Q1 Study Group Information

0 Points

Students can optionally form study groups of *no more than 3 students* to complete lab activities.

Study groups are not allowed to collaborate to complete any other assignments in the course besides written lab activities.

Please enter the names/unityIDs (for example: Laurie Williams, lawilli3) of the students in your study group:

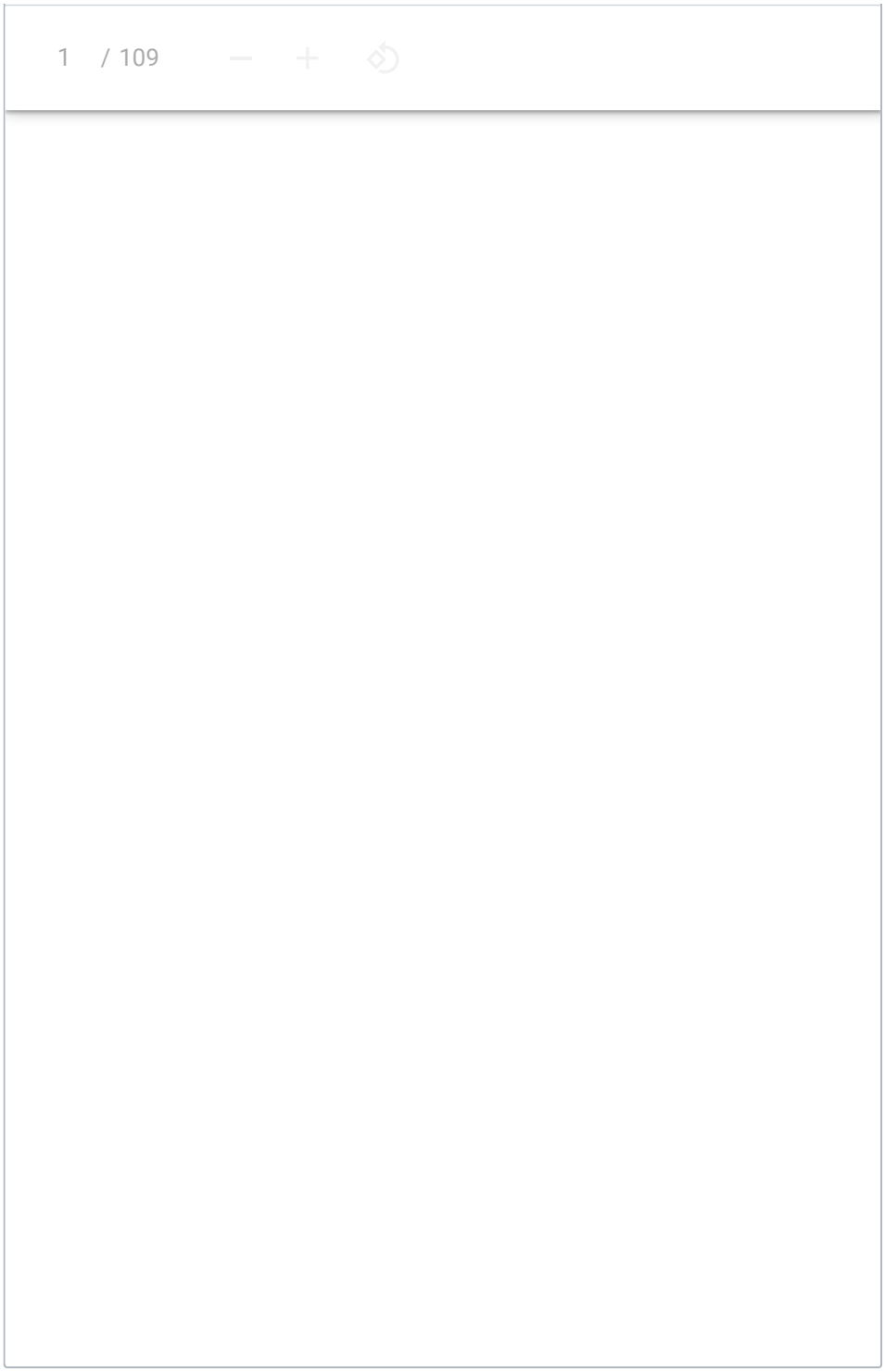
Vishnu Challa, vchalla2
Srujan Ponnur, sponnur
Varun Kumar Veginati, vvegina

Q2 Report Upload

50 Points

Upload the OWASP Dependency Check Report as a PDF.

▾ Dependency-Check Report.pdf Download



Q3 Potential Vulnerability
50 Points

From the report output, select a vulnerability that you find interesting.

Q3.1 Description
16 Points

In 3-4 sentences, briefly describe (in your own words) the vulnerability.

1. Cross-site-scripting vulnerability in jquery at wolfpack-juice-shop-2.0/node_modules/selenium-webdriver/lib/test/data/js/jquery-1.4.4.min.js.
2. jQuery version 1.9.0 and below is vulnerable to cross-site scripting attacks.
3. The CVE numbers of vulnerability are CVE-2011-4969 and CVE-2012-6708.

Q3.2 Impact

16 Points

In 3-4 sentences, briefly describe the potential impact to the web application if the vulnerability were exploited.

1. When using location.hash to select elements, attackers can remotely inject arbitrary web-script or HTML via a crafted tag.
2. When using HTML tags as strings, jquery differentiates them by looking at '<'. So, this is not a very reliable way to differentiate. This gives a lot of scopes for the attacker to embed faulty HTML code inside the string.
3. Using the web script or HTML, attackers can steal the cookie information of users.

Q3.3 Security Objectives

18 Points

In 3-4 sentences, briefly describe how the security objectives are threatened by this vulnerability.

1. Cross-site scripting helps attackers gain confidential insights over user information which can cause a monetary loss.
2. Users lose confidence in the credibility of the application thereby losing integrity if such a vulnerability is exploited.
3. It can also affect the availability of the application by taking control over the system.

Workshop 8: OWASP Dependency Check

GRADED

GROUP

Vishnu Challa
Srujan Ponnur
Varun Kumar Veginati
View or edit group

TOTAL POINTS

100 / 100 pts

QUESTION 1

Study Group Information — **0** / 0 pts

QUESTION 2

Report Upload — **50** / 50 pts

QUESTION 3

Potential Vulnerability — **50** / 50 pts

3.1 Description — **16** / 16 pts

3.2 Impact — **16** / 16 pts

3.3 Security Objectives — **18** / 18 pts