Opdracht 3B: Attacks

3B.1: Terminologie

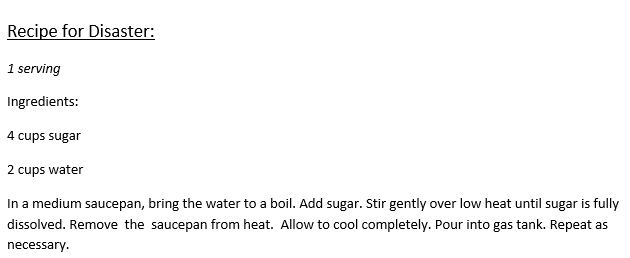
|  |  |  |
| --- | --- | --- |
| Zombies | A computer connected to the internet who has been infected with a virus. | PC dat geïnfecteerd is met een virus en gebruikt kan worden voor kwaadaardige aanvallen. |
| Maliciously Formatted Packets | A network packet is a formatted unit of data carried by a packet-switched network.  Malicious means that the packets has evil intentions. | Een network packet is een geformatteerde unit van data die gecarried wordt door een packet-switched network. Malicious betekent dat het packet kwaadaardige bedoelingen heeft. |
| ICMP packets | Mainly used by the system to send errormessages, usually to inform that the internetservice is unavailable. | Vooral door besturingssysteem gebruikt om foutmeldingen te sturen. Meestal om te melden dat een netwerkvoorziening niet beschikbaar is. |
| Evil Twin Attack | Duplicate wi-fi access point that appears legit but is set to steal info from the user, example: setting up a wireless mobile network in a place where there are frequent ‘free networks’ issued by the companychain. | Een duplicatie van een access point dat veilig en echt lijkt, maar kwaadaardig is opgezet om de informatie te stelen van gebruikers die ermee verbinden. |
| ARP | Het address resolution protocol (ARP) is een protocol binnen TCP/IP dat computers die allemaal op hetzelfde subnetwerk zijn aangesloten in staat stelt het unieke hardware adres (MAC-adres) van een andere PC binnen dat netwerk te leren, aan de hand van het IP-adres van deze PC. | The Address Resolution Protocol (ARP) is a communication protocol used within TCP/IP, so PC’s who are all connected to the same network, enables to remember and learn the unique hardware addresses (MAC-address) of a PC within that network by using the IP-address of that PC. |
| MAC | Unique identification number that is assigned on a network. | Uniek identificatienummer dat aan een apparaat in een ethernetnetwerk is toegekend. In het OSI-model valt een MAC-adres in de  datalinklaag |
| Domain Name Service | Used to translate the ip-addresses to their connected ‘readable’ names. However this is no encryption based translation, but rather a look up in a table to find the respective connection. | DNS wordt gebruikt om namen van computers te vertalen naar ip-adressen en omgekeerd. Het is geen letterlijke vertaling, maar eerder een manier van gelinkte info in een tabel op te zoeken. |
| Cryptographic authentication | Uses a PKI (Public Key Infrastructure).  Allows principals to authenticate one another using asymmetric encryption. A client (A) claiming to be a principal (P) authenticates to a server (S) as follows:   1. S sends C a random number R. 2. C encrypts R with his private key, and sends the result to S. 3. S decrypts the result with P’s public key. 4. If the result matches R, then S knows that C must posses P’s private key, and so C is assumed to be P. | Gebruikt een PKI (Public Key Infrastructure).  Staat toe principes om te authenticeren van één tot ander gebruik makend van asymmetrische encryptie.  Een client A beweert een principaal te zijn authenticeert met een server S. Dit gebeurt als volgend:   1. S stuurt C een willekeurig getal R. 2. C encrypteerd R met zijn private key, en stuurt het resultaat door naar S. 3. S decrypt het resultaat met P’s public key. 4. Als het resultaat overeenkomt met R, dan weet S dat C P moet bezitten, en zo is C verondersteld om P te zijn. |
| Session Token | Piece of data which indicates the session, usually used by HTTP. | Stuk unieke data dat gebruikt wordt om een sessie te identificeren, vaak gebruikt door HTTP. |
| DMZ | Part of a network that is available to everyone. | Gedeelte van het netwerk dat voor de buitenwereld volledig toegankelijk is, tegenovergestelde van intranet. |
| Metasploit | Open source securityproject that issues vulnerabilities about computersystems that are used by hackers. | Online project dat info verstrekt over kwetsbaarheden van systemen. Hackers gebruiken dit platform om kwetsbaarheden te onderzoeken. |
| Sandbox | Closed space where programs can work without interrupting other processes. Code is locked into a box which means it is an easy way to test unreliable code. | Afgesloten ruimte waarin computer-programma’s gerund kunnen worden zonder dat deze andere processen van het systeem verstoord. |
| Disclosure | Publicly exposing a vulnerability in a piece of code. | Een zwak punt in de software openbaren. |

3B.2: Sniffing easy

1. Hij heeft de pointer gebruikt en toetsen ingedrukt in de VNC
2. notepad can you see me en erna met wat geprul EKO{not\_anymore\_vnc\_hax}. Dit hebben we gevonden door te filteren op vcn.key\_down==”Yes”
3. Gmail
4. 8c:04:ff:9d:28:47
5. Tussen 192.168.0.22 en 192.168.0.26

3B.3: Sniffing intermediate

1. Sec558user1
2. Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumbdrive and you're good to go &gt;:-)
3. Recipe.docx
4. 4d07
5. 8350582774e1d4dbe1d61d64c89e0ea1



3B.4: Cross-Site Scripting

1: <script>alert()</script>

2: <img src="0" onerror="javascript:alert(“#C-is-een-scriptkiddie-taal)"/>

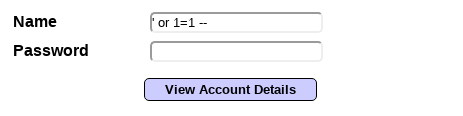
3: 'onerror='alert(1)'; (achteraan URL)

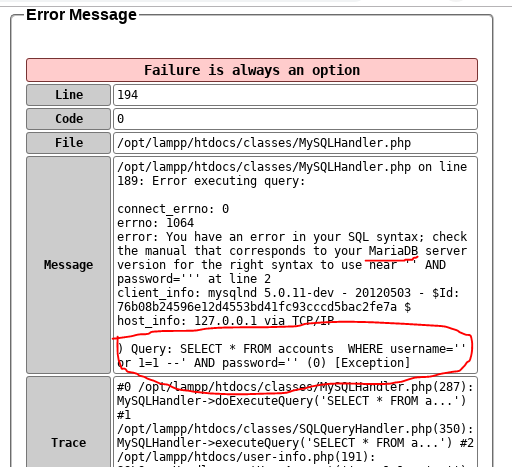
4: <https://xss-game.appspot.com/level4/frame?timer=%27)%3Balert(1)%3Bvar> b=(' (OOK URL)

5: Vervang de confirm in de url het woordje confirm met javascript:alert(1)

6: [https://xss-game.appspot.com/level6/frame#data:text/plain,alert(‘lolz’)](https://xss-game.appspot.com/level6/frame#data:text/plain,alert(%E2%80%98lolz%E2%80%99))

3B.5: SQL Injection



****

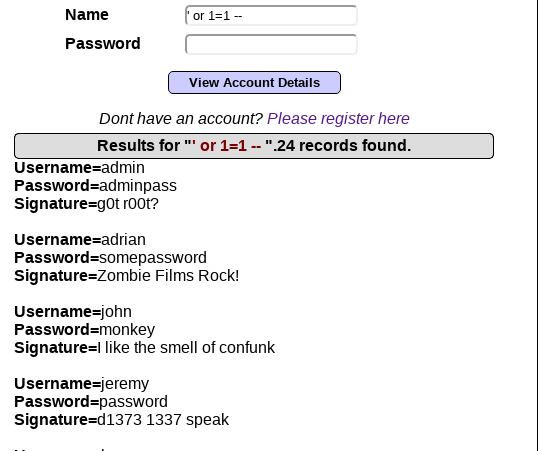
We hebben geprobeerd om SQL injection te gebruiken.

We kregen de volgende error message.

Hier is duidelijk te zien dat ze werken met MariaDB.

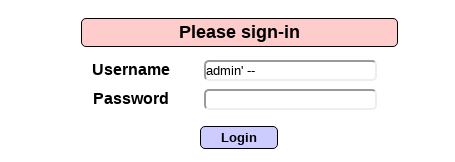
De query gebruikt dus de MariaDB syntax.

Na een snelle google search blijkt dat na het commentaar een spatie verplicht is.

Na het zetten van een spatie achter de – , (wat dus de rest van de regel in commentaar zet), bleek het te werken.

Het password van admin is adminpass

Inloggen als admin met SQL injection:

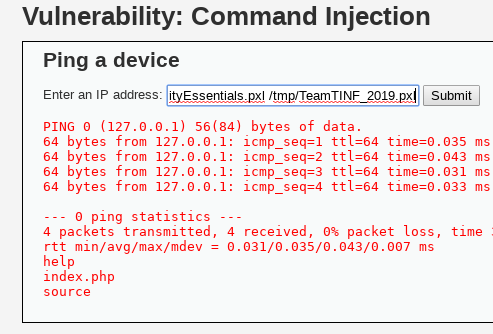




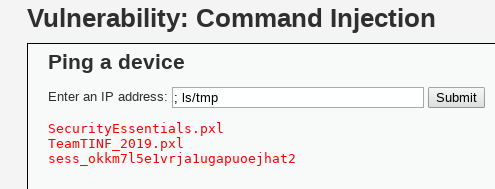
Het maakt dus niet uit wat we meegeven als password want dat wordt toch niet gecontroleerd.

(Alles in het grijs is commentaar en wordt niet uitgevoerd)

3B.6: Remote Code Execution



vanvoor staat een ;



3B.7: Sniffing

1. Als deel van het infectie process heeft Miss Muntenheuvel’s browser 2 Java Applets gedownload. Wat zijn de namen van de 2 .jar bestanden van deze applets?



Sdfg.jar

Q.jar

2. Wat was de gebruikersnaam van Miss Muntenheuvel op het geïnfecteerde windows systeem?



Administrator

3. Wat was de url waarop Miss Muntenheuvel klikte in de email die dit allemaal veroorzaakte?

Nrtjo.eu

4. Als deel van de infectie werd er een kwaadaardige Windows Executable gedownload naar Miss Muntenheuvel’s computer, wat was de MD5hash van dit bestand?



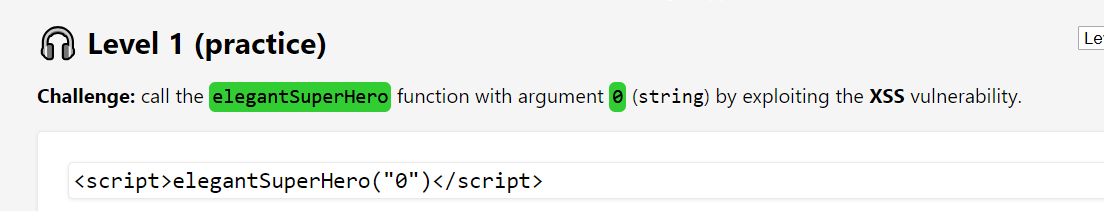
5942ba36cf732097479c5198eee91ed

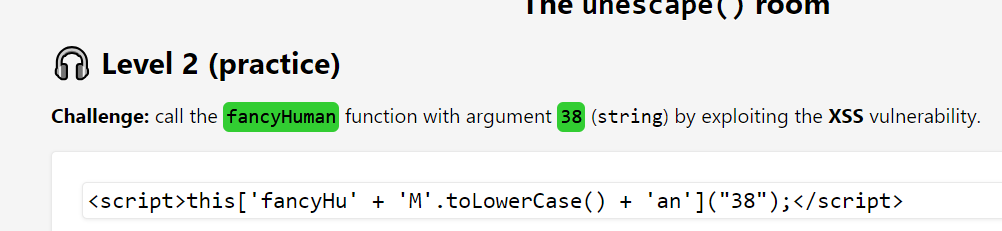
5. Wat is de naam van het Packer programma dat gebruikt werd om de kwaadaardige executable te beschermen? Hint: Dit is een van de populairste publieke packers gebruikt in hedendaagse malware.

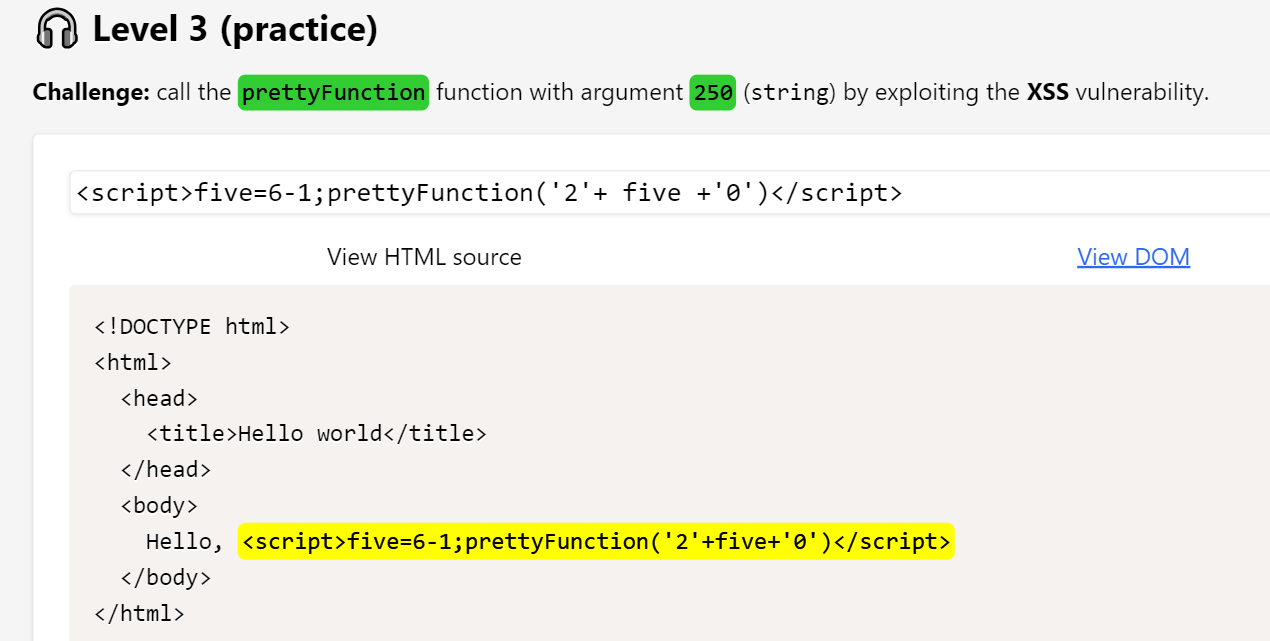
6. De kwaadaardige executable probeert een internet host te bereiken via een IP adres dat hard-coded is (er gebeurt geen DNS lookup hiervoor). Wat is het IP adres van deze internet host?

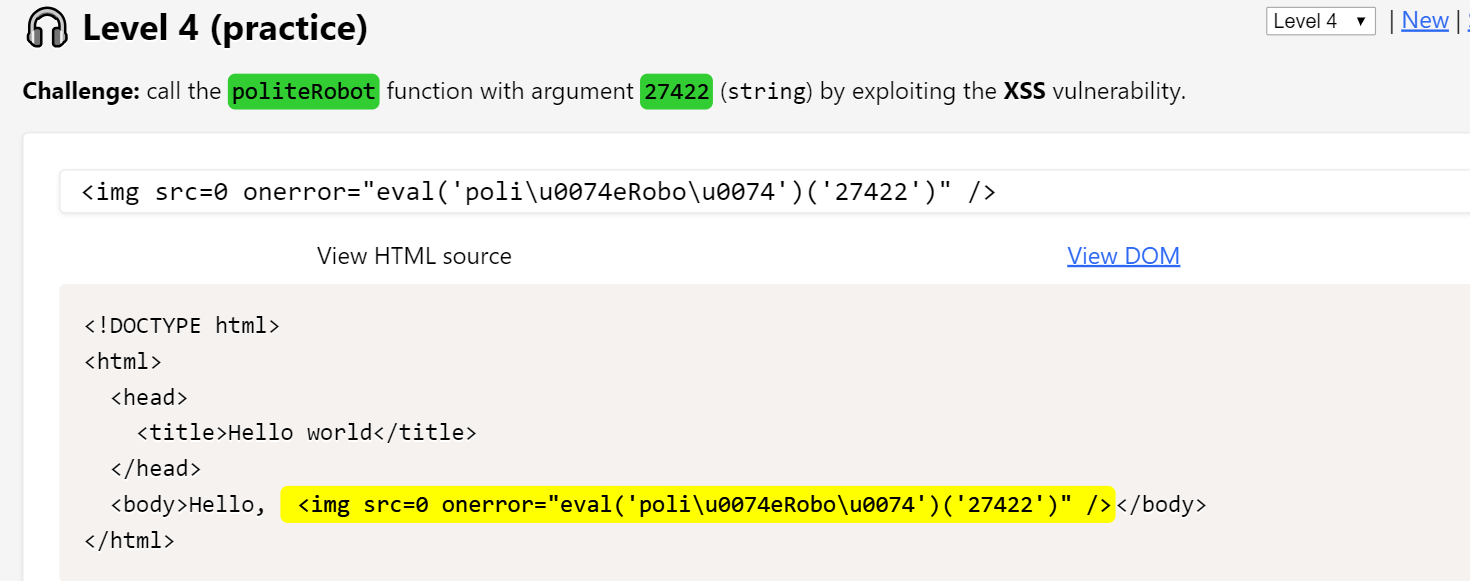
212.252.32.20

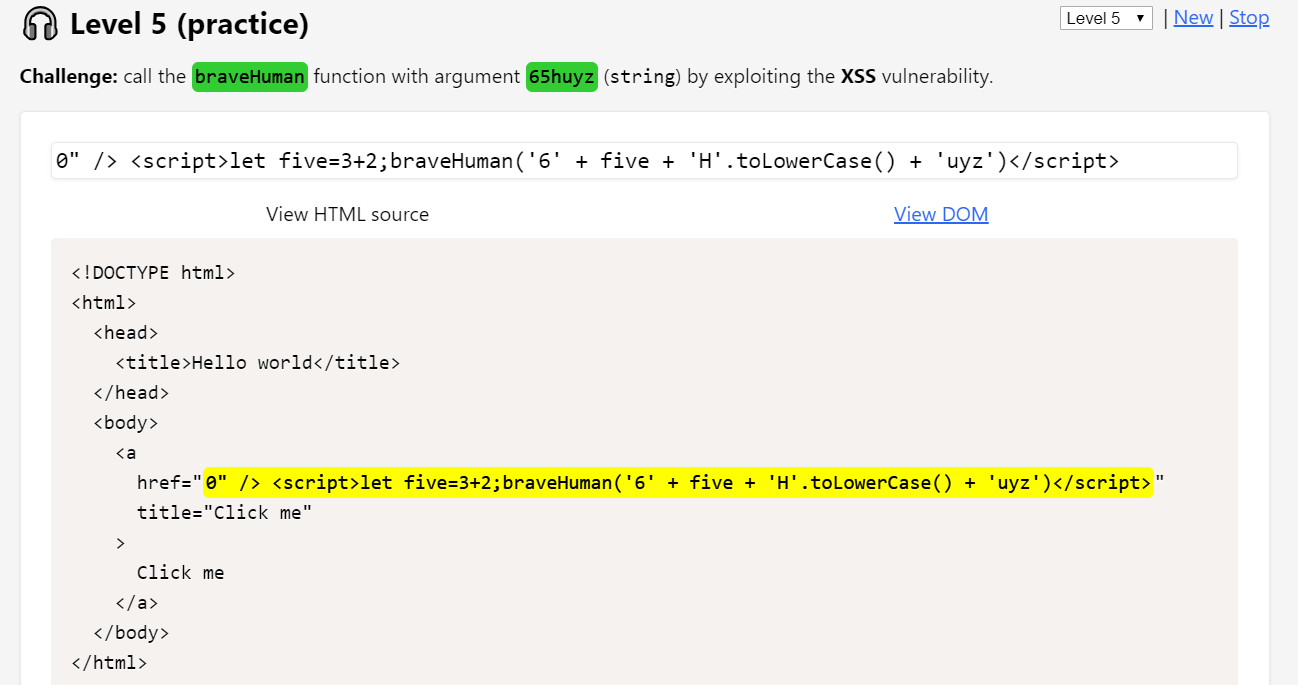
3B.8: XSS

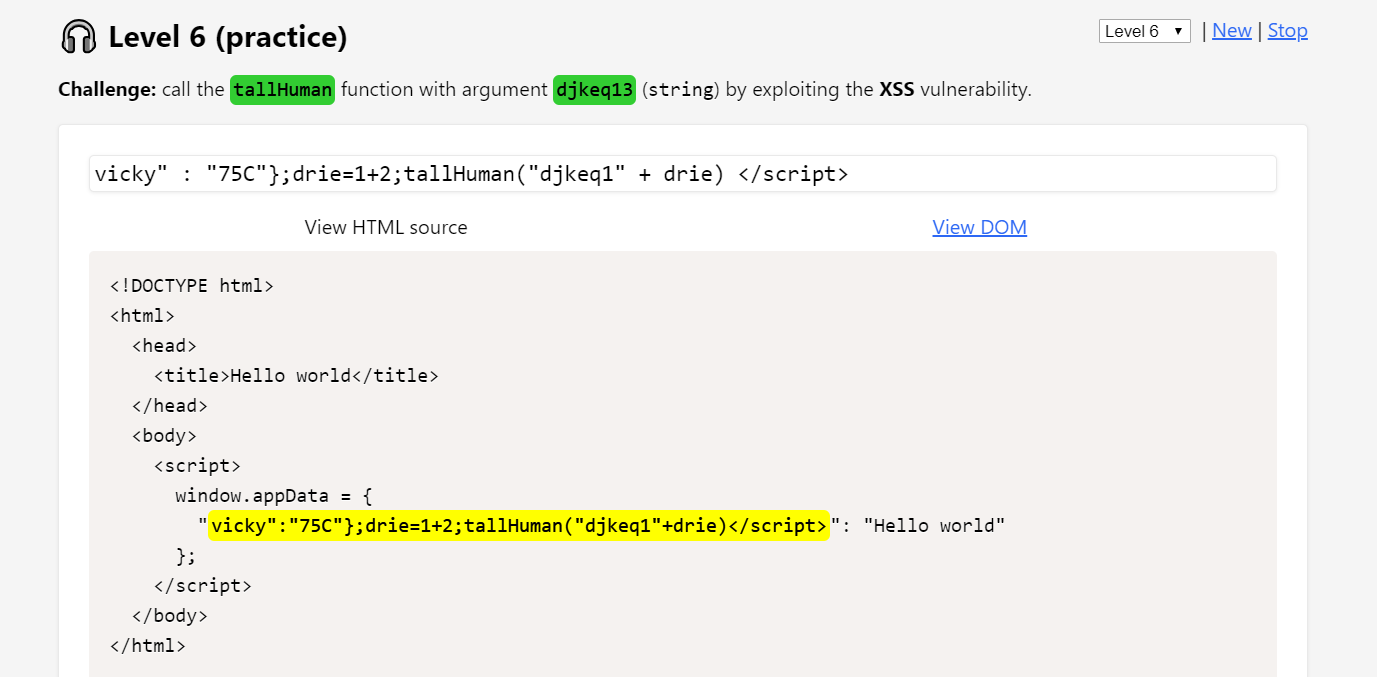




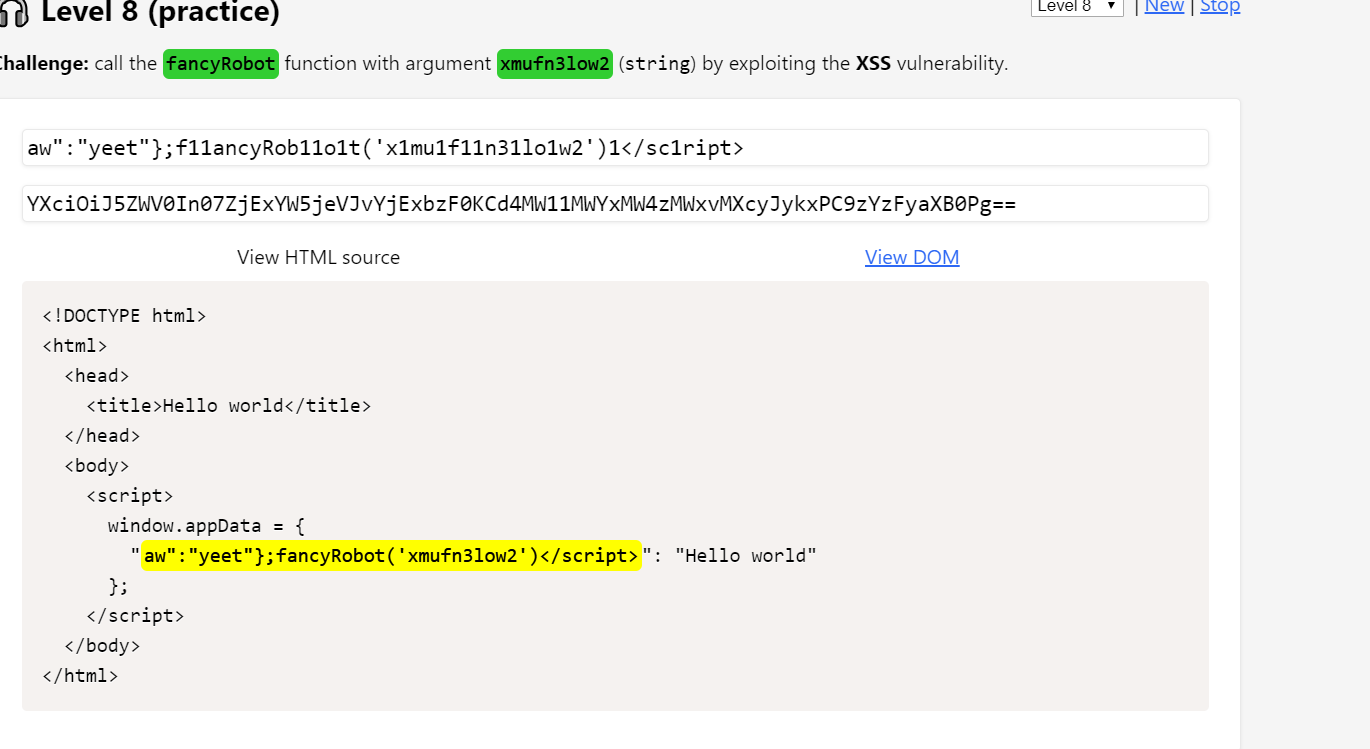


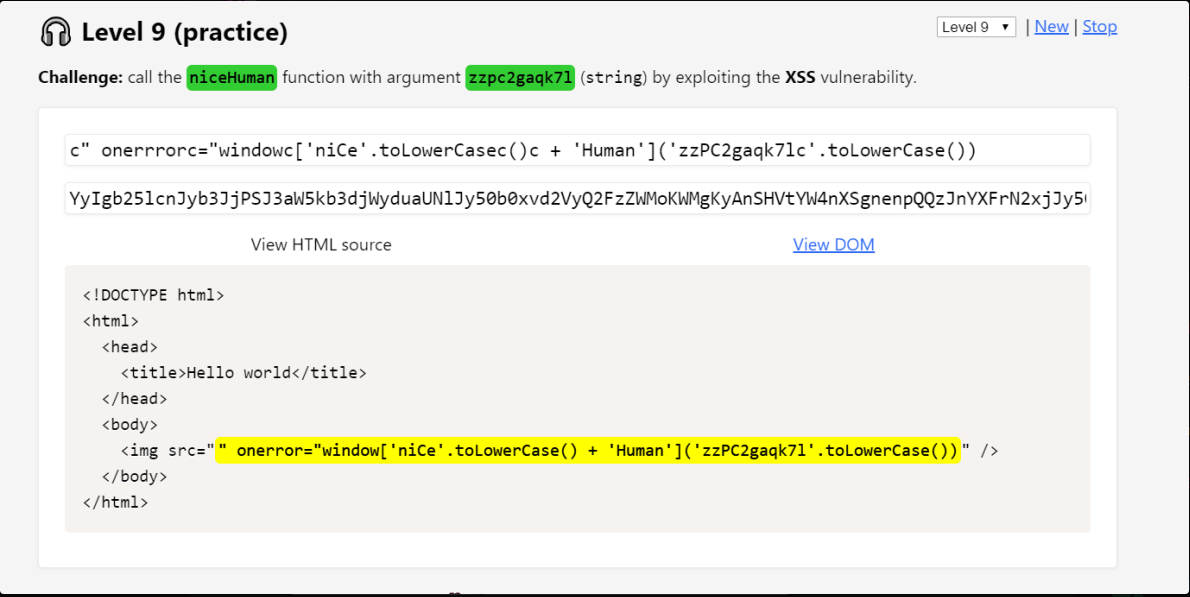


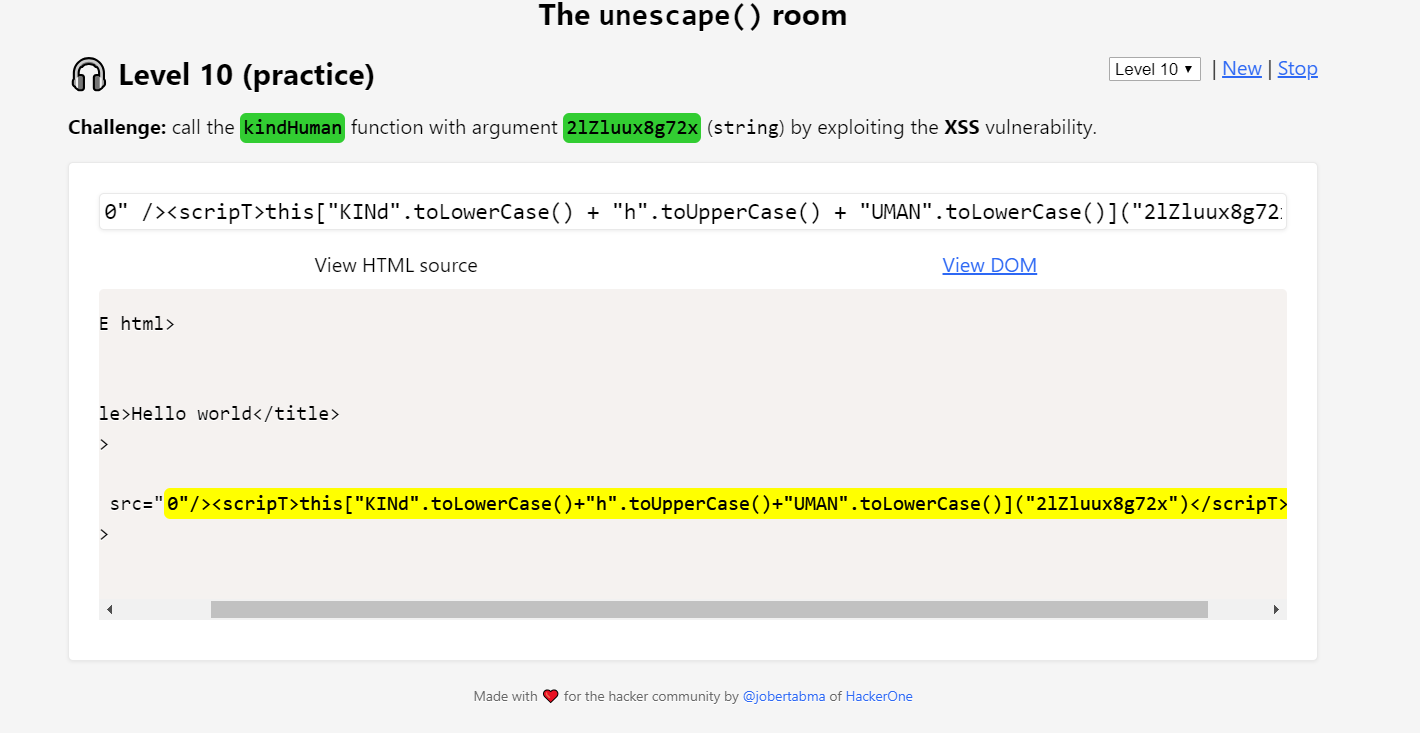












|  |  |  |  |
| --- | --- | --- | --- |
| Naam | Opdracht | Tijd | Totaal |
| Vicky | 3B.1 - 3 - 5 - 6 - 8  Opmaak | 1 uur - 15 min - 15 min - 15 min - 4 uur - 30 min | 6.15 uur |
| Igor | 3B.1 - 2 - 4 - 5 - 6   * hulp met opdracht 8 * nakijken document | 1 uur - 30 min - 30 min - 15 min - 30 min - 3 uur - 15 min | 6 uur |
| Vincent | 3B.2 | 1 uur | 1 uur |
| Bram | 3B.7 | 1 uur | 1 uur |

Nakijken Document = Igor