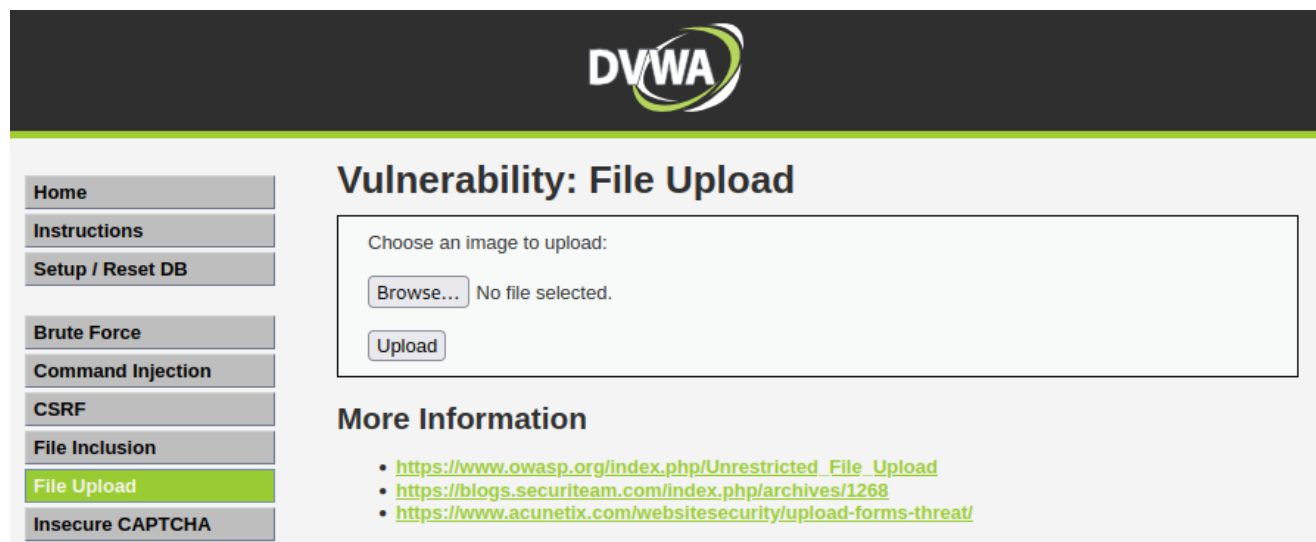
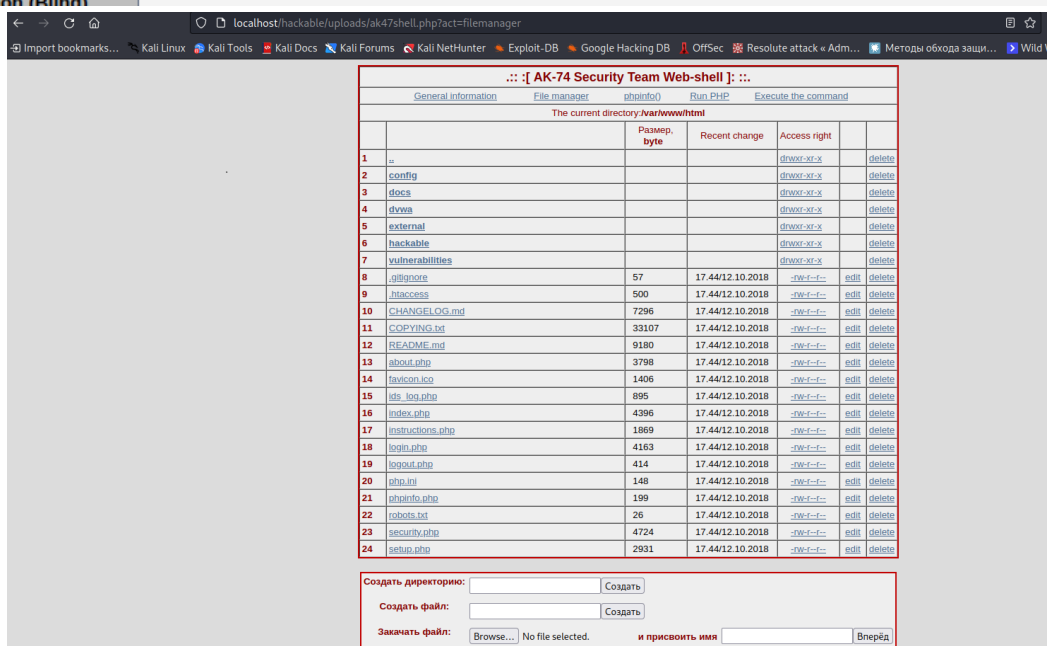
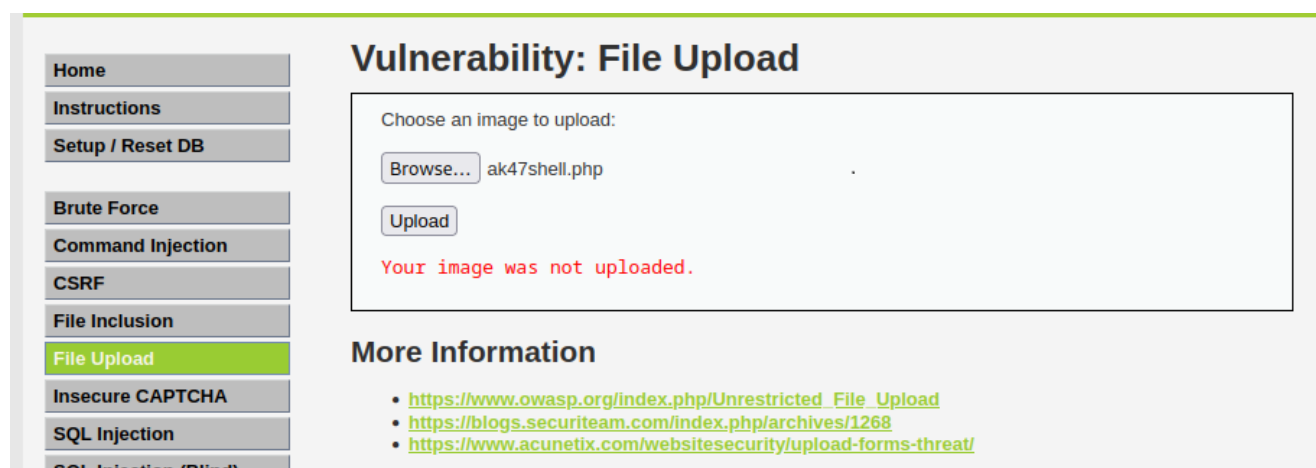


Задание 1: Решите задание File Upload из проекта DVWA на уровне сложности Low так, чтобы получить шелл на исследуемом ресурсе.



Смотрю "что предлагает" данная лабораторная машина - загрузка файлов на сервер. Пробую в прямую грузить шелл, чтоб не особо мучаться.



При удачной загрузке он указывает директорию загрузки, прохожу в директорию **localhost/hackable/uploads/ak47shell.php**

Далее уже тыкаю в кнопки шелла и можно смотреть через него весь состав сервера, выполнение команд и прочее. (выбор пал на этот шелл, за "его красоту" и функционал. Из того же набора шеллов на гите есть более удачные для работы ирл).

Задание 2: Решите задание “Session Mgmt. - Administrative Portals” из bwapp на уровне сложности medium.

The screenshot displays the bWAPP web application interface. The main heading is "Session Mgmt. - Administrative Portals". Below the heading, a red message states "This page is locked." and a hint suggests "HINT: check the cookies...". The navigation bar at the top contains links for Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. The footer shows the license information and a list of social media links.

Choose your bug
bWAPP v2.2

Set your security level:
low Set Current: medium

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ Session Mgmt. - Administrative Portals /

This page is locked.

HINT: check the cookies...

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ Session Mgmt. - Administrative Portals /

This page is locked.

HINT: check the cookies...


bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME-IT on Twitter and ask for our cheat sheet containing all solutions! / Need an exclusive training?

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Cache Storage Cookies Indexed DB Local Storage Session Storage

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly
admin	0	localhost	/	Sat, 10 Jun 2023 13:18:33 GMT	6	false
PHPSESSID	b603imjenu6vcqpojK73Fv3u2	localhost	/	Session	35	false
security_level	1	localhost	/	Sun, 09 Jun 2024 13:06:31 GMT	15	false
security	low	localhost	/	Session	11	false
showhints	1	localhost	/	Session	10	false




bwAPP 
an extremely buggy web app!


Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ Session Mgmt. - Administrative Portals /

Cowabunga...

You unlocked this page using a cookie manipulation.

bwAPP is licensed under  © 2014 MME BVBA / Follow [@MME-IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive [training](#)?

Inspector Console Debugger Network Style Editor Performance Memory **Storage** Accessibility Application

Filter Items

	Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly
Cache Storage	admin	1	localhost	/	Sat, 10 Jun 2023 13:18:33 GMT	6	false
Cookies	PHPSESSID	b603imjenu6vcgpojk737v3u2	localhost	/	Session	35	false
http://localhost	security_level	1	localhost	/	Sun, 09 Jun 2024 13:06:31 GMT	15	false
Indexed DB	security	low	localhost	/	Session	11	false
Local Storage	showhints	1	localhost	/	Session	10	false
Session Storage							

bWAPP
an extremely buggy web app !

Choc

Set
low

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Bee

/ Session Mgmt. - Administrative Portals /

Cowabunga...

You unlocked this page using a cookie manipulation.

bWAPP is licensed under [\[CC BY-NC-ND\]](#) © 2014 MME BVBA / Follow [@MME_it](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive [license](#)?

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly
admin	1	localhost	/	Sat, 10 Jun 2023 13:18:33 GMT	6	false
PHPSESSID	b603imjenu6vcqojk73f7v3u2	localhost	/	Session	35	false
security_level	1	localhost	/	Sun, 09 Jun 2024 13:06:31 GMT	15	false
security	low	localhost	/	Session	11	false
showhints	1	localhost	/	Session	10	false

Открывая лабораторную, страница указывает, что нужно посмотреть что творится с куками. Есть в куках параметр `admin = 0`. Меняю на `admin = 1`. Обновляю страницу. Лаба решена.

Задание 3: Исследуйте страницу «Old, Backup & Unreferenced Files» проекта bWAPP на наличие уязвимостей. Может ли злоумышленник использовать найденные уязвимости для проникновения на сервер? Ответ обоснуйте.

bWAPP
an extremely buggy web app !

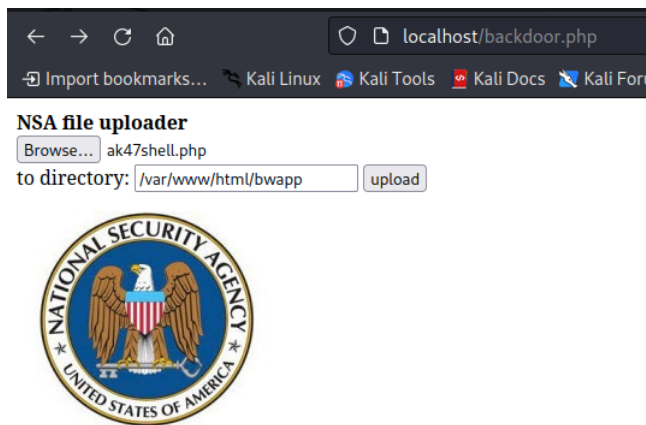
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

/ Old, Backup & Unreferenced Files /

How to find old, backup and unreferenced files on a web server?

An overview of these files, slightly obfuscated for privacy reasons :p

- backd00r.php
- c0nfig.inc
- p0rtal.bak
- p0rtal.zip
- web.c0nfig
- web.c0nfig.bak
- wp-c0nfig.bak



При открытии этой лабораторки даются вновь подсказки. Первое что пробую - на странице backd00r.php меняю в backdoor.php перехожу на страницу, где доступна загрузка. Спокойно грузит php как в голем виде, так и со сменой MIME и прочих приключений. Больше абсолютно ничего не нужно, чтобы получить полный доступ к этому серверу. "Дыра" размером с АААвстралию, над которой не хватает только надписи "Welcome".