Initial Dynamic Security Scan of Hackazon using Burp

Yingwei Liu

Liberty UniversityAuthor Note

Abstract

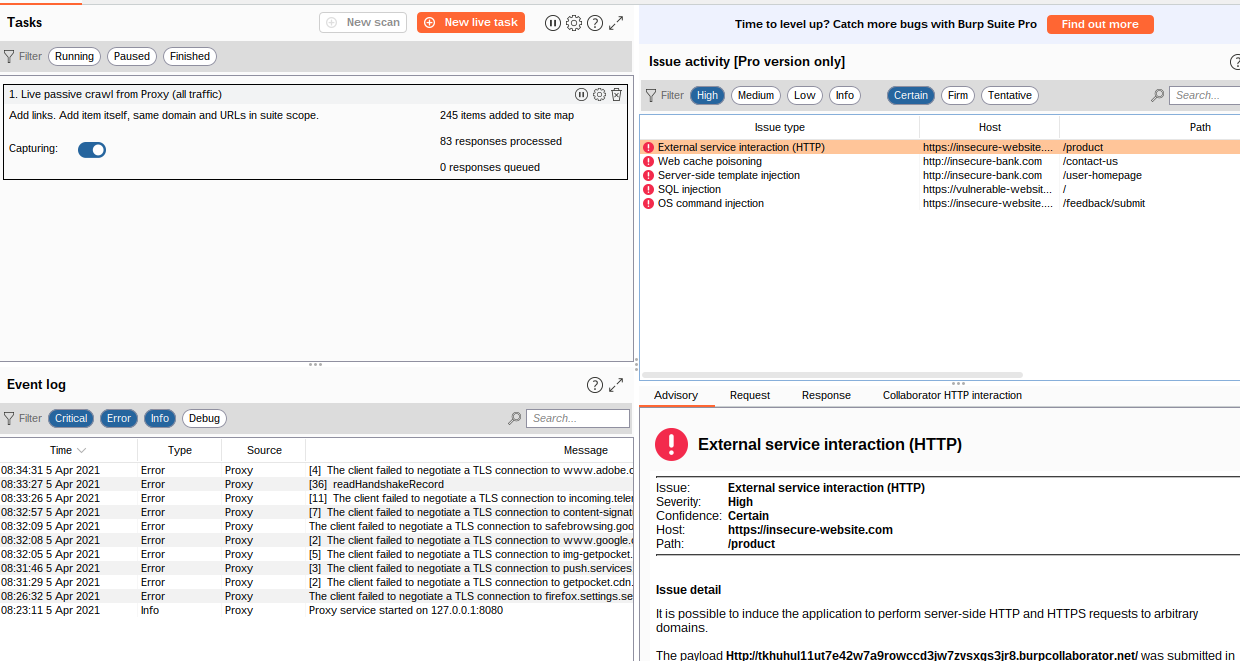
The goal of this phase is to perform the security scan of Hackazon web application by the Burp Site security scan software. This section requires to familiarize the scanning and enumeration via Burp. Also, it will provide a detailed vulnerability report of the Hackazon web application which based on the Burp security scan. After the report, it will demonstrate a personal reflection based on the Christian worldview.

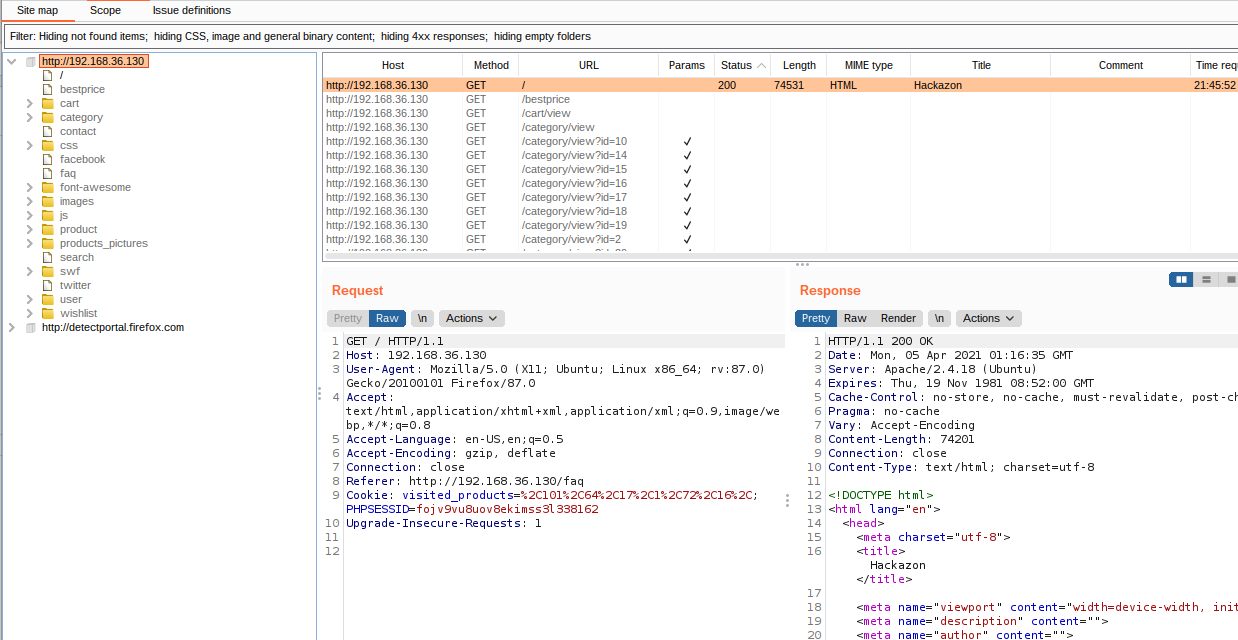
Keywords: Hackazon, Burp, Security, Scan

Initial Dynamic Security Scan of Hackazon using Burp

The phase one’s context is to apply the skills that we have and detect the vulnerabilities of the Hackazon web application. First, I need to provide the evidence of the configuration of burp. Second, I will present a detailed vulnerability report of the Hackazon Web Services. Third, it will demonstrate a discussion of how biblical worldview can impact in eh cybersecurity and ethical hacking field.

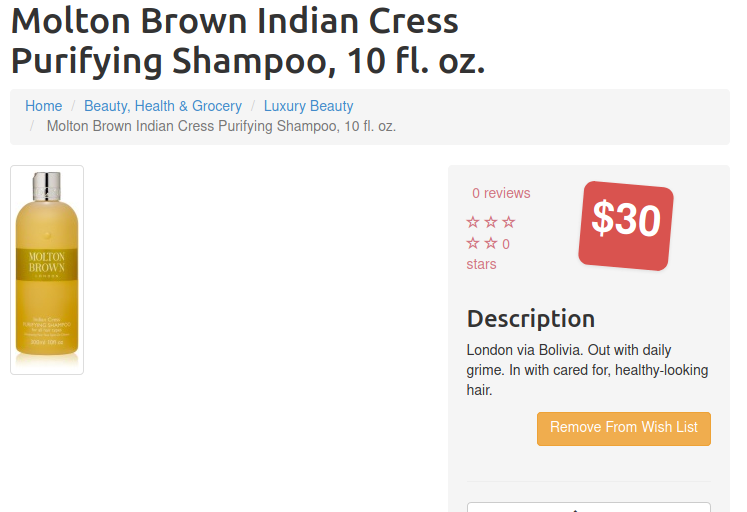
# Evidence of Configuration Screenshots

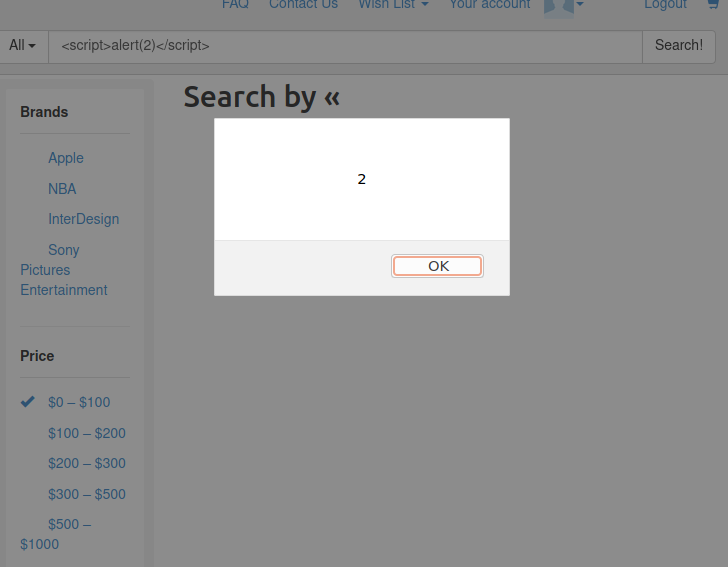




Scan the Hackazon web application through burp.

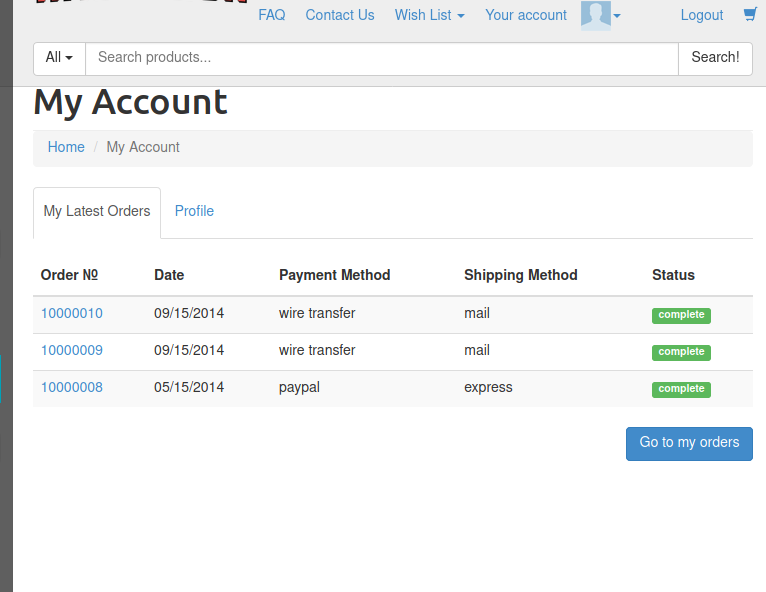
## XXS Scripting Threat

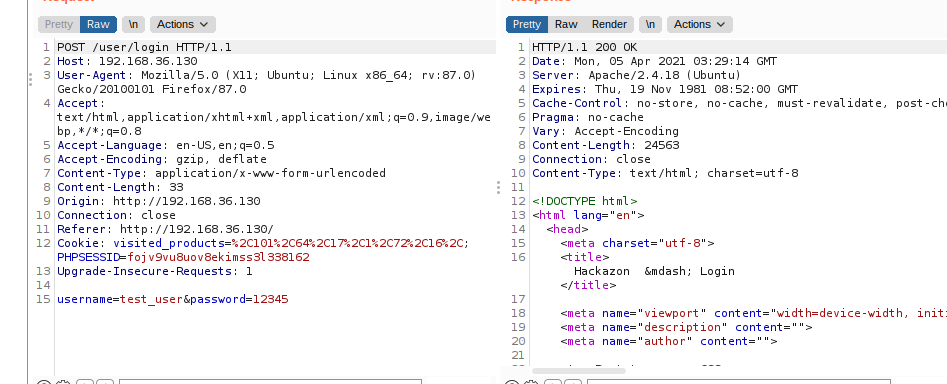




During the vulnerability testing process, I discovered that various Hackazon Endpoint accept user-supplied input. And the Hackzon does not validate input that come from client. So I tried Cross-site scripting as the injection attack that allows me to execute malicious scripts. I insert <script>alter(2)</script> into the product searching bar.

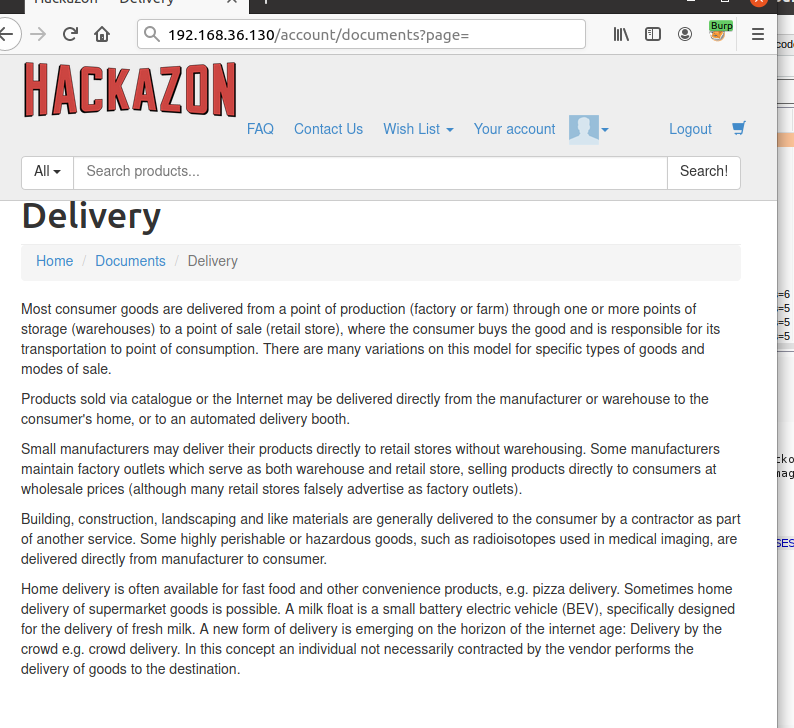
### Sensitive Data Exposure





Sensitive data exposure is another vulnerability that I detected during Burp security scanning. I used the default username and password that provided by the Hackazon web application to login. The data was not encrypted during the transfer process. And the websites does not have an SSL certificate.

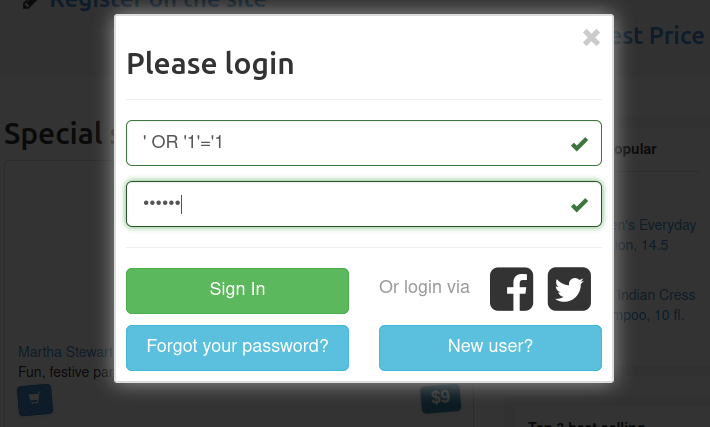
#### Injection

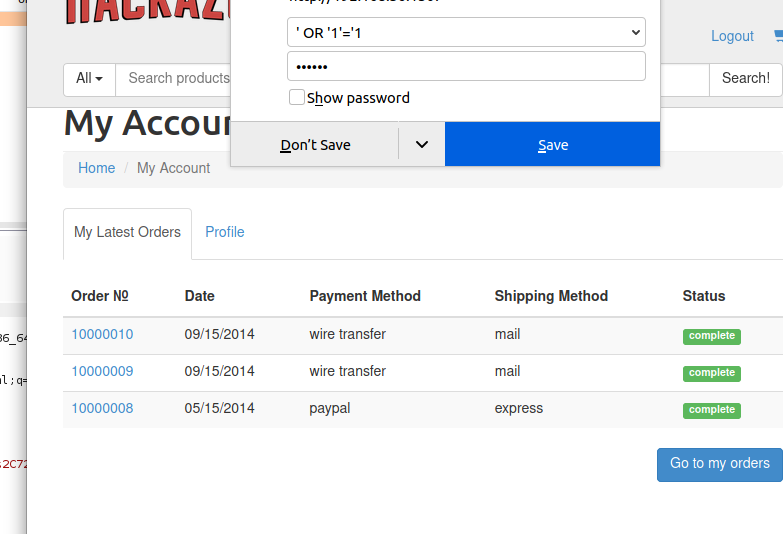




On command Injection is another threat that I detected through Burp. The delivery page in the Hackazon Web application is presented the html file of the page. So, if I changed the URL and make it switch to different directory. Then, all of the information will just be presented in the page.

**SQL Injection**





SQL injection is another type of injection that based on the SQL code. For example, like when we try to find the product or customer information in the Hackazon Web application. We are using the SQL command to connect with SQL server and search the information that we need. For the SQL injection vulnerabilities, I do not need to know any username or password, I can just apply based on the SQL command they are using and implement an extra line of code.

Through the completion of this lab, I think all these vulnerabilities could potentially result huge damage to the company. Especially, the sensitive information that we hold from our customers. We need to take the responsibilities for their privacy, since they entrusted our company. According to Ezra 8:21-23, “Then I proclaimed a fast there at the river of Ahava, that we might humble ourselves before our God to seek from Him a safe journey for us, our little ones, and all our possessions. For I was ashamed to request from the king troops and horsemen to protect us from the enemy on the way, because we had said to the king, “The hand of our God is favorably disposed to all those who seek Him, but His power and His anger are against all those who forsake Him.” So we fasted and sought our God concerning this matter, and He listened to our entreaty.” Just like cross-site vulnerabilities, it will the operating of the Hackazon website. The SQL injection could result the invalid access and data exposure of the Hackazon Web application. According to Kevin Graunke, “This spiritual reality is everlasting, and as we begin to comprehend the total goodness and all-power of God and His creation, the powerlessness of evil becomes more apparent. Seeking out the truth of being in this way makes us more conscious of the protecting and preserving power of God. We realize we have God-given dominion over attack, harm, and evil intent.” (2015) Cyber crime will not stop if we do not make any action.

References

Bible. Ezra 8:21-23. Retrievedfrom https://bible.knowing-jesus.com/topics/Security.

Graunke, K. (2015). Cybersecurity - and Prayer as an Active Protection*.* Retrieved from https://www.csmonitor.com/Commentary/A-Christian-Science-Perspective/2015/0403/Cybersecurity-and-prayer-as-an-active-protection.