Web хуудас hack хийх

www.tuguldur.tk

Одоо та бүхэнд зарим нэг web хуудас хэрхэн hack хийхийг харуулая!
Та бүхэний орох дуртай Asuult.net Forum бол phpBB дээр хийгдсэн байгаа болно. Энэ нь бэлэн open source script дээр хийгдсэн Forum юм. Ийм төрлийн open source script-тай хуудасууд hack-дуулах нь элбэг байдаг.

1-рт Exploit
2-рт SQL Injection
3-рт **Cookie Faking**
4-рт Autologin Bug

Аргуудаар hack-даж болдог. Манай администууд тухай бүрд нь ямар нэг ийм төрлийн алдаа илэрхэд засах эсвэл шинэ ver-р update хийх хэрэгтэй.

Ийм төрлийн монгол Forum мөн Fotoalbum-д ихээр нэмэгдэж байна. Одоо та бүхэнд Cookie Faking хийхийг харуулая. Энэ арга phpBB 2.0.x - 2.0.12 болно.

Эхлээд та бүртгүүлсэн байх хэрэгтэй
Одоо өөрийнхөө cookie-г ол.
Firefox хэргэлдэг бол: X:\Documents and Settings\Хэрэглэгчийн нэр\ApplicationData\Mozilla\Firefox\Profiles\profile.ямар нэг бичиг\cookies.txt
Одоо txt-ээсээ web-ийн нэр өгөөд хай(forum.asuultserver)

Iexplorer хэргэлдэг бол: X:\Documents and Settings\ Хэрэглэгчийн нэр \Cookies\Хэрэглэгчийн нэр @domain.txt
Одоо үүнийгээ нээ.

Asuult.net/forum-х бол
Хэрэглэгчийн нэр @forum.asuultserver.txt

Нээгээд харахаар ийм бичлэг байгаа болно.

a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bs%3A0%3A%22%22%3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%22X%22%3B%7D

X гэдэг нь таны хэрэглэгчийн ID болно.
Одоо

a%3A2%3A%7Bs%3A11%3A%22autologinid%22%3Bb%3A1%3Bs%3A6%3A%22userid%22%3Bs%3A1%3A%222%22%3B%7D

гэж солиж өгөөд сануул

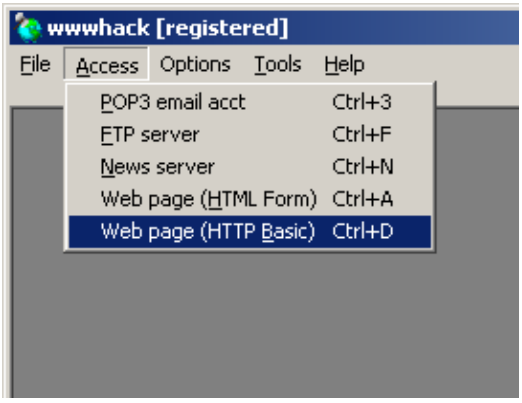
2 гэдэг маань Admin ID болно. Ингээд та admin-ний эрхээр орох болно.

Хэрэв та Asuult.net дээр турших гэж байгаа бол нэмэргүй. Asuult.net phpBB 2.0.13 болно. Одоогоор манайд үүнийг засаагүй маш олон Forum-ууд байгаа болно.
Хурдан засаарай!

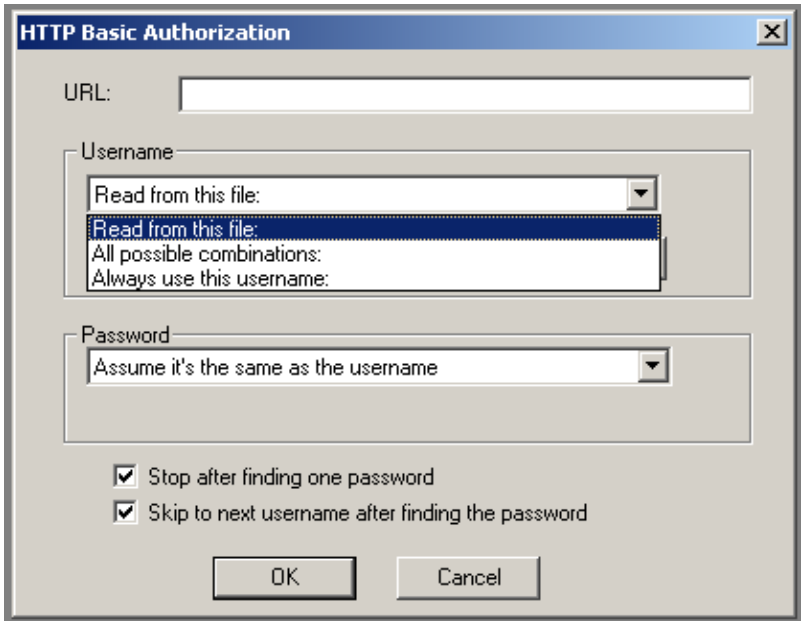
Одоо та бүхэнд Хэрэглэгч түлхүүр үг асуудаг хуудасыг hack-ийг харуулая.

1-рт BruteForce(бүх төрөлийн үг) эсвэл Dictionary Attack(Үгийн сан) хийдэг Tool.
Жиш: WebHammer, BrutusA2 мөн wwwhack гэх мэт
2-рт Маш том үгийн сан(dic, txt)
3-рт Тэвчээр ☺

wwwHack:

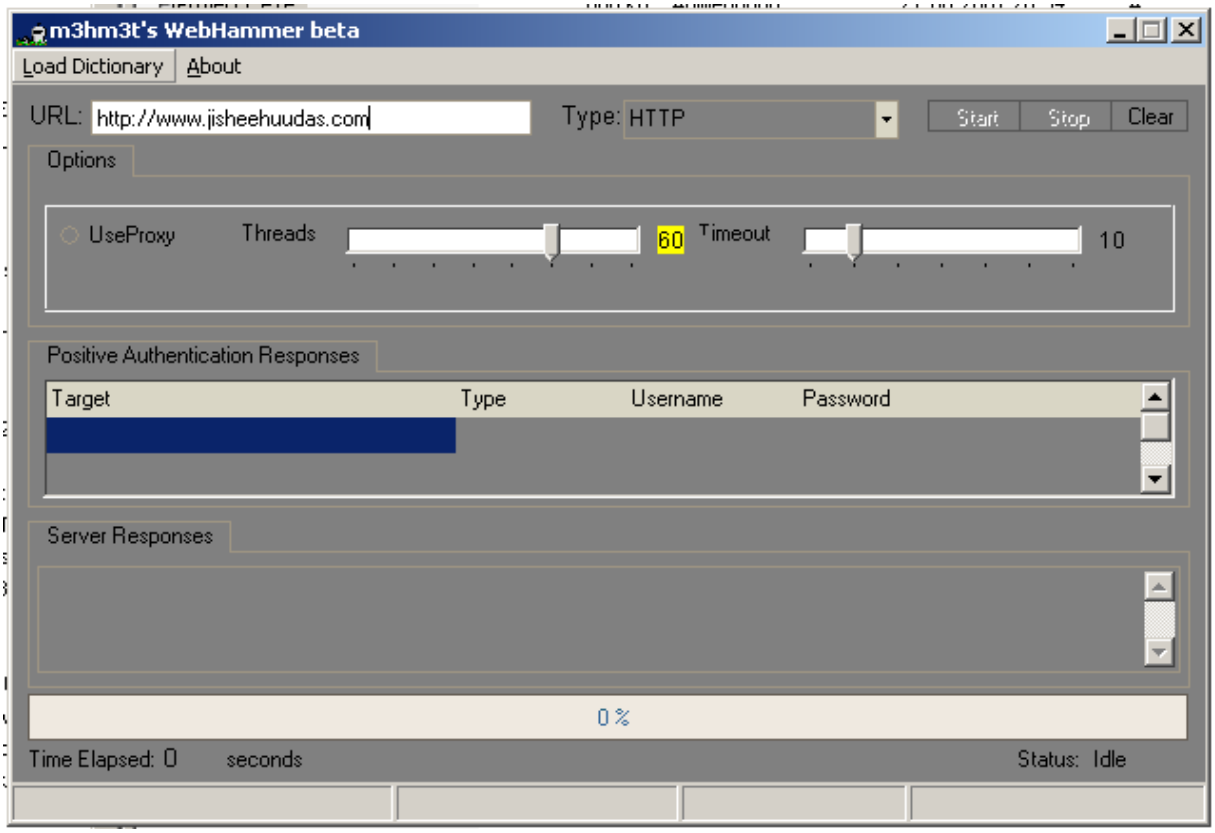


Сонго



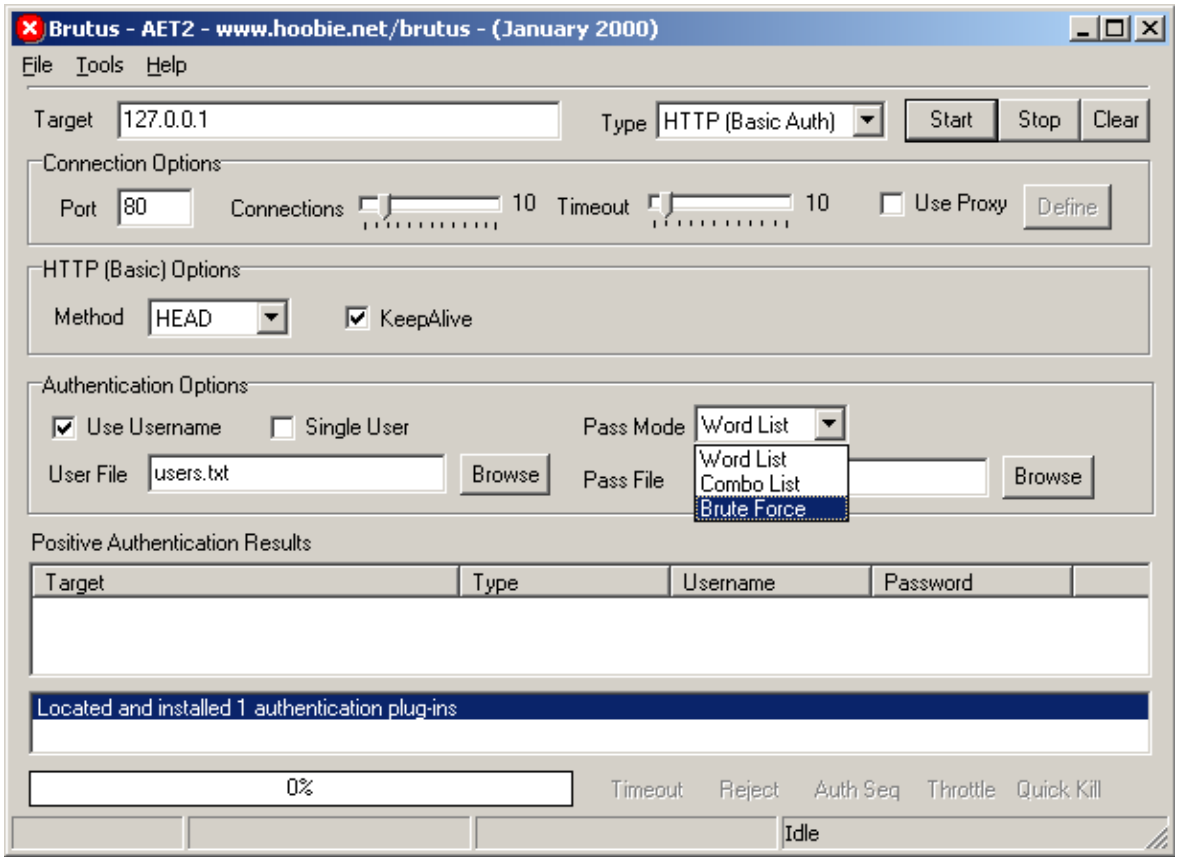
Read from this File: гэдэг нь үгийн сантай txt file-с
All possible combinations: гэдэг нь бүх төрлийн үг
Allways use this username: гэдэг нь зөвхөн өгсөн нэрээр
Assume it’s the same as the username: гэдэг нь ижил нэр түлхүүр үгээр

Одоо WebHammer:



Load Dictionary дээр дараад Үгийн сантай txt file-аа оруулаад хайлга

Одоо Brutus:



User File гэдэг дээр хэрэглэгчийн нэр хадгалсан сантай txt оруул.
Pass mod дээрээс аль дуртайгаа сонгож авч болно.
Word list бол үгийн сан
Combo list бол хосолсон үгийн сан
Brute Force бол төрөлийн үгээр

За амжилт!

BiBO