

**Finding Name: hidden directories and files**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Byeongnam Choe | PT | Project Co-lead | EchoNet |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

I have scanned the web server with Wfuzz to discover any hidden directories or files within the server that do not appear on web pages, and I have found a few files and directories that should not be exposed to normal users. Wfuzz is a tool designed for brute-forcing web applications; it can be used to find resources. Discovering hidden files and directories can negatively affect the web application, as it may lead to the exposure of sensitive information, the disclosure of system vulnerabilities, or even the insertion of malicious code.

**Risk Rating**  
Impact: Minior  
Likelihood: unlikely

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**

Hidden files or folders may contain sensitive data such as passwords and usernames, which can be stolen and lead to data breaches, causing significant damage to the company's reputation. Additionally, if these files include information related to system vulnerabilities, attackers could use it to hack into the system or inject malicious code.

**Affected Assets**

Web application

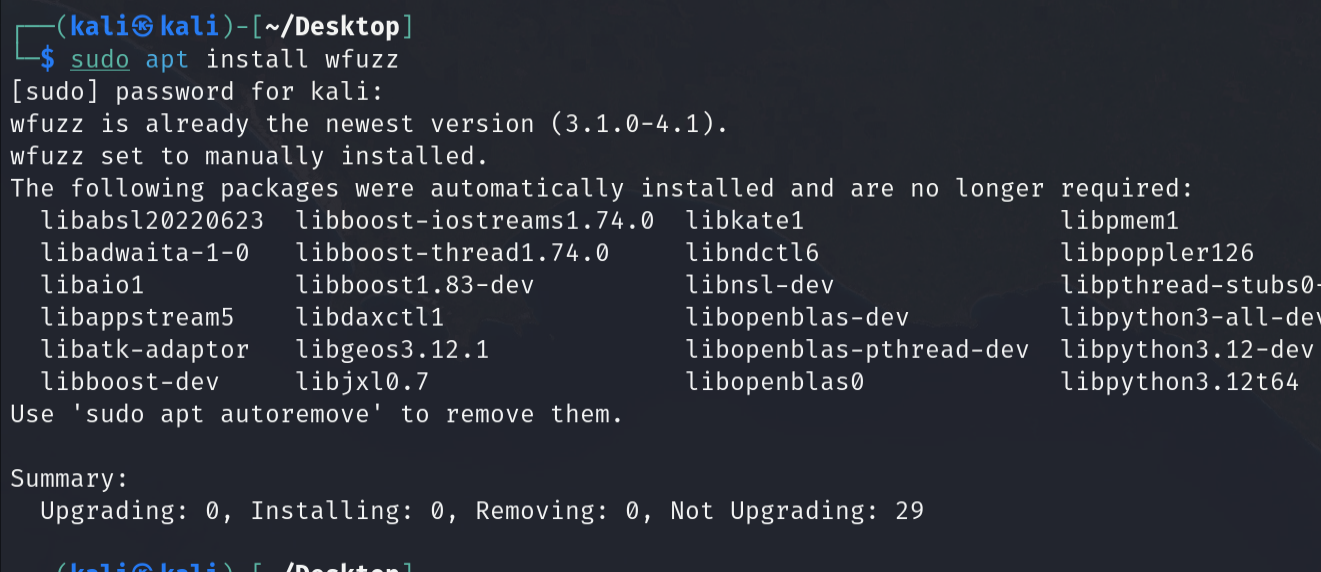
Data

**Evidence**

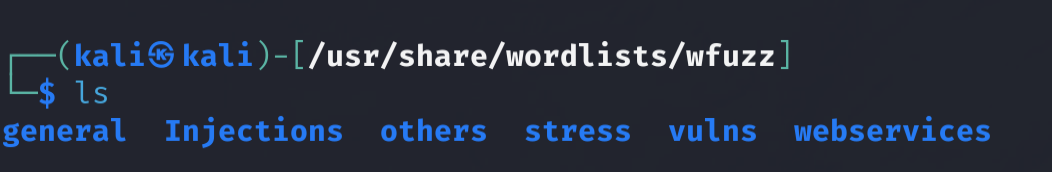
Provide a step by step guide on how to reproduce the vulnerability with screenshots

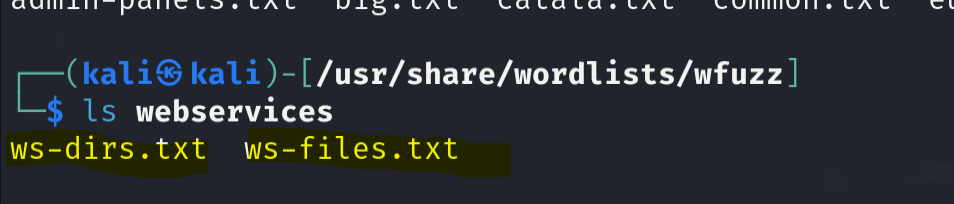
Step 1. Install Wfuzz

“sudo apt-get install wfuzz” to install wfuzz



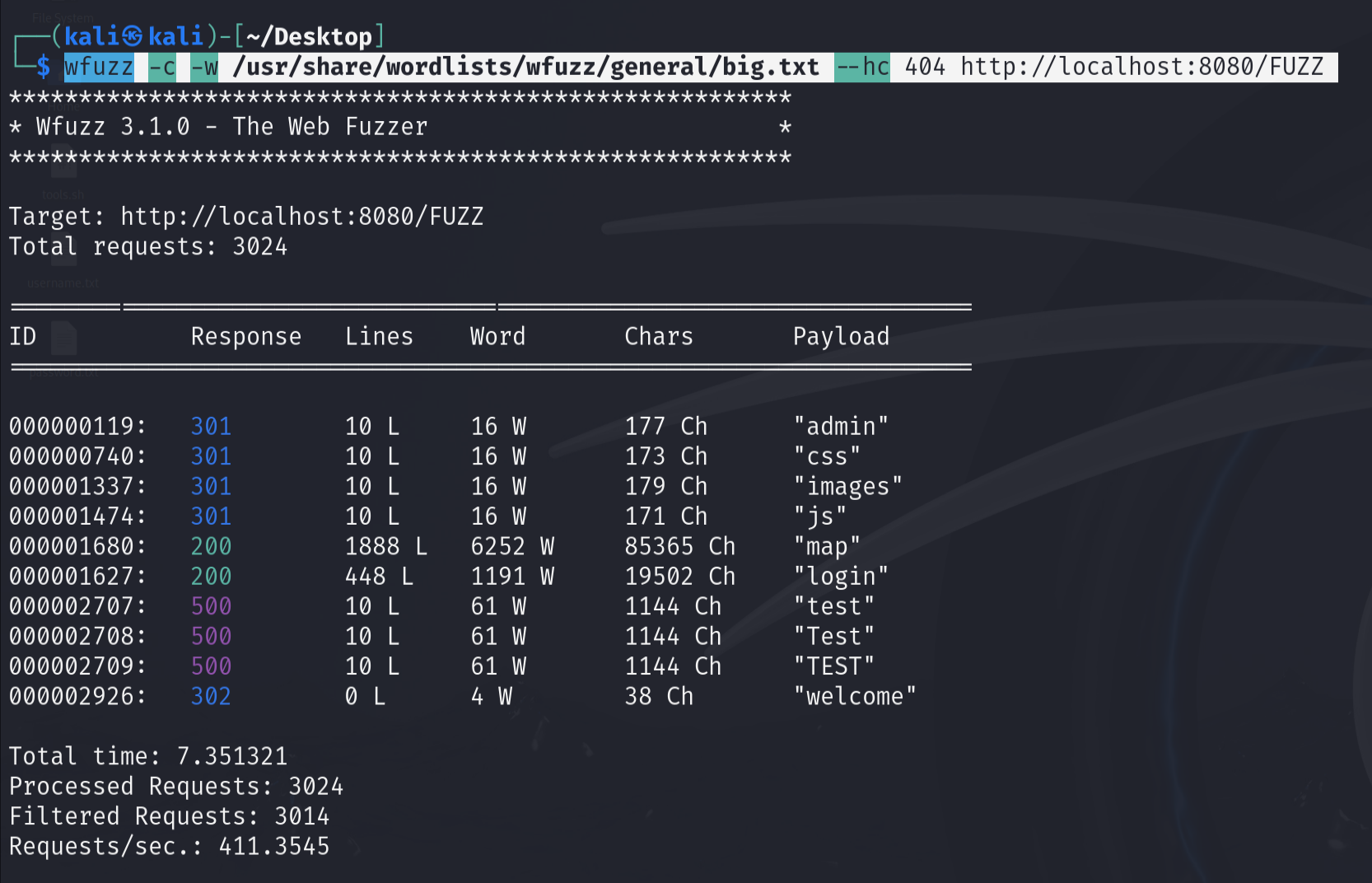
Step 2. discover .txt files to scan the web server

I am going to use three different text files: one general file (big.txt) and two related to webservices (ws-dirs.txt and ws-files.txt).

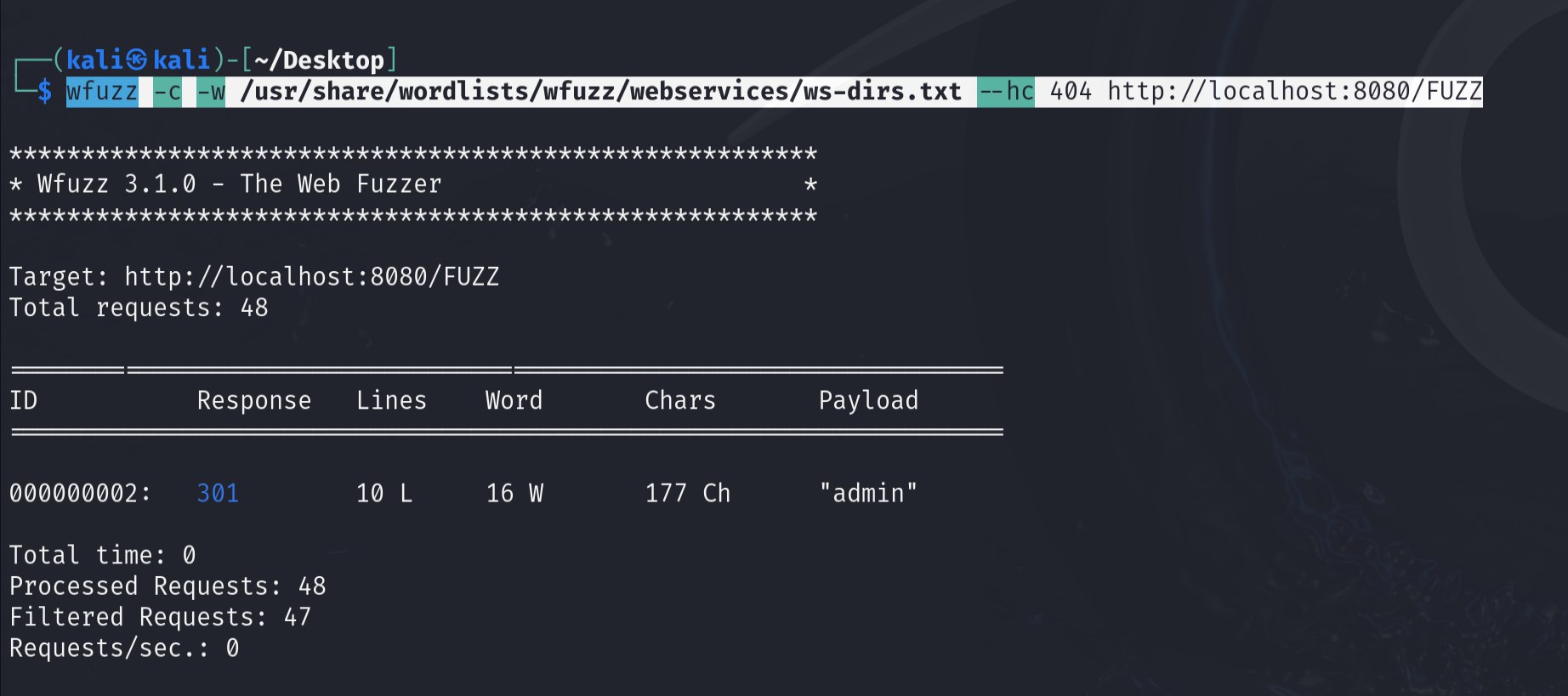


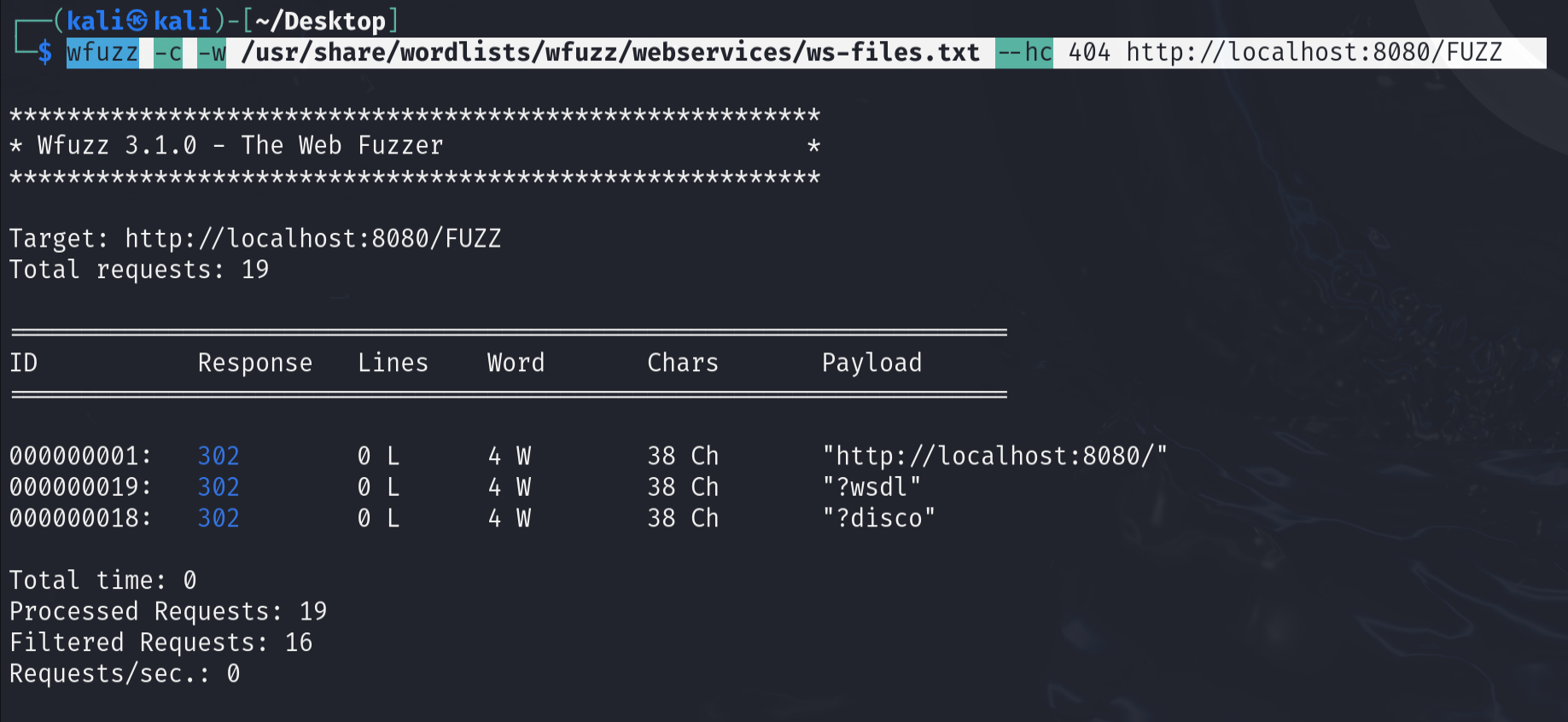
Step 3. scan the web application

**“wfuzz -c -w /usr/share/wordlists/wfuzz/general/big.txt --hc 404** [**http://localhost:8080/FUZZ**](http://localhost:8080/FUZZ)**”**



**“wfuzz -c -w /usr/share/wordlists/wfuzz/webservices/ws-dirs.txt --hc 404** [**http://localhost:8080/FUZZ**](http://localhost:8080/FUZZ)**”**

**“wfuzz -c -w /usr/share/wordlists/wfuzz/webservices/ws-files.txt --hc 404 http://localhost:8080/FUZZ ”**



Discovered hidden files such as WSDL, DISCO, and web pages including CSS, images, JS, test, Test, and TEST.

**Remediation Advice**

Rate limiting:

limiting the number of requests from a specific IP address within a certain timeframe,

IP blocking:

block IP addresses if abnormal traffic is detected

WAF:

A WAF can detect the characteristics of tools like Wfuzz and can automatically block.

**References**

<https://github.com/xmendez/wfuzz>

<https://www.kali.org/tools/wfuzz/>

**Contact Details**

Byeongnam Choe (s222106547@deakin.edu.au)

**Pentest Leader Feedback.**

The lead will provide feedback to enact on