

localhost/index.php?page=set-background-color.php

Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Resolute attack « Adm... Методы обхода


Привет! Для создания меню правого шельма

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.11.4 Security Level: 0 (Hosed) Hints: Enabled Not Logged In

Home | Login/Register | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data

Set Background Color

 Help Me!

Hints and Videos

Please enter the background color you would like to see

Enter the color in RRGGBB format
(Example: Red = FF0000)

The current background color is 000000

Request

Raw Hex

```
1 POST /index.php?page=set-background-color.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
  Gecko/20100101 Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost/index.php?page=set-background-color.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 83
10 Origin: http://localhost
11 Connection: close
12 Cookie: security_level=1; PHPSESSID=o0mf4mob7kopnb72lc21qksuu3;
  showhints=1
13 Upgrade-Insecure-Requests: 1
14 Sec-Fetch-Dest: document
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18 background_color=000000&set-background-color-php-submit-button=
  Set+Background+Color
```

Response

Pretty Raw Hex Render

```
1 <div style="margin-right: 5px;" />
2 <a class="hint-header" href="
3 hints-page-wrapper.php?levelHin
  tIncludeFile=55" title="Click to
  open Cross-site Scripting with
  BeEF Framework hint in new tab"
  target="_blank" />Cross-site
  Scripting with BeEF Framework
4 </a>
5 </div>
6 <form action="
7 index.php?page=set-background-color.ph
  p"
8 method="post"
9 enctype="
10 application/x-www-form-urlencoded"
11 onsubmit="return onSubmitOffForm(this);
  "
12 style="background-color: #000000"
13 >
14 <table>
15 <tr id="id-bad-cred-tr" style="
16 display: none;">
```

Sec-Fetch-Site: same-origin	1207	onsubmit="return onSubmitOfForm(this);"
Sec-Fetch-User: 71	1208	style="background-color: #parrot<>"
background_color=#parrot<>&set-background-color-php-submit-button=	1209	>
Set+Background+Color	1210	<table>
	1211	<tr id="id-bad-cred-tr" style="display: none;">

При вводе нагрузки `<script>alert(XSS-alert)</script>` атакуемый сайт благополучно съедает скрипт и на сайте выдѣт информационное окно.

```

<tr>
  <td class="informative-message"
  colspan="2" style="text-align:
  center;">
    The current background color
    is <script>
      alert(XSS-alert)
    </script>
  </td>
</tr>

```

Выводы и рекомендации по устранению

Уязвимость позволяет ввести исполняемую нагрузку в поле ввода. Не требуются дополнительные уязвимости для эксплуатации.

Рекомендации по устранению:

- Необходима настройка валидации входных данных.
- Экранирование вывода.
- Настройка CSP.

Используемое программное обеспечение

- BurpSuite
- Браузер Firefox browser 102.8.0esr (64-bit)