Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

CrypTO CONFERENCE

Politecnico di Torino 1859
Telsy A TIM ENTERPRISE BRAND
DISMA

OFFENSIVE SECURITY SPECIALISTS

SU DI NOI

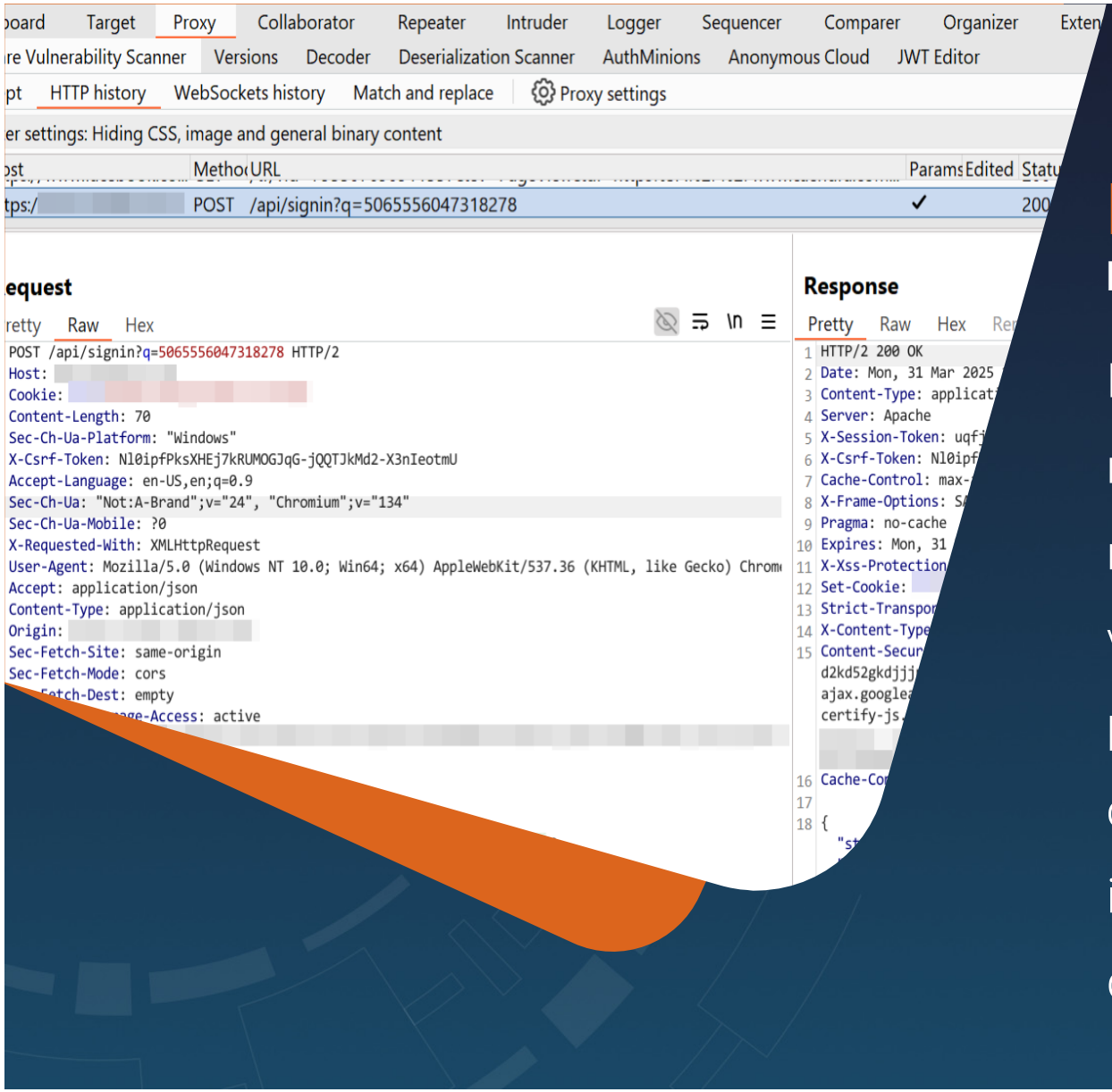
HN Security nasce a Torino nel 2021 come **startup** del gruppo **Humanativa** con il focus sull'offensive cybersecurity.

Fondata da un gruppo di persone con esperienza quasi trentennale in **etical hacking** .

OFFENSIVE SECURITY

ETHICAL HACKING, PENETRATION TESTING, RED TEAMING

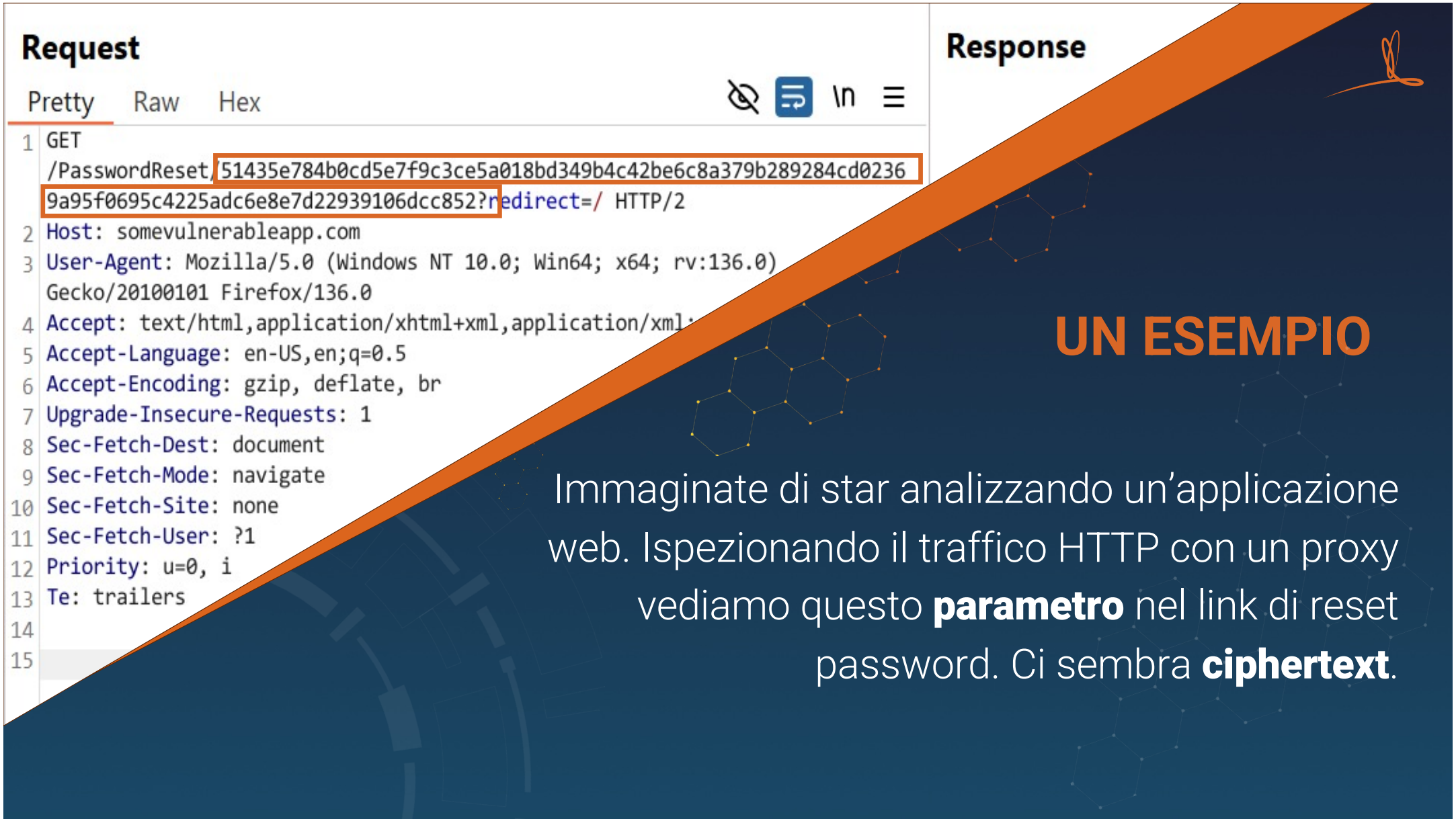
La disciplina dell'offensive security consente di identificare falle nei **controlli di sicurezza**, allo scopo di valutare la capacità di un sistema di difendersi in presenza di condizioni avverse.

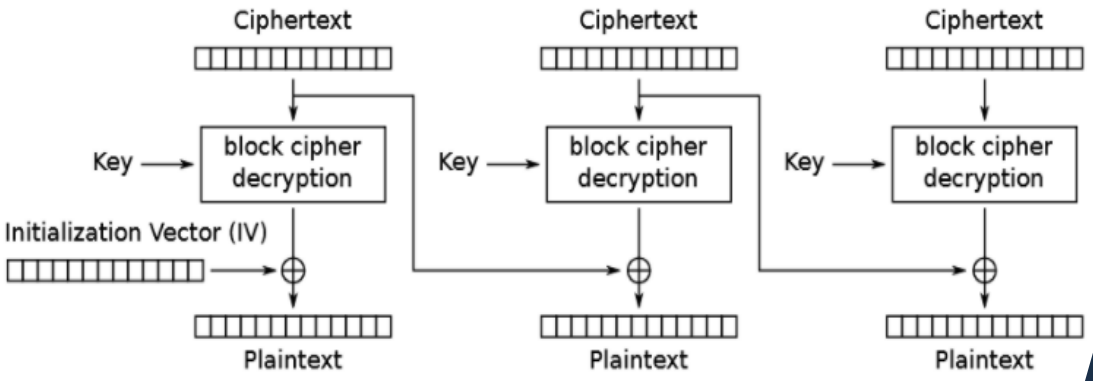


NEL PRATICO

FOCUS SULLE APPLICAZIONI

Le analisi di applicazioni (web, mobile, API etc.) sono le attività più richieste. Già questo offer grande varietà di tecnologie e liguaggi, ma poi ci sono anche altri tipi di attività come analisi di sistemi e infrastrutture, reti, firmware, IoT, devices (SCADA, PLC), etc. etc.


Request
Pretty
Raw
Hex
1 GET /PasswordReset/51435e784b0cd5e7f9c3ce5a018bd349b4c42be6c8a379b289284cd02369a95f0695c4225adc6e8e7d22939106dcc852?redirect=/ HTTP/2
2 Host: somevulnerableapp.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
4 Accept: text/html,application/xhtml+xml,application/xml;
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Upgrade-Insecure-Requests: 1
8 Sec-Fetch-Dest: document
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Site: none
11 Sec-Fetch-User: ?1
12 Priority: u=0, i
13 Te: trailers
14
15
Response
UN ESEMPIO
Immaginate di star analizzando un'applicazione web. Ispezionando il traffico HTTP con un proxy vediamo questo **parametro** nel link di reset password. Ci sembra **ciphertext**.



Cipher Block Chaining (CBC) mode decryption

UN ESEMPIO

Normalmente non sappiamo che algoritmo venga utilizzato, ma sappiamo che alcuni tipi di cifrari sono notoriamente vulnerabili ad una problematica chiamata **padding oracle**, un attacco che sfrutta la **validazione del padding** che viene effettuata con i **cifrari a blocchi**.


Response
Pretty Raw Hex Render
7
8 <!DOCTYPE html>
9 <html>
10
11 <h4>
Invalid Token!this is not a valid reset url...
</h4>
12
13
14
15 </body>
UN ESEMPIO
Se l'applicazione ci permette di capire che è avvenuto un **errore di validazione del padding** possiamo sfruttare questo comportamento per **cifrare e decifrare** il ciphertext senza aver bisogno della chiave .

Response

Pretty Raw Hex Render

```
7
8  <!DOCTYPE html>
9  <html>
10   <div class="error">
11     <h4>
         404 – Not Found
       </h4>
12
13   </div>
14 </div>
15 </body>
16 </html>
17
```

UN ESEMPIO

Se l'applicazione ci permette di capire che è avvenuto un **errore di validazione del padding** possiamo sfruttare questo comportamento per **cifrare e decifrare** il ciphertext senza aver bisogno della chiave .

QUALCHE PAROLA CHIAVE SU DI NOI..

FORMAZIONE

CERTIFICAZIONI

RICERCA E SVILUPPO

SMART WORKING

VARIETA’

FLESSIBILITA’

CRESCITA

GRAZIE PER L'ATTENZIONE

DOMANDE?