Polymorfic Non-Alphanumeric Javascript Generator

Vložil/a RubberDuck [1], 11 Srpen, 2013 - 22:54

- Programming [2]

Výzkumníci a programátoři stále hledají nové výzvy. Nejkratší možný program podle zadání, nejméně přehledný program podle zadání a další. Jednou z těchto výzev byla rovněž neoficiální soutěž o vytvoření non-alfanumerického javascriptového kódu na fóru sla.ckers.org [3].

Výsledkem této soutěže byly základní poznatky o možnostech vytvoření non-alfanumerického javacriptového kódu, který může sloužit k úspěšnému bypassovaní WAF nebo IDS a dalších podobných detekčních systémů. Na začátku září 2012 Patricio Pallandino [4] vytvořil pro svůj blog komplexní generátor napsaný v Javascriptu. Pořád tomu ale scházela jakási pokročilejší forma a proto jsem se před pár dny rozhodl využít doposud získaných znalostí a posunout celý projekt o stupeň dále. Výsledkem je polymorfní (nebo možná spíš oligomorfní?) generátor. Aktuálně jsou některé znaky zastoupeny až čtyřmi různými variantami a další jsou připraveny pro budoucí rozšíření.

Z jakých znaků se skládá výstup?
Původní záměr byl držet se pokud možno nejmenšího možného počtu znaků:
{, }, (,), <, >, !, +
Následně jsem dospěl k názoru, že nebude na škodu rozšířit tuto sadu ještě o znak */*.

Jak velký je výstup?
Vzhledem k problematickému generování některých znaků dosahuje velikost výsledného kódu řádově tisíců až desetitisíců znaků pro jednoduché řetězce typu <script>alert('Rubber Duck');</script>.

K čemu se podobný kód hodí?
Využití tohoto kódu není příliš valné. Hodí se pro řetězce o rozumné délce několika málo desítek znaků. Prakticky se spíše jedná o demonstraci síly programování.

Je možné v některých ohledech výsledný kód zjednodušit?
Tato možnost tady rozhodně je. Z důvodu vázání na konkrétní typy prohlížečů (IE, FF, Opera, Chrome) je však jejich nasazení problematické. Rovněž je problematické využití výsledného kódu jako lokálního souboru z důvodu vazby některých znaků na specifické hodnoty prostředí.

Kde najdu aktuální verzi?
Aktuální verze bude uveřejněna na BFLOW [5].

URL článku: https://security-portal.cz/clanky/polymorfic-non-alphanumeric-javascript-generator

Odkazy:
[1] https://security-portal.cz/users/rubberduck
[2] https://security-portal.cz/category/tagy/programming
[3] http://sla.ckers.org/forum/
[4] http://patriciopalladino.com/blog/2012/08/09/non-alphanumeric-javascript.html
[5] http://bflow.security-portal.cz/projects/Polymorfic_Non-Alphanumeric_Javascript_Generator/