

A2 - Broken Authentication



Agenda - A2 - Broken Authentication



1. Do que se trata?
2. Exemplos
3. Como se Proteger?
4. Saidajaula Monster Fit

Do que se trata?

globo
.com



Um atacante é capaz de comprometer senhas, chaves ou tokens com a finalidade de assumir outra identidade.





Account does not exist

Please sign-in

Username

aaa

Password

aaa

Login

Dont have an account? [Please register here](#)

Password incorrect

Please sign-in

Username

user

Password

password

Login

Dont have an account? [Please register here](#)

Mensagens de Erro Diferentes



E-mail

Senha

Seu usuário ou senha estão incorretos.

[Esqueceu sua senha?](#)

Não tem conta? [CADASTRE-SE.](#)

ou entre com

Mensagens de Erro Diferentes



http://site.com/?sessionID=AFC3D35F216AAEFC

██

██

██



Session Hijacking



Wi-Fi: en1

http

No.	Time	Source	Destination	Protocol	Length	Info
172	8.00...	10.127.36.243	186.192.81.31	HTTP	1262	GET / HTTP/1.1
180	8.02...	186.192.81.31	10.127.36.243	HTTP	672	HTTP/1.1 301 Moved Permanently (text/html)
10974	24.0...	10.127.36.243	186.192.81.31	HTTP	1303	GET /?SESSIONID=MEUSESSIONID HTTP/1.1
10992	24.0...	186.192.81.31	10.127.36.243	HTTP	671	HTTP/1.1 301 Moved Permanently (text/html)
16120	80.7...	10.127.36.243	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7\r\n

[truncated]Cookie: _ga=GA1.2.1900000000.1529000000; _cb_ls=1; _cb=Cx...; glb_uid="yU..."; _ga=GA1.2.1900000000.1529000000

Cookie pair: _ga=GA1.2.1900000000.1529000000

Cookie pair: _cb_ls=1

Cookie pair: _cb=Cx...

Cookie pair: glb_uid="yU..."

Cookie pair: _ga=GA1.2.1900000000.1529000000

Cookie pair: _gid=GA1.2.1900000000.1529000000

Cookie pair: __gads=ID=dfd...

Cookie pair: nav13574=65af6...

Cookie pair: _gid=GA1.2.1900000000.1529000000

Cookie pair: _cb_svref=null

Cookie pair: hsid=b4...

Cookie pair: _gat_g1_portal=1

Cookie pair: utag_main=v_id:0168b...

Cookie pair: _chartbeat2=.1529...

\r\n

[Full request URI: http://g1.globo.com/?SESSIONID=MEUSESSIONID]

[HTTP request 1/1]

```

0000 00 1b 17 00 02 30 5c 96 9d 8d 52 cd 08 00 45 00 .....0\..R...E.
0010 05 09 a1 db 40 00 40 06 58 c2 0a 7f 24 f3 ba c0 ....@.@.X...$.
0020 51 1f cc 7c 00 50 c1 db 44 d6 c1 50 ba ce 80 18 Q..|.P..D..P...
0030 10 15 2c cd 00 00 01 01 08 0a 0c 3e 1d 83 75 fe .....>..u.
0040 42 d1 47 45 54 20 2f 3f 53 45 53 53 49 4f 4e 49 B.GET /? SESSIONI
0050 44 3d 4d 45 55 53 45 53 53 49 4f 4e 49 44 20 48 D=MEUSES IONID H
0060 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 67 TTP/1.1. .Host: g
    
```


Hypertext Transfer Protocol: Protocol

Packets: 16382 · Displayed: 8 (0.0%)

Profile: Default

Session Hijacking



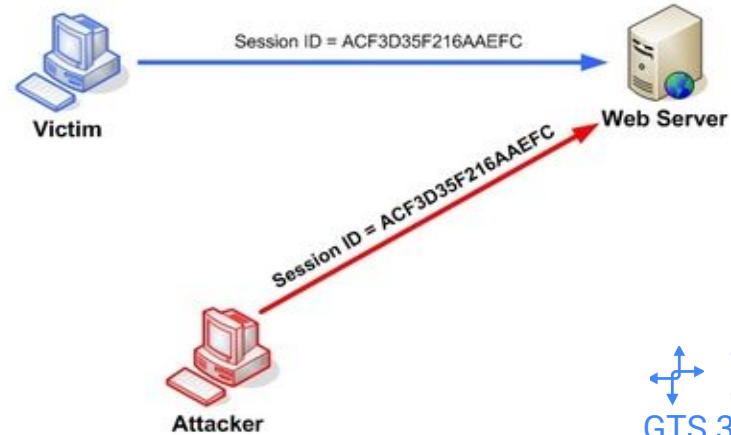
 https://[REDACTED]/?sessionID=MEUSessionID

Session Hijacking



https://site.com

```
{'user' : 'user1',  
'sessionID' : 'ACF3D35F216AAEFC'}
```



Session Hijacking



Wi-Fi: en1

ip.addr == 10.127.36.52

No.	Time	Source	Destination	Protocol	Length	Info
718	78.260721	10.127.36.52	18.228.99.199	TLSv1.2	129	Application Data
719	78.260951	10.127.36.52	18.228.99.199	TLSv1.2	129	Application Data
726	78.282141	18.228.99.199	10.127.36.52	TLSv1.2	129	Application Data
727	78.282245	10.127.36.52	18.228.99.199	TCP	66	54099 → 443 [ACK] Seq=638
728	78.282673	18.228.99.199	10.127.36.52	TLSv1.2	129	Application Data
729	78.282739	10.127.36.52	18.228.99.199	TCP	66	54104 → 443 [ACK] Seq=505

▶ Ethernet II, Src: Apple_2d:b1:98 (e0:f8:47:2d:b1:98), Dst: PaloAlto_00:02:30 (00:1b:17:00:02:30)

▶ Internet Protocol Version 4, Src: 10.127.36.52, Dst: 18.228.99.199

▼ Transmission Control Protocol, Src Port: 54104, Dst Port: 443, Seq: 442, Ack: 1674, Len: 63

- Source Port: 54104
- Destination Port: 443
- [Stream index: 10]
- [TCP Segment Len: 63]
- Sequence number: 442 (relative sequence number)
- [Next sequence number: 505 (relative sequence number)]
- Acknowledgment number: 1674 (relative ack number)
- 1000 = Header Length: 32 bytes (8)
- ▶ Flags: 0x018 (PSH, ACK)
- Window size value: 4096
- [Calculated window size: 4096]
- [Window size scaling factor: -1 (unknown)]
- Checksum: 0x0c3b [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- ▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
- ▶ [SEQ/ACK analysis]
- ▶ [Timestamps]
- TCP payload (63 bytes)

▼ Secure Sockets Layer

- ▼ TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
- Content Type: Application Data (23)
- Version: TLS 1.2 (0x0303)
- Length: 58
- Encrypted Application Data: 000000000000199c2f2ca85ef537e12c275843ca38bd939...

```

0000  00 1b 17 00 02 30 e0 f8 47 2d b1 98 08 00 45 00  . . . . 0 . G . . . . E .
0010  00 73 00 00 40 00 40 06 95 27 0a 7f 24 34 12 e4  . s . . @ . . . . $ . .
  
```

wireshark_en1_20190522151826_JqxSh7_pcapng Packets: 1214 · Displayed: 275 (22.7%) Profile: Default

Session Hijacking



Intruder attack 5

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		403	<input type="checkbox"/>	<input type="checkbox"/>	236	
4	admin	301	<input type="checkbox"/>	<input type="checkbox"/>	454	
1	senha1	403	<input type="checkbox"/>	<input type="checkbox"/>	236	
2	senha2	403	<input type="checkbox"/>	<input type="checkbox"/>	236	
3	senha3	403	<input type="checkbox"/>	<input type="checkbox"/>	236	
5	senha5	403	<input type="checkbox"/>	<input type="checkbox"/>	236	
6	senha6	403	<input type="checkbox"/>	<input type="checkbox"/>	236	

Request Response

Raw Params Headers Hex

```
POST /login HTTP/1.1
Host: localhost:10006
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:66.0) Gecko/20100101
Firefox/66.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost:10006/login
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
DNT: 1
Connection: close
Cookie:
Token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1IjoiYmFtY2U0NTU0NjI3NjAwLCJleHAiOiJlNTg2Mjc5MDB9.Z9Hc001Q9Ur0MO6eFMnclqBFLjjfe3odWa90TaVbDSQ
Upgrade-Insecure-Requests: 1
```

Ataque Força Bruta



Nome completo

E-mail

Senha - 8 a 15 dígitos

Verificação de segurança

Não sou um robô



reCAPTCHA
Privacidade - Termos

Li e concordo com os [Termos de Uso](#) e [Política de Privacidade](#).

CADASTRAR

Como se proteger?







1. **Uso de sistemas multistage** com barreiras adicionais ao sistema de autenticação. 🚫
2. **Uso de CAPTCHA** para mitigar um ataque de força bruta em rotas específicas da aplicação. 🐱
3. **Conscientizar usuários** sobre os benefícios de utilizar senhas fortes e **não reaproveitadas**. 🔍

A mockup of a login form with three input fields: 'email' (with a person icon), 'senha' (with a lock icon), and 'token' (with a key icon). Below the fields is a checkbox labeled 'Lembrar por 30 dias'. The form is flanked by vertical grey bars on both sides.

Como se proteger?



4. **Envio de e-mails** para a conta registrada do usuário informando sobre alterações importantes na conta, como troca de senha, login realizado num dispositivo desconhecido etc. 
5. **Padronizar mensagens de erro** para que elas não acusem exatamente que elementos do formulário estão inválidos. 
6. **Evitar uso de dados de usuários previsíveis** na geração de cookies e identificadores de sessão, por exemplo. 
7. **Manuseio seguro de credenciais**, transmitindo em um canal seguro como, por exemplo, o HTTPS. 



One Page Wonder - Start Boo... x +

localhost:10082 ☆

SAIDAJAULA MONSTRO FIT

SIGN UP LOG IN

Saidajaula Monstro Fit

Você vai ser um verdadeiro
MONSTRO!



Narrativa do ataque



1. Entrar na pasta da app

```
$ cd owasp-top10-2017-apps/a2/saidajaula-monster
```

2. Inicializar o container

```
$ make install
```

3. Acessar a página

```
localhost:10082
```



A2 - Broken Authentication

