

**Finding Name: URL links**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Byeongnam Choe | SCR | Project Member | Ontrack | Oliver Power | No |
|  |  |  |  |  |  |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

I’ve discovered that OnTrack platform blocks users from posting suspicious and malicious scripts, but it allows users to post domain addresses and URLs. It seems it lets users redirect to the site without any warning message when a user clicks the link. Threat actors can exploit this to redirect users to their malicious websites, harvesting information such as IP addresses and types of internet browsers. Other web applications and sites, like Reddit and Quora, block users from posting domain addresses and URLs to protect their users from potential breaches.

**Risk Rating**  
Impact: Major  
Likelihood: High

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

If an attacker exploits this vulnerability, attackers could create websites designed to extract sensitive information from users, including their IP addresses. This could lead to breaches of privacy, potential identity theft, and damage to the reputation of the OnTrack platform

**Affected Assets**

User’s information

User's system

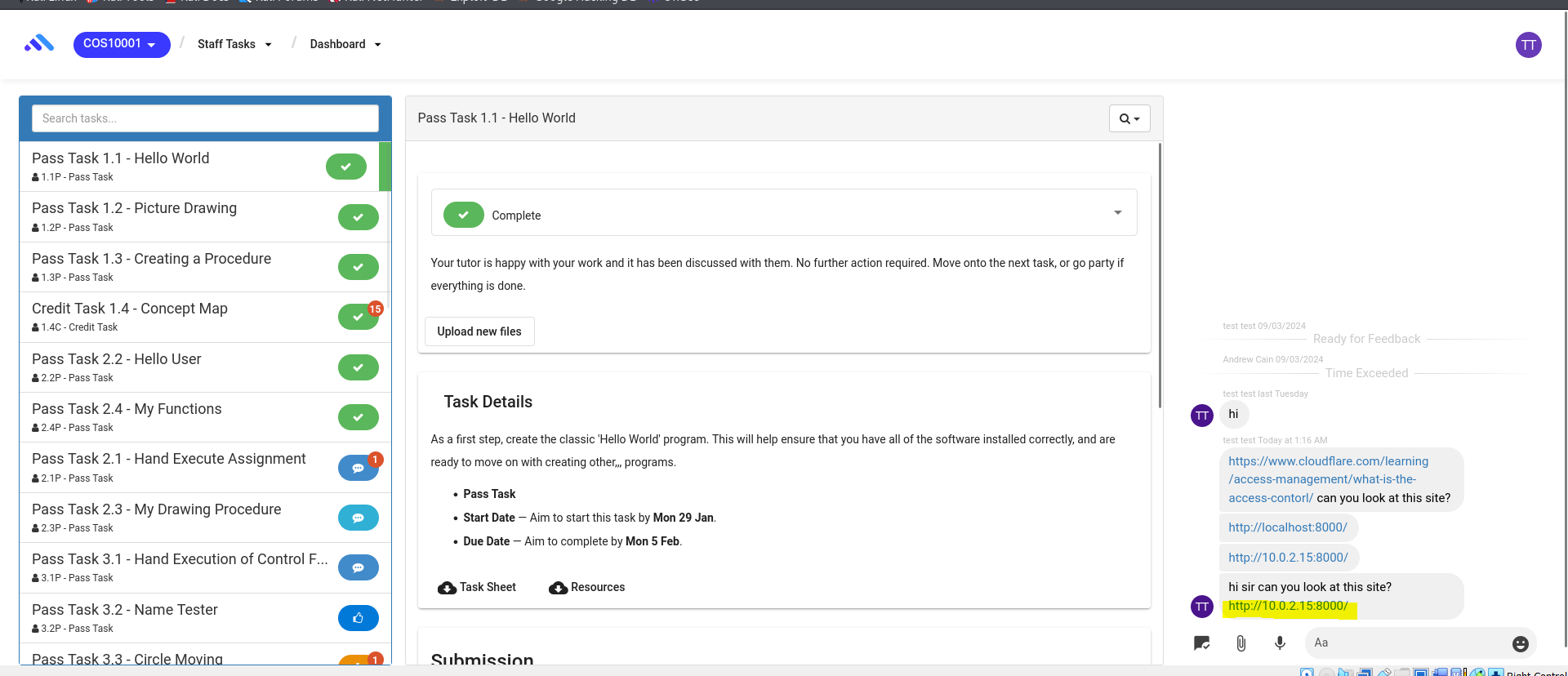
**Evidence**

Provide a step-by-step guide on how to reproduce the vulnerability with screenshots

**Step 1.**

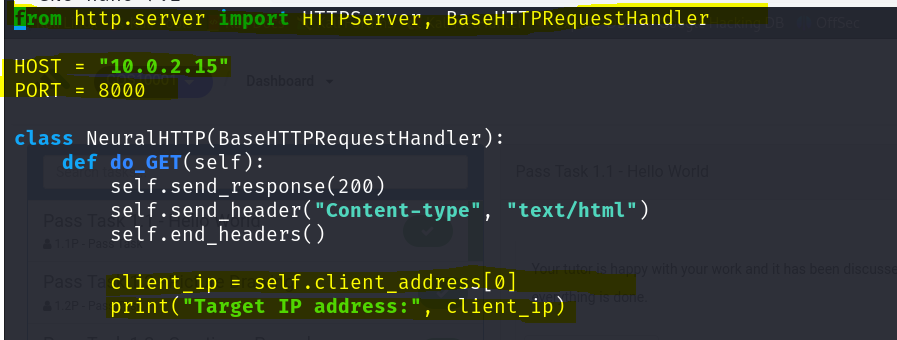
OnTrack allows users to post URLs, but it doesn't allow them to post suspicious scripts in comments.A screenshot of a chat

Description automatically generated



**Step 2.**

Create website designed to extract information from users



A screen shot of a computer

Description automatically generated

**Step 3.**

Login with username “student\_1” write “Hi, sir. Please look at this website. I'd like to know whether I can use lines of code from it in my own code?? http://10.0.2.15:8000 (seems legit website in real world case )” to trick the tutor into accessing the website. A screenshot of a computer

Description automatically generated

A screenshot of a computer

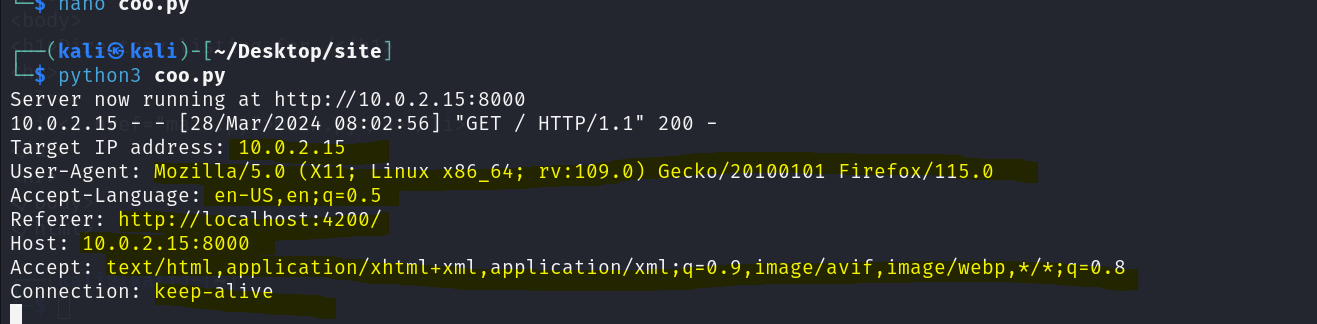
Description automatically generated

<http://10.0.2.15:8000> , The tutor may read the comment and click the link, as the link is accessible and not being blocked by OnTrack. User will be redirected to web site without any warming message once user click the link

Step4:

A screenshot of a computer

Description automatically generated

If a tutor clicks the link and accesses the website, they may see a message saying 'Sorry, you are hacked.'"

The attacker successfully harvest the information from the tutor.

**Remediation Advice**

Provide guidelines to tutors on avoiding clicking suspicious links or train tutors to enhance their cybersecurity awareness.

Implement a security policy that includes coding measures to detect domain addresses and URLs posted by users, subsequently blocking them from being posted on the website.

**References**

[**https://www.digitalocean.com/community/tutorials/python-simplehttpserver-http-server**](https://www.digitalocean.com/community/tutorials/python-simplehttpserver-http-server)

[**https://docs.python.org/3/library/http.server.html**](https://docs.python.org/3/library/http.server.html)

**Contact Details**

Byeongnam Choe (s222106547@deakin.edu.au)

**Pentest Leader Feedback.**

Thanks for your submission.

* Can you elaborate a bit more on the affected assets e.g., what if the link downloads a virus to the tutor's computer?
* I would recommend the likelihood to be high as it is very easy to implement, and the only line of defense is the tutor's cyber security awareness.
* What about remediations from a technical aspect?