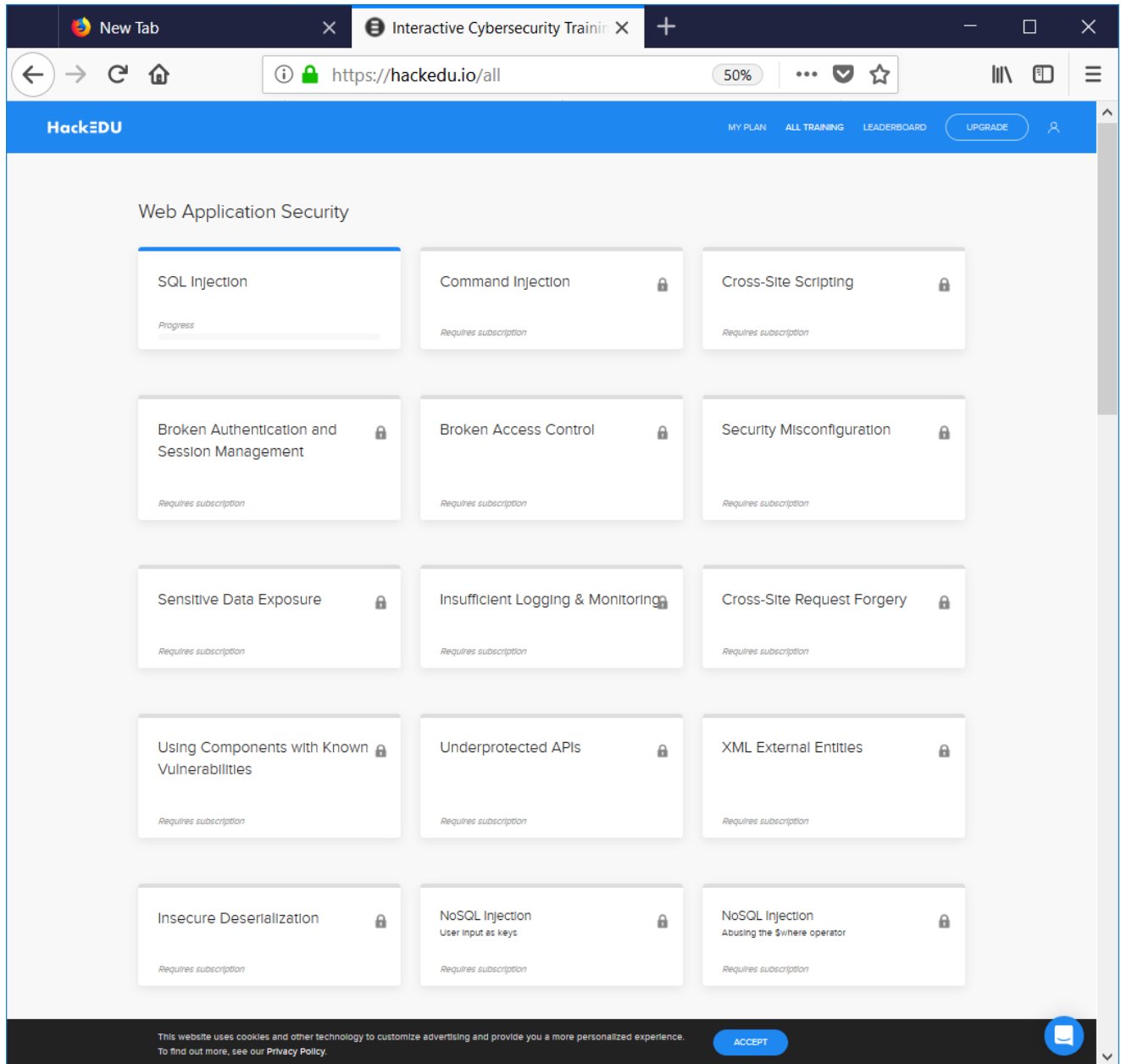
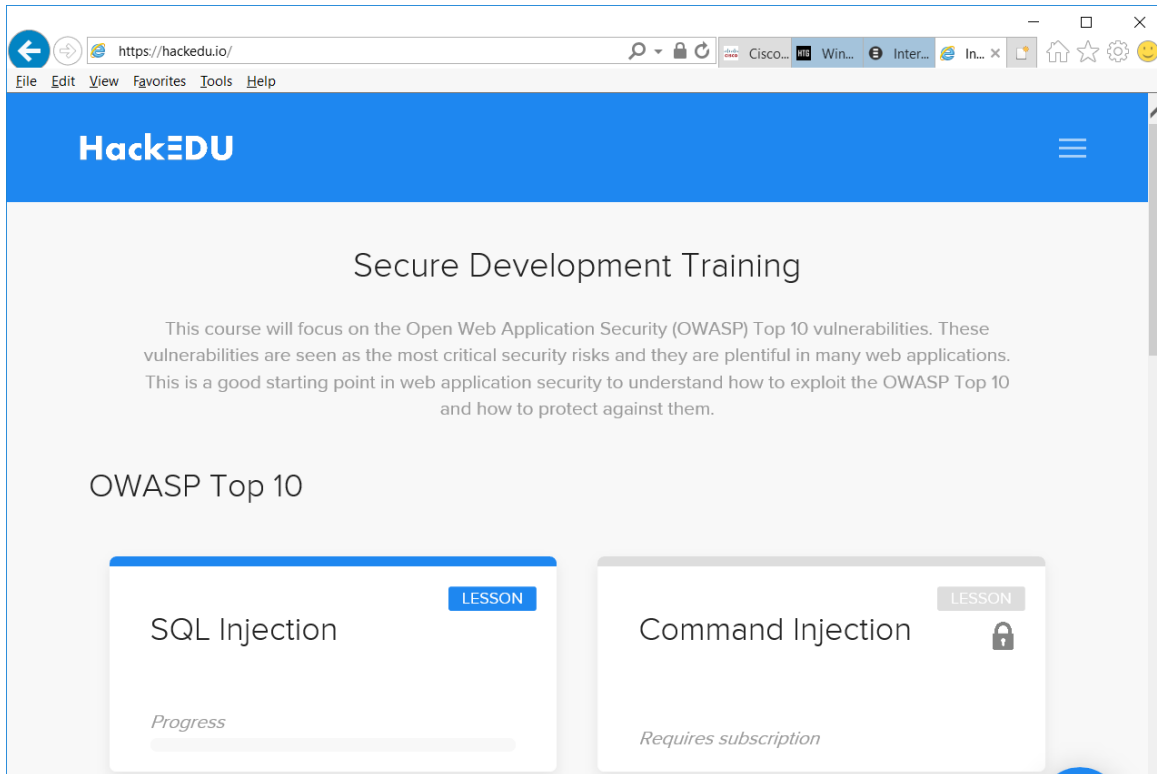


Web Application Security, Vulnerabilities, and Challenges v1.0

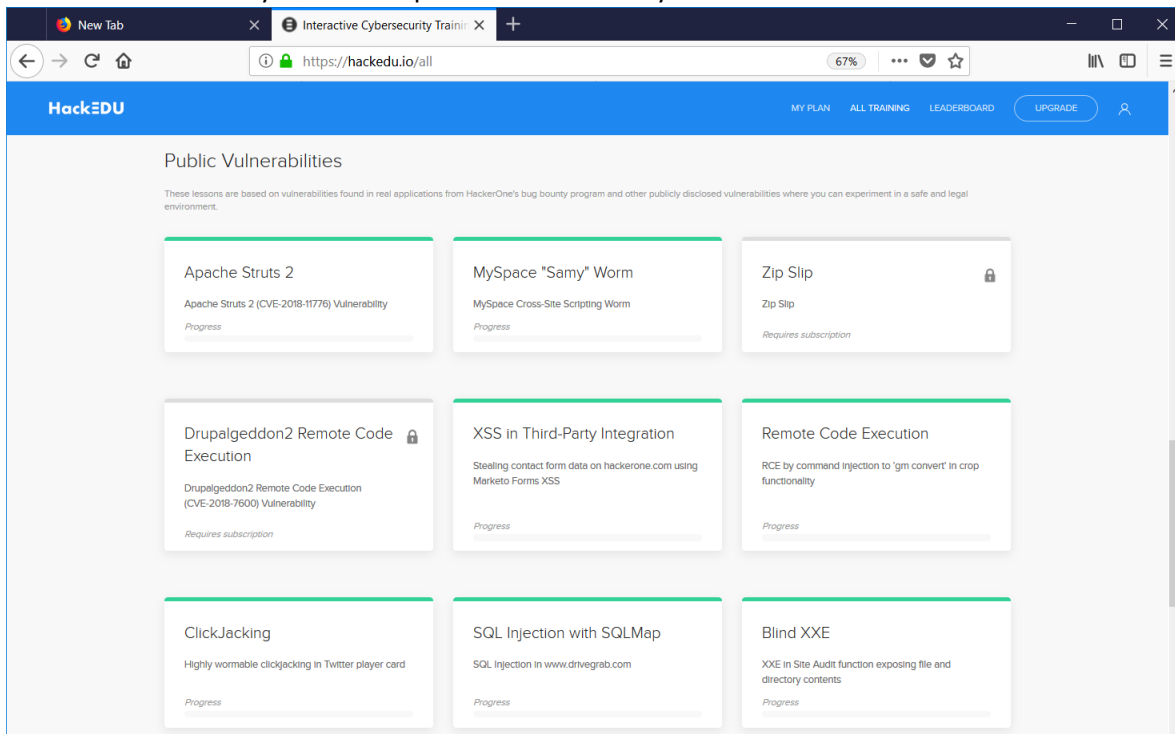
Create an account at <http://www.hackedu.io>

1. Within <https://hackedu.io/all> Web Application Security, do SQL Injection. Document and provide screenshots on what you did to exploit the vulnerability.





- Go to <https://hackedu.io/all> and go through any one of the public vulnerabilities. Document and provide screenshots on what you did to exploit the vulnerability.



3. Go to <https://hackedu.io/all> and go through any **three** of the challenges. Document and provide screenshots on what you did to complete the challenges successfully.

The screenshot shows a web browser window with the URL <https://hackedu.io/all>. The page title is "HackEDU" and the navigation bar includes "MY PLAN", "ALL TRAINING", "LEADERBOARD", and an "UPGRADE" button. The main content area is titled "Challenges" and contains a grid of 12 challenge cards. Each card displays the challenge name, a brief description, and the points and difficulty level.

Challenge Name	Description	Points	Difficulty
Steal A Startup Invite	Get an invite code to this hot new startup.	Worth 50 Points	(Hard)
Indicating Hints	Get information	Worth 15 Points	(Moderate)
Bank Transfer	Craft a link and submit it that you would send to the user eve to transfer 1000 into bob's account.	Worth 20 Points	(Moderate)
JS Safe	Well it's definitely the 90s with the Aluminum-Key Hardware password storage device. Let's see what it has in store. The answer is of the form: CTF{????}	Worth 20 Points	(Moderate)
Mind Reader	Can you read my mind? The answer is of the form: CTF{????}	Worth 50 Points	(Hard)
Bank Account Number	Get into the bank vault and steal the account number.	Worth 10 Points	(Easy)
Steal Bitcoin	Steal all of the bitcoin. Login using the credentials username: namey@sapohack.com password: AvhRDPDK. Steal all of the money from bob@mail.org. What is your flag?	Worth 20 Points	(Moderate)
/tmp/secrets File	Steal the /tmp/secrets file	Worth 50 Points	(Hard)
/etc/passwd File	Steal the /etc/passwd file	Worth 15 Points	(Easy)
Regain Session Access	Every new account is hacked within a few seconds and taken over with the hackers changing the victims password. Try to re-gain access to your account. The answer is of the form: flag{????}	Worth 30 Points	(Hard)
JS Safe 3.0	We've found this JS Safe on the Internet, and want to know the password it was created with. Can you help? The answer is of the form: CTF{????}	Worth 30 Points	(Easy)
robots.txt is not the only one	Get information	Worth 10 Points	(Easy)

At the bottom of the page, there is a cookie consent banner that says "This website uses cookies and other technology to customize advertising and provide you a more personalized experience. To find out more, see our Privacy Policy." with an "ACCEPT" button.