

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*

Уязвимость на Habrahabr или как украсть инвайт

antonk18 12 апреля 2013 в 14:54 👁 159k

Все началось с попытки получить инвайт на хабр белыми методами, но, увы, получилось иначе и инвайт достался совсем нечестным способом, об этой истории я и хотел бы поведать храброчитателям.

Заранее прошу прощения у пользователя, которому не повезло, и чей инвайт был использован мною.

Я как всегда находился в поисках интересной темы для статьи, на которую обратили бы внимание и прислали приглашение на хабр, и вот меня посетила интересная идея: **«А что если найти какую нибудь уязвимость на самом хабре и написать про это статью?»**

Все, цель была выбрана, и я приступил к поискам узких мест сайта:

После долгих попыток я остановился на страничке загрузки приглашения, тут после нескольких экспериментов стало ясно что изображение должно быть в формате PNG (т.к. на другие форматы форма не реагировала), я загрузил первое попавшееся изображение и увидел что в ответ аякс вернул какой-то ID

Профиль

Аккаунт

Ключница

Уведомления

Ангрейд

Раз

Если у вас есть приглашение, вы можете загрузить его в форму ниже и получить все доступные для полноценных аккаунтов возможности.

Приглашение:

Файл загружен. [Загрузить другой?](#)



Приглашение у нас особое — это картинка, выполненная в духе [супрематизма](#).



[← обновить](#)

Введите 6 символов с картинки:

Мы должны убедиться, что вы не Вселенский Аннигилятор Ландшафтный Лёгкий Интеллектуальный.

Elements
Resources
Network
Sources
Timeline
Profiles
Audits
Console

Name
Path

jquery.form.js
/
javascripts
/
libs

ajax-loader.gif
/
images

about:blank

/upload/
/upload

4fa0468e3797ac289971156666b7b6a9.png
/uploads
/invites

68 requests | 530.31KB transferred | 25.9min (onload: 1.29s, ...

Headers
Preview
Response
Cookies
Timing

```

1 <?xml version="1.0" encoding="UTF-8"?>
2 <xmlresponse>
3
4   <id>57093</id>
5   <url>http://habrahabr.ru/uploads/invites/4fa0468e3797ac289971156666b7b6a9.png</url>
6   <message>ok</message>
7
8
9
10
11 </xmlresponse>

```

который подставлялся в скрытое поле формы как некий **invite_code**

Сохранить

antonk18

Разделы

Посты

Инфо

Услуги

Elements
Resources
Network
Sources
Timeline
Profiles
Audits
Console

```


<div class="content_left">
  <table class="menu"></table>
  <div class="submenu"></div>
  <div class="clear"></div>
  <div class="user_settings">
    <form id="upgrade_settings_form" class="upgrade_settings_form" action="#" method="post">
      <p></p>
      <div class="item invite_code required">
        <label for="invite_code"></label>
        <iframe src="/uploader/?t=invite&name=invite_code" frameborder="0" width="100%" height="30" class="iframe_uploader" scrolling="no"></iframe>
        <div class="iframe_uploader_preview"></div>
        <script type="text/javascript"></script>
        <div class="error" style="display: none;"></div>
        <div class="description"></div>
      </div>
      <div class="item captcha habracaptcha"></div>
    </form>
  </div>
</div>

```

Далее поэкспериментировав, я понял, что это некий счетчик загруженных файлов, я предположил: «а что если подставить данный ID в поле, только изменить значение на +2 или +3», получалось что когда я отправлял форму с подставным id, система бы воспринимала как будто я залил приглашение на сайт. И действительно после 10 минут усердного ввода капчи я успел перехватить id файла приглашения другого человека и естественно раньше него успел ввести капчу и, вуаля!!!, выдало сообщение что настройки сохранены, тут же сразу захожу на свою страничку и вижу


[habrahabr.ru](#) > Хабрацентр им. antonk18 / Хабрахабр

[antonk18](#) [настройки](#) [выйти](#)
[трекер](#) [+4](#) [диалоги](#) [избранное](#)
У вас недостаточно кармы для голосования



[лента](#) [посты](#) [q&a](#) [события](#) [хабы](#) [компании](#)

Windows Server 2012
От сервера до облака

 **antonk18** карма **0,0** рейтинг **0,0**
0 голосов

[Профиль](#) [Моё](#) [Подписчики](#)

[Whois](#) [Избранное \(11\)](#) [Инвайты](#) [Reset](#)

Антон

Не участвует в [рейтинге](#) хабралюдей

Дата рождения: 5 июля 1987

Откуда: [Россия, Ростовская обл.](#)

Интересы: [web разработчик](#)

Состоит в: [Game Development](#)

Зарегистрирован: 14 мая 2012 в 21:08 по приглашению [НЛО](#)

Активность: Последний раз был на сайте 11 апреля 2013 в 16:59

Моей радости не было предела, наконец то я полноценный участник сообщества.

Я сразу же отписался в суппорт, даже позвонил по номеру телефона в компанию ТМ, в течении получаса со мной по почте связался тех. специалист компании я объяснил подробно данную уязвимость. Спустя час уязвимость была локализована, я получил благодарность от компании в виде инвайта, который собственно и украл.

Еще раз прошу прощения у потерпевшего.

Проголосовать:



+581



Поделиться:



Сохранить:



Комментарии (138)

Похожие публикации

В системе защиты от подделки запросов PayPal обнаружена уязвимость

vladislavPetushkov • 10 декабря 2014 в 01:44

4

Нифига себе сходил за хлебушком, или история одного взлома

147

kay • 15 ноября 2011 в 21:24

Обнаружена серьезная уязвимость в протоколе защиты данных WPA2

68

marks • 26 июля 2010 в 14:37

Популярное за сутки

Наташа — библиотека для извлечения структурированной информации из текстов на русском языке

14

alexkuku • вчера в 16:12

Unit-тестирование скриншотами: преодолеваем звуковой барьер. Расшифровка доклада

4

lahmatiy • вчера в 13:05

Люди не хотят чего-то действительно нового — они хотят привычное, но сделанное иначе

25

ПЕРЕВОД

Smileek • вчера в 10:32

Руководство по SEO JavaScript-сайтов. Часть 2. Проблемы, эксперименты и рекомендации

2

ПЕРЕВОД

Как адаптировать игру на Unity под iPhone X к апрелю

0

P1CACHU • вчера в 16:13

Лучшее на Geektimes

Стивен Хокинг, автор «Краткой истории времени», умер на 77 году жизни

33

HostingManager • вчера в 13:49

Обзор рынка моноколес 2018

70

lozga • вчера в 06:58

«Битва за Telegram»: 35 пользователей подали в суд на ФСБ

40

alizar • вчера в 15:14

Стивен Хокинг и его работа — что дал ученый человечеству?

8

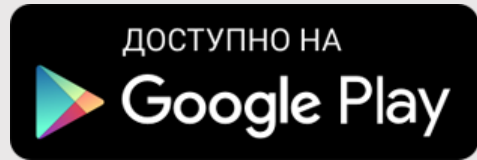
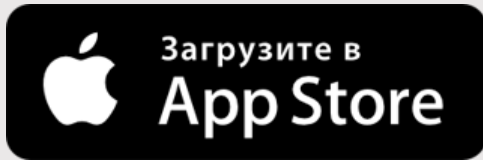
marks • вчера в 14:46

Sunlike — светодиодный свет нового поколения

17

AlexeyNadezhin • вчера в 20:32

Мобильное приложение



Полная версия

2006 – 2018 © TM