

1.

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

Vulnerability: File Upload

Choose an image to upload:

Browse...

No file selected.

Upload

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- <https://blogs.securiteam.com/index.php/archives/1268>
- <https://www.acunetix.com/websitesecurity/upload-forms-threat/>

Данная лабораторная машина - загрузка файлов на сервер. Пробую в прямую грузить шелл

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

Vulnerability: File Upload

Choose an image to upload:

Browse...

ak47shell.php

Upload

Your image was not uploaded.

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- <https://blogs.securiteam.com/index.php/archives/1268>
- <https://www.acunetix.com/websitesecurity/upload-forms-threat/>

::: [AK-74 Security Team Web-shell] :::					
General information		File manager	phpinfo()	Run PHP	Execute the command
The current directory /var/www/html					
		Powerp. byte	Recent change	Access right	
1	..			down-xc-x	delete
2	centip			down-xc-x	delete
3	docs			down-xc-x	delete
4	down			down-xc-x	delete
5	external			down-xc-x	delete
6	hackable			down-xc-x	delete
7	vulnerabilities			down-xc-x	delete
8	.gitignore	57	17/44/12.10.2018	file-t-t-	edit delete
9	.htaccess	500	17/44/12.10.2018	file-t-t-	edit delete
10	CHANGELOG.md	7296	17/44/12.10.2018	file-t-t-	edit delete
11	COPYING.txt	33107	17/44/12.10.2018	file-t-t-	edit delete
12	README.md	9180	17/44/12.10.2018	file-t-t-	edit delete
13	about.php	3798	17/44/12.10.2018	file-t-t-	edit delete
14	advcon.php	1406	17/44/12.10.2018	file-t-t-	edit delete
15	ids_log.php	895	17/44/12.10.2018	file-t-t-	edit delete
16	index.php	4396	17/44/12.10.2018	file-t-t-	edit delete
17	instructions.php	1889	17/44/12.10.2018	file-t-t-	edit delete
18	login.php	4163	17/44/12.10.2018	file-t-t-	edit delete
19	logout.php	414	17/44/12.10.2018	file-t-t-	edit delete
20	php.ini	148	17/44/12.10.2018	file-t-t-	edit delete
21	phpinfo.php	199	17/44/12.10.2018	file-t-t-	edit delete
22	robots.txt	26	17/44/12.10.2018	file-t-t-	edit delete
23	security.php	4724	17/44/12.10.2018	file-t-t-	edit delete
24	setup.php	2931	17/44/12.10.2018	file-t-t-	edit delete

Создать директорию:

Создать

Создать файл:

Создать

Загрузить файл:

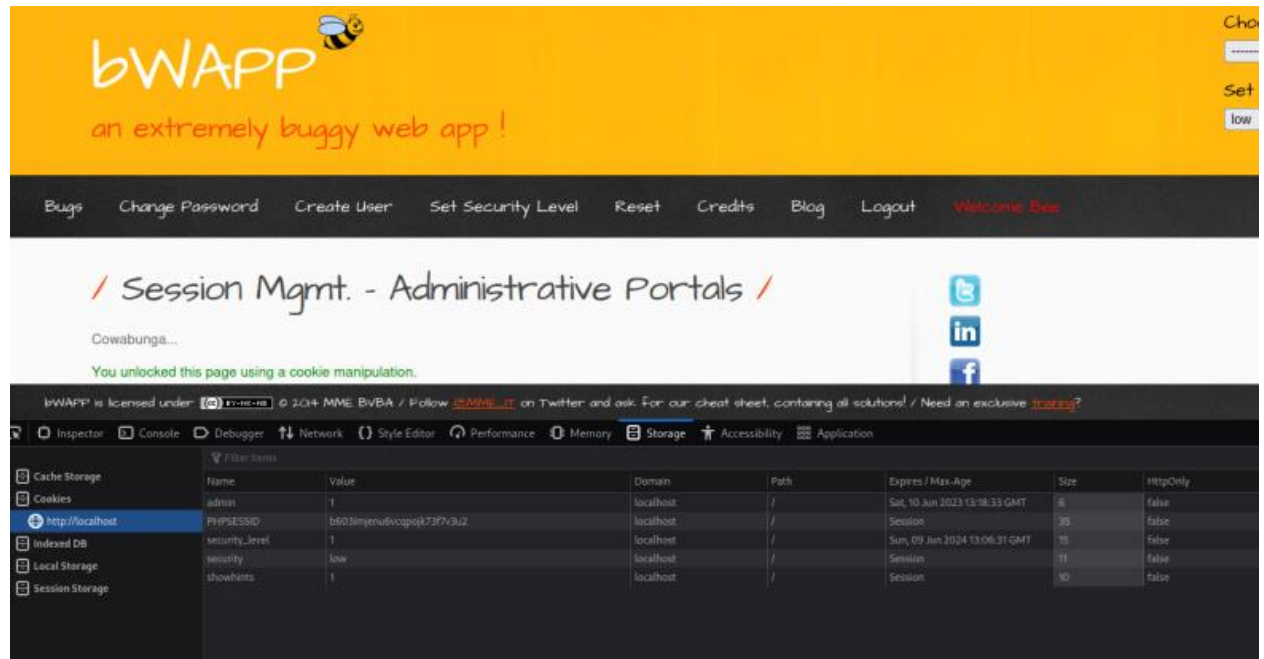
Browse...

No file selected.

и присвоить имя

Внедрить

2.



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 [GPLv3](#) © 2014 MME BVBA / Follow [@MME_bvba](#) 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
admin	1	localhost	/	Sat, 10 Jun 2023 13:18:33 GMT	6	false
PHPSESSID	b603mjemulicopnK73f7u2	localhost	/	Session	35	false
security_level	1	localhost	/	Sun, 09 Jun 2024 13:06:31 GMT	15	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. Лабораторная решена.

3.

bWAPP
an extremely buggy web app !

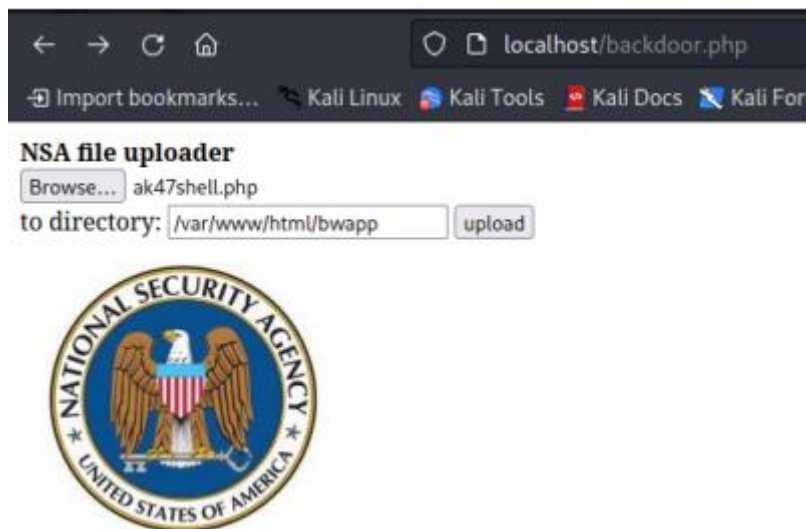
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

/ 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 лабораторной даются вновь подсказки. Первое что пробую - на странице backd00r.php меняю в backdoor.php перехожу на страницу, где доступна загрузка. Спокойно грузит php, так и со сменой MIME. Больше ничего не нужно, чтобы получить полный доступ к этому серверу.