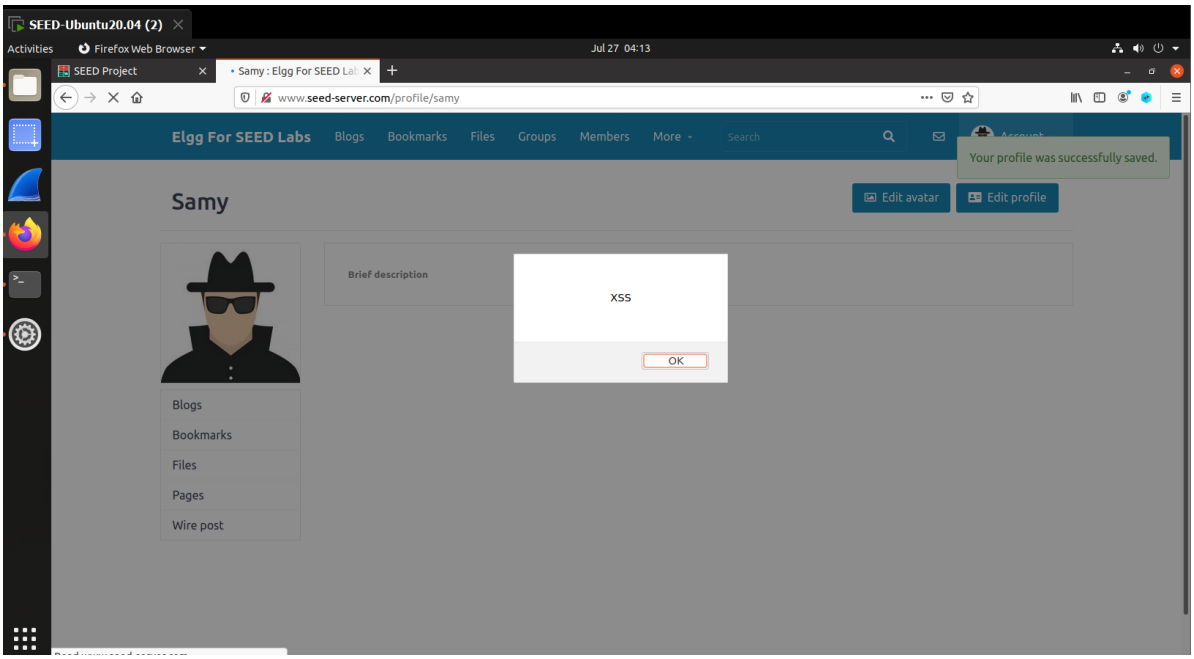
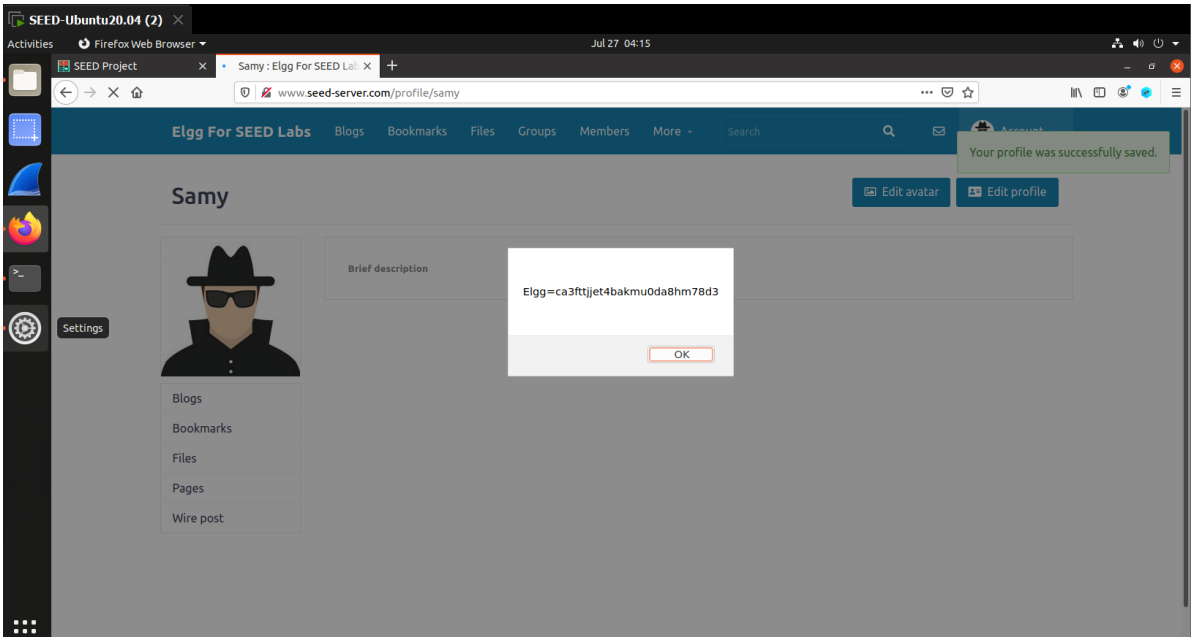
XXS

task1

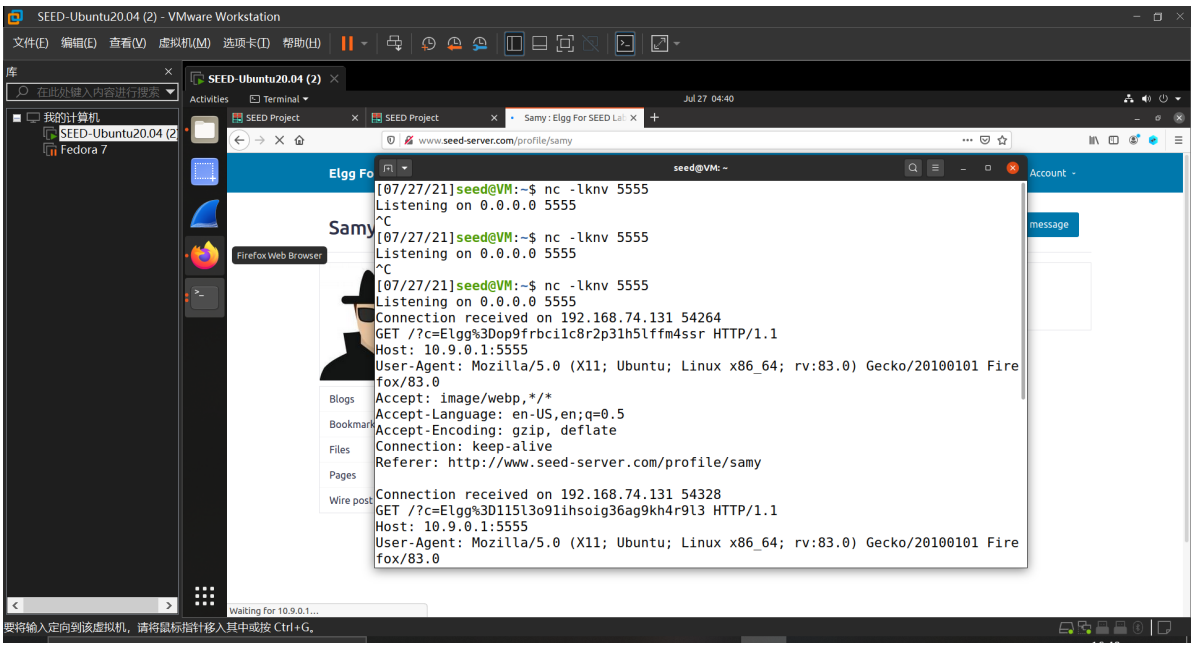
修改samy主页



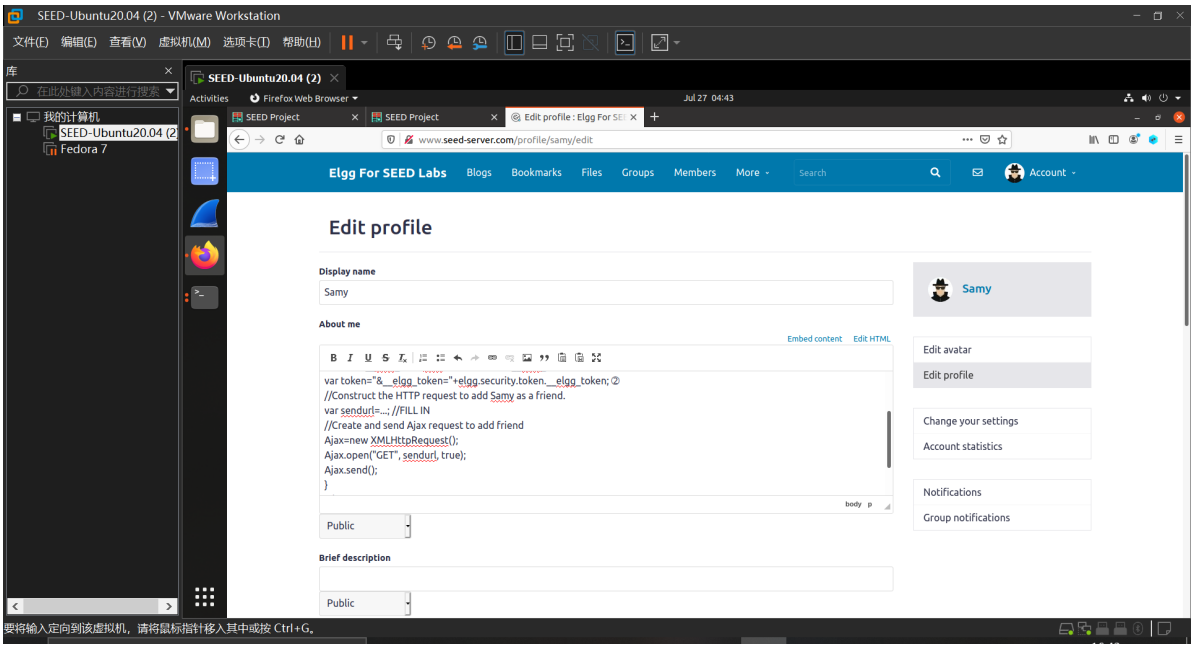
Task 2: Posting a Malicious Message to Display Cookies

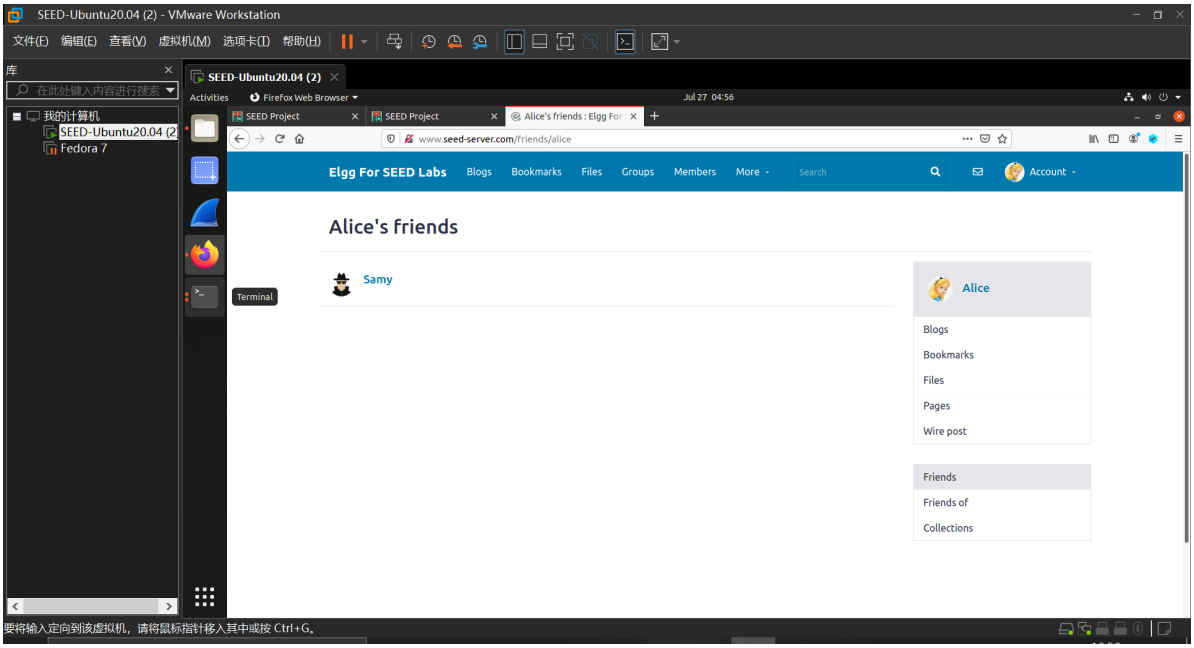


Task 3: Stealing Cookies from the Victim’s Machine

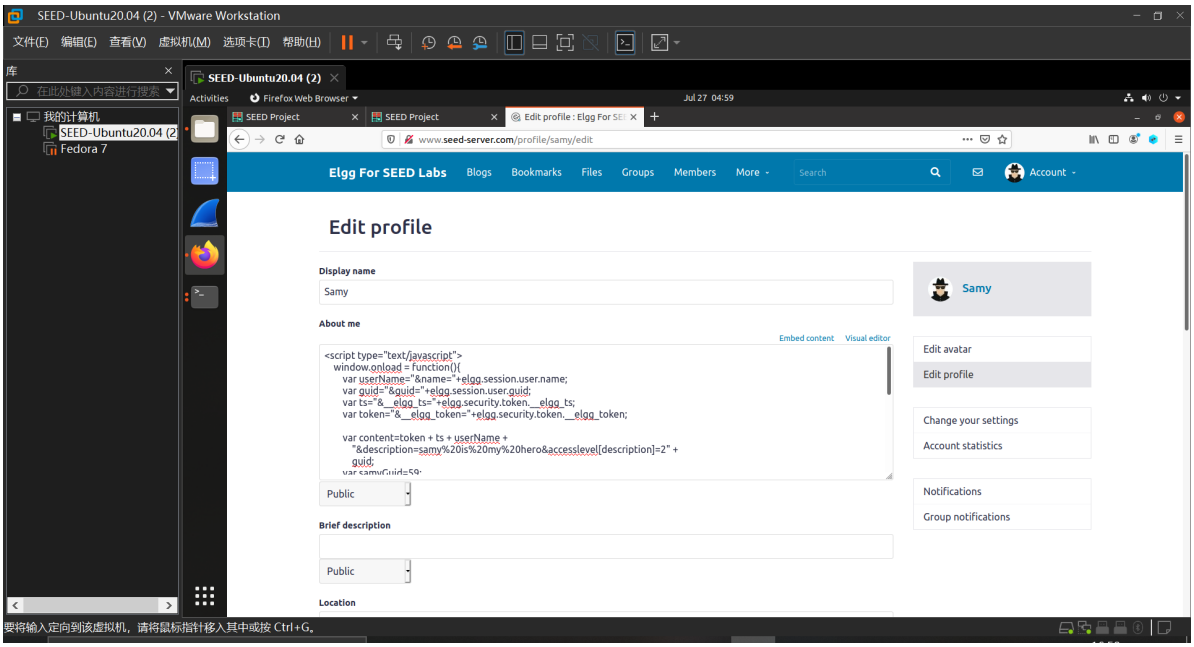


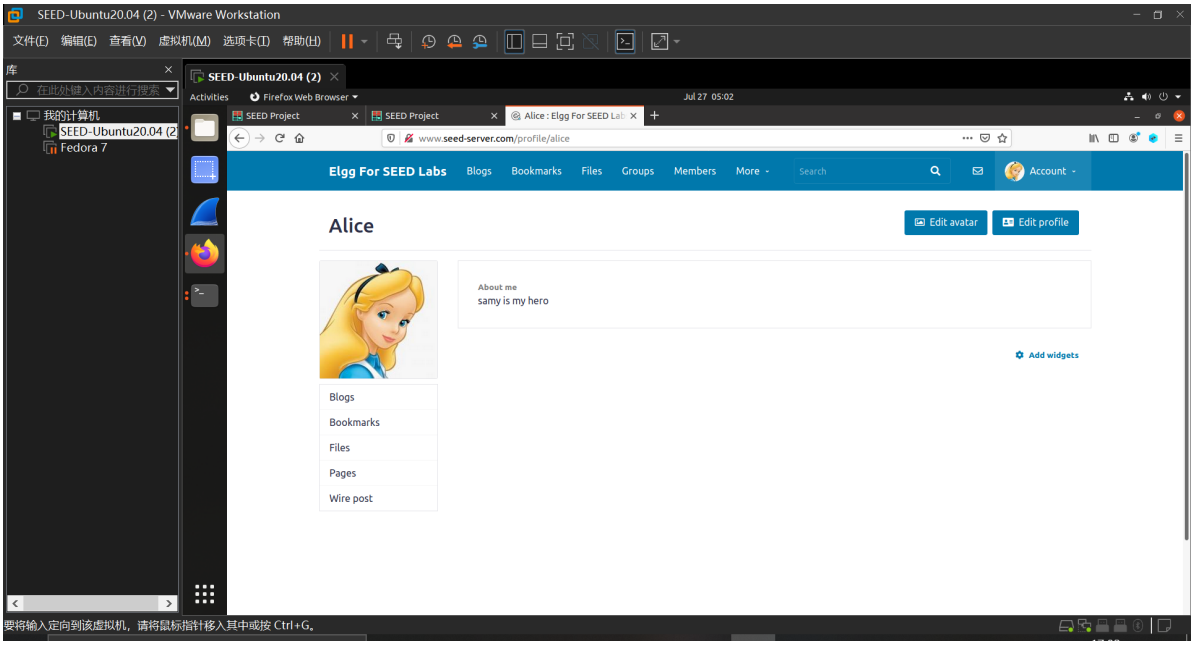
Task 4: Becoming the Victim's Friend



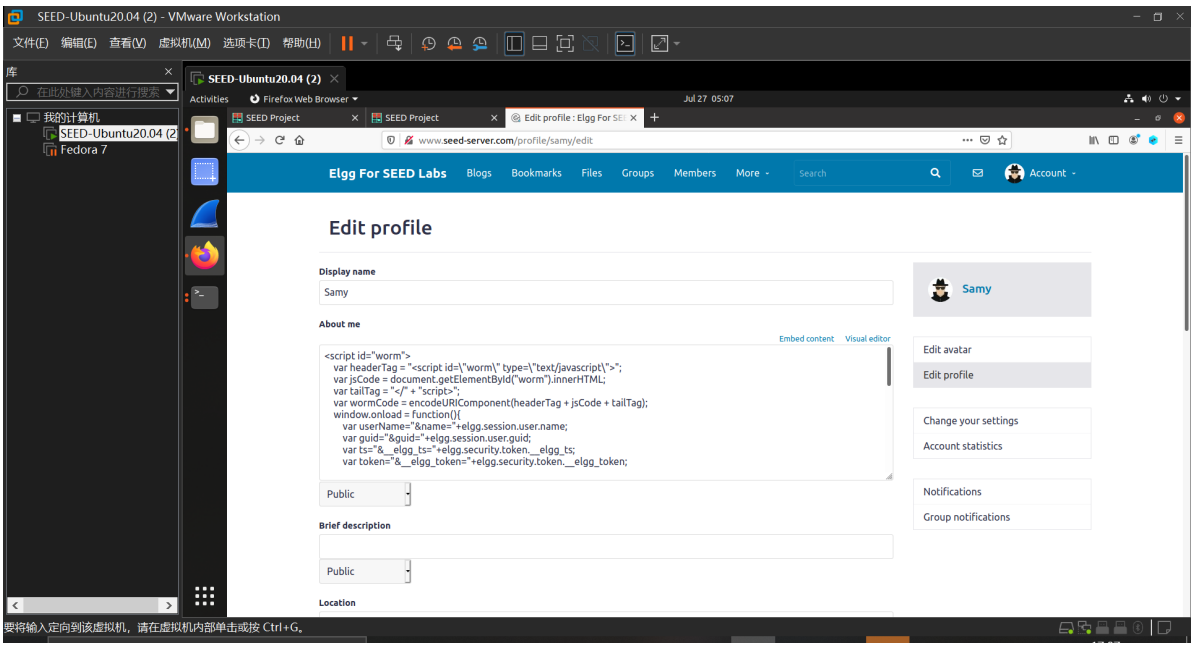


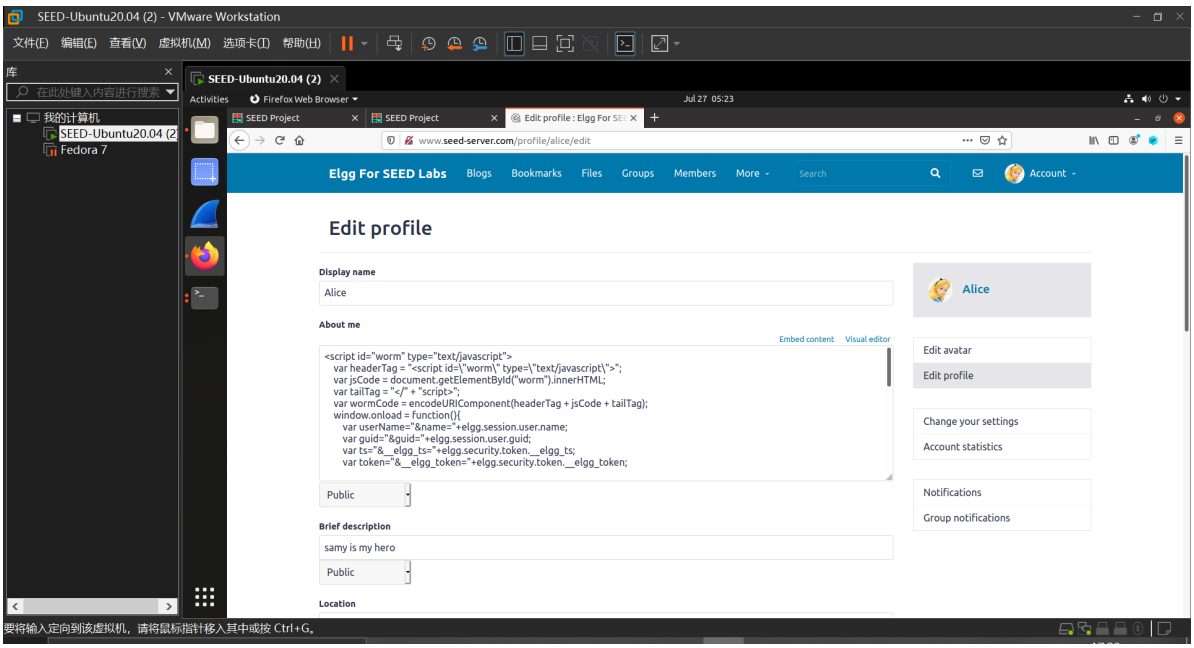
Task 5: Modifying the Victim's Profile

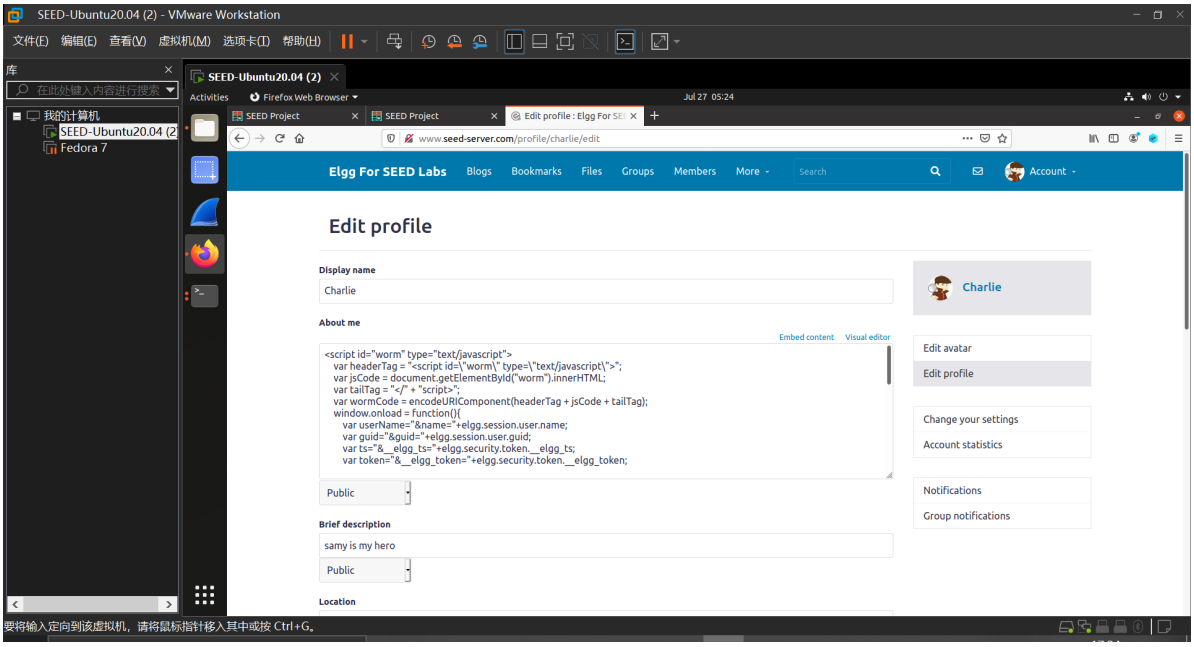




Task 6: Writing a Self-Propagating XSS Wor

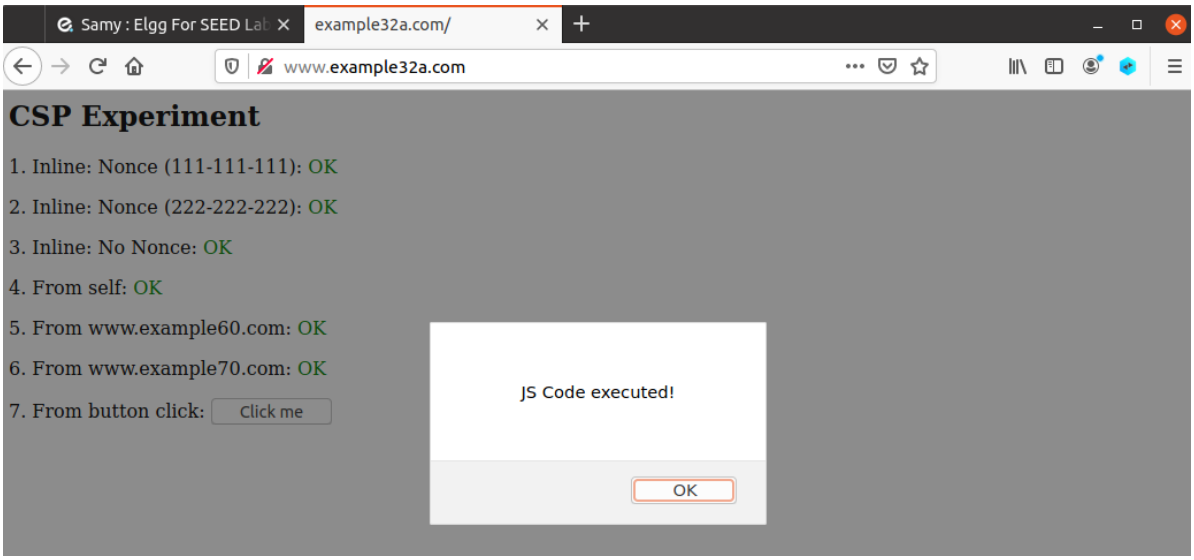


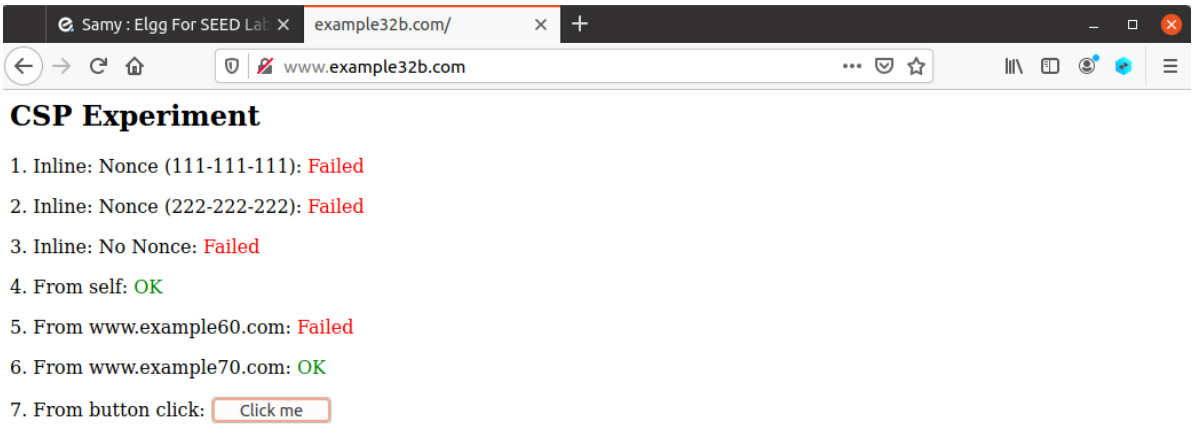


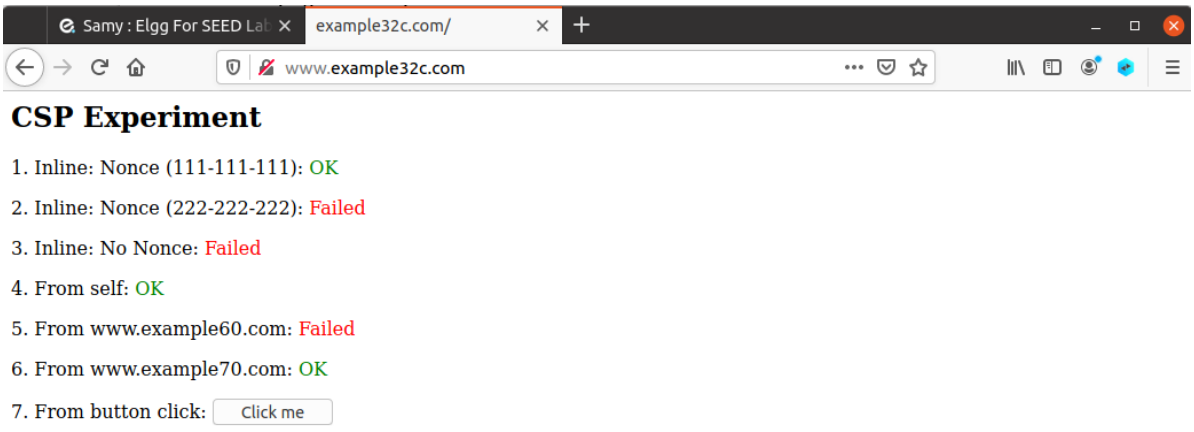


Task 7: Defeating XSS Attacks Using CSP

这个 Task 探究 CSP 防御 XSS 的作用。原始状态为





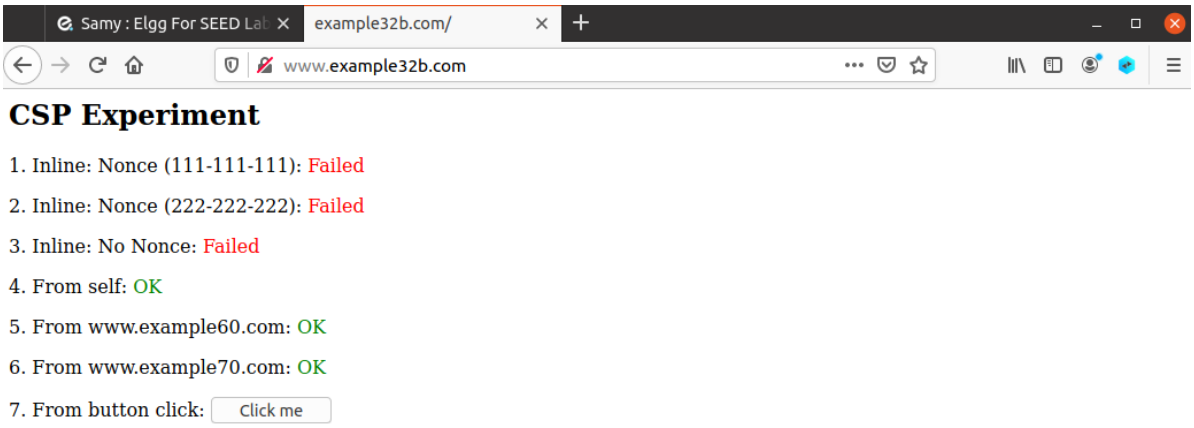


修改 apache_csp.conf

```
# Purpose: Setting CSP policies in Apache configuration
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32b.com
    DirectoryIndex index.html
    Header set Content-Security-Policy " \
            default-src 'self'; \
            script-src 'self' *.example60.com \
            script-src 'self' *.example70.com \
        "
</VirtualHost>
```

```
# Purpose: Setting CSP policies in Apache configuration
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32b.com
    DirectoryIndex index.html
    Header set Content-Security-Policy " \
              default-src 'self'; \
              script-src 'self' *.example60.com \
              script-src 'self' *.example70.com \
            "
</VirtualHost>
```

看到 example32b.com 的 4、5、6 变成了 OK



修改 phpindex.php

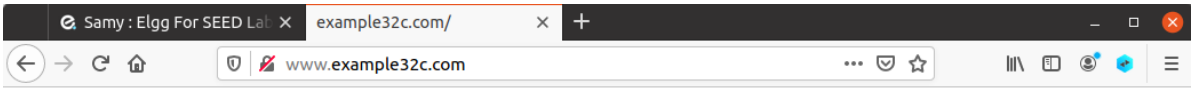
```
<?php
    $cspheader = "Content-Security-Policy:".
                 "default-src 'self';".
                 "script-src 'self' 'nonce-111-111-111' 'nonce-222-222-222'
*.example60.com *.example70.com".
    header($cspheader);
?>

<?php include 'index.html';?>
```

```
<?php
  $cspheader = "Content-Security-Policy:".
               "default-src 'self';".
               "script-src 'self' 'nonce-111-111-111' 'nonce-222-222-222' *.example60.com
*.example70.com".
  header($cspheader);
?>

<?php include 'index.html';?>
```

看到 example32c.com 的 1、2、4、5、6 变成了 OK



CSP Experiment

1. Inline: Nonce (111-111-111): OK
2. Inline: Nonce (222-222-222): OK
3. Inline: No Nonce: OK
4. From self: OK
5. From www.example60.com: OK
6. From www.example70.com: OK
7. From button click: Click me

> Please explain why CSP can help prevent Cross-Site Scripting attacks.

显然的，CSP 就是白名单制度，明确告诉客户端，哪些外部资源可以加载和执行。