# IT666 – Secure Testing Lab – Gruyere

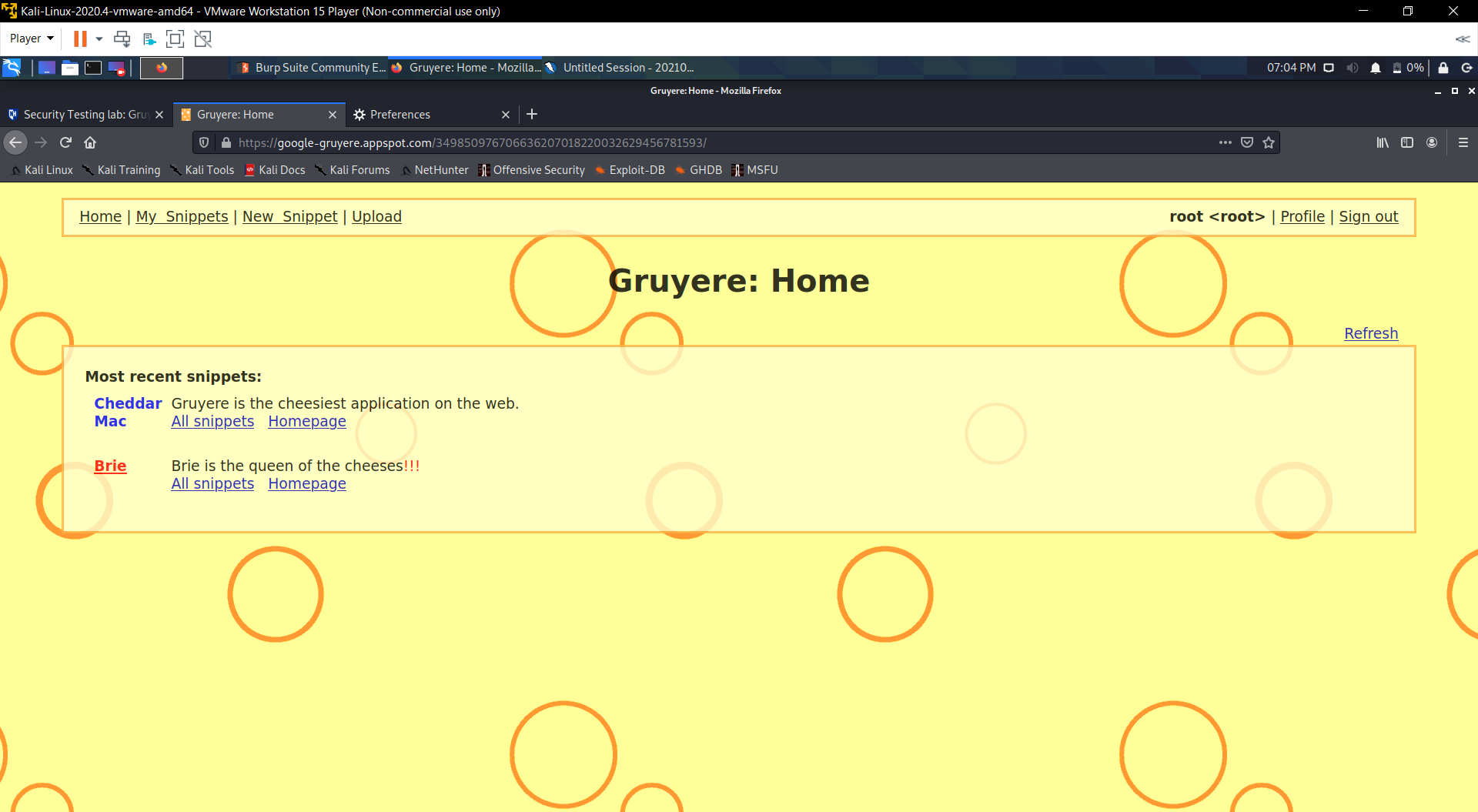
Ryan J. Skelly

[Rjs1070@wildcats.unh.edu](mailto:Rjs1070@wildcats.unh.edu)

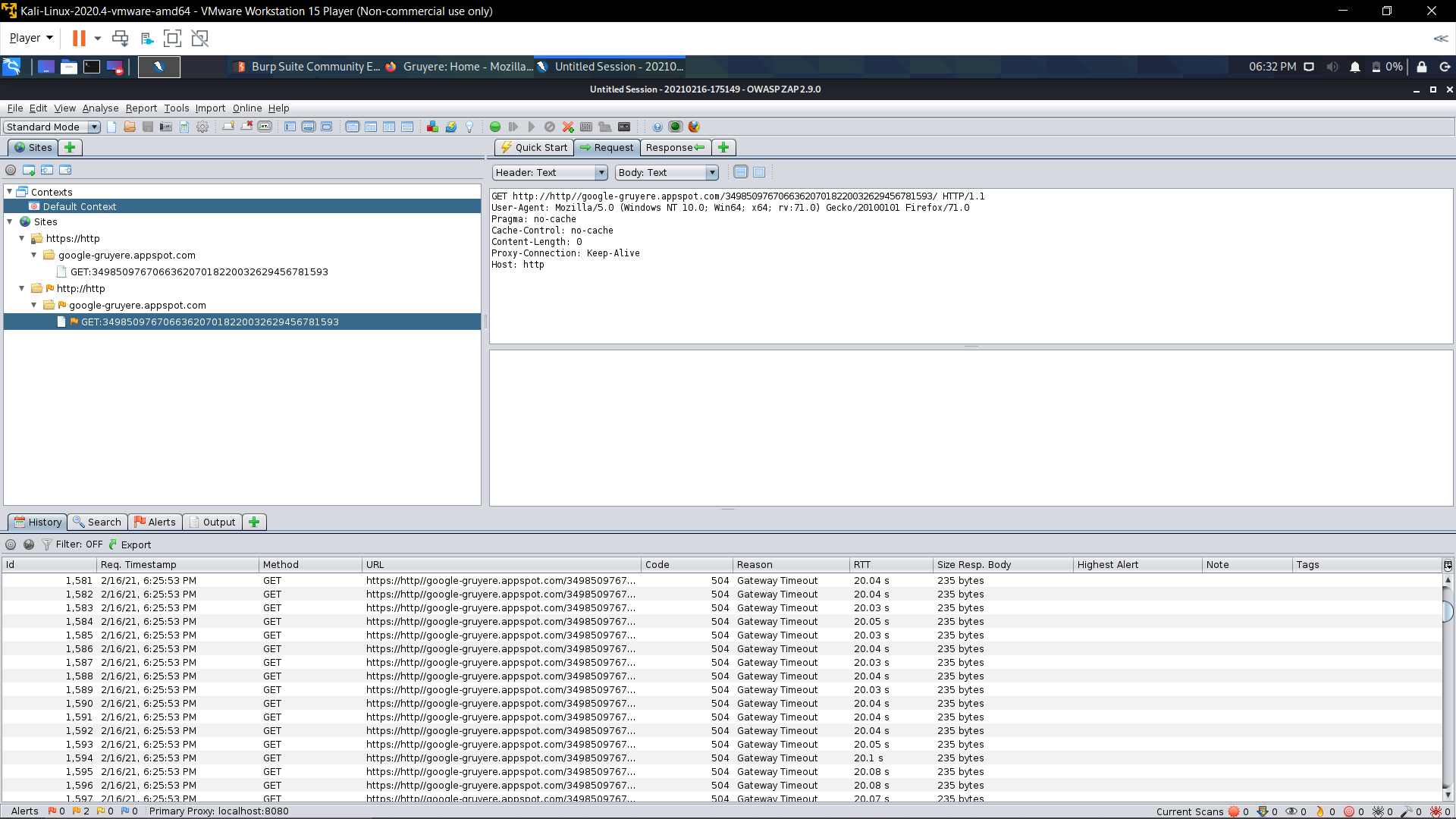
988977861

**Lab report**:

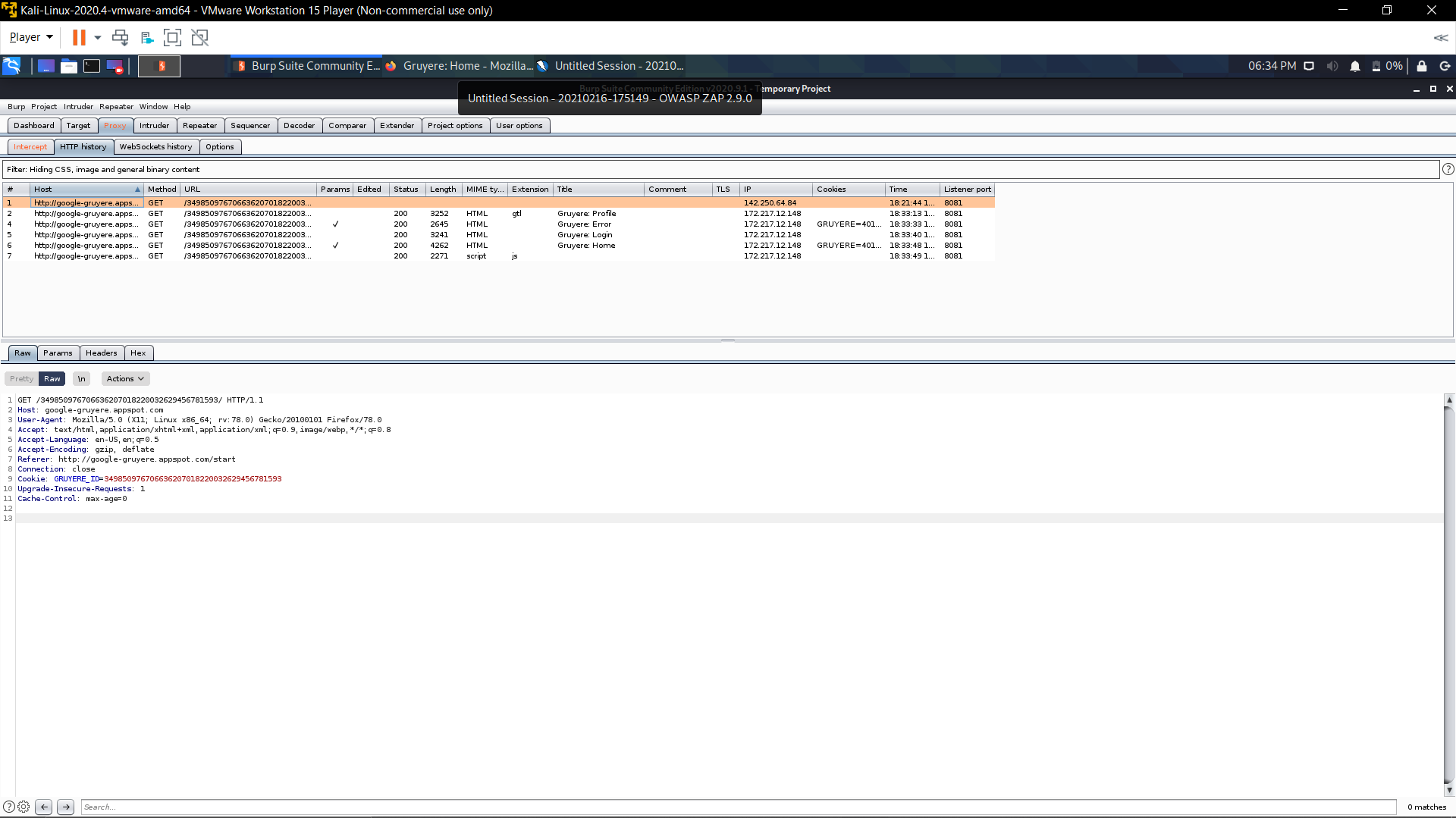
Task 1.1: (5 points) provide, a screen shot of your Gruyere instance



Task 1.2: (10 points) provide, a screen shot of the OWASP ZAP window

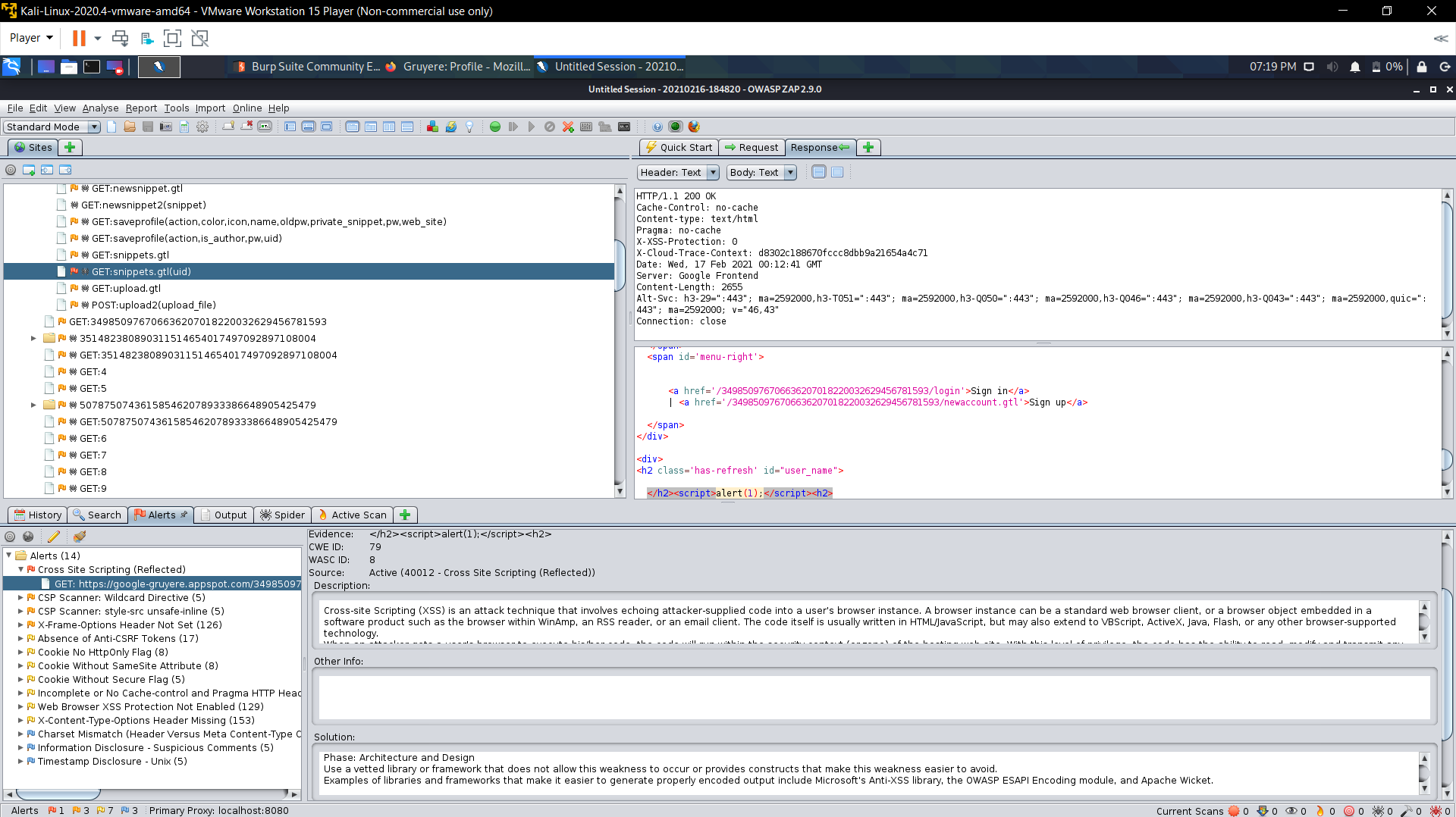


Task 1.3: (10 points) provide, a screen shot of the Burpsuite proxy - http history tab



**Lab report:**

Task 2.1: (10 points) Provide a screen capture of the ZAP window showing the alerts pane.



Task 2.2: (5 points) What "High Priority Alert" did ZAP find?

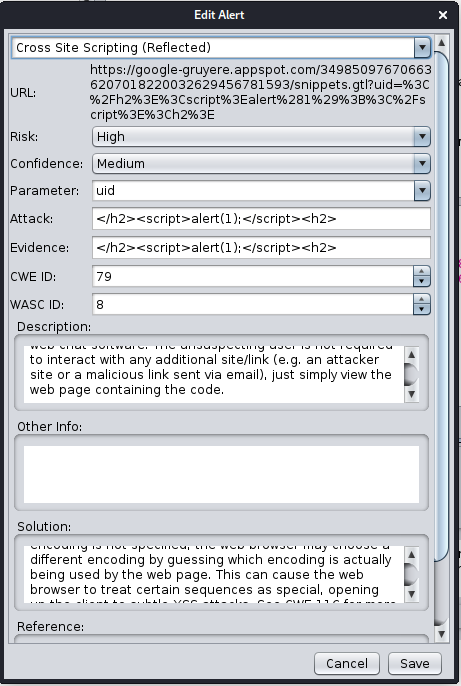
Cross Site Scripting(Reflected)

Task 2.3: (10 points) List the titles of all alerts generated by ZAP

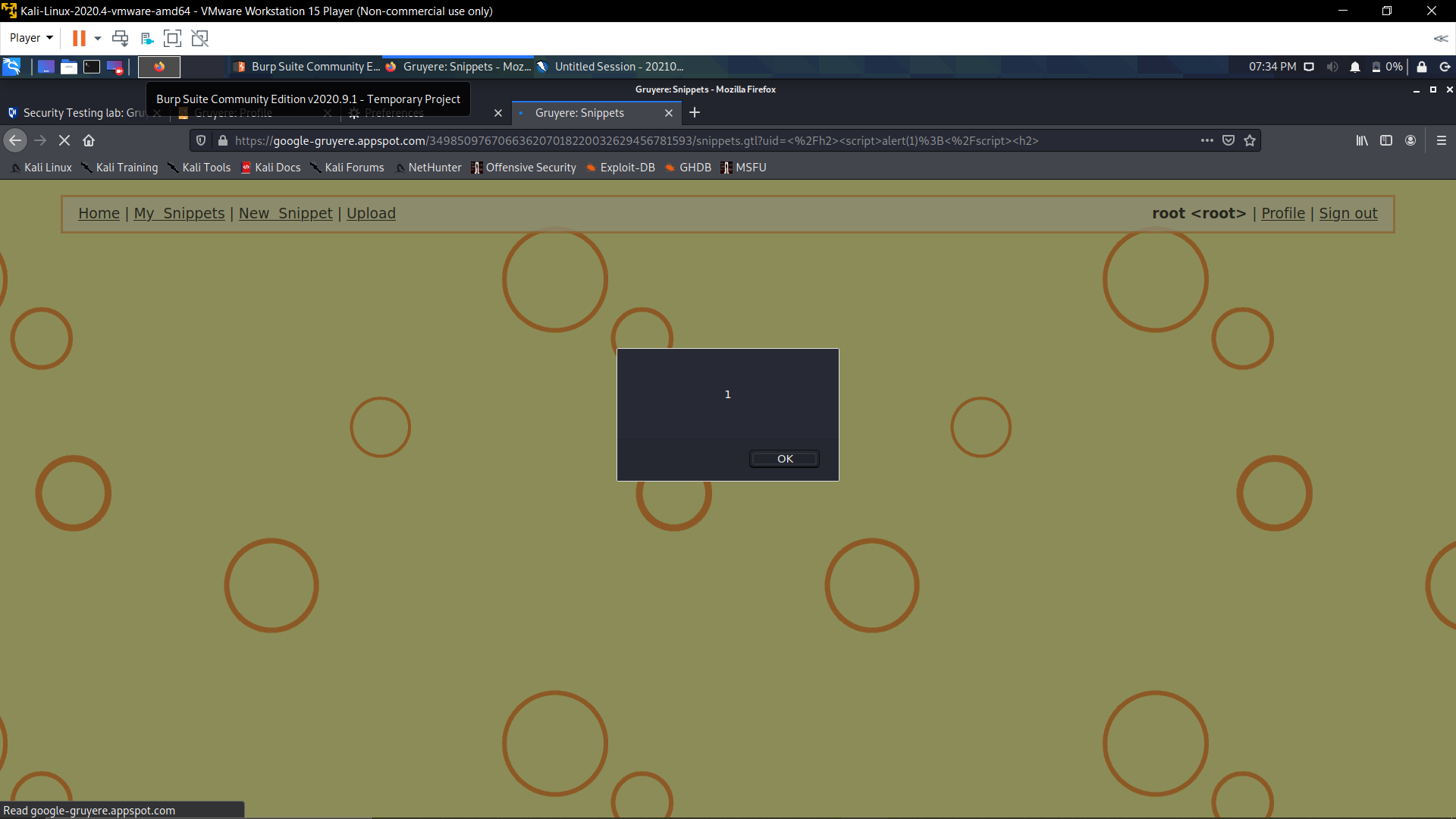
1. Cross Site Scripting(Reflected)
2. CSP Scanner: Wildcard Directive
3. CSP Scanner: style-src unsafe-inline
4. X-Frame-Options Header Not Set
5. Absence of Anti-CSRF Tokens
6. Cookie No HttpOnly Flag
7. Cookie Without SameSite Attribute
8. Cookie Without Secure Flag
9. Incomplete or No Cache-control and Pragma HTTP Header Set
10. Web Browser XSS Protection Not Enabled
11. X-Content-Type-Options Header Missing
12. Charset Mismatch (Header Versus Meta Conetnt-Type Charset)
13. Information Disclosure – Suspicious Comments
14. Timestamp Disclosure - Unix

**Lab report:**

Task 3.1: (10 points) Double click the reflected XSS alert and provide a screen capture of the "Edit Alert" dialog



Task 3.2: (15 points) provide, a screen shot of the validated XSS finding.



Task 4.1: (10 points) List the titles of all alerts generated by ZAP

1. Cross Site Scripting(Persistent)
2. Cross Site Scripting(Reflected)
3. SQL Injection
4. CSP Scanner: Wildcard Directive
5. CSP Scanner: style-src unsafe-inline
6. X-Frame-Options Header Not Set
7. Absence of Anti-CSRF Tokens
8. Cookie No HttpOnly Flag
9. Cookie Without SameSite Attribute
10. Cookie Without Secure Flag
11. Incomplete or No Cache-control and Pragma HTTP Header Set
12. Web Browser XSS Protection Not Enabled
13. X-Content-Type-Options Header Missing
14. Charset Mismatch (Header Versus Meta Content-Type Charset)
15. Information Disclosure – Suspicious Comments
16. Timestamp Disclosure - Unix

Task 4.2: (5 points) List the alerts "fixed" by using Burpsuite to rewrite headers

1. CSP Scanner: Wildcard Directive
2. CSP Scanner: style-src unsafe-inline
3. Cross Site Scripting(Persistent)

Task 4.3: (5 points) True/False: Adding the X-XSS-Protection header is the right thing to do?

True

Task 4.4: (5 points) What header(s) would you recommend to address XSS?

The X-XSS-Protection header protects against most cross-site scripting attacks