuje a requst si uloží a vrací klientovi session ID ve formě cookie, který pak může použít pro následující komunikaci.

Token

Po přihlášení do serveru uživatel dostane autorizační dokument, ‘token’, který následovně využívá při dalších requestech

*Cookies jsou soubory, který uživatel dostane od serveru pro uložení informací*

**Hesla**

Kvůli bezpečnosti by hesla neměla být použita v databázi. Kvůli tomu se s nimi dělají tyto dvě věci

**Hashing**

Aby se hesla dala porovnávat, ale nebyla přímo v databázi uložená tak se heslo zahashuje – algoritmicky se zašifruje na nevratně obfuskovanou verzi sebe sama. Při zadání hesla do aplikace se porovnávají pouze hashe hesel a samotné heslo se nemusí ukládat

**Salting**

Pro další bezpečnost, v případě že dva lidé mají stejné heslo, se do algoritmu který heslo hashuje přidá další parametr (například jméno), aby vznikl unikátní hash a byl složitější na breaknutí

*Další*

**AJAX**

Asynchronní JavaScript a XML pro interaktivní aplikace které se dynamicky mění bez potřeby stránku opět načíst

**Objektový model dokumentu – DOM**

Propojuje webové stránky a skriptovací jazyky  
Ukládá si strukturu dokumentu (například HTML) do paměti.  
Reprezentuje dokument s logickým stromem, každé větvení je node a každý node obsahuje objekt. Metoda DOM umožňuje přístup po ’stromě’, umožňje úpravu struktury dokumentu, stylu nebo obsahu. (Element, event, etc.)

Zdroje: (haha necitovaný naser si)  
[Browser | Web surfing, navigation, search engine | Britannica](https://www.britannica.com/technology/browser)[JavaScript | History, Applications, & Facts | Britannica](https://www.britannica.com/technology/JavaScript)[JavaScript – Wikipedie (wikipedia.org)](https://cs.wikipedia.org/wiki/JavaScript)[WebAssembly | MDN (mozilla.org)](https://developer.mozilla.org/en-US/docs/WebAssembly)[Computer scripting language | Definition & Facts | Britannica](https://www.britannica.com/technology/computer-scripting-language)[Sending form data - Learn web development | MDN (mozilla.org)](https://developer.mozilla.org/en-US/docs/Learn/Forms/Sending_and_retrieving_form_data)[HTTP Methods GET vs POST (w3schools.com)](https://www.w3schools.com/tags/ref_httpmethods.asp)[Client-side form validation - Learn web development | MDN (mozilla.org)](https://developer.mozilla.org/en-US/docs/Learn/Forms/Form_validation)[Difference between Stateless and Stateful Protocol - GeeksforGeeks](https://www.geeksforgeeks.org/difference-between-stateless-and-stateful-protocol/)

**🐧 LINUX BABY 🐧**

