enchant97 / **note-mark** Public

Code | Issues 9 | Pull requests | Discussions | Actions | Projects | Se

Commit 6bb6284

enchant97 committed 5 days ago Verified

```
(backend) prevent XSS attack from opening attachment

fixes GHSA-9pr4-rf97-79qh.
```

main · v0.19.2

1 parent a42a33c commit 6bb6284

1 file changed +12 -4 lines changed

Top

Filter files…

backend/handlers

assets.go

1 file changed +12 -4 lines changed

Search within code

backend/handlers/assets.go

```
@@ -144,13 +144,21 @@ func (h AssetsHandler) GetNoteAssetContentByID(
144 144            }
145 145            return &huma.StreamResponse{
146 146                Body: func(ctx huma.Context) {
147     -                  ctx.SetHeader("Content-Type", info.MimeType)
    147 +                  ctx.SetHeader("X-Content-Type-Options", "nosniff")
    148 +                  if info.MimeType == "" || info.MimeType == "text/html" ||
        info.MimeType == "image/svg+xml" {
    149 +                      ctx.SetHeader("Content-Type", "application/octet-stream")
    150 +                      ctx.SetHeader(
    151 +                          "Content-Disposition",
    152 +                          fmt.Sprintf("attachment; filename=\"%s\"", asset.Name))
    153 +                  } else {
```

```
      154 +                   ctx.SetHeader("Content-Type", info.MimeType)
      155 +                   ctx.SetHeader(
      156 +                       "Content-Disposition",
      157 +                       fmt.Sprintf("inline; filename=\"%s\"", asset.Name))
      158 +               }
148   159                 ctx.SetHeader(
149   160                     "Last-Modified",
150   161                     core.TimeIntoHTTPFormat(info.LastModified))
151         -           ctx.SetHeader(
152         -               "Content-Disposition",
153         -               fmt.Sprintf("inline; filename=\"%s\"", asset.Name))
154   162           writer := ctx.BodyWriter()
155   163           io.Copy(writer, stream)
156   164           stream.Close()
```

Comments 0

Please sign in to comment.