Autors: **Labi** Raksta ID= **84**

Kā es "uzlauzu" Dportal

WAPā es dzīvojos jau diezgan sen, tā kā toreiz nopietnu latviešu WAP lapu gandrīz nebija (šobrīd ir, bet maz), tad nācās dzīvot pa krievu mājaslapām. Laikam, pirms 4 gadiem, kad es vēl nemācēju neko pats programmēt, bija sācies WAP "dzinēju" bums. Populārākais bija arī šobrīd vēl dzīvais "WAP-motor", kuru veidoja Vantuz, bet otrs bija Dportal(wdt.org.ru), kuru veidoja *Dionisij*. Dportālu izmantoja lielākoties tikai tie, kam nepatika "WAP-motor" dominance un tie, kam patika vienkāršība, jo Dportal bija saprotamāks un vieglāk lietojams.
Tas bija tāds kā ievads, bet tagad pastāstīšu kā tad es "uzlauzu" oficiālo Dportal mājaslapu wdt.org.ru Kapēc es to darīju? Neatceros, bet tas laikam bija vairāk tāds kā eksperiments nevis ar ļaunu nolūku pastrādāts nedarbs, jo nekādus zaudējumus es Dportal nenodarīju, kaut gan varēju.=) Var teikt, ka Dportal vājā vieta bija vienkāršība. Tā kā Dportal skripti bija publiski pieejami, es zināju ka Dionisij lietotāju datus saglabāja failos ar tādu pašu nosaukumu kā nikiem t.i., ja mans niks ir TEST, tad mana parole glabājas failā /mape/TEST. Tas ko es izdarīju - ieguvu administratora paroli. Lai to izdarītu vajadzēja zināt mapes nosaukumu kurā glabājas lietotāju dati un vajadzēja veidu kā atvērt šo failu, jo pieeja failiem bija liegta .htaccess failā - deny from all. Stundu *čakarējoties* pie Dportal foruma, es atklāju ka viens parametrs, kurš parādās URL ir foruma tēmas faila nosaukums t.i. ja pārlūkā bija adrese wdt.org.ru/forum/topic.php?t=4&s=23&r=2 , tad neatceros kurš tieši (liekas parametrs t) bija šīs tēmas faila nosaukums t.i. tēmas faila adrese bija wdt.org.ru/forum/2/4. Zināju, ka mapes nosaukums, kurā glabājas lietotāju reģistrācijas faili ir atrodams failā dan.php, tad nu es izmēģināju savu laimi un ierakstīju pārlūkā kaut ko līdzīgu - wdt.org.ru/forum/topic.php?t=../../dan.php&s=23&r=2 (Dportal skriptā dan.php atradās nevis "forums" mapē, bet galvenajā "/" mapē). Un man žoklis atkārās, kad ieraudzīju, ka tur kur parasti bija foruma tēmu teksti, man *nodevīgi* parādījās "dan.php" faila saturs. Ko tas man deva? - es uzzināju kurā mapē glabājas lieotāju reģistrācijas faili (bija "dportal"), uzzināju administratora niku (bija "Admin") un pats svarīgākais - caur šo "caurumu" es varēju atvērt jebkuru Dportal failu, tai skaitā lietotāju reģistrācijas datus, ko es arī veiksmīgi izdarīju. Ierakstīju pārlūkā kaut ko līdzīgu - wdt.org.ru/forum/topic.php?t=../../dportal/Admin&s=23&r=2 , un man foruma tēmas tekstu vietā atvērās administratora reģistrācijas fails - tā es uzzināju viņa paroli (bija "orel!"). Tālāk varēju vienkārši ielogoties ar administratora niku "Admin" un paroli "orel!" un darīt Dportal, ko vien gribēju, jo tad es biju "saimnieks". Kā jau teicu es negribēju nodarīt Dportal nekādus zaudējumus, tāpēc tikai papētīju, Dportal struktūru no iekšienes, izdzēsu pāris tekstu un galvenajā lapā jaunumos pierakstīju - *"Hacked by hako"* ("hako" bija mans tā laika niks), tā lai apmeklētāji redzētu, ka šis portāls nav tik ideāls un neuzlaužams kā viņi pirmstam domāja. Nebiju ļauns, tapēc neko sliktu nedarīju, kaut gan sliktākais, ko varēju izdarīt bija - izdzēst visu Dportal no iekšienes.=) Tas viss notika vēlu vakarā, tāpēc Dionisij laikam gulēja, tāpēc nekas lietas labā netika darīts, taču kad nākamajā rītā iegāju Dportal jau bija notikšas sekojošas lietas - pirmkārt

nobanoja manu IP adresi .htaccess failā, tāpēc nācās lietot proksi, lai tiktu iekšā, otrkārt foruma "caurums" tika "salāpīts" un galvenajā lapā ievietots *patch* fails, kuru ieteica steidzami ielādēt un uzstādīt Dportal lietotājiem, lai netiktu uzlauztas viņu mājaslapas. Līdz ar to Dionisij vairs neko īpaši jaunu neveidoja un Dportal ar laiku pazuda pavisam, kaut gan visus šos skriptus var atrast http://visavi.net ielādēs. Kā mēs redzam izdzīvo stiprākais - WAP-motor. Tā nekādā gadījumā nav viena vai otra "dzinēja" popularizēšana, jo pats nekad neesmu lietojis nevienu WAP "dzinēju", es tikai pētu to struktūru.=) Ā, vēl gribu teikt, ka jaunie *censoņi* var nemēģināt "uzlauzt" nopietnos projektus, jo pašreiz programmētāji ļoti nopietni pievēršas savu skriptu drošībai, tāpēc "uzlauzt" mājaslapu tādā veidā kā es to izdarīju šobrīd praktiski nav iespējams.

Uzrakstīts:13:22 28-08-10