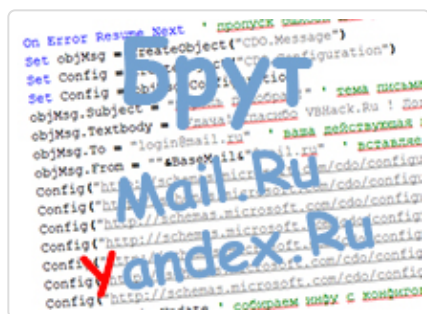


◀ (<http://vbhack.ru>) Брут почтовых сервисов (Yandex.ru, Mail.ru) на VBScript

📅 19 августа, 2015 📁 Примеры VBScript (<http://vbhack.ru/category/primery-vbscript>) 🔍

[brute](http://vbhack.ru/tag/brute) (<http://vbhack.ru/tag/brute>) , [Mail.ru](http://vbhack.ru/tag/mail-ru) (<http://vbhack.ru/tag/mail-ru>) , [vbs](http://vbhack.ru/tag/vbs) (<http://vbhack.ru/tag/vbs>) ,
[VBScript](http://vbhack.ru/tag/vbscript) (<http://vbhack.ru/tag/vbscript>) , [Yandex.ru](http://vbhack.ru/tag/yandex-ru) (<http://vbhack.ru/tag/yandex-ru>) , [брут](http://vbhack.ru/tag/brut) (<http://vbhack.ru/tag/brut>) ,
[Настройка брута](http://vbhack.ru/tag/nastroyka-bruta) (<http://vbhack.ru/tag/nastroyka-bruta>)



VBScript как и все остальные криптоновые языки программирования очень урезаны в своих возможностях. Но всё же не на столько, что бы при помощи него нельзя было создать брутфорс.

В этой статье я расскажу и покажу, **как сделать брут (Brute) почтовых сервисов (Yandex.ru, Mail.ru) на VBScript (vbs).**

Стоит отметить, что я знаю два способа создания Брута почтовых сервисов на языке VBScript. **Я покажу наиболее простой способ.**

Всё началось с простого **vbs скрипта отправки почты** с которым я немного начал экспериментировать. Как в последствии оказалось удачно. Суть моего открытия заключалась в том, что если я указывал не верный пароль от почты с которой собираюсь отправить письмо, то выдавалась ошибка. Тут-то меня и осенило!

Обязательно к прочтению:

- Циклы Do ... loop и While ... Wend (<http://vbhack.ru/uroki-vbscript/urok-vbscript-n4-cikly-while-wend-i-do-loop.html>)
- Цикл For ... Next (<http://vbhack.ru/uroki-vbscript/urok-vbscript-n6-cikly-for-next-i-for-each-next.html>)
- Условные операторы if ... else (<http://vbhack.ru/uroki-vbscript/urok-vbscript-n2-sozdanie-usloviy-pri-pomoshhi-o.html>)
- Строковые функции VBS. Работа с текстом. (<http://vbhack.ru/uroki-vbscript/urok-vbscript-n9-strokovye-funkcii-rabota-s-t.html>)
- Работа с текстовыми документами при помощи VBS (<http://vbhack.ru/uroki-vbscript/urok-vbscript-n10-rabota-s-tekstovymi-dokument.html>)

- Математические функции VBScript (<http://vbhack.ru/uroki-vbscript/urok-vbscript-n8-matematicheskie-funkcii-funk.html>)
- Конструкция On Error Resume Next и обработка ошибок vbs (Err.Number) (<http://vbhack.ru/uroki-vbscript/urok-vbscript-n11-obrabotka-oshibok-on-error-resume-next.html>)
- Процедура Sub в VBScript (<http://vbhack.ru/uroki-vbscript/urok-vbscript-n3-funkcii-function-end-function-i-procedura-sub-end-sub.html>)
- Объект Shell
- Объекты Message и Configuration (Отправка почты)
- Функции для работы с датой и временем (<http://vbhack.ru/uroki-vbscript/urok-vbscript-n7-funkcii-dlya-raboty-s-datoy-i-v.html>)

Далее, после кода, последует объяснение принципа действия и код статистики. Код **брута vbscript**:

```
</>
new_ost_time = vrem_2 & " Мин."
end if
elseif ost_time < 60 and ost_time > 0 then ' если осталось меньше 60 сек и больше 0
new_ost_time = ost_time & " Сек."
else
new_ost_time = "Неизвестно" ' если не подходит ни один вариант
end if

Set Status = FSO.CreateTextFile("Status.txt", True) 'создаём файл со статистикой
Status.Write ("Всего: "& pp & vbCrLf & "Проверено: " & ll & vbCrLf & "Осталось: " & ost
Status.Close

if l = Ubound(arrBase) and i = Ubound(arrPass) then
GoodTxt.Close ' закрываем гуды
BadTxt.Close ' закрываем бэды
ErrorTxt.Close ' закрываем ошибки
End if
End Function
```

Я постарался описать всё как можно подробно. Теперь опишу принцип действия и как его настроить.

Принцип действия


Вначале у нас имеется переменная «Login_Pass». Если она равна 1, то пароли и логины находятся в одном файле — **base.txt** и разделены «;». Если переменная равна 0, то пароли и логины находятся в разных файлах — **base.txt** и **pass.txt**. Создаём из 'этих данных два массива. В след за не начинается **цикл For ... Next** в котором мы перебираем массив с паролями. И если «Login_Pass» равно 0, то уже в нём мы начинаем ещё один такой же цикл, но уже с массивом паролей. То есть мы получаем один логин, и пока мы не подставим все пароли к нему цикл не сможет вернуть нам следующий логин. Там же мы вызываем процедуру «sub_brute», в котором и происходит проверка пароля.

Далее в процедуре «sub_brute» я поместил код отправки почты. Если пароль подойдёт к логину, то вам на почту отправится сообщение. Жертва не узнает об этом. Этого письма не будет у неё в «отправленных».

Далее мы обрабатываем ошибки ошибки и сортируем их при помощи **Err.Number**. Легко и просто мне удалось узнать номер ошибки. В случае неправильного пароля (-2147220975). Эти логины с паролями я сохраняю в **bad.txt**. Если пароль правильный, то это значение будет **нуль** и этот логин с паролем сохранится в **good.txt**. Все остальные ошибки (отсутствие интернета, капча и т.д.) сохраняются в **Error.txt**. Вот и всё! По окончании подбора появится сообщение «Подбор паролей закончен! Проверьте результаты!». Так же я сделал небольшую статистику, которая сохраняется в файл «Status.txt».

Статистика для брута

С брутом мы разобрались. Теперь нам нужна статистика. Вы у меня в долгу, так как я не поленился и смастерил её! Данная статистика показывает не только прогресс, но и сколько осталось времени. Точность таймера +-1 мин, а может и точнее. Статистика записывается в файл «Status.txt», а при помощи Status.vbs она удобно выводится с возможностью обновления. Смотрим код:

```
</> 

'*****
' Статистика брута почтовых сервичов VBScript
' Автор: Соколов Игорь (Dom0_0)
' Сайт: VBHack.Ru
' Skype: domo.free
'*****
Set FSO = CreateObject("Scripting.FileSystemObject")
Set WShell = WScript.CreateObject("WScript.Shell")

Do
Set FileStatus = FSO.OpenTextFile("Status.txt", 1, False)

' выводим статистику в переменную Meassage
Message = FileStatus.ReadAll
Stat = WShell.Popup(Message, 0, "Статистика", 5) ' выводим окошко со статистикой и кнопками "Повт
Loop until Stat = 2 ' закончить цикл, если нажмут кнопку "Отмена"
FileStatus.Close
```

Статистика сохранена отдельным файлом **status.vbs**. Она автоматически запускается во время начала работы брута. У вас появится окошко с двумя кнопками: «Повторить» и «Отмена».

Если вы нажмёте «Повторить», то статистика обновится. Если же нажмёте «Отмена», то окошко просто закроется. Его можно будет опять запустить.

Подводные камни

- **Отсутствие прокси** — Этот очень большой минус. Так как если вы за очень короткое время сможете подобрать пароли, где то к 500 почтам, то система вас заблокирует на время.
- **Однопоточный** — Малость медленный.
- **Застывание таймера** — Когда происходит ожидание ответа от сервера, происходит временная остановка скрипта и таймера соответственно.
- **Незаконный** =)

P.S. Данная статья только для ознакомления возможностей **VBScript**. Я настоятельно не рекомендую использовать данный скрипт, так как это влечёт за собой нарушение законодательства Российской Федерации. Всем удачи!

Скачать исходники (<https://yadi.sk/d/ZaPDYU0SiZija>)

2 comments



Сергей 3 года ago

<https://hack.ru/primery-vbscript/brut-pochtovykh-servisov-yandex-ru-mail-ru-na-vbscript.html?replytoocom=13432#respond>

Доброго времени суток!

Пытаюсь сделать скрипт на проверку пароля и логина к сетевому оборудованию. Сеть очень большая... У меня есть файл в нем IP, логин и пароль... я провожу периодическую смену паролей...



Андрей 3 года ago

<https://hack.ru/primery-vbscript/brut-pochtovykh-servisov-yandex-ru-mail-ru-na-vbscript.html?replytoocom=16899#respond>

Здравствуйте. При запуске вылезает ошибка, в строке 12



Reply

Preview

Help

Markdown enabled

Name

E-Mail

URL

Код безопасности *



Введите символы отображаемые выше:

Post comment

↑ Back to top

© VBHack

Theme by nehalist.io (<http://nehalist.io>)