VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Protokol

Škodlivý Javascript

Esport, základní principy a metody, ZS 2020/2021

Cvičení: **PO 10:45 – 12:15**

Adam Šárek

SAR0083

Získání dat z objektu window.navigator

Objekt window.navigator obsahuje informace jak o prohlížeči uživatele, tak o samotném klientském zařízení. Údaje mohou mimo informativní charakter sloužit také jako identifikační nástroj pro případného útočníka, jelikož je možné pomocí kombinace několika údajů vytvořit unikátní kombinaci identifikující specificky jednoho daného uživatele.

Údaje poskytnuté tímto objektem se liší v rámci různých prohlížečů i jejich verzí, tedy není možné určit přesně, které údaje lze u daného uživatele získat. Já jsem konkrétně ve svém řešení využil tyto data:

- **cookieEnabled**: povolení cookies
- **doNotTrack**: požadavek do not track
- **geolocation**: získání polohy
- **hardwareConcurrency**: počet logických procesorů zařízení
- **javaEnabled**: povolení Javy v prohlížeči
- **languages**: seznam jazyků
- **maxTouchPoints**: maximální počet dotyků současně (u dotykových zařízení)
- **onLine**: informace, zda je prohlížeč připojen k internetu
- **plugins**: seznam pluginů prohlížeče
- **userAgent**: uživatelský agent – řetězec, identifikující prohlížeč a operační systém
- **vendor**: společnost, která vytvořila daný prohlížeč
- **webdriver**: informaci, zda je prohlížeč ovládán pomocí automatizace

Zachycení dat z HTML formuláře

Ve svém řešení jsem využil události *onsubmit* na element formuláře, z něhož jsem následně získal data pomocí objektu třídy *FormData*. Data z formuláře jsem pak společně s daty z objektu *window.navigator* vložil do lokální proměnné a tuto proměnnou jsem pak pomocí funkce *fetch* odeslal na web útočníka. Na útočníkově webu poté JSON data s pomocí PHP ukládám do souboru a společně s již dříve uloženými daty zobrazuji na výstupu stránky. Tuto stránku pak zobrazuji pomocí *<iframe>* v rámci testovacího webu pro jednodušší prezentaci funkčnosti mého řešení.

form			navigator											
username	password	remember	cookieEnabled	doNotTrack	geolocation	hardwareConcurrency	javaEnabled	languages	maxTouchPoints	onLine	plugins	userAgent	vendor	webdriver
a	b	on	1	1	49.77445, 18.45385	4	0	cs, en, en-GB, en-US	0	1	Microsoft Edge PDF Plugin, Microsoft Edge PDF Viewer, Native Client	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36 Edg/86.0.622.69	Google Inc.	0
c	d		1	1		4	0	cs, en-US, en	0	1		Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0		0
e	f	on	1	1	49.8209226, 18.2625243	4	0	cs, cs-CZ, en	0	1	Chrome PDF Plugin, Chrome PDF Viewer, Native Client	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36	Google Inc.	0

Obrázek 1 - Příklad získaných dat z útočníkova webu