

## Insecure Direct Object Reference (IDOR) – All Student Homework Downloadable

### Observation:

The students of different classes using the application have option to upload their respective HomeWorks. However, it was observed that student and homework have unique ID's which are sequential and guessable. It makes it easy for one student from one class to download homework done by another student of another class.

### Steps To Replicate:

**Step 1:** Login inside **Student1** user account and traverse to homework section of the application and upload a homework.

The screenshot shows the 'Student Profile' page of the NFIX application. The browser address bar displays 'http://127.0.0.1/student-profile'. The page features a sidebar with navigation options like 'My Profile', 'Fees', 'Class Routine', 'Lesson Plan', 'Homework List', 'Study Material', 'Attendance', 'Leave', 'Chat', 'Examinations', 'Notice Board', 'Subjects', 'Online Exam', 'Teacher', and 'Transport'. The main content area is titled 'Student Details' and contains a profile card for 'Ash Ketchum' with fields for 'Admission Number' (1), 'Class' (one), 'Section' (hero), 'Gender' (Male), and 'Behaviour Records Point' (0). To the right, there are tabs for 'PROFILE', 'LEAVE', 'EXAM', 'ONLINE EXAM', 'DOCUMENTS', 'RECORD', and 'MY ATTENDANCE'. The 'PERSONAL INFO' section includes fields for 'Admission Date' (1st Jan, 2025), 'Date Of Birth' (4th Feb, 2020), 'Type', 'Religion', 'Phone Number' (9999999999), 'Email Address' (student1@campcodes.com), 'Present Address', and 'Permanent Address'. Below this is the 'PARENT/GUARDIAN DETAILS' section.

Once homework is uploaded it can be observed a student can download the homework. It can be observed that **Student1** has URL containing **"/1"** indicating **1<sup>st</sup> Admission** and **"/2"** indicating the attachment number.

The screenshot shows the 'Homework List' page of the NFIX application. The browser address bar displays 'http://127.0.0.1/student-homework'. The page features a sidebar with navigation options like 'Fees', 'Class Routine', 'Lesson Plan', 'Homework List', 'Study Material', 'Attendance', 'Leave', 'Chat', 'Examinations', 'Notice Board', 'Subjects', 'Online Exam', 'Teacher', 'Transport', and 'Library'. The main content area is titled 'Homework List' and contains a table with columns for 'Subject', 'Marks', 'Homework Date', 'Submission Date', 'Evaluation Date', 'Obtained Marks', and 'Status'. A row is visible with Subject 'ONE (HERO)', Marks '90', Homework Date '13th Jan, 2025', Submission Date '14th Jan, 2025', and Status 'INCOMPLETED'. Below the table, there is an 'ACTION' section with a 'SELECT' button and a 'VIEW' button. The 'VIEW' button is highlighted with a red box. The URL in the browser is 'http://127.0.0.1/download-uploaded-content/1/2'.

**Step 2:** Similarly, login inside **Student2** user account which is in a completely different class.

The screenshot shows the NFIX Student Profile page for a user named Ram Ram. The browser address bar shows the URL `127.0.0.1/student-profile`. The page features a sidebar with navigation options like My Profile, Fees, Class Routine, Lesson Plan, Homework List, Study Material, Attendance, Leave, Chat, Examinations, Notice Board, Subjects, Online Exam, Teacher, and Transport. The main content area is titled 'Student Details' and includes a profile picture placeholder. Below the picture, a red box highlights the following information:

- Student Name: Ram Ram
- Admission Number: 2
- Roll Number: (blank)
- Class: two
- Section: academy
- Gender: Male
- Behaviour Records Point: 0

To the right of the profile details is a 'PERSONAL INFO' section with the following data:

- Admission Date: 18th Jan, 2025
- Date Of Birth: 17th Jan, 2000
- Type: (blank)
- Religion: Hinduism
- Phone Number: 8989898989
- Email Address: student2@campcodes.com
- Present Address: (blank)
- Permanent Address: (blank)

At the bottom of the page, there is a 'PARENT/GUARDIAN DETAILS' section which is currently empty.

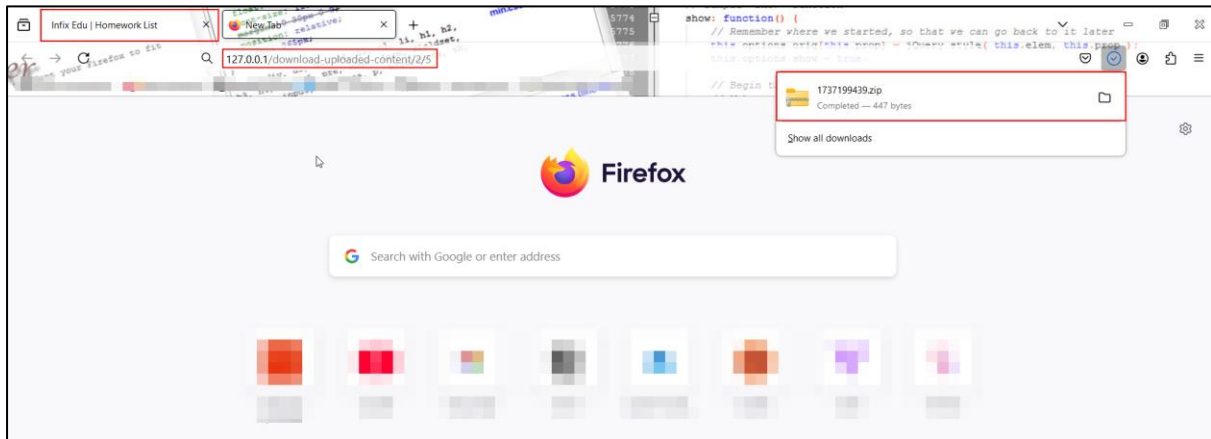
Repeat the same steps of uploading the homework and checking the download URL. It can be observed that **“/2”** in the URL indicates the **2<sup>nd</sup> Admission Number** and **“/5”** indicating the attached file number.

The screenshot shows the NFIX Homework List page. The browser address bar shows the URL `127.0.0.1/student-homework`. The page has a sidebar with navigation options including Class Routine, Lesson Plan, Homework List, Study Material, Attendance, Leave, Chat, Examinations, Notice Board, Subjects, Online Exam, Teacher, Transport, and Library. The main content area is titled 'Homework List' and shows a table with the following data:

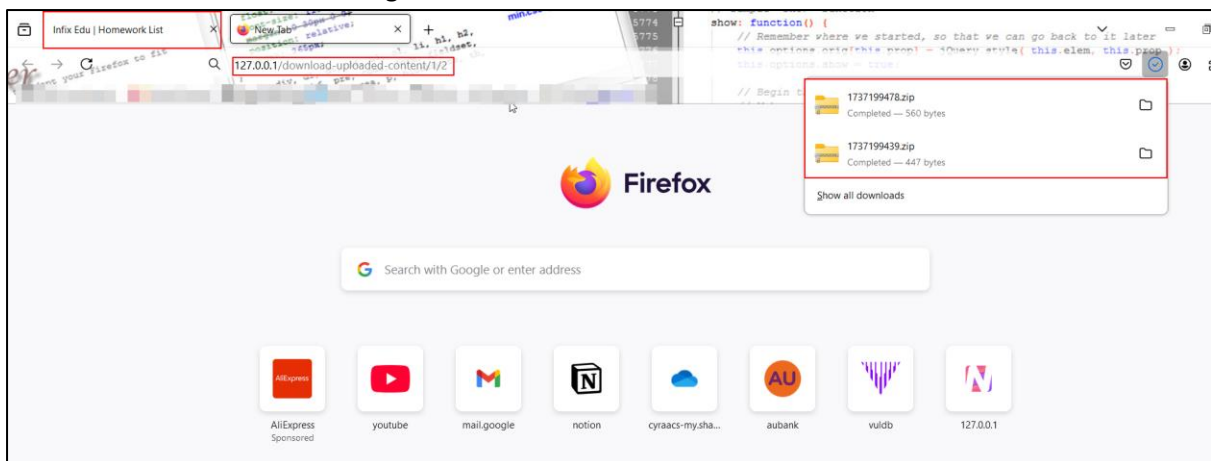
Subject	Marks	Homework Date	Submission Date	Evaluation Date	Obtained Marks	Status
Subject - Demo	100	18th Jan, 2025	18th Jan, 2025			INCOMPLETED

Below the table, there is an 'ACTION' section with a 'SELECT' button. A dropdown menu is open, showing options: VIEW, ADD CONTENT, DELETE UPLOADED CONTENT, and DOWNLOAD UPLOADED CONTENT. The 'DOWNLOAD UPLOADED CONTENT' option is highlighted with a red box. The browser address bar shows the download URL `127.0.0.1/download-uploaded-content/2/5`.

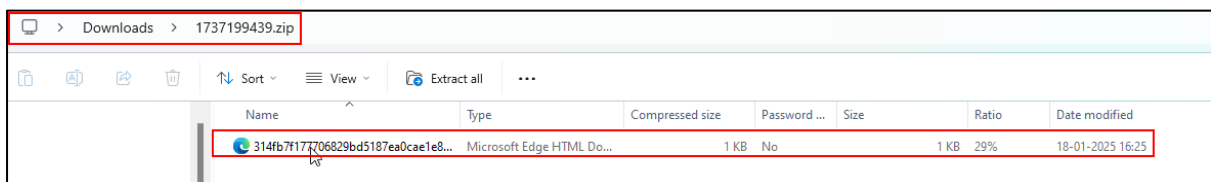
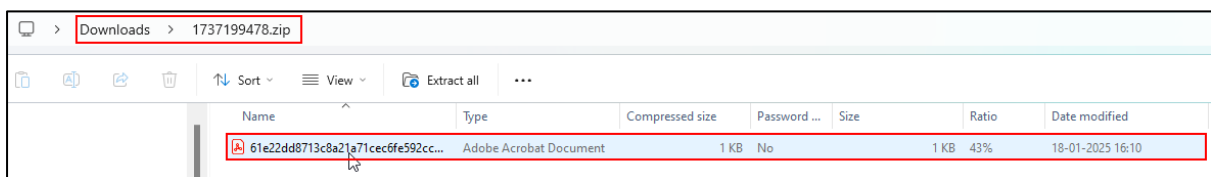
**Step 3:** From **Student2** Account make a request to download the **5<sup>th</sup> attachment** which belongs to **Student2** as well as **2<sup>nd</sup> attachment** which belong to **Student1**.



It can be observed that two different ZIP files could be downloaded. One zip containing homework of **Student2** and another containing homework of **Student1**.



**Step 4:** Open the Zip files. It can be observed that one zip file has PDF, and another has Image indicating successful IDOR and unauthorized download being allowed to a student to download all other student HomeWorks.



**Recommendation:**

To mitigate IDOR, implement access control checks for each object that users try to access. Web frameworks often provide ways to facilitate this. Additionally, use complex identifiers as a defence-in-depth measure, but remember that access control is crucial even with these identifiers. Avoid exposing identifiers in URLs and POST bodies if possible. Instead, determine the currently authenticated user from session information. When using multi-step flows, pass identifiers in the session to prevent tampering.