

ИНТЕЛЛЕКТУАЛЬНЫЕ МЕТОДЫ В ЗАДАЧАХ ЗАЩИТЫ ОТ КИБЕРУГРОЗ

ЛАБОРАТОРНАЯ РАБОТА № 5
Атаки на веб-ориентированные системы.

Выполнил:
Мосолков Е.Н.
Преподаватель:
Исхаков А.Ю.

Москва 2021 г.

ЦЕЛЬ РАБОТЫ

Изучение и отработка базовых атак на веб-ориентированные системы

ЗАДАЧА ПРАКТИЧЕСКОЙ РАБОТЫ

Зарегистрироваться в проекте <https://root-me.org>

Выполнить минимум 1 задание из рубрики (Web client / Web Server)

РЕШЕННЫЕ ЗАДАЧИ С ROOT.ME

Web-Client:

- HTML disabled buttons
- Javascript - Authentication

Web-Server

- HTML - Source code
- Weak Password

ОПИСАНИЕ НАЙДЕННЫХ УЯЗВИМОСТЕЙ

HTML disabled buttons

В Web-Client задании «HTML disabled buttons» была найдена уязвимость Logical Attacks/ Abuse of Functionality – а именно использование тега «disabled» для отключения функционала ввода данных. Пользователь может спокойно изменить код HTML документа, из-за чего получит доступ к функционалу, который заведомо был отключен автором.

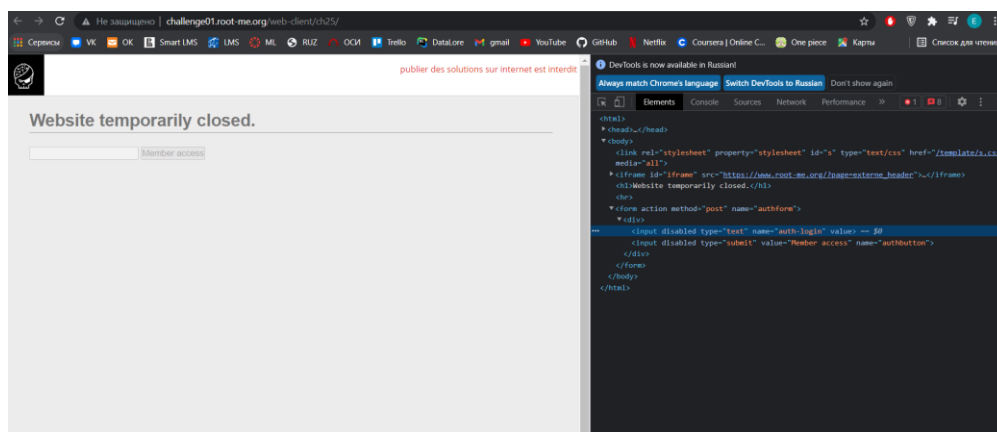


Рисунок 1. Начало вызова «HTML disabled buttons»

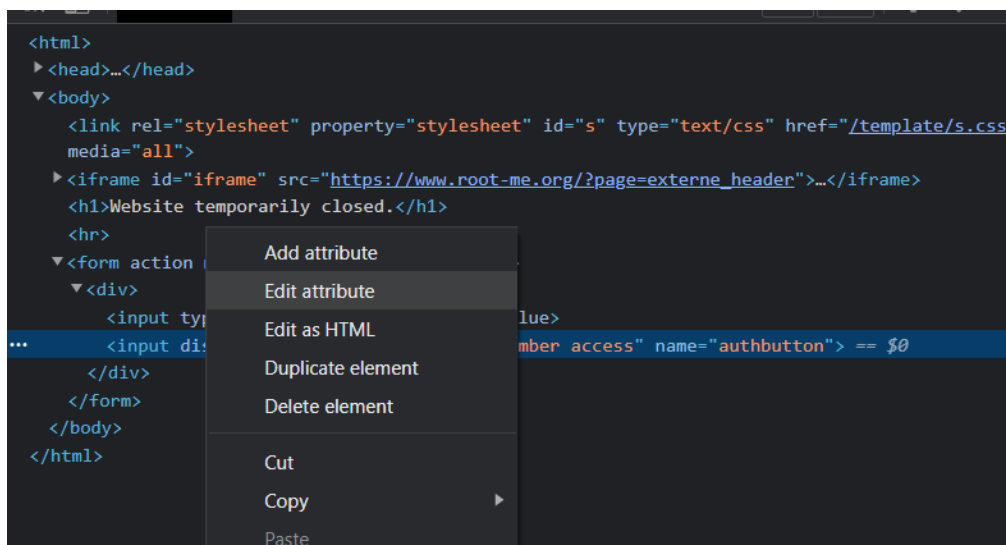


Рисунок 2. Удаляем атрибут disabled

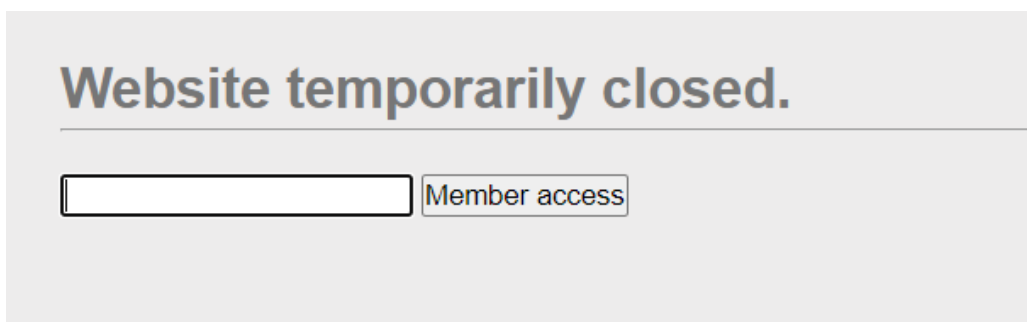


Рисунок 3. Поле ввода и кнопка теперь доступны

Website temporarily closed.

Member access granted! The validation password is HTMLCantStopYou

Рисунок 4. Получили пароль для прохождения испытания

Javascript – Authentication

В задании «Javascript - Authentication» была найдена уязвимость Information Disclosure/Predictable Resource Location - а именно логика аутентификации была вынесена в клиентскую часть (хранилась в файле login.js). Данный файл элементарно найти (находиться в head) и открыть (нужно просто дописать название файла к ссылке) и вот у нас есть логика с логином и паролем, по которым можно легко зайти и просмотреть приватную информацию.

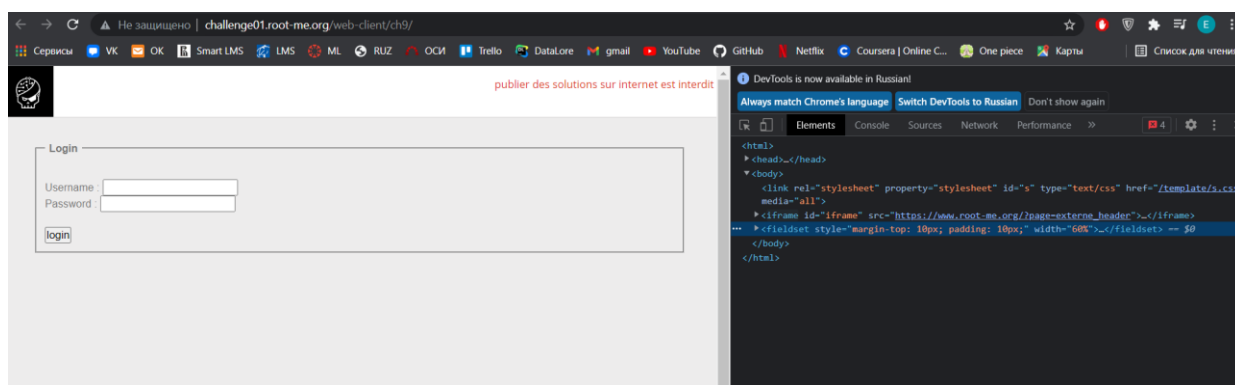


Рисунок 5. Начало вызова «Javascript authentication»

```
<html>
  <head>
    <script type="text/javascript" src="login.js"></script> == $0
  </head>
  <body>
    <link rel="stylesheet" property="stylesheet" id="s" type="text/css" href="/template/s.css"
      media="all">
    <iframe id="iframe" src="https://www.root-me.org/?page=externe_header"></iframe>
    <fieldset style="margin-top: 10px; padding: 10px; width="60%"></fieldset>
  </body>
</html>
```

Рисунок 6. Нашли файл с подозрительным именем

```
/*  */
function Login(){
    var pseudo=document.login.pseudo.value;
    var username=pseudo.toLowerCase();
    var password=document.login.password.value;
    password=password.toLowerCase();
    if (pseudo=="4dm1n" &amp;&amp; password=="sh.org") {
        alert("Password accepté, vous pouvez valider le challenge avec ce mot de passe.\nYou an validate the challenge using this password.");
    } else {
        alert("Mauvais mot de passe / wrong password");
    }
}
/* ]]&gt; */</pre></div><div data-bbox="281 219 785 237" data-label="Caption"><p>Рисунок 7. Перешли в файл и нашли связку логин/пароль</p></div><div data-bbox="195 244 872 422" data-label="Image"><img alt="Screenshot of the challenge01.root-me.org web-client/ch9/ page. The page shows a login form with fields for Username (4dm1n) and Password (*****). A modal dialog box is displayed over the form, containing the text: 'Подтвердите действие на странице challenge01.root-me.org', 'Password accepté, vous pouvez valider le challenge avec ce mot de passe.', and 'You an validate the challenge using this password.' with an OK button."/></div><div data-bbox="219 434 850 452" data-label="Caption"><p>Рисунок 8. Получили сообщение о том, что пароль – ключ к испытанию</p></div><div data-bbox="137 488 318 504" data-label="Section-Header"><h2>HTML - Source code</h2></div><div data-bbox="137 515 843 551" data-label="Text"><p>В задании «HTML Source code» была найдена уязвимость Information Disclosure/ Information Leakage – пароль хранился в комментариях к коду в HTML файле.</p></div><div data-bbox="210 558 859 724" data-label="Image"><img alt="Screenshot of the challenge01.root-me.org web-serveur/ch1/ page. The page shows a login form with a Password field and a login button. The title of the page is 'Login v0.00001'."/></div><div data-bbox="316 734 750 753" data-label="Caption"><p>Рисунок 9. Начало вызова «HTML – Source code»</p></div>
```

```

<html>
<head></head>
<body>
  <link rel="stylesheet" property="stylesheet" id="s" t
  1">
  <iframe id="iframe" src="https://www.root-me.org/2pag
  <!--

  Bienvenue sur ce portail,
  Welcome on this portal,

  J'espère que vous passerez un agréable moment parmi n
  choses dans la tête...
  I hope that you will enjoy your time among us, and ab
  in the head ...

  @ très bientôt
  See ya

  -->
  <h1>Login v0.00001</h1>
  <form>...</form>
  <!--

  Je crois que c'est vraiment trop simple là !

  It's really too easy !

  password : nZ^&q5&sjJHev0

  --> == $0
  </body>
</html>

```

Рисунок 10. Сразу же находим ключ-пароль в комментарии к коду

Weak password

В задании «Weak password» была найдена уязвимость Authentication/Brute Force – а именно был использован ненадежный пароль, совпадающий с логином. Так как admin – один из самых распространенных логинов – а дублирование логина в пароле достаточно простая гипотеза для проверки, пароль подобрать не составило труда.

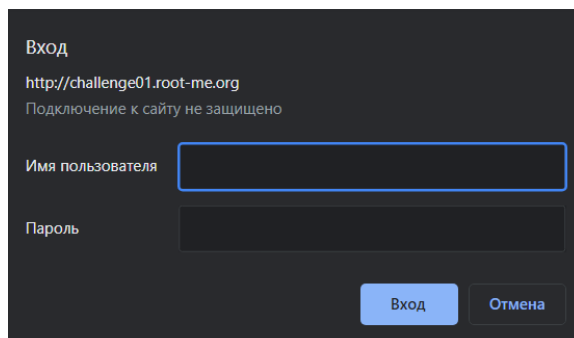
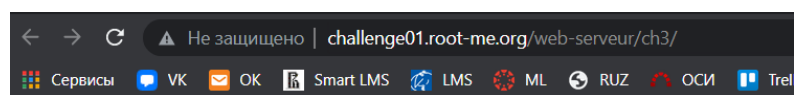


Рисунок 11. Начало вызова «Weak password»



Bien joué, vous pouvez utiliser ce mot de passe pour valider le challenge

Well done, you can use this password to validate the challenge

Рисунок 12. Небольшой перебор и пароль подобран

ОПИСАНИЕ ПОДХОДОВ, ЧТОБЫ ИЗБЕЖАТЬ ПОДОБНЫЕ УЯЗВИМОСТИ

В случае с «HTML disabled buttons» - лучшей практикой будет не использовать тег disabled для отключения функционала, у которого уже присутствует логика.

В случае с «Javascript - Authentication» - лучшей практикой будет избежать аутентификации через фронтэнд и вынести эту логику на серверную часть.

В случае с «HTML Source code» - лучшей практикой будет воздержаться от написания паролей в комментариях к коду.

В случае с «Weak password» - лучшей практикой для пользователя - будет использовать надежные пароли, которые трудно подбираются через брутфорс, а для автора – не дать возможности пользователю использовать легкий для подбора пароль.

ВЫВОД

Я изучил и отработал базовые атаки на веб-ориентированные системы